ANKARA YILDIRIM BEYAZIT UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

SPECKLE MASKING FOR HYBRID CRYPTOLOGY

M.Sc. Thesis by
Abdurrahman HAZER

Department of Electrical and Electronics Engineering

May, 2019
ANKARA

SPECKLE MASKING FOR HYBRID CRYPTOLOGY

A Thesis Submitted to

The Graduate School of Natural and Applied Sciences of

Ankara Yıldırım Beyazıt University

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Electrical and Electronics Engineering, Department of Electrical and Electronics Engineering

by

Abdurrahman HAZER

May, 2019

ANKARA

M.Sc. THESIS EXAMINATION RESULT FORM

We have read the thesis entitled "**SPECKLE MASKING FOR HYBRID CRYPTOLOGY**" completed by **ABDURRAHMAN HAZER** under supervision of **PROF. DR. REMZI YILDIRIM** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Dr. Remzi YILDIRIM

Supervisor

Prof. Dr. Recep DEMİRCİ

Jury Member

Dr. Özkan KILIÇ

Jury Member

Prof. Dr. Ergün ERASLAN

Director

Graduate School of Natural and Applied Sciences

ETHICAL DECLERATION

I hereby declare that, in this thesis which has been prepared in accordance with the Thesis Writing Manual of Graduate School of Natural and Applied Sciences,

- All data, information and documents are obtained in the framework of academic and ethical rules,
- All information, documents and assessments are presented in accordance with scientific ethics and morals,
- All the materials that have been utilized are fully cited and referenced,
- No change has been made on the utilized materials,
- All the works presented are original,

and in any contrary case of above statements, I accept to renounce all my legal rights.

Date: **Signature: ……**

Name & Surname:……...

ACKNOWLEDGMENTS

I would like to extend my thanks to my tutor and supervisor Professor Dr. Remzi Yıldırım, who gave me the opportunity to work with him and encouraged me with his support, guidance and enthusiasm.

I would also like to thank my parents Ayfer and Mustafa Reşit, my sister Nurefşan, my brother Ahmet Said and even my younger brother Akif Serdar, who provided me every opportunity and supported me in every sense.

2019, 8 May **Abdurrahman HAZER**

SPECKLE MASKING FOR HYBRID CRYPTOLOGY

ABSTRACT

The increasing amount of data with the increasing use of the Internet has led to an increase in the studies on the protection of these data in the scientific world. This thesis has been written to develop a new optical image encoding system by addressing the problems of both commonly used optical encryption systems and multiple image encryption methods.

Hybrid method has been developed combining diffractive imaging and image hiding algorithms by considering the weak points of double random phase encoding (DRPE), phase truncated Fourier transform (PTFT) and diffractive imaging based optical image encryption systems. The carrier and the parameters used in the hiding step provide additional key space in the hybrid method while simultaneously encrypting more than one image. The problems of PTFT, DRPE and diffractive imaging systems can be solved by the hybrid method developed in nonlinear structure.

The problems faced by the multiple image encryption methods are briefly discussed and a hybrid multiple image encryption method based on compressive sensing and diffractive imaging is developed. Space multiplexing enables images to be combined on a single plane and authorized for different users. By recombining the phase and amplitude of the images, the size of the matrix carrying the images is further reduced. The method with a non-linear structure can solve the problems of multiple-image encryption methods.

In this thesis, in the coding stage of the images with diffractive imaging used for both hybrid methods, two different masks are used, one is a private key and the other one is a public key that changes at each encryption and consists of different values for each receiver. The fact that both masks must be on the receiving side in order to decrypt the password and the total number of probabilities to be tried to obtain these masks correctly

for the first method is $256^{2\times512\times512}$ and for the second method is $256^{2\times256\times256}$ for a 256×256 matrix sized image, which provides strong key space to hybrid methods.

Two different hybrid methods developed in this study provide different solutions to optical image encryption and multiple image encryption methods. This study could be further developed for practical application and could be an example for future studies.

Keywords: Optical image encryption, Fourier optic signal and image processing, speckle processing, phase retrieval, multiple-image encryption.

HİBRİT KRİPTOLAMA İÇİN BENEKLİ MASKELEME

ÖZ

İnternet kullanımının yaygınlaşması ile artan veri miktarı, bilim dünyasında bu verilerin korunmasına ilişkin yapılan çalışmaların da artmasına sebep olmuştur. Bu tez hem çokça kullanılan optik şifreleme sistemlerinin hem de çoklu görüntü şifreleme metotlarının sorunlarını ele alarak yeni bir optik görüntü şifreleme sistemi geliştirmek için yazılmıştır.

Double random phase encoding (DRPE), phase truncated Fourier transform (PTFT) ve difraktif görüntüleme tabanlı optik görüntü şifreleme sistemlerinin zayıflıklarını gidererek difraktif görüntüleme ve görüntü gizleme algoritmalarını birleştiren hibrit metot geliştirilmiştir. Gizleme aşamasında kullanılan taşıyıcı ve parametreler hibrit metoda ek anahtar alanı sağlarken aynı anda birden fazla görüntünün şifrelenmesini de sağlamaktadır. Doğrusal olmayan yapı da geliştirilen hibrit metot ile PTFT, DRPE ve difraktif görüntüleme sistemlerinin yaşadıkları sıkıntılar giderilebilmiştir.

Çoklu görüntü şifreleme metotlarının yaşadıkları problemler kısaca ele alınarak compressive sensing ve difraktif görüntüleme tabanlı hibrit çoklu görüntü şifreleme metodu geliştirilmiştir. Uzay çoklama sayesinde görüntüler tek düzlemde birleştirilebilmiş ve yetkilendirilebilmiştir. Görüntülerin fazını ve genliğini ayırarak yeniden birleştiren yöntem ile de görüntüleri taşıyan matrisin boyutu daha da düşürülmüştür. Doğrusal olmayan bir yapıya sahip olan metot çoklu görüntü şifreleme metotlarının sorunlarını çözebilmektedir.

Bu tezde, her iki hibrit metot için de kullanılan difraktif görüntüleme ile görüntüleri kodlama aşamasında biri özel diğeri ise her şifrelemede değişen ve her alıcı için farklı değerlerden oluşan genel bir anahtar olmak üzere iki farklı maske kullanılmaktadır. Şifrenin çözülebilmesi için iki maskenin de olmak zorunda olması ve 256×256 matris boyutunda ki bir görüntü için bu maskelerin doğru bir şekilde elde edilebilmesi için

gerekli olan olasılık sayısının birinci hibrit metot için $256^{2\times512\times512}$ ve ikinci metot için $256^{2\times256\times256}$ olması hibrit metotlara güçlü bir anahtar alanı sağlamaktadır.

Bu çalışmada geliştirilen iki farklı hibrit metot ile optik görüntü kriptolama ve çoklu görüntü şifreleme metotlarına farklı çözümler sunulmaktadır. Yapılan bu çalışma pratik uygulama için daha da geliştirilebilir ve gelecek çalışmalar için de örnek olabilir.

Anahtar Kelimeler: Optik görüntü şifreleme, Fourier optik sinyal ve görüntü işleme, benek işleme, faz geri elde etme, çoklu görüntü şifreleme.

CONTENTS

Page

ABBREVATIONS

AES	Advanced Encryption System
CC	Correlation Coefficient
CCD	Charge Coupled Device
CM	Cell Matrix
CPA	Chosen Plaintext Attack
CPRA	Cascaded Phase Retrieval Algorithm
CS	Compressive Sensing
CT	Cell Transform
DES	Data Encryption Standard
DRPE	Double Random Phase Encoding
DRPAE	Double Random Phase-Amplitude Encoding
EMD	Equivalent Modulus Decomposition
ER	Error Reduction
FrT	Fresnel Transform
FsT	Fractional Fourier Transform
FT	Fourier Transform
GS	Gerchberg-Saxton
GT	Gyrator Transform
HIO	Hybrid-Input Output
HM	Half Mirror
HT	Hartley Transform
IFT	Inverse Fourier Transform

IoT	Internet Of Things
LcT	Linear Canonical Transform
MGSA	Modified Gerchberg-Saxton Algorithm
MSE	Mean Square Error
PC	Photon Counting
POF	Phase Only Function
PSNR	Peak Signal to Noise Ratio
PTFT	Phase Truncated Fourier Transform
RSA	Rivest-Shamir-Adleman
SLM	Spatial Light Modulator
WF	Wirtinger Flow

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

With the increase of internet usage worldwide, the amount of data produced and shared in almost every field such as health, education, transportation, tourism, communication, banking, industrial and defense industry is increasing. Produced data continues to grow even faster with the introduction of Internet of Things (IoT). The creation and sharing of these data in daily life brings with it information security problems. With the widespread use of social media, it is difficult to ensure the security of data shared over the Internet. If the data is transmitted from unsafe lines, it is possible for malicious people to reach easily. The data seized by malicious people can be information that will reveal a person's credit card, passport, credentials or privacy. The attacker has the opportunity to commit a number of offenses such as withdrawing money with the information he has obtained, trading illegal goods or blackmailing confidentiality information. The data that is intended to be transmitted is not only a personal data, but also a data that contains a country's top-secret information, and the infiltration of such information can drag that country into destruction. Protecting and conveying information is an important problem of our day. Very common encryption algorithms, such as Advanced Encryption System (AES) [1], Data Encryption Standard (DES) [2] and Rivest-Shamir-Adleman (RSA) [3] have been proposed to ensure reliable data transmission. AES and DES have a symmetric cryptography system using the same key for the sender and receiver, while the RSA has an asymmetric cryptographic system using both the private and public key.

The optical encryption algorithms have recently become very popular due to their ability to be implemented in parallel and effective coding. The Double Random Phase Encoding (DRPE) algorithm [4] is the first study in this field and is also the source of subsequent optical encryption methods [5-10]. Optical encryption has some characteristic advantages. The most noticeable of these advantages is that all pixels of the image can be processed at the same time as the optical instruments have parallel

processing property in which both amplitude and phase of the image can be processed. When the same process is attempted by electronic devices, one bit is processed at a time due to the serial processing feature of the electronic part. As the length of the data to be processed increases, the processing time with the electronic components increases. Optical tools can process a few hundred frames per second on 2D data so that they can encrypt data much faster than their electronic counterparts. Besides fast data processing, the optical encryption methods can be more secure than their electronic counterparts because they can operate in multiple dimensions (wavelet, phase, polarization etc.). Since the optical encryption systems do not perform bit-bit processing, the gray scale attributes are much better than the gray scale quality provided by the electronic components processing at the bit (0 or 1) level. Generally, an optical encryption system consists of light source, lenses, mirrors, beam splitters, spatial light modulators (SLMs) and detectors. Using these optical tools, a wide variety of variations have been implemented and encryption has been attempted. In order to increase the robustness of the encryption against attacks, additional operations are performed before or after the optical cryptography system. Thus, it is necessary to know the correct keys to obtain the decrypted data.

1.1 Optical Image Encryption

DRPE, which is commonly used in optical encryption systems, converts the data into white noise with random phase masks in both spatial and Fourier space [4]. However, DRPE has a linear and symmetric cryptographic system where the keys are identical to the transceiver. Due to its linear structure, the DRPE cannot resist the chosen-ciphertext, known-plaintext and chosen-plaintext attacks [11-13]. Therefore, it is the general objective to increase the reliability by converting linear optical encryption systems into a non-linear structure.

Nonlinear and asymmetric cryptographic Phase Truncated Fourier Transform (PTFT) based systems have been proposed to eliminate the weaknesses of linear symmetric based optical encryption systems [5]. Different phase masks are used in the encryption

and decryption stages in the PTFT based optical encryption systems which send only the amplitude information of the encrypted image to the receiver. The transmission of only the amplitude information of the encoded image provides a non-linear structure to the system and ensures that the system is robust against the attacks in which the linear optical encryption systems are weak. However, these systems are also weak against some phase retrieval based attacks [14, 15]. In 2015, the proposed asymmetric encryption method based on the equivalent modulus decomposition (EMD) was found to be resistant to phase retrieval attacks [9]. In 2016, a new type of attack against EMD-based asymmetric cryptography was developed and an algorithm was proposed to increase the robustness of the algorithm to this attack in the same study [16]. The encrypted image can be decrypted with a modified phase retrieval based attack applied to the EMD-based asymmetric system with increased resistance to attacks [17]. Different optical encryption method based on diffractive imaging which is robust against attacks due to its nonlinear structure has also been proposed [10]. However, in this method, phase masks with chosen plaintext attack (CPA) attack using Multislice Ptychographic phase retrieval can be obtained properly and encryption can be broken [18]. New algorithms are always needed since an attack is developed against each encryption method. Therefore, it is desirable to develop an algorithm that is non-linear and robust to attacks.

Nowadays, the rapid increase in the amount of data produced not only raises the problem of the reliable transmission of these data, but also the problem of efficient use of the bandwidth of transmission lines. For this reason, multi-image encryption methods are studied intensively to enable data to be encrypted and transmitted simultaneously. With the advantage of the ability to process all pixels at the same time, multi-image encryption algorithms are mainly developed using optical methods. Several algorithms such as wavelength multiplexing [19], position multiplexing [20] and interference-based position multiplexing [21] have been proposed for multiple-image encryption. However, the general problems of these algorithms are that the noise in the decrypted images is caused by cross-talk and the number of images to be encrypted is limited. Iterative phase

back access algorithms [22, 23] have been proposed to achieve cleaner images by minimizing the cross-talk effect. With these algorithms, despite the decrease in cross-talk induced noise, the image capacity to be encrypted at the same time is still limited. A 4-f optical-based system has also been proposed to eliminate the constraint problem [24]. However, this system has a structure that cannot decrypt the image before decrypting the previous image because of its hierarchical order. This makes users dependent on each other at the authorization stage. Providing independent and noiseless access to the transmitted images does not make sense if there is no strong encryption algorithm against attacks. For this reason, it is expected to increase the number of images sent with a limited carrier for multi-image encryption, to transmit images without noise, to authorize different images to different users, and most importantly to develop a non-linear encryption method which is robust to attacks.

1.2 Scope and Outline of Thesis

Although the optical encryption methods proceed very quickly, it is necessary to carefully examine the existing structures and to solve the problems and develop new algorithms so that the practical applications can fully meet their needs. One of the problems to be investigated and solved is the development of nonlinear algorithms to increase the robust to attacks where the linear optic image encryption systems are weak. Another problem is to examine the troubles experienced by multiple image encryption methods and to develop a solution. These problems can be listed as sending noiseless image, efficient use of bandwidth, authorizing different users to different images, and developing a non-linear system.

The aim of this study is to develop hybrid optical encryption algorithm considering the problems of optical encryption systems and multiple image encryption methods. These objectives can be summarized as follows:

1. To develop a nonlinear and attack-resistant algorithm considering the problems experienced by the mentioned DRPE, PTFT and diffraction pattern algorithms.

2. To develop an algorithm that solves the problem of multiple-image encryption, sending noiseless images, using bandwidth efficiently, authorizing different users to different data and developing a non-linear system. Several publications have emerged from this study as given in the appendix. The optical encryption algorithm designed in this study can be reliable, as well as the source of different studies.

The thesis consists of six sections.

In the first part, a brief introduction is made about data security and optical image encryption. In addition, the problems experienced by optical encryption systems are defined briefly. Finally, the aim and importance of this study is presented.

In the second chapter, the studies in the literature are examined. This section is divided into two parts. In the first part, it is examined DRPE, PTFT, Interference, Ghost imaging and Diffraction imaging based optical encryption systems for using in encoding single image. In the second part, position multiplexing, 4-f and phase retrieval based optical image encryption algorithms are examined.

In the third chapter, the importance of phase in images and phase retrieval algorithms are described.

In the fourth chapter, the hybrid method is given which is nonlinear and robust to attacks by using phase retrieval based diffractive imaging framework and hiding algorithm.

In the fifth chapter, multiple-image encryption algorithms are considered and a multiple-image hybrid encryption algorithm is developed using compressive sensing and phase retrieval based diffractive imaging framework.

In the sixth chapter, the findings of this study and its contributions to future studies are discussed.

CHAPTER 2

OPTICAL IMAGE ENCRYPTION TECHNIQUES

The symbols used for this section belong only to the title under which they are used and are not general.

2.1 Double Random Phase Encoding (DRPE)

The DRPE optical encryption method is very popular due to its simplicity [4]. The DRPE method encodes the image into noise-like image using two random phase masks. One of the phase masks is in the spatial domain and the other is in the Fourier space. The physical installation diagram of the system is shown in Figure 2.1. In order to obtain the encoded image according to this installation, $h(a,b)$ which is modulated with the phase mask in the Fourier space is found as follows:

$$h(a,b) = \mathrm{FT}\{ f(a,b)\exp[i2\pi y(\mu,\nu)]\} \quad \textbf{(2.1)}$$

In equality, FT represents the Fourier transform, $f(a,b)$ represents the image to be encrypted and $\exp[i2\pi y(\mu,\nu)]$ represents the random phase mask (MASK2) in the Fourier space [4]. Then, the complex encrypted image obtained by modulating $h(a,b)$ with a phase mask (MASK1) in the spatial domain $\psi(a,b)$ can be written as:

$$\psi(a,b) = \mathrm{IFT}\{h(a,b)\exp[i2\pi x(a,b)]\}, \quad \textbf{(2.2)}$$

where IFT and $\exp[i2\pi x(a,b)]$ represent the inverse Fourier transform and the random phase mask (MASK1) in the spatial domain, respectively [4]. The process required to decrypt the encoded image with random phase masks is applied to $\psi(a,b)$. According to this, the decrypted image $\left| f(a,b)\exp[i2\pi x(a,b)] \right|$ in the set of positive real numbers can be found follows:

$$\left| f(a,b)\exp[i2\pi x(a,b)] \right| = \left| IFT\{FT\left(\psi(a,b)\right)\exp[-i2\pi y(\mu,\nu)]\} \right|, \qquad \textbf{(2.3)}$$

where $\exp[-i2\pi y(\mu,\nu)]^*$ and $\left|\ \right|$ represent the complex conjugate of the random phase mask in the frequency domain and the absolute value notation, respectively. As for the non-negative message images, the input level MASK1 does not need to be processed, as can be seen in Equation (2.2) at decryption step.

Figure 2.2 (a) shows the encryption step in which an image is encoded to the noise-like image by DRPE. Similarly, the decryption step of DRPE is given in Figure 2.2 (b). In addition, it is shown in Figure 2.2 (b) that the image of the message cannot be reached when an incorrect phase mask is used. Using the phase mask processed in the frequency domain only as a key in the decryption phase of the DRPE indicates that the key field is very limited. For this reason, DRPE was applied in different matrix spaces such as Fractional Fourier transform (FsT) [25], Fresnel transform (FrT) [26], Linear Canonical Transform (LcT), Gyrator transform (GT) and Hartley transform (HT) to increase the reliability of the encryption system [6]. The ability of the system to be applied in different matrix spaces has enabled the parameters (fractional order and propagation distance etc.) used in the encryption step to be additional keys to the system.

DRPE has been weak against chosen-cipher text and known-plaintext attacks due to its linear structure. First, in 2005, DRPE was found to be weak against the chosen-cipher text attack [11].

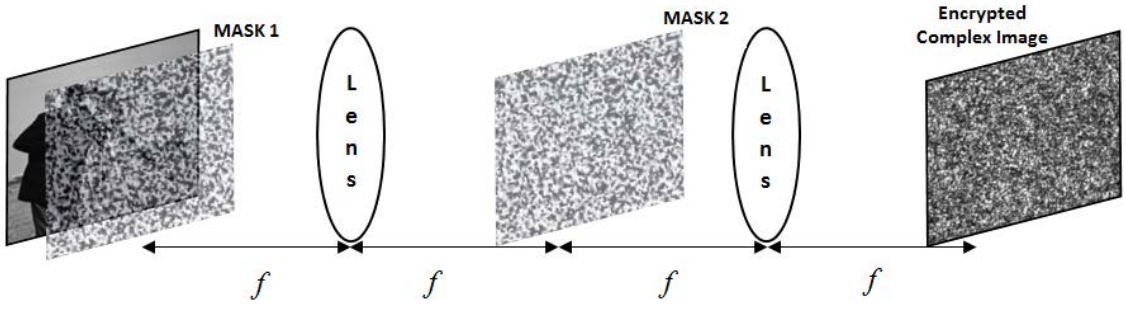
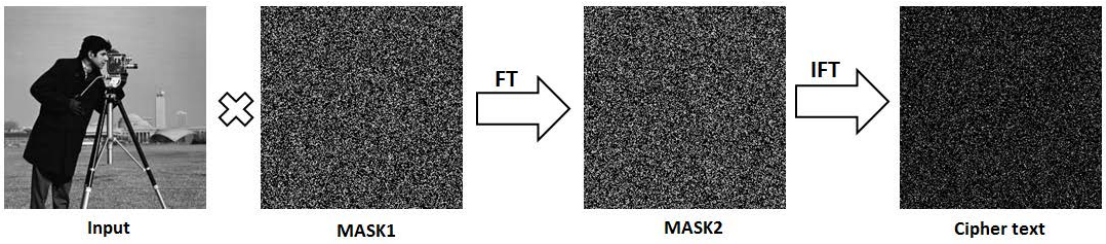
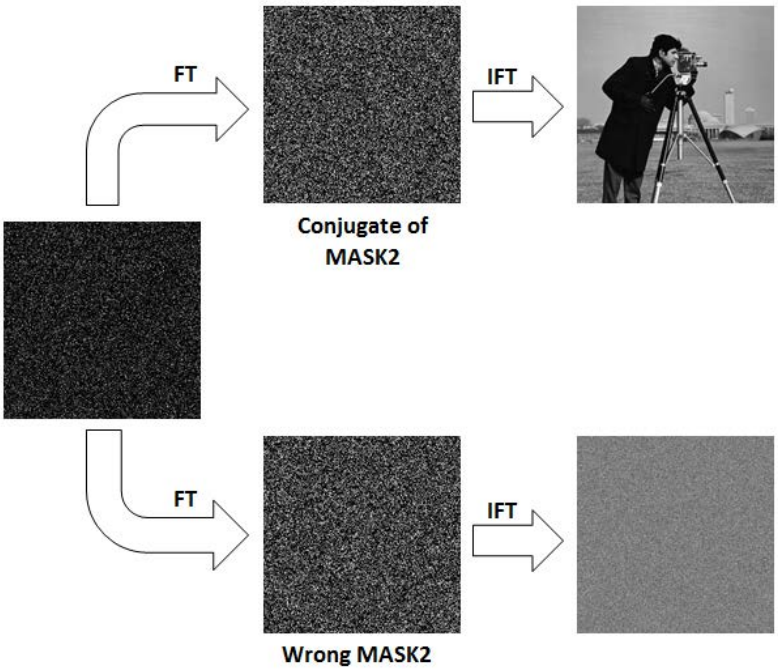


Figure 2.1 Physical experiment system of DRPE (MASK1 and MASK2 are randomly generated phase masks)



(a)



(b)

Figure 2.2 (a) DRPE encryption process and (b) decryption process

In addition, it has been determined by studies that it is possible to decrypt image which is encrypted by DRPE with a known-plaintext attack using iterative phase retrieval algorithm [12]. The DRPE adapted to the Fresnel domain is also vulnerable against the chosen-plaintext attack [13] and in 2009 a known-plaintext attack developed for fractional Fourier-based DRPE was found to be successful [27].

In 2008, double random phase-amplitude encoding (DRPAE) method was proposed by adding not only the phase coding but also the amplitude coding to minimize the weakness of DRPE against attacks and to make the system non-linear [28]. However, in order to obtain amplitude and phase masks used as a key in DRPAE, an attack has been developed which is composed of known plaintext and chosen-plaintext attacks [29]. In addition, in another study, it is seen that DRPAE is actually a linear structure and amplitude-phase masks can be obtained by using the point spread function [30].

2.2 DRPE and Photon Counting

Recently, methods used with photon counting (PC) technique have been developed as DRPE is vulnerable against attacks such as known-plaintext and chosen-cipher text [31-33]. Photon counting method is used in many fields such as night vision systems, laser radars, medical imaging and space imaging [35-38]. In the PC technique, the number of photons per pixel is adjusted in a controlled manner [32]. In the optical encryption system utilizing this feature of the PC technique, a small number of photons are taken from the DRPE encoded image to obtain a new encrypted image. The use of photons at low rates prevents the image from reaching the original during the decryption step, but it can be verified that the decrypted image is related to the message image by the correlation analysis. Correlation algorithms can be used to make the detail information in the image obtained in the decryption step more understandable [39].

In order to obtain the encoded image having the limited number of photons, the number of photons, N_p, falling into the detector is limited by the PC imaging technique. In this default assumed to have a Poisson distribution, the probability value $P\left(c_j;\lambda_j\right)$ of the number of photons falling to the pixel $\left(x_j\right)$ of the image can be modeled as follows:

$$P\left(c_j;\lambda_j\right)=\frac{\left[\lambda_j\right]^{c_j}e^{-\lambda_j}}{c_j!},\quad c_j=0,1,2... \tag{2.4}$$

In the equation, the total number of photons falling into the pixel x_j is represented by the c_j, λ_j represents the Poisson parameter and $\lambda_j = N_p f\left(x_j\right)$. The normalized radiation at pixel x_j is denoted by $f\left(x_j\right)$ and M represents the total number of pixels $\left(\sum_{j=1}^{M} f\left(x_j\right) = 1\right)$.

Figure 2.3 (a) and (b) show a 256×256 pixel sized binary message image and the amplitude of the image encoded with DRPE, respectively. The photon-limited amplitude image with $\left(N_p = 10^3\right)$ photons from the encoded image is shown in Figure 2.3 (c). Figure 2.3 (d) shows that no information has been obtained from the decrypted image. To authenticate the image obtained by the PC imaging technique, the original image with decrypted image is correlated using the *k*th-law nonlinear correlation $\left(k = 0,3\right)$. The result of nonlinear correlation is given in Figure 2.3 (e). As shown in the Figure, the correlation analysis results in only one point reaching the top and the remaining part consist of noise. Thus, the decrypted image is confirmed to belong to the message image. The PC-DRPE encryption method provides a more reliable encryption technique than DRPE by simply verifying the original image without showing it.

2.3 Diffractive Imaging Based Optical Image Encryption

When encryption is performed with DRPE, cipher text is a complex image. Because holographic techniques [40] are used to record a complex image, the encryption system is complex and the system must have a stable structure. While the diffractive imaging-based optical encryption methods [10, 41] proposed by Chen et al. simplifies the system which is complicated because of holographic techniques, it increases the reliability of the encryption thanks to its non-linear structure.

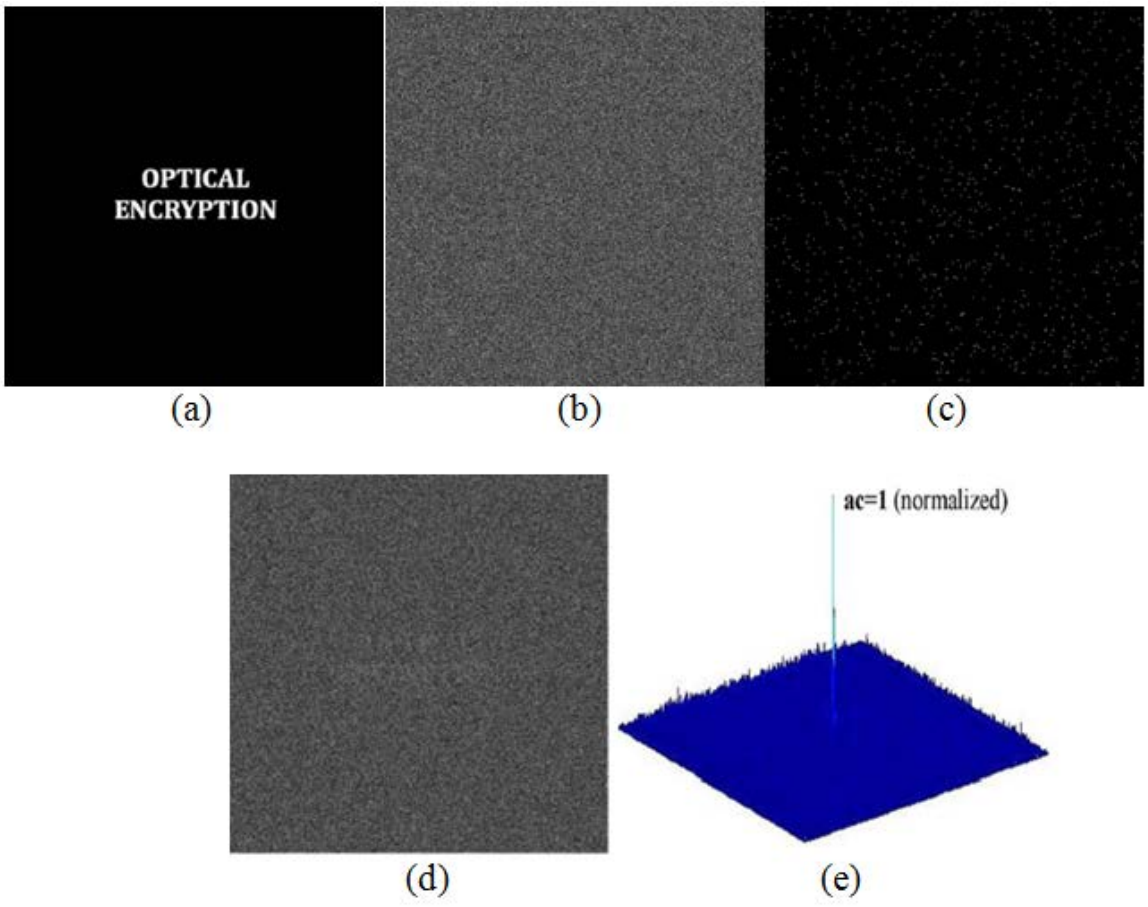


Figure 2.3 (a) Binary message image, (b) DRPE encoded amplitude image, (c) photon-limited amplitude image, (d) decrypted image and (e) correlation analysis result [31]

Figure 2.4 shows the physical installation of diffractive imaging based optical image encryption system generated by recording multiple intensity values of images with a shifted CCD camera along the axis. According to Figure 2.4, diffraction maps (cipher texts) recorded with CCD, $I_k(\eta,\varsigma)$ can be calculated as:

$$I_k(\eta,\varsigma)=\left|\mathrm{FsP}_{d2+\Delta d\times(k-1)}\left\{\left\{\mathrm{FsP}_{d1}\left[f(a,b)RPM_1(a,b)\right]\right\}RPM_2(\mu,\nu)\right\}\right|^2, \qquad \textbf{(2.5)}$$

where $I_k(\eta,\varsigma)$ $(k=1,2,3)$ represents the recorded diffraction density patterns, $f(a,b)$ represents the image to be encrypted (plaintext) and FsP represents the Fresnel

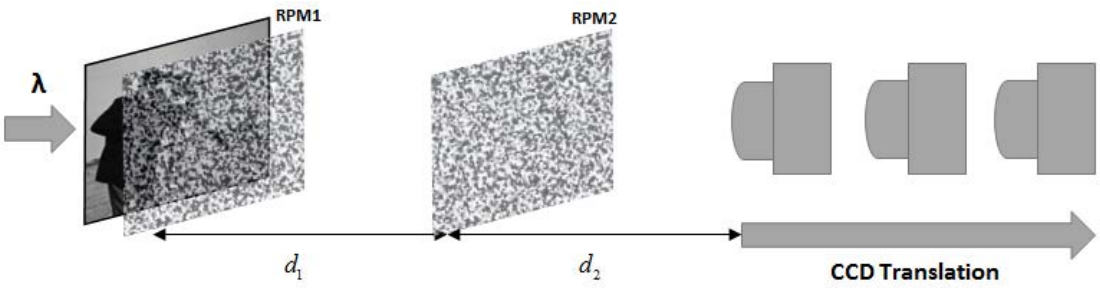


Figure 2.4 Physical experiment system of diffractive imaging based optical encryption system (λ denotes wavelength of light)

distribution. In equation, RPM_1 and RPM_2 represent random phase masks, $d1$ and $d2$ represent axis distances, and Δd represents CCD displacement intervals on axis.

In order for the system to be exemplary in the decryption stage, the number of density patterns obtained by equation (2.3) is determined as three. In order to decrypt the encrypted image on the receiver side, the phase retrieval algorithm is executed. If the plaintext prediction is indicated by $f_n(a,b)$, then iterative phase retrieval algorithm is given as follows:

1. While the CCD is in the first position, the matrix $P_n(\eta,\varsigma)$ obtained by treating the plaintext prediction $f_n(a,b)$ with the phase masks given in equation (2.5) is calculated as follows:

$$P_n(\eta,\varsigma) = \mathrm{FsP}_{d2+\Delta d\times(k-1)}\left\{\left\{\mathrm{FsP}_{d1}\left[f_n(a,b)RPM_1(a,b)\right]\right\}RPM_2(\mu,\nu)\right\}, \qquad \textbf{(2.6)}$$

where $n=1$ and $k=1$ for the first iteration.

2. The density value $I_k(\eta,\varsigma)$, which is recorded by the equation 2.5, is used as the limitation which is replaced by the amplitude of the $P_n(\eta,\varsigma)$ obtained in the first step, and the amplitude-modified matrix $\tilde{P}_n(\eta,\varsigma)$ is found as follows:

$$\tilde{P}_n(\eta,\varsigma) = \sqrt{I_k(\eta,\varsigma)}\left[P_n(\eta,\varsigma)/\left|P_n(\eta,\varsigma)\right|\right] \quad \textbf{(2.7)}$$

3. Using the $\tilde{P}_n(\eta,\varsigma)$ updated in Equation (2.7), the plaintext prediction $\tilde{f}_n(a,b)$ is propagated back to the input plane as follows:

$$\tilde{f}_n(a,b) = \mathrm{FsP}_{-d1}\left\{\left\{\mathrm{FsP}_{-[d2+\Delta d\times(k-1)]}\left[\tilde{P}_n(\eta,\varsigma)RPM^*{}_2(\mu,\nu)\right]\right\}RPM^*{}_2(\mu,\nu)\right\}, \quad \textbf{(2.8)}$$

where asterisk represents complex conjugate. The amplitude of the $\tilde{f}_n(a,b)$ obtained by the equation (2.8) is again the new plaintext prediction for the first step and represents the decrypted image when all iterations are completed. The position of the next cipher text and CCD is calculated with $k = k+1$ and $d2+\Delta d\times(k-1)$ respectively, and this process continues until $k=3$. When the steps described above are applied for all three density patterns, one iteration is completed in the algorithm. Iteration error rate ε can be calculated as follows:

$$\varepsilon = \sum_{a,b}\left[\left|\tilde{f}_{n+1}(a,b)\right| - \left|\tilde{f}_n(a,b)\right|\right]^2. \quad \textbf{(2.9)}$$

Total number of iterations varies according to ε. The algorithm stops working when the iteration error rate ε reaches a specified threshold.

While the original image to be encrypted is given in Figure 2.5 (a), three density images (cipher texts) recorded during the encryption are given in Figure 2.5 (b) - (d). The decrypted image and the graph showing iteration error rate are given in Figures 2.5 (e) and (f), respectively.

The physical installation of the diffractive imaging-based optical image encryption system is simpler than the DRPE-based optical encryption, as it does not require holographic techniques, and the system stability is higher than in the DRPE. The system also has a nonlinear structure because only the amplitude of the complex image is used as cipher text.

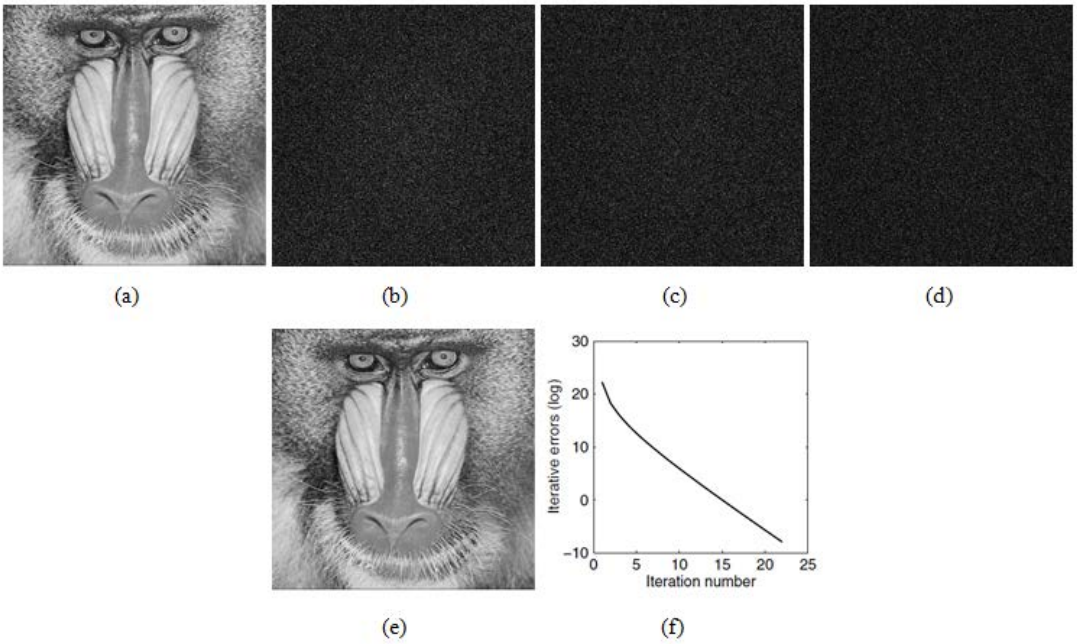


Figure 2.5 (a) the original image; (b)-(d) three density patterns recorded in the encryption phase; (e) the decrypted image (22 iterations); (f) the error rate graph in the decrypted stage [41]

As the iterative phase retrieval algorithm is used in the decryption stage, encryption reliability is increased. Later on, the single-step diffractive imaging based optical encryption system was developed which further simplified the encryption step [42]. With this algorithm, only one density pattern of the image is recorded with CCD. However, it is necessary to add a certain amount of zeros around the image with the oversampling method before encrypting it in order to obtain the image without noise during decryption [42]. In addition, another optical image encryption system based on single diffractive imaging was proposed which did not require an oversampling method during encryption [43].

Unfortunately, a special chosen-plaintext attack has been developed against diffractive imaging based optical encryption method which is more reliable with its simpler and non-linear structure compared to DRPE. This attack, developed by Li and Shi and based on the multi-slice Ptychographic phase retrieval algorithm, can decrypt the encrypted image obtained by using diffractive imaging based optical encryption [18].

2.4 PTFT Based Asymmetric Optical Image Encryption

A PTFT-based non-linear asymmetric optical image encryption system was proposed in 2010 to develop a system robust to attacks with weak linear optical encryption systems [5]. In PTFT system, the random two phase mask used for the encryption image is not used during decryption. Instead, two different phase masks created during encryption are used for decryption image and the system has an asymmetric characteristic thanks to this. Transmitting only the amplitude of the encrypted image with the phase truncation function provides a non-linear structure to the system, while it also strengthens the system against attacks in which the DRPE is weak.

The encryption step of the PTFT based asymmetric algorithm is given in Figure 2.6 (a). For the encryption step, two phase masks are used, one $R_1(a,b)$ in the input plane and the other $R_2(x,y)$ in the Fourier space. According to Figure 2.6 (a), the amplitude matrix $g(x,y)$ obtained by processing the input image $f(a,b)$ with the random phase mask in the Fourier space can be calculated as follows:

$$g(x,y) = \mathrm{PT}\left\{\mathrm{FT}\left[f(a,b)R_1(a,b)\right]\right\}, \tag{2.10}$$

where $\mathrm{PT}\{\ \}$ represents phase truncation operator. Finally, the cipher text $C(u,v)$ obtained by encoding the amplitude matrix with the random phase mask in the input plane can be written as follows:

$$C(u,v) = \mathrm{PT}\left\{\mathrm{IFT}\left[g(x,y)R_2(x,y)\right]\right\} \tag{2.11}$$

As shown in Figure 2.6 (a), new phase masks are obtained by using the PR operator for the decryption phase when creating the cipher text. The keys required for decryption (new phase masks) $P_2(x,y)$ and $P_1(u,v)$ are obtained as follows:

$$P_2(x,y) = \mathrm{PR}\left\{\mathrm{FT}\left[f(a,b)R_1(a,b)\right]\right\}, \tag{2.12}$$

$$P_1(u,v) = \mathrm{PR}\left\{\mathrm{IFT}\left[g(x,y)R_2(x,y)\right]\right\}, \quad \textbf{(2.13)}$$

In equalities, $\mathrm{PR}\{\ \}$ represents phase reservation operator. Since the $P_2(x,y)$ and $P_1(u,v)$ masks used in the decryption step are derived from the phase of the original image, they receive different values for each encrypted image. The decryption block scheme of the PTFT based optical image encryption system is given in Figure 2.6 (b). According to Figure 2.6 (b), after processing cipher text $C(u,v)$ with $P_1(u,v)$ in the Fourier space, the amplitude matrix $g(x,y)$ obtained using PT operator can be written as follows:

$$g(x,y) = \mathrm{PT}\left\{\mathrm{FT}\left[C(u,v)P_1(u,v)\right]\right\}, \quad \textbf{(2.14)}$$

Then, after the amplitude matrix is processed in the input plane with $P_2(x,y)$, the decoded image $f(a,b)$ using the PT operator can be written as follows:

$$f(a,b) = \mathrm{PT}\left\{\mathrm{IFT}\left[g(x,y)P_2(x,y)\right]\right\}, \quad \textbf{(2.15)}$$

The change of the phase masks created for decryption depending on the message image increased the durability of PTFT against known-plaintext attacks in which DRPE is weak.

Figure 2.7 shows the encoding of an image with asymmetric PTFT optical encryption. As shown in Figure 2.7 (d), the original image is accessible when all phase masks are correct. However, in Figure 2.7 (c), a silhouette problem occurs in the image obtained by a phase mask wrong in the decryption stage. In addition to the silhouette problem, iterative phase retrieval algorithm based attacks [15] and a special attack [14] are problem for the system. In order to increase the robustness of PTFT, which is particularly weak against phase retrieval-based attacks, amplitude modulation [44] and spherical wave illumination [45] techniques have been used, while optical image encryption systems with more complex pattern phase masks generated by using Yang-

Gu phase retrieval algorithm has been also developed [46]. Although the system with these studies increased robustness against attacks, the problem of silhouette which is a big problem for the system should be solved.

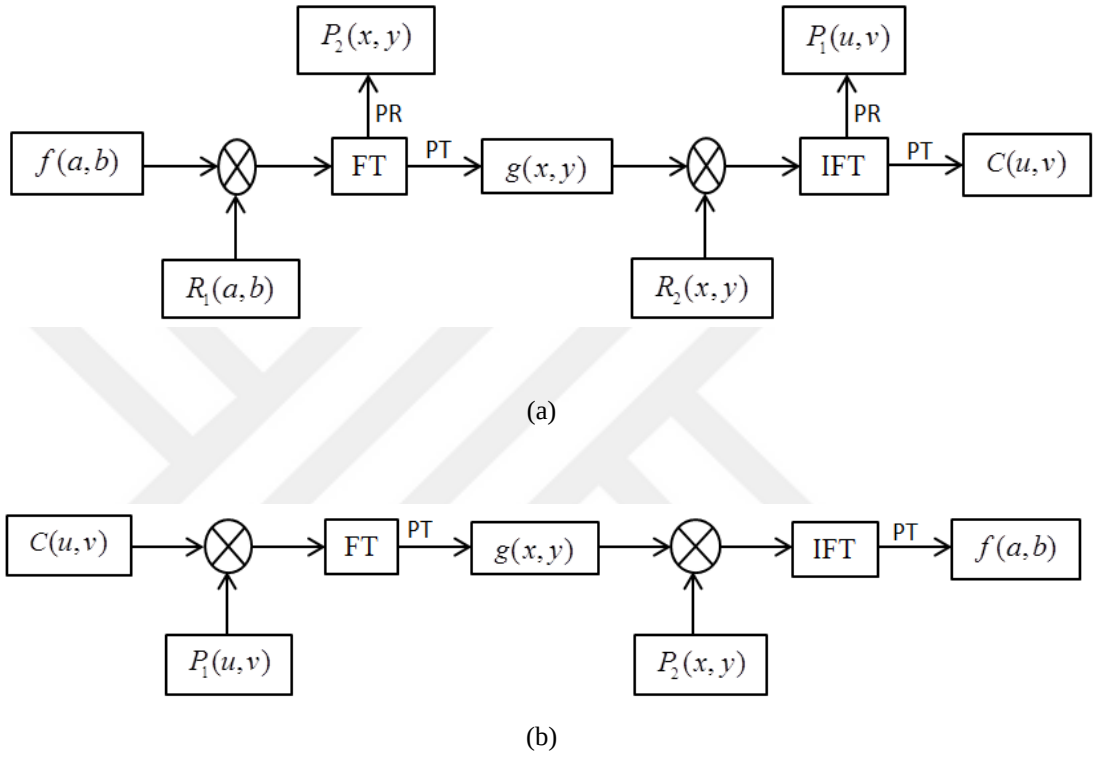


Figure 2.6 (a) PTFT encryption block diagram and (b) PTFT decryption block diagram

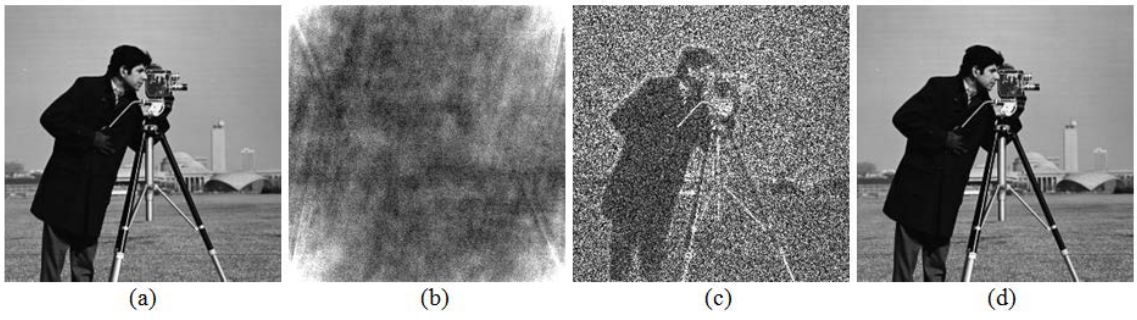


Figure 2.7 (a) Original image; (b) encrypted image; (c) decrypted image when one of the masks is wrong; (d) the decrypted image while all the masks are correct

2.5 Interference Based Image Encryption

Interference-based optical encryption methods are also preferred because they do not need iterative algorithms in the decryption stage [7]. The physical installation diagram of the system is given in Figure 2.8. Parallel simultaneous beams are modulated with two random phase masks RPM1 and RPM2 as in Figure 2.8 and then they are synthesized with half mirror (HM) to form the encoded image. Encryption is more convenient to perform digitally, but it is appropriate to perform the decoding in an optical or digital manner.

The complex image $\sqrt{f(a,b)}\exp\left[i2\pi rand\left(a,b\right)\right]$ encrypted according to Figure 2.8 can be found as follows:

$$\sqrt{f(a,b)}\exp\left[i2\pi rand\left(a,b\right)\right]=\left[\exp\left(iRPM1\right)+\exp\left(iRPM2\right)\right]\otimes h\left(x,y,d\right) \quad \textbf{(2.16)}$$

In the equation, $rand\left(a,b\right)$ represents the uniformly distributed random function in the range $\left[0,1\right]$, $\otimes$ represents the convolution process and d represents the distance

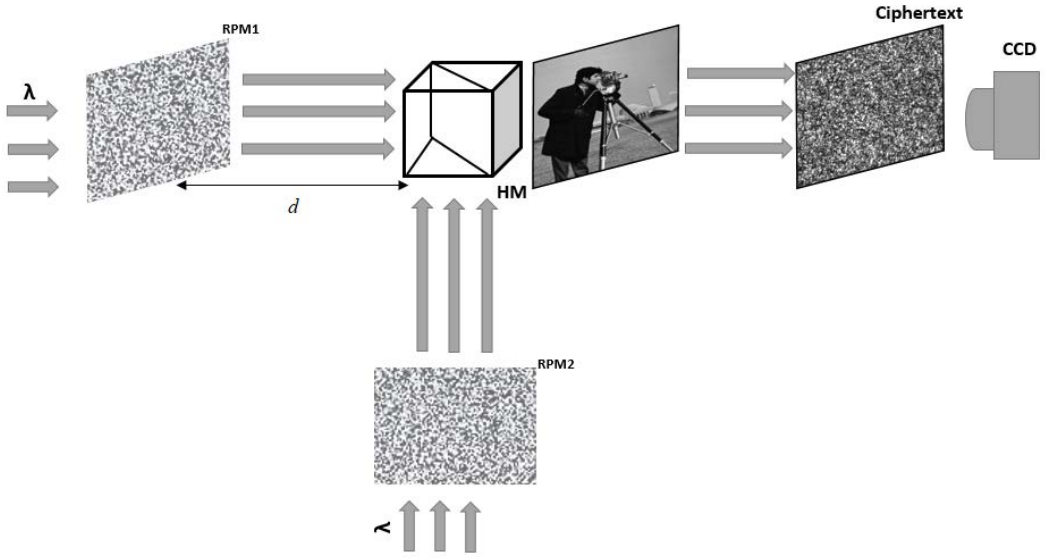


Figure 2.8 Physical experiment system of interference-based optical cryptography

between the phase masks and the image plane. $h(x,y,d)$, which represents the point pulse function at the equation, can be calculated as follows:

$$h(x,y,d)=\frac{\exp(i2\pi d/\lambda)}{id\lambda}\exp\left[\frac{i\pi}{d\lambda}\left(x^2+y^2\right)\right], \quad \textbf{(2.17)}$$

where λ represents the wavelength. The sum of the two phase masks $\left[\exp(iRPM1)+\exp(iRPM2)\right]$ on one side of Equation (2.16) can be left alone using the convolution theorem as follows:

$$\left[\exp(iRPM1)+\exp(iRPM2)\right]=\mathrm{IFT}\left\{\frac{\mathrm{FT}\left\{\sqrt{f(a,b)}\exp\left[i2\pi rand(a,b)\right]\right\}}{\mathrm{FT}\left[h(x,y,d)\right]}\right\} \quad \textbf{(2.18)}$$

Phase-only masks $RPM1$ and $RPM2$ can be written as follows:

$$RPM1=\arg(D)-\arccos\left[abs(D)/2\right], \quad \textbf{(2.19)}$$

$$RPM2=\arg\left[D-\exp(iRPM1)\right], \quad \textbf{(2.20)}$$

where $\arg(\ )$ and $\mathrm{abs}(\ )$ represent phase extraction and absolute value operations, respectively and D can be calculated as follows:

$$D=\mathrm{IFT}\left\{\mathrm{FT}\left\{\sqrt{f(a,b)}\exp\left[i2\pi rand(a,b)\right]\right\}\Big/\mathrm{FT}\left[h(a,b,d)\right]\right\}. \quad \textbf{(2.21)}$$

Although the system is often preferred as the decryption phase is difficult to copy and does not need an iterative algorithm, the silhouette of the image appears as in the PTFT based method when decryption step is performed with one wrong phase mask [47]. This means reaching at least a silhouette of the message image with any mask. Different methods have been proposed to solve the silhouette problem and establish a more reliable system [48-55]. Zhang et al. solve the silhouette problem by adding two half-

mirrors with two phase masks to the system to encrypt the image [48]. To solve the silhouette problem, Han et al. add a spatial light modulator (SLM) to the system and encode the image information in a phase mask and an amplitude mask [49]. The silhouette problem was solved in another system using jigsaw transformation [50]. Wen Chen and Xudong Chen solved the silhouette problem by developing a system in which multiple phase masks are used in series [51]. Liu et al. developed a system that encodes the image into a phase mask using the improved GS algorithm to solve the silhouette problem [52]. Wang and Zhao [53] solved the silhouette problem by coding the image in three-phase masks and in another study Wang [54] mixed three-phase masks with a linear phase mixing process and developed a system that encodes the image into these phase masks with an orthogonal transformation matrix.

2.6 Ghost Imaging Based Optical Image Encryption

Ghost imaging is a remarkable technique because it has a very different structure than other optical imaging methods [8]. In general, ghost imaging is based on the fact that the two related beams are transmitted over different paths. One of the beams is reflected in the object to be recorded with the bucket detector (single pixel sensor without spatial resolution). The other beam (so-called reference beam) which is propagated in the empty space without hitting any object is recorded directly with CCD camera. Finally, the image of the object is created by correlating the intensity recorded with the CCD camera and the intensity recorded with the bucket detector. An illumination pattern prepared in the computer can also be used instead of the illumination patterns generated by recording the reference beam to the CCD camera [55].Ghost imaging is used in many areas such as remote sensing, space imaging and optical image encryption [8, 55].

Ghost imaging technique enriches conventional optical image encryption methods due to their different characteristics. In the Ghost imaging-based optical encryption system, several phase masks are used as keys and the image recorded with the bucket detector are used as cipher text. The large number of phase masks provides the key reliability.

In the physical installation diagram shown in Figure 2.9, the radiation to the random phase masks falls first to the spatial light modulator. Then, one of the beams which are divided into two with the beam splitter cube is recorded with the bucket detector. The total radiation B_i which is recorded with the bucket detector passing through the phase masks $\psi_i(x) = (i = 1, 2, 3, ..., N)$ in the SLM can be calculated as follows:

$$B_i = \int I_i(x) \left| f(x) \right|^2 dx, \tag{2.22}$$

where $f(x)$ represents the amplitude transmittance of the object, while $I_i(x)$ represents the Fresnel diffraction pattern obtained by the rays passing through phase masks $\psi_i(x)$. $I_i(x)$ can be written as follows:

$$I_i(x) = \left| \exp\left[j\psi_i(x) \right] \otimes h(x, d) \right|^2, \tag{2.23}$$

where $h(x, d)$ and d represent the point pulse function of the Fresnel transformation and the distance between the SLM and the CCD camera, respectively. It should be kept in mind that $I_i(x)$ can be obtained without CCD camera using only the equation (2.23).

The correlation $O(x)$ between the intensity pattern recorded with the CCD camera and the intensity pattern recorded with the bucket detector in the decryption step of the system can be found as follows:

$$O(x) = \frac{1}{N} \sum_{i=1}^{N} \left[B_i - \langle B_i \rangle \right] I_i(x). \tag{2.24}$$

In Equality B_i and $\langle \bullet \rangle \equiv \frac{1}{N} \sum_i \bullet$ represent the measurements obtained by the bucket detector and the average of the N recorded measurements, respectively.

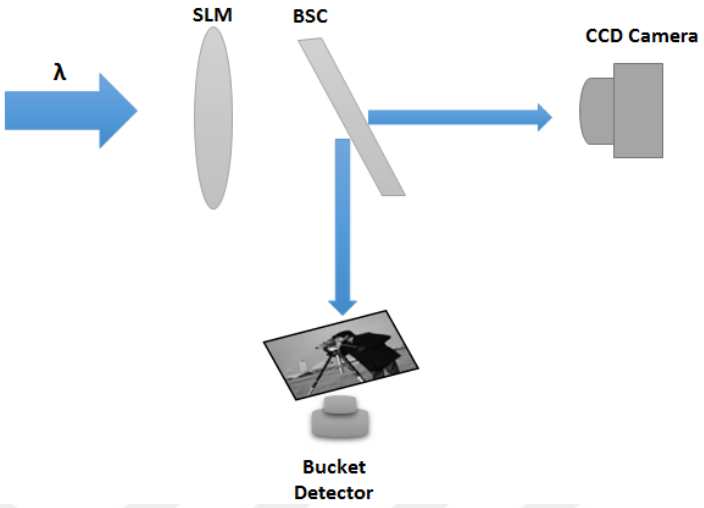


Figure 2.9 Ghost imaging physical experiment system. SLM Spatial Light Modulator, BCS Beam Splitter Cube and lambda plane wave

2.7 Wavelength Multiplexing based Multiple Image Encryption

The continuous increase in the amount of data brings along the problem of safe transmission of these data from lines with limited bandwidth. For this reason, optical multiple-image encryption methods have been studied in recent times. Wavelength multiplexing based multiple image encryption method is one of the first in this field [19]. The physical installation of the system, which encrypts different images with different wavelengths, is given in Figure 2.10. In order to make the installation easier to understand, the scheme of the physical installation is drawn without a lens. In Figure 2.10, $f_k(a,b)$ represents images to be encrypted, while sub-index k represents the total number of images. In order to facilitate the narrative, if the system is explained on two images, the mathematical expression of $x_1(\tilde{a},\tilde{b})$ obtained by coding the first image $f_1(a,b)$ to be encrypted on the first phase mask RPM1 can be written as follows:

$$x_1(\tilde{a},\tilde{b}) = \mathrm{FRT}_{\lambda_1}\{f_1(a,b)\exp[i2\pi\varphi(a,b)];\mathrm{d}_1\}, \qquad \textbf{(2.25)}$$

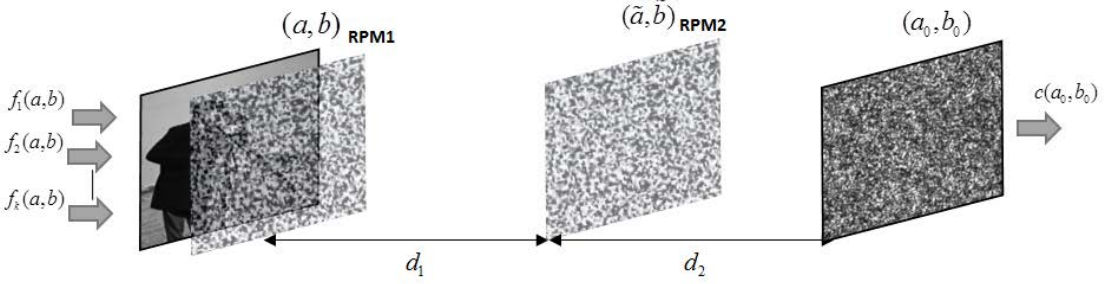


Figure 2.10 Non-lensed physical experiment system of wavelength multiplexing based optical image cryptography

where $\exp[i2\pi\varphi(a,b)]$, FRT and λ_1 represent the first random phase mask (RPM1), Fresnel transform and the first wavelength used for Fresnel transform, respectively. Then, the mathematical expression of the encrypted image $c_1(a_0,b_0)$ obtained for the first input image by coding $x_1(\tilde{a},\tilde{b})$ on the second phase mask $\exp[i2\pi\psi(\tilde{a},\tilde{b})]$ (RPM2) can be written as follows:

$$c_1(a_0,b_0)=\mathrm{FRT}_{\lambda_1}\{x_1(\tilde{a},\tilde{b})\exp[i2\pi\psi(\tilde{a},\tilde{b})];\mathrm{d}_2\}. \quad \textbf{(2.26)}$$

The second image $f_2(a,b)$ is also encoded in the same manner as described above. The only difference in the encryption of the second image is that $c_2(a_0,b_0)$ is obtained by using a different wavelength λ_2 than the first. As a final stage, images are combined in a single complex image by $c(a_0,b_0)=c_1(a_0,b_0)+c_2(a_0,b_0)$ operation. If the difference between λ_1 and λ_2 is below a certain threshold, then the decryption process is faulty and the original images cannot be accessed. In the decryption stage, the complex conjugate of the encrypted image $c^*(a_0,b_0)$ is first found by the phase shifting algorithm. The complex conjugate of the encrypted image $c^*(a_0,b_0)$ is then processed in the Fresnel space and $\tilde{f}_1(a,b)$ including the first image $f_1(a,b)$ together with the noise caused by cross-talk can be written as follows:

$$\tilde{f}_1(a,b) = \mathrm{FRT}_{\lambda_1}\left\{\mathrm{FRT}_{\lambda_1}\left\{c^*(a_0,b_0);\mathrm{d}_2\right\}\exp[i2\pi\psi(\tilde{a},\tilde{b})];\mathrm{d}_1\right\}. \quad \textbf{(2.27)}$$

The expression on the left side of the equation is also $\tilde{f}_1(a,b) = f_1(a,b) + \mu_1(a,b)$ and $\mu_1(a,b)$ is calculated as follows:

$$\mu_1(a,b) = \mathrm{FRT}_{\lambda_1}\left\{\begin{matrix}\mathrm{FRT}_{\lambda_1}\left\{c_2^*(a_0,b_0);\mathrm{d}_2\right\}\times \\ \exp[i2\pi\psi(\tilde{a},\tilde{b})];\mathrm{d}_1\end{matrix}\right\}\exp[i2\pi\varphi(a,b)] \quad \textbf{(2.28)}$$

According to the equation, $\mu_1(a,b)$ is defined as cross-talk noise in the first image $f_1(a,b)$. The second image $f_2(a,b)$ encoded by λ_2 is also obtained in conjunction with cross-talk noise using the same decryption operations.

Undoubtedly, one of the biggest problems of the system is that the decoded images are noisy due to cross-talk. The second problem is that the system is not robust to known-plaintext attacks because of the use of DRPE framework [12]. In 2006, a position multiplex based optical encryption method with an encryption system similar to wavelength multiplexing was proposed [20]. While the wavelength is kept constant in the proposed system, encryption is carried out by shifting to different distances for different images on the CCD recorder plane. There are two options for the decryption phase: unfiltered and low pass filter. In the case of filtered use, the noise is somewhat removed, but still not satisfactory. Interference and position multiplexing techniques have been combined to develop an optical encryption system for multiple-image encryption, but this system has also been exposed to cross-talk noise [21].

2.8 Phase Retrieval based Multiple Image Encryption

The use of iterative phase retrieval algorithms has been greatly increased in order to eliminate the noise caused by cross-talk of multiple image encryption methods [22, 23]. An optic multiple image encryption method generated by combining Modified Gerchberg-Saxton algorithm (MGSA) and multiplexing (position or wavelength)

techniques has been the source of the following methods [22]. First, the image to be encrypted is subjected to the MGSA given the block diagram in Figure 2.11 to obtain the phase mask where the image will be encoded. According to Figure 2.11, the phase $\phi_f(a_0,b_0)$ of the image obtained by taking inverse Fresnel transformation (IFrS) of the image $f(a_1,b_1)$ is combined with the unit amplitude. Then $\phi_{\hat{f}}(a_1,b_1)$ and $\hat{f}(a_1,b_1)$ are the phase and the amplitude of the approximated image obtained by taking Fresnel transform (FrS) of the combined image, respectively. After the new phase information $\phi_{\hat{f}}(a_1,b_1)$ is combined with the target image $f(a_1,b_1)$, again the inverse Fresnel transformation is taken. This loop continues until the similarity between the input image $f(a_1,b_1)$ and the updated image $\hat{f}(a_1,b_1)$ reaches a certain level. When the loop ends, the last phase information $\phi_f(a_0,b_0)$ obtained by the inverted Fresnel transformation is considered to be the phase in which the image is to be encoded. After the MGSA step is finished, each image $f_n(a_1,b_1)$ is encoded to different wavelength λ_n (the wavelength of light in the input) or different position z_n (difference between input images and output plane) with its own specific phase information $\phi_{\lambda_n}(a_0,b_0)$ or $\phi_{z_n}(a_0,b_0)$. If the process of combining the images on a single plane is to be done by the wavelength multiplexing

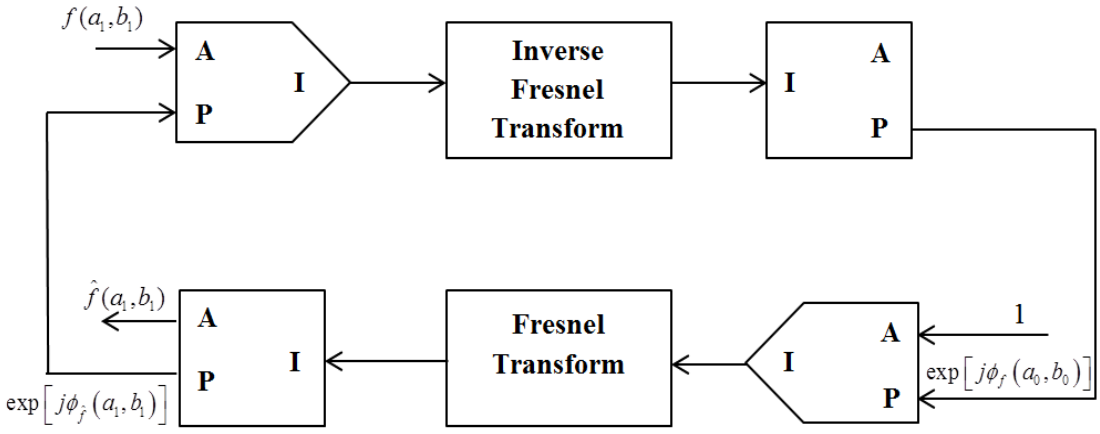


Figure 2.11 Block diagram of Modified Gerchberg-Saxton Algorithm

method, $\phi_{\lambda_n}(a_0,b_0)$ must provide the following condition:

$$\mathrm{FrS}\left\{\exp[j\phi_{\lambda_n}(a_0,b_0)];\lambda_n;z\right\}=\hat{f}_n(a_1,b_1)\exp[j\phi^{\lambda}_{\hat{f}_n}(a_1,b_1)]. \quad \textbf{(2.29)}$$

At equality, $\phi^{\lambda}_{\hat{f}_n}(a_1,b_1)$ represents the phase information corresponding to the current image. Similarly, if the process of combining the images on a single plane is to be done by the position multiplexing method, $\phi_{z_n}(a_0,b_0)$ must provide the following condition:

$$\mathrm{FrS}\left\{\exp[j\phi_{z_n}(a_0,b_0)];\lambda;z_n\right\}=\hat{f}^{z}_{n}(a_1,b_1)\exp[j\phi^{z}_{\hat{f}_n}(a_1,b_1)], \quad \textbf{(2.30)}$$

At equality, $\phi^{z}_{\hat{f}_n}(a_1,b_1)$ represents the phase information corresponding to the current image. Phases $\left(\phi^{z}_{\hat{f}_n}(a_1,b_1)\text{ or }\phi^{\lambda}_{\hat{f}_n}(a_1,b_1)\right)$ encoded at different wavelengths or positions with wavelength multiplexing or position multiplexing are combined in a single plane by simple addition. Original images $\hat{f}^{\lambda}_{n}(a_1,b_1)\left[\text{or }\hat{f}^{z}_{n}(a_1,b_1)\right]$ can be recovered with the noise caused by cross-talk from a single plane encoded. To reduce the cross-talc effect, the mathematical expression of the $\mathrm{FrS}\left\{\exp[j\phi'_{\lambda_n}(a_0,b_0)];\lambda_n;z\right\}$ obtained by moving the approximate images $\hat{f}_n(a_1,b_1)$ to different positions using phase modulation, which is the characteristic of the Fresnel transformation, can be written as follows:

$$\mathrm{FrS}\left\{\exp[j\phi'_{\lambda_n}(a_0,b_0)];\lambda_n;z\right\}=\hat{f}^{\lambda}_{n}(a_1-u_n,b_1-v_n)\exp[j\psi(a_1,b_1)], \quad \textbf{(2.31)}$$

At equality, $\psi(a_1,b_1)$ represents the phase of the currently encoded image, u_n and v_n represent the shift amounts of $\hat{f}^{\lambda}_{n}$ in the a_1 and b_1 axes on the output plane, respectively. In addition, $\phi'_{\lambda_n}(a_0,b_0)$ is calculated as follows:

$$\phi'_{\lambda_n}(a_0,b_0)=\phi'_{\lambda_n}(a_0,b_0)+\frac{2\pi\left(u_n a_0+v_n b_0\right)}{\lambda_n z}. \quad \textbf{(2.32)}$$

The noise caused by cross-talk was significantly eliminated by the shifting operations [22]. In order to synthesize the Single Phase Only Function (POF), the phases corresponding to the $\phi'_{\lambda_n}(a_0,b_0)$ are subjected to normalization after collection, and the $\exp\left[j\phi_T^{\lambda}(a_0,b_0)\right]$ (for wavelength multiplexing) can be calculated as follows:

$$\phi_T^{\lambda}(a_0,b_0)=\arg\left\{\frac{\sum_{n=1}^{N}\exp\left[j\phi'_{\lambda_n}(a_0,b_0)\right]}{\left|\sum_{n=1}^{N}\exp\left[j\phi'_{\lambda_n}(a_0,b_0)\right]\right|}\right\}, \tag{2.33}$$

where arg {} and N represent the phase calculation operator and the total number of images to be encrypted, respectively.

In the decryption stage, the decrypted images $\left|\hat{f}_n^{\lambda}(a_1-u_n,b_1-v_n)\right|+\left|n_{\lambda_n}(a_1,b_1)\right|$ from the encrypted images at different wavelengths can be written as follows:

$$\begin{aligned}&\left|\hat{f}_n^{\lambda}(a_1-u_n,b_1-v_n)\right|+\left|n_{\lambda_n}(a_1,b_1)\right|\approx\\&\left|\hat{f}_n^{\lambda}(a_1-u_n,b_1-v_n)\exp\left[j\phi_{\hat{f}_n}^{\lambda}(a_1-u_n,b_1-v_n)\right]+n_{\lambda_n}(a_1,b_1)\right|\end{aligned} \tag{2.34}$$

In the expression, $n_{\lambda_n}(a_1,b_1)$ represents the remaining cross-talk noise after the image has been decrypted. The difference between this technique and the others is the minimization of cross-talk-related noise by the use of shift operators (u_n,v_n). The use of a phase retrieval algorithm in the system further helps to reduce the cross-talk noise by providing different phase masks for each image. Similarly, a method in which optical installation is simpler because of its non-lens structure and the increasing reliability due to the parallel phase retrieval algorithm is used to minimize the noise caused by cross-talk has been proposed [56]. Iterative phase retrieval based multiple image encryption systems with similar structures have also been proposed [57, 58]. Although the problem

of the noise caused by cross-talk is solved with these systems, the number of images to be encrypted at the same time is still a problem.

2.9 4-f Correlator Based Image Encryption

In order to solve the problem of the number of encrypted images to be sent at the same time, 4-f based multi-image encryption method has been proposed [24]. The physical installation scheme of the system developed for single image encryption to understand the 4-f based image encryption is given in Figure 2.12. The system encodes images to corresponding phases using the cascaded phase retrieval algorithm (CPRA). According to the diagram in Figure 2.12, Let $f(a,b)$ is the image to be encrypted and $g(a,b)$ is the encoded target image. The system obtains the phase masks necessary to encode the input image $f(a,b)$ to the target image $g(a,b)$ using a CPRA which has forward and backward propagation in each cycle. In the *n*th step of forward iteration, the output image $O(a,b)$ obtained by applying forward iteration to input image with phase masks defined as $\psi^n(a,b)$ and $\varphi^n(\mu,\nu)$ can be written as follows:

$$\begin{aligned} O(a,b) &= g^n(a,b)\cdot\exp[j\phi^n(a,b)] \\ &= IFT\left(FT\left\{f(a,b)\exp[j\psi^n(a,b)]\right\}\times\exp[j\varphi^n(\mu,\nu)]\right), \end{aligned} \tag{2.35}$$

where $f(a,b)$ represents the restriction in each forward propagation step and its value does not change in any step, while $g^n(a,b)$ and $\phi^n(a,b)$ represent the *n*th approximate

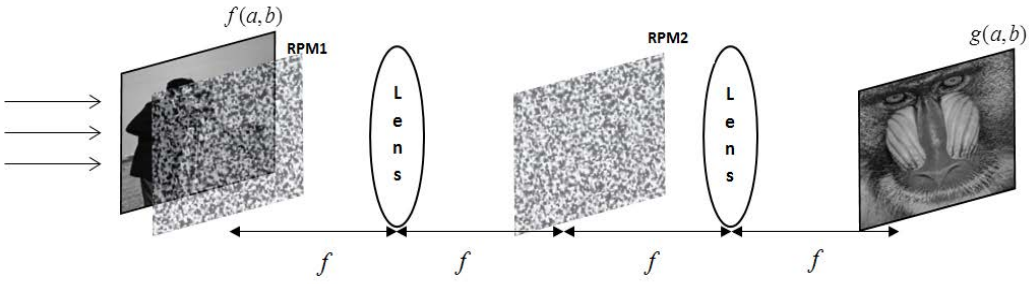


Figure 2.12 Physical experiment system of 4-f based optical image encryption

amplitude image and the *n*th iterative phase in the output image, respectively. The same path is followed when backward propagation is performed and $g^n(a,b)$ is replaced with $g(a,b)$ as the encoded image in each backward iteration step. In addition, in each step $\varphi^{n+1}(\mu,\nu)$ is updated as follows:

$$\varphi^{n+1}(\mu,\nu) = \text{angle}\left(\frac{FT\left\{ g(a,b)\exp[\,j\phi^n(a,b)]\right\}}{FT\left\{ f(a,b)\exp[\,j\psi^n(a,b)]\right\}} \right), \quad \textbf{(2.36)}$$

and $\psi^{n+1}(\text{a},b)$ is updated as follows:

$$\psi^{n+1}(\text{a},b) = \text{angle}\left[IFT\left(FT\left\{ g(a,b)\exp[\,j\phi^n(a,b)]\right\} \times \exp[\text{-}i\varphi^{n+1}(\mu,\nu)]\right)\right], \quad \textbf{(2.37)}$$

where the expression *angle()* represents the operator taking the phase of the image. This cycle ends when the correlation coefficient between $g(a,b)$ and $g^n(a,b)$ reaches the desired value. This system, which is described for encrypting single image, can be adapted to multiple-image encryption in Figure 2.13.

For the 4-f-based multiple-image encryption, N single image encoding system is combined as in Figure 2.13 and therefore there are N target images in the system. The phase masks $\exp(j\psi_k)$ and $\exp(j\varphi_k)$ used for each image in the system are obtained iteratively from the relationship between the input and output images $\left\{ g_{0k}^n(a,b), g_{0k+1}(a,b)\right\}$ by phase retrieval algorithms. The encrypted image A from the images $g_{0k}^n(a,b)$ encoded using these phase masks is obtained as follows:

$$A = g_{0k+1}^n \exp(i\phi_k) = IFT\left\{ FT\left[g_{0k}^n \exp(i\psi_k)\right]\exp(i\varphi_k)\right\} \quad \textbf{(2.38)}$$

Since it is required that the equation of the input image $\left(g_{0k}^n\right)$ in equation (2.38) should be changed to $g_{0k}^n \exp(i\phi_{k-1})$ for the optical installation of the system, the right side of

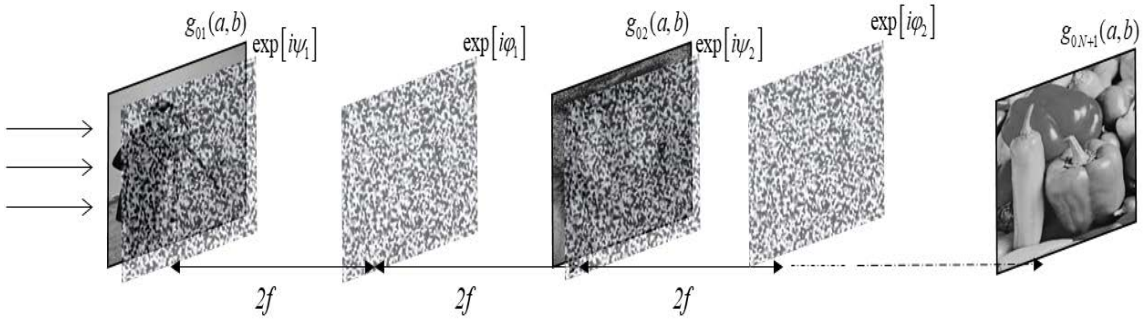


Figure 2.13 Physical experiment system of 4-f based multiple image encryption

the equation is multiplied by $\exp(i\phi_{k-1})\times\exp(-i\phi_{k-1})$ to calculate the new A as follows:

$$A = IFT\left\{FT\left[g_{0k}^{n}\exp(i\phi_{k-1})\times\exp(-i\phi_{k-1})\exp(i\psi_k)\right]\exp(i\varphi_k)\right\}, \quad \textbf{(2.39)}$$

The final encrypted image A obtained by further editing of Equation (2.39) can be written as follows:

$$A = IFT\left[FT\left\{g_{0k}^{n}\exp(i\phi_{k-1})\times\exp\left[i(\psi_k-\phi_{k-1})\right]\right\}\right]\exp(i\varphi_k) \quad \textbf{(2.40)}$$

In the decryption step of the multiple image encryption system provided with Equation (2.40), the decrypted images $g_{0k}^{n}\exp(i\phi_{k-1})$ obtained from A can be calculated as follows:

$$g_{0k}^{n}\exp(i\phi_{k-1}) = IFT\left[FT\left\{A\times\exp(-i\varphi_k)\right\}\right]\exp\left[-i(\psi_k-\phi_{k-1})\right] \quad \textbf{(2.41)}$$

In combination with the CPRA and 4-f, the number of encrypted images sent simultaneously without noise caused by cross-talk is increased compared to previous studies [22]. The problem of the 4-f based multi-image encryption system is that the authorization in the system cannot be performed properly due to the hierarchical structure it has. Since the images are encrypted in series with each other, the image

cannot be decrypted before the previous image is decrypted. This makes users dependent on each other.

Several methods have been developed in the multiple-image encryption area, such as 3D particle distribution phase retrieval based optical encryption [59], compressive sensing-based multiple-image encryption methods [60], spectrum multiplex based image encryption [61] and Parallel optical based multi-image encryption [62].

CHAPTER 3

IMPORTANCE OF PHASE IN IMAGES AND PHASE RETRIEVAL ALGORITHMS

The symbols used in this chapter are specific to this chapter, not general expressions.

3.1 Importance of Phase in Images

A beam of light carries both intensity and phase information. Since optical detectors such as charged-coupled devices (CCD) cameras and light-sensitive films cannot detect phase information in the beam wave, including the human eye, this process is possible with high-tech products [63]. Optical measuring devices that obtain image by converting photons, which they capture, into electrons cannot record phase information of an electromagnetic wave with a frequency of about 10^{15} Hz or higher [63]. For such cases, there are expensive hologram techniques where both phase information and amplitude information can be recorded [64]. In addition, in these techniques there exists the problem of speckle noise and it is solved with some strategies given in [64]. As the details of the image are retained in the phase information, the detail information of the images composed of only the intensity (amplitude) is lost. Two tests are performed in order to understand the importance of phase in the images. The first test results in which only the amplitude information of the image is left by subtracting the phase information are given in Figure 3.1. In Figure 3.1 (b) and (c), the Fourier amplitude and phase information of the image are given respectively. In Figure 3.1 (d), the image obtained by taking the inverse Fourier transform of the image with only the amplitude information is given. As a result, there is no detail left on the image in the phase-out image. In the second test, the phase values of the two different images in the Fourier space are swapped and then their inverse Fourier transforms are taken. According to the test results given in Figure 3.2, the detail information in an image is carried by the phase of the image.

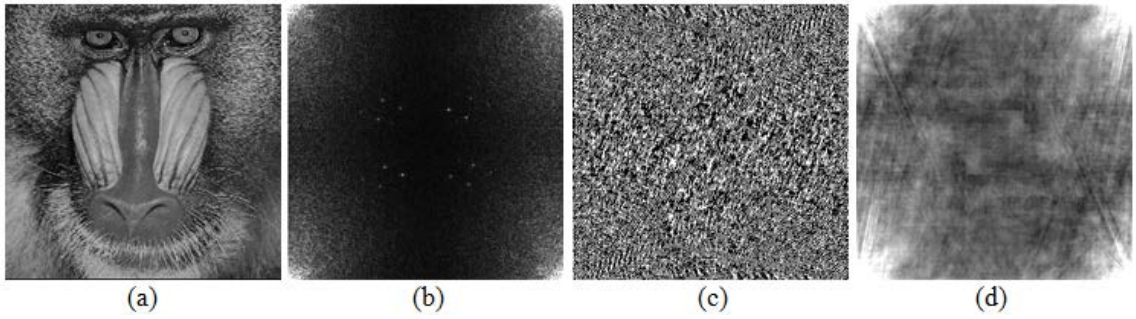


Figure 3.1 (a) the original image; (b) the Fourier amplitude of the image; (c) Fourier phase information of the image; (d) Image obtained by taking inverse Fourier transform of Fourier amplitude

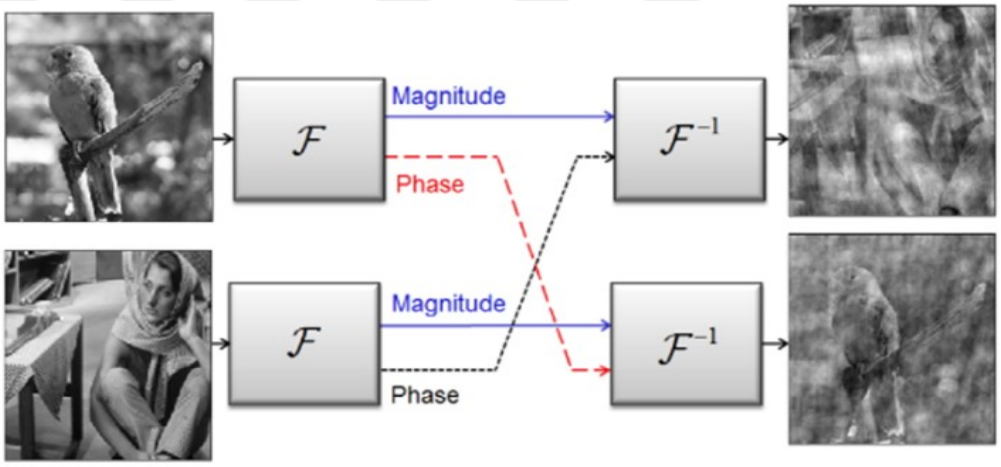


Figure 3.2 The test applied to understand the importance of phase information [63]

3.2 Phase Retrieval Algorithms

Phase retrieval algorithms have been developed in order to restore phase information from the amplitude values of the images, whose phase information cannot be recorded and consisting only of the intensity. Phase retrieval algorithms are extensively used in x-ray crystallography [63], hologram technology [63], transmissive electron microscopy [65] and astronomy [66]. In addition to these fields, phase retrieval algorithms are also widely used in the field of optical image encryption [10, 22, 42, 43, 57, 58]. In 1971, phase retrieval techniques starting with the Gerchberg-Saxton (GS) algorithm [67]

continue to evolve with algorithms like Yang-Gu, Error Reduction (ER), Hybrid-Input Output (HIO), Wirtinger Flow (WF) and prDeep [68-71]. In this thesis, ER and HIO/ER are used separately from phase back access algorithms [69]. In order to understand the two algorithms, first the ER and then the HIO algorithm are explained. The Fourier amplitude G of the positive image matrix for which the phase should be obtained can be defined as follows:

$$G = \left| FT\left(z\left(a,b \right) \right) \right|. \tag{3.1}$$

In the equation, Fourier amplitude value G, positive image matrix Z and matrix row-column numbers are represented by (a,b). In this case, the ER algorithm is first defined by Algorithm-1.

Algorithm-1 (ER)

Inputs: G, y, S

G - Fourier amplitude of the desired image to be reconstructed.

$y(a,b)$ - Initial matrix to be updated at every step.

S - Number of iterations.

Output: y_{s+1} - The resulting image, which is compatible with the amplitude of the input image in real space and its amplitude in Fourier space.

Start. Create a random initial matrix

$y_0 = rand\left(a,b \right),\ rand\left(a,b \right)$: *Random Matrix Generator*.

$y_s = y_0$.

General Steps (S =1,2, …) **:**

1) Fourier transform: $FT(y_s)$
2) The Fourier phase information and the Fourier amplitude information of the image is wanted to find the phase are combined: $y'_s = g_{a,b} \dfrac{FT(y_{s,(a,b)})}{\left| FT(y_{s,(a,b)}) \right|}$

3) Calculate projection operator with inverse Fourier transform: $\rho_f = FT^{-1}(y'_s)$

4) $y_{s+1} = \begin{cases} \rho_f\left(y'_{s,(a,b)}\right) & \text{if } (a,b) \geq 0 \\ 0 & \text{otherwise} \end{cases}$

5) Return to Step 1.

Up to: *Total number of iterations* $= s$

$|FT(\ )|$, $FT(\ )/|FT(\ )|$, $FT^{-1}(\ )$ from the parameters used in Algorithm-1 denote the Fourier amplitude, Fourier phase information and inverse Fourier transform of the image, respectively. Secondly, the HIO algorithm is as in Algorithm-1 and only in the fourth step the updated matrix y_{s+1} changes as follows:

$$y_{s+1} = \begin{cases} \rho_f\left(y'_{s,(a,b)}\right) & \textit{otherwise} \\ y_s - \beta\rho_f\left(y'_{s,(a,b)}\right) & \text{if } (a,b) \geq 0 \end{cases} \quad \textbf{(3.2)}$$

In Equation, the constant β represents the Fienup parameter and is chosen to be close to one [69]. In this way, HIO / ER algorithm is completed by applying the HIO algorithm first to the Fourier amplitude of the image in which the phase is to be reconstructed and then the ER algorithm to the output of HIO. The oversampling method which commonly used in phase retrieval algorithms and adds zeros to around the image according to the Nyquist sampling criterion so that the image can be reconstructed without noise from its amplitude, is also used in the ER and HIO/ER algorithm. While the image sampled with oversampling method is given in Figure 3.3 (a), the Fourier amplitude of the sampled image is given in Figure 3.3 (b). The image obtained by applying the inverse Fourier transform to the phase-removed image is shown in Figure 3.3 (c) and it is seen that the detail information of the image is removed along with the phase. According to this, the image reconstructed by applying ER algorithm to only the Fourier amplitude of the image without Fourier phase information is shown in Figure 3.3 (d). As seen in the Figure, although the image obtained by ER algorithm is not of good quality it is given in section 4 where the original image is obtained quite well from the

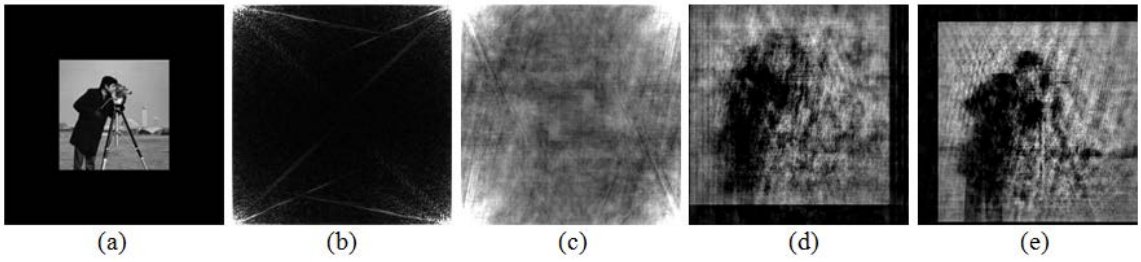


Figure 3.3 (a) the original image sampled by the oversampling method; (b) the Fourier amplitude of the image; (c) the image obtained by taking the inverse Fourier transform of the Fourier phase removed image; (d) Image recovered from (b) by the ER algorithm and (e) Image recovered from (b) by the HIO / ER algorithm

oversampled image by using ER algorithm with diffractive imaging method. In the same way, the result of the HIO / ER algorithm to reconstruct the original of the sampled image only from the Fourier amplitude is given in Figure 3.3 (e). As shown in the Figure, the quality of the image reconstructed by the HIO / ER algorithm is better than the quality of the image reconstructed by the ER algorithm. As a result of the use of the HIO / ER algorithm with the diffractive method, it is shown in section 5 that the original of the image is reconstructed from only the Fourier amplitude of the non-oversampled image very good quality.

CHAPTER 4

IMAGE HIDING WITH HYBRID METHOD

The symbols used in this chapter are specific to this chapter, not general expressions. Since the Double Random Phase Encoding (DRPE) method is weak against some attacks [11-13], different methods have been developed based on Equivalent Modulus Decomposition (EMD), diffractive imaging, and phase truncated Fourier transform (PTFT) [5, 9, 10]. Among the developed methods, diffractive imaging-based methods are even more notable with their non-linear structure than others [10]. However, optical image encryption methods designed with diffractive imaging are also weak against a specific attack [18]. Similarly, other conventional optical encryption methods are also vulnerable to various known plaintext, chosen-cipher text, and chosen-plaintext attacks [14-16, 27].

In order to reduce the weaknesses of existing methods and to design a strong encryption method against attacks, simplified diffractive imaging is the framework of this work. In this study, a hybrid method has been developed which diffuses the encoded information into a carrier composed entirely of noise together with diffractive imaging, block separation and pixel mixing.

While some parameters and the carrier matrix in the developed hybrid method provides additional key space for the method, it is also provided to encrypt more than one image at the same time according to the matrix size of the carrier used. Hybrid method is determined to be robust to attacks such as known-plaintext and chosen-plaintext by the tests, while significant advantages of the method are presented with experimental studies and reliability tests.

4.1 Diffractive Imaging and Phase Retrieval Algorithm

It is shown in section 3 that the detail information in an optical image is carried in the Fourier phase and the images can be reconstructed from the Fourier amplitudes by phase retrieval algorithms. In this study, Fourier transform based diffractive imaging framework is used considering the importance of phase. The diffractive imaging method used for the developed method is given in Figure 4.1. The image $f(a,b)$ sampled by the oversampling method is modulated with two random phase masks $(RPM1, RPM2)$ according to the designed method in Figure 4.1 and the Fourier amplitude G of the diffractive coded image is calculated as follows:

$$G = \left| \mathrm{FT}\left\{ \Lambda f(a,b) \right\} \right|, \quad \Lambda = RPM1 \times RPM2 \tag{4.1}$$

In equality, FT represents the Fourier transform and Λ represents the diagonal matrix formed by the multiplication of the phase masks. In order to recover the image encoded by the diffractive imaging method, the Error Reduction (ER) algorithm given in section 3 is used.

4.2 Creating of the Carrier

The carrier used to hide the image modulated with random phase masks is formed from a particularly noisy image. The reason of creating a particularly noisy image for the carrier is that the information matrix initially transformed into noise-like image is no different from the noise in the carrier. In addition, the reason why the carrier is also created in large matrix size is to increase the capacity of the data to be transmitted at the same time and to hide the actual matrix size of this data confidential. Therefore, a photograph is taken with an ordinary camera in a dark environment and then the pixel size is increased to 4608×3870 as in Fig. 4.2 (a). By converting the image increased the matrix size to 16-bit depth gray tone the hidden data is prevented from being easily extracted from the inside of the carrier. The image with a depth of 16-bit is then

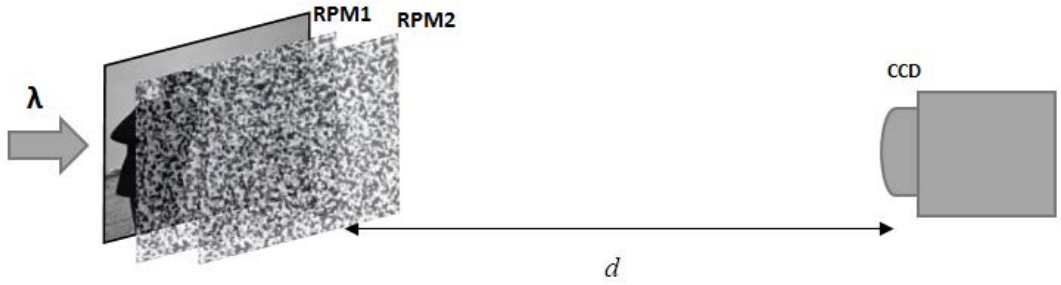


Figure 4.1 Block system of diffractive imaging used for encryption

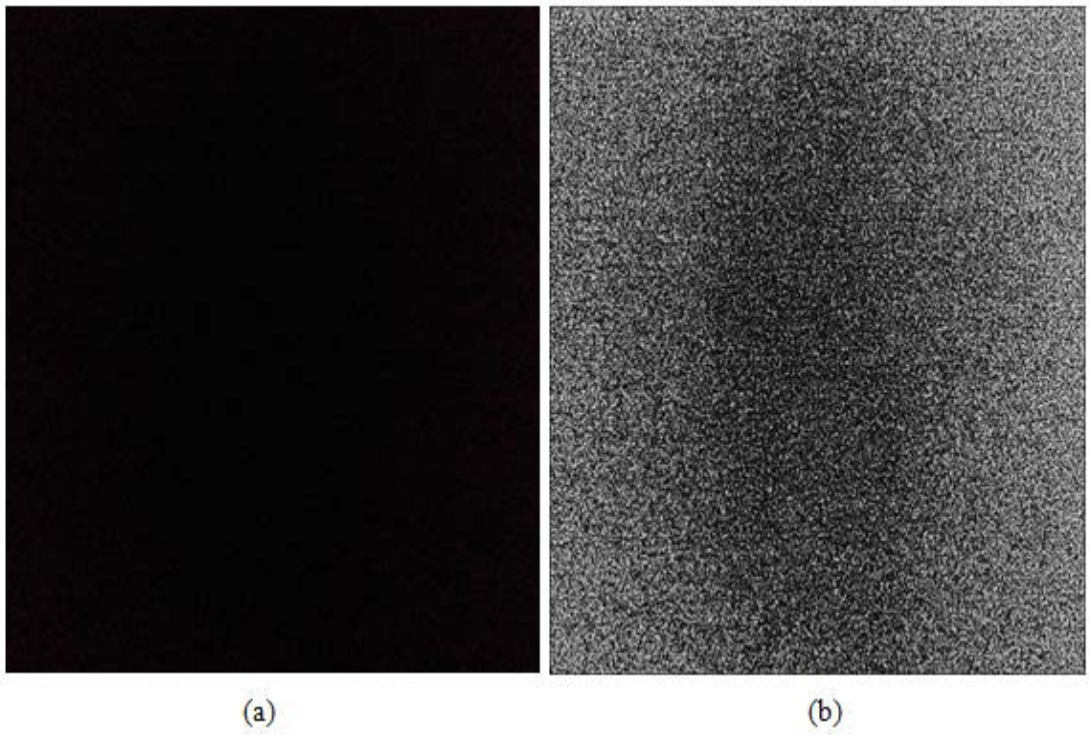


Figure 4.2 (a) 4608×3870 matrix sized photo taken in the dark and (b) the noisy carrier with 16-bit depth gray tone contrast enhancement of dark image (a)

subjected to contrast enhancement [72] to form a completely noisy carrier as in Figure 4.2 (b). Contrast enhancement is often used to improve the quality of images taken in low-light or inadequate lighting [72]. However, contrast enhancement processing

applied to images taken in very low-light environments (dark environments) produces only the so-called Speckle noise in images as shown in Figure 4.2 (b).

4.3 Encryption Process

First, the image to be encrypted is sampled according to the Nyquist sampling criteria [28] so that the recovered image is not noisy. Sampling is carried out by adding zeros to around of the image to be encrypted at least the size of the image with the oversampling method which is frequently used in phase retrieval algorithms. As a result of the sampling, the image whose the matrix size is increased is modulated with random phase masks such as equality (4.1) and only the Fourier amplitude of the image is recorded. In this method, RPM1 is a key that is fixed at the receiver and transmitter sides, while RPM2 is a key that changes at each encryption. Since the Fourier amplitude of the image to be encrypted is modulated by the Λ in equation (4.1) before Fourier transform is taken, the projection operator P_f in the third step of the ER algorithm given in chapter 3 is changed as follow:

$$\rho_f = \frac{FT^{-1}(y'_s)}{\Lambda},\ y'_s = \begin{cases} G_{a,b}\dfrac{FTy_{a,b}}{\left|FTy_{a,b}\right|}, & \text{if } Fy_{a,b} \neq 0 \\ FTy_{a,b}, & \text{otherwise} \end{cases} \qquad \textbf{(4.2)}$$

One of the variables in the equation $y_{a,b}$ represents the random input matrix of $a \times b$ matrix sized initially created for the ER algorithm and updated in each iteration, while $G_{a,b}$ represents the Fourier amplitude of the image obtained in equation (4.1). The other variables used in the equation FT and FT^{-1} represent Fourier and inverse Fourier transformations respectively, while $FTy_{a,b} \big/ \left|FTy_{a,b}\right|$ represents the Fourier phase information of the image. New image $G_{a,b}$ consisting of only Fourier amplitude information and turned into noise-like image is randomly distributed into the carrier according to the algorithm in Figure 4.3. Firstly, according to this algorithm, new image is divided into cellular matrices CM (Cell Matrix), each of which is 4×4 size, with the

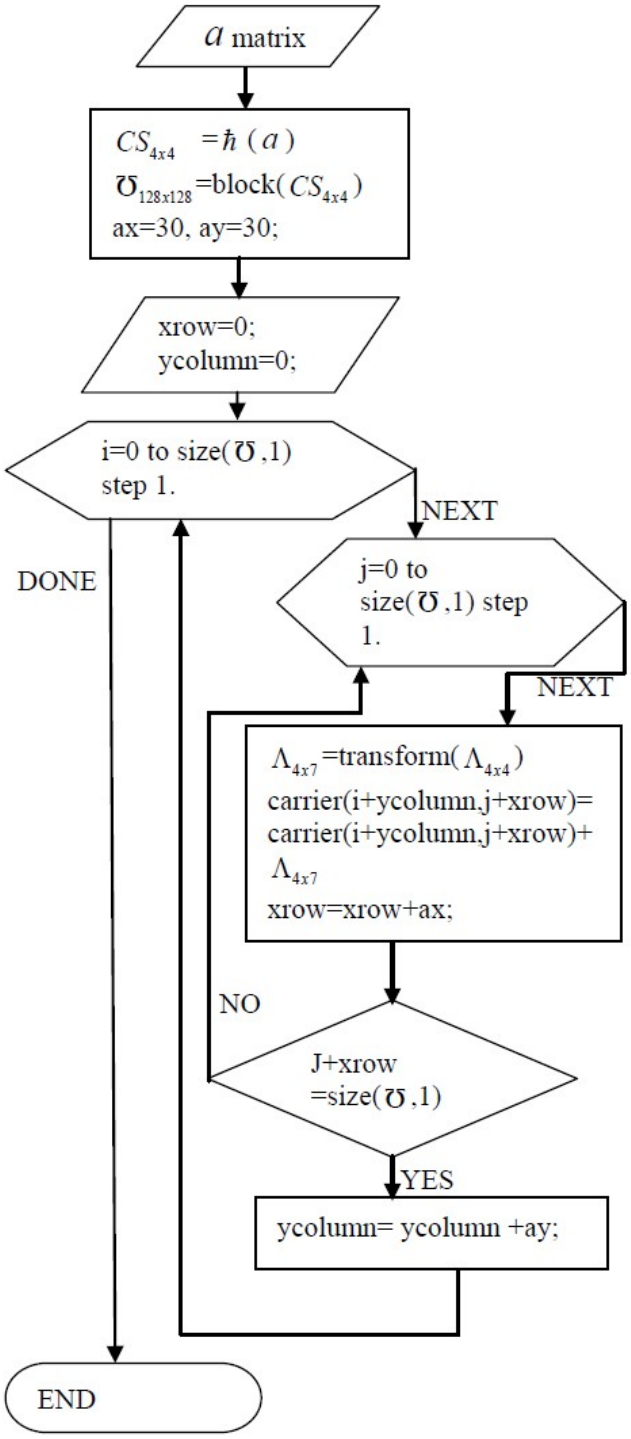


Figure 4.3 Flowchart of the algorithm to distribute the encrypted image into the carrier

$$CS = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}, \ \mho = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{31} & a_{41} & \\ & a_{22} & a_{23} & a_{24} \\ & a_{32} & a_{42} & \\ & & a_{33} & a_{34} \\ & & a_{43} & \\ & & & a_{44} \end{pmatrix}$$

Figure 4.4 The algorithm to distribute 4×4 cellular matrix and (b) 4×7 transformed cellular matrix

$\hbar$ function. Then a block matrix $\mho$ consisting of these cellular matrices and whose total numbers vary according to the size of the image is formed. In the algorithm, "*ax*" and "*ay*" represent row and column shift operators respectively, and the values they receive can be changed to increase the clutter of image considering the size of image to be hidden. With the Cell Transform (CT) function, each cell of the $\mho$ matrix is transformed into a new 4×7 sized cellular matrix, as in Figure 4.4 (b). Each transformed cell is scattered into the carrier according to "*ax*" and "*ay*" values. Since only the Fourier amplitude of the data that is modulated with random phase masks is scattered into the noisy image by the algorithm given in Figure 4.3, it is nearly impossible to extract the true Fourier amplitude from the carrier without the algorithm in Figure 4.3. Therefore, the hybrid method developed is more resistant to attacks such as "chosen-cipher text" and "known-plaintext" attacks in which the linear optical image encryption methods are weak [18].

4.4 Decryption Process

In the decryption process, firstly the block matrix is reached by applying the reverse of the algorithm in Figure 4.3 to the noisy image in which is hidden data. The cellular matrices that make up the block matrix are separated again to obtain the matrix consisting of noise-like image, which is the Fourier amplitude of the encrypted data. Then the diagonal matrix, which is the main key, is created by using the second key

RPM2 and the fixed key RPM1 as in equation (4.1). Finally, using the diagonal matrix, the ER algorithm defined in section 3 reveals the original state of the encrypted image from noise-like image.

4.5 Experimental Results

The experimental results are taken by using digital simulations. The number of iterations for the phase retrieval algorithm can be selected at the desired value. However, if the iteration value is less than 130 for this study, noise is generated when decoding the encrypted data. If the iteration value is greater than 130, it has been determined that there is no additional contribution to the algorithm. Therefore, the number of iterations is chosen as 130 for this study. The "*ax*" and "*ay*" values in the hiding image into the carrier can be changed to increase or decrease the clutter between the pixels by considering the size of the image.

The developed hybrid method was applied on Cameraman image with a matrix size of 512×512 and the "*ax-ay*" values for application were selected as 35 and 45, respectively. Figure 4.5 shows the encryption of the image and the decryption of the encrypted image. The image sampled according to the Nyquist criteria is transformed into matrix of 1024×1024 size as in Figure 4.5 (a) and then the Fourier amplitude of the image modulated with the diagonal matrix as shown in Figure 4.5 (b). While the image obtained by distributing the amplitude of the phase-coded image with the algorithm in Figure 4.3 is given in Figure 4.5 (c), the original image reconstructed by the ER algorithm from encrypted image extracted from the carrier is given in Figure 4.5 (d).

The method was also used to encrypt a message written on MATLAB workspace. The message to be encrypted was first recorded as ".txt" extension and then converted to 256×256 matrix sized image. Finally, it was subjected to the hybrid method in this study. Image of the message to be encrypted is shown in Figure 4.6 (a), while noisy image hosting message as shown in Figure 4.6 (b) and the recovered message is given in Figure 4.6 (c).

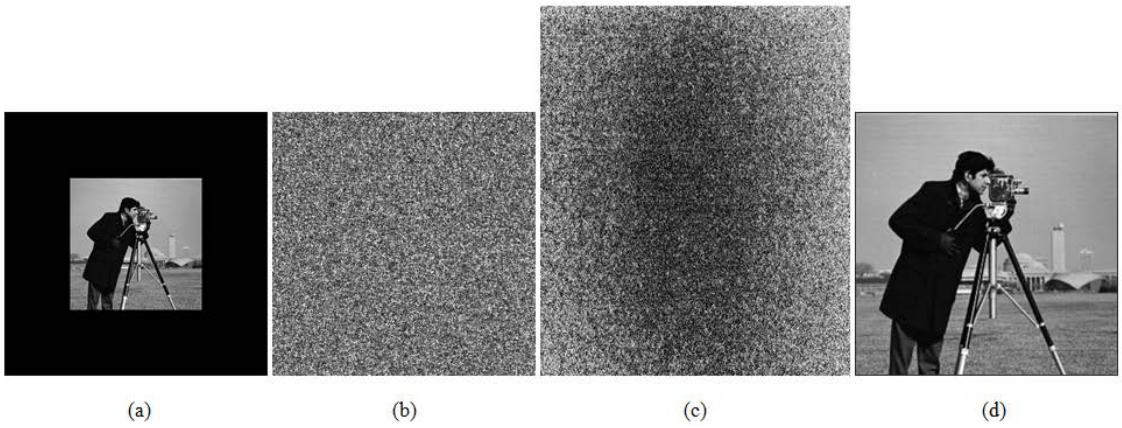


Figure 4.5 (a) 1024×1024 sized sampled Cameraman, (b) modulated Cameraman with diagonal matrix, (c) the noisy image in which the image is scattered and (d) recovered image

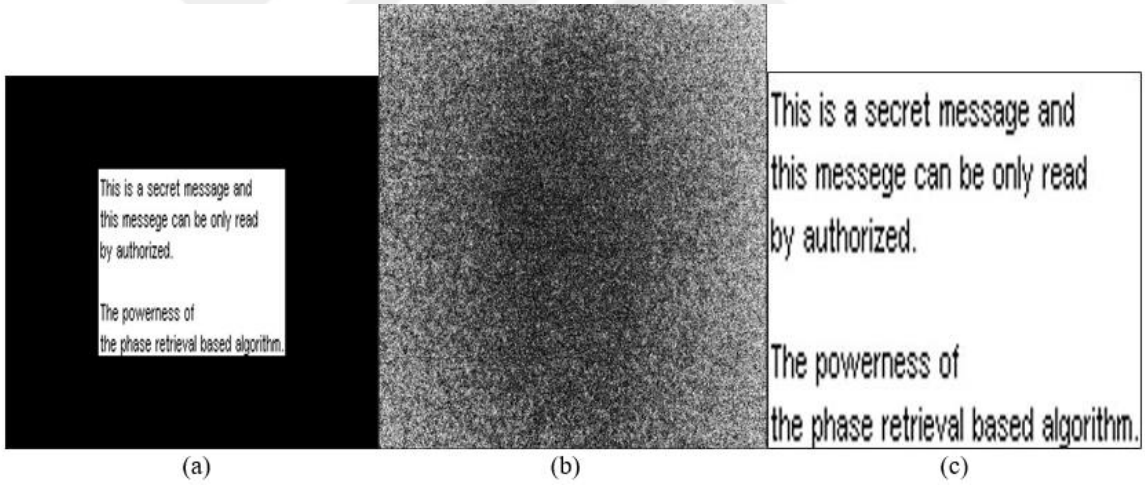


Figure 4.6 (a) 512×512 sized sampled message image, (b) message hidden in a noisy matrix and (c) image of the recovered message

4.6 Security Tests

Statistical analyzes such as histograms and correlations are used to test the reliability of the hybrid method. Noise attacks, contrast stretching and occlusion tests during transmission are applied on the hybrid method and compared with DRPE based algorithms. Known-plaintext and chosen-plaintext attacks are applied to the method and

the durability of the method has been tested. In addition, the sensitivity of the parameters and keys in the algorithm is tested under this heading.

4.6.1 Noise Attacks and Occlusion Tests

In order to test the resistance of the algorithm against noise attacks, the Gaussian noise into the noisy matrix, in which is hidden information, can be added as follows:

$$im = im + \sigma \times rand(\text{size}(im)), \tag{4.3}$$

where "*im*" represents data hidden noise image, σ represents density value of noise, $\text{size}(im)$ and "*rand*" denote matrix size of the image and the function used to generate random matrices. Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) parameters are used to measure the quality of decrypted data after noise and occlusion attacks. The MSE value indicating the error rate between the two images is calculated as:

$$MSE = \frac{1}{nm}\sum_{m=0}^{m-1}\sum_{n=0}^{n-1}\left(y(\text{m},\text{n}) - z(\text{m},\text{n})\right)^2 \tag{4.4}$$

In the equation, y denotes the original image, z denotes the image obtained after decoding and (m, n) denotes the number of rows and columns of image matrices, respectively. The smallest MSE value indicates that the error rate is low between the two images, whereas the large error rate is higher. The PSNR parameter is frequently used in noise reduction algorithms and gives the ratio of the image to noise. The PSNR as a Decibel Unit can be written as follows:

$$PSNR = 10\log_{10}\frac{S^2}{MSE} \tag{4.5}$$

In equation, S and MSE denote the maximum pixel value in the image and the mean square error value defined in equation (4.4), respectively. The higher the PSNR value, the lower the noise in the image. The images obtained after the noise attacks are given in

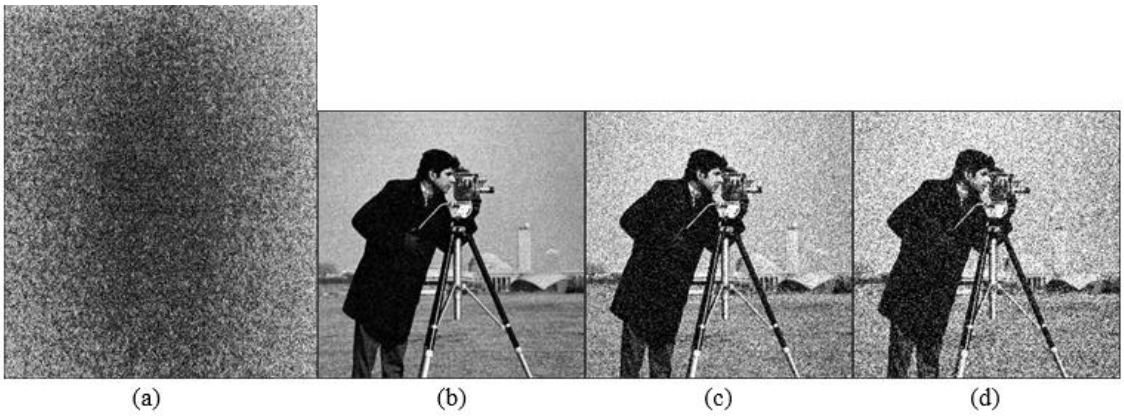


Figure 4.7 (a) Encrypted image hidden in the carrier (a), recovered images for σ =20 (b), σ =50 (c) and σ =70 (d)

Figure 4.7. Comparison of hybrid method, Fractional-based DRPE, Fresnel-based DRPE and LCT-based DRPE optical encryption algorithms were performed against the noise and occlusion attacks at different levels. Table 4.1 shows that the hybrid method by looking at the noise attack analysis applied at three different levels (σ =20, 50, 70) has the highest PSNR (22.7480, 18.7993, 18.0314) and the lowest MSE (0.0072, 0.0272, 0.0384) values, respectively. According to Table 4.1, the algorithm with the highest resistance to noise attacks is the hybrid method. In order to analyse the losses that may occur during the transmission of the encrypted image, some parts of the data hidden image are made zero as in Figure 4.8 and then it is tested that how much of the encrypted data can be recovered. The results of occlusion analysis and the comparison of the developed hybrid method with DRPE based optical encryption algorithms are given in table 4.2. According to this analysis, assuming data loss from the corners and midpoints of the encrypted images it is shown that the most resistant algorithm against occlusion attacks is the hybrid method with the highest PSNR (20.2714, 20.7723) and the lowest MSE (0.0206, 0.0265) values.

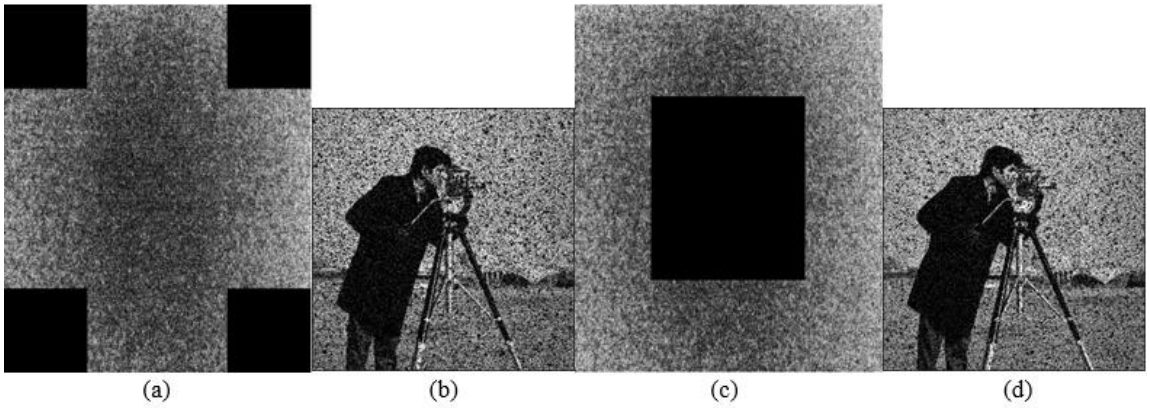


Figure 4.8 (a) Data loss is 1/4 of the encrypted image from corners, (b) decrypted image, (c) Data loss is 1/4 of the encrypted image from midpoint and (d) decrypted image

Table 4.1 Gaussian noise attack analysis and comparison

Gaussian noise	**Classic DRPE**		**FrT DRPE**		**FrS DRPE**		**Lct DRPE**		**Hybrid method**	
σ =%20	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)
	0.0397	17.6386	0.2101	22.7215	0.0083	20.8117	1.1897	21.6513	**0.0072**	**22.7480**
σ =%50	0.2480	15.3311	1.6778	15.4132	0.0382	14.1839	1.3331	16.4831	**0.0272**	**18.7993**
σ =%70	0.4891	13.7584	3.5789	14.4946	0.0538	12.6915	3.5986	14.7932	**0.0384**	**18.0314**

Table 4.2 Occlusion attacks and comparison

Occlusion attack (1/4)	**Classic DRPE**		**FrT DRPE**		**FrS DRPE**		**Lct DRPE**		**Hybrid method**	
From corners	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)
	0.0430	15.1184	0.0253	20.2699	0.0654	11.8435	7.5958	10.5369	**0.0206**	**20.2714**
From center	0.0431	14.9087	0.0292	20.6607	0.0616	12.1063	7.7695	10.2828	**0.0265**	**20.7723**

4.6.2 Contrast Stretching Test

Contrast stretching is usually applied to brighten images taken in the dark and to improve the image [72]. In this study, the contrast stretching is applied to the carrier image included hidden encrypted image and tested to see if there is an abnormal condition that could capture understanding pattern or data from the image. The fact that the encrypted image in the noise-like image is composed of noise has strengthened the relationship between the carrier and the concealed image and only a noisy image can be obtained by contrast stretching as can be seen from Figure 4.9.

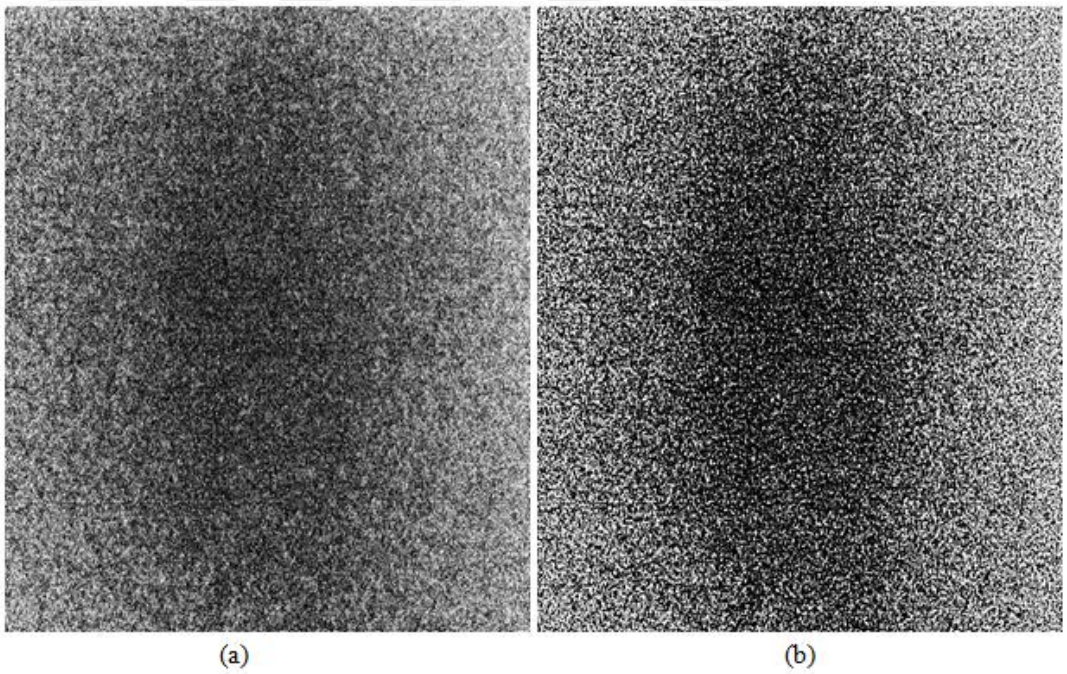


Figure 4.9 (a) Encrypted image hidden in the carrier and (b) image as a result of contrast stretching

4.6.3 Correlation Analysis

The correlation coefficient is used to determine how strong the relationship between pixels is based on the difference between the two selected pixels in an image. In addition, the correlation coefficient can be applied in two different images and the relationship between the pixels of these two images can be analyzed. The correlation coefficient r_{xy} between the two images can be calculated as follows:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}. \tag{4.6}$$

While x and y variables represent the two pixels to be differentiated and $\operatorname{cov}(x, y)$ denotes covariance function, $D(x)$ and $D(y)$ denote the variance values of x and y respectively. The covariance function $\operatorname{cov}(x, y)$ is defined as:

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right), \tag{4.7}$$

where $E(x)$ and $E(y)$ denotes the expected values of x and y respectively, and N represents the number of pairs of pixels. Expected value $E(x)$ and variance $D(x)$ can be calculated as follows:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2, \tag{4.8}$$

The correlation coefficient is in the range [0, 1] and the closer it is to 1, the stronger the relationship between the pixels. The value of the correlation coefficient, which is used to analyze the relationship between the carrier used in the hybrid method and the image in which the data is hidden, is one as shown in Figure 4.10 (b). This shows that there is no difference between the noisy carrier and the image in which is hidden data.

In Figure 4.10 (a), the correlation analysis of the Fourier amplitude of encrypted image (CC = -0.0282) is given, while in Figure 4.10 (b), the correlation graph of the noisy carrier containing the encrypted image is given (CC = 1). As a result, the hiding process is successfully performed.

4.6.4 Histogram Analysis

Histogram analysis is used to measure the quality of cryptography in encryption algorithms. The similarity or difference of two images can be measured using histogram analysis. In this study, the histogram analysis applied to the data to be encrypted, carrier and data concealed image is given in Figure 4.11. In this study, the histogram analysis applied to the image to be encrypted, carrier and image concealed noisy carrier is given in Figure 4.11. While the histograms of the carrier and the data concealed image were almost identical, the histogram of the data to be encrypted was different from the other two images. Thus, it has seen that data is hidden into the noisy carrier successfully.

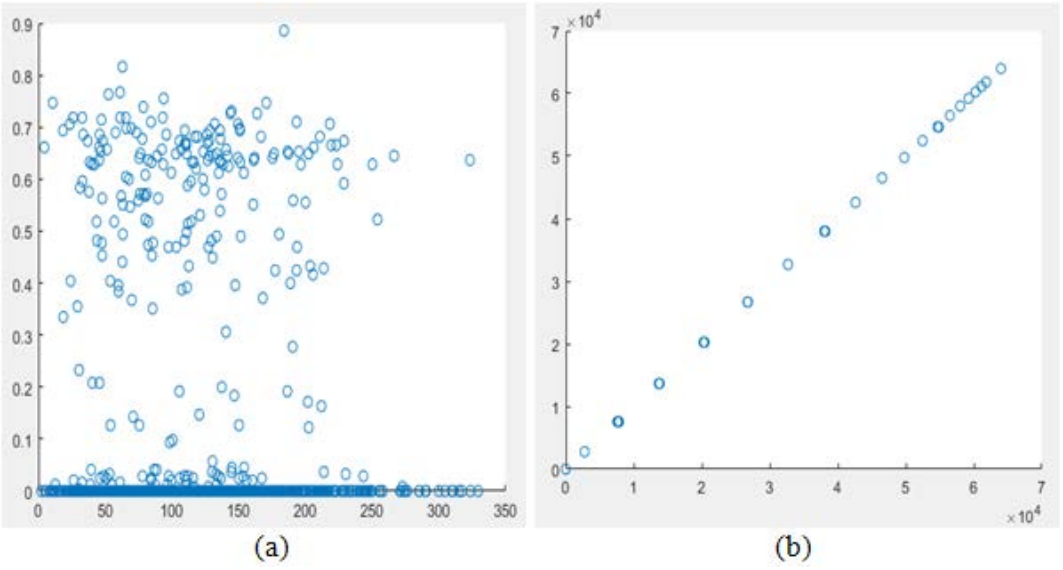


Figure 4.10 (a) Correlation analysis of the image modulated by random phase masks; and (b) Correlation analysis of the carrier hiding the image

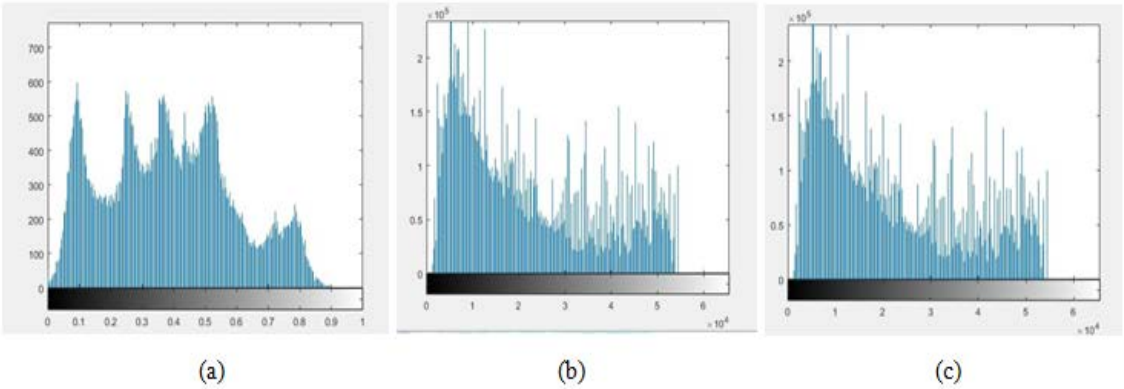


Figure 4.11 (a) Histogram of the image (Cameraman) to be encrypted, (b) histogram of the noisy carrier and (c) histogram of image hidden carrier

4.6.5 Parametric Sensitivity Analysis of Algorithm

A total of three keys are used for the hybrid method developed, two of which are random phase masks and the other is the carrier matrix itself. One of the random phase masks is found both the transmitter and the receiver, while the other mask is randomly generated and sent to the receiver in each encryption. The reason for using two random masks is to reinforce the phase retrieval algorithm against known-plaintext attacks. To measure the power of the keys, assume that the data hiding algorithm, the second stage of the hybrid method developed, is captured. In this case, the phase retrieval algorithm is applied to the noise-like matrix, which is extracted from noisy carrier, with the wrong key and the results are given in Figure 4.12. In the case that one of the phase masks used is incorrect, no meaningful data is obtained is given in Figure 4.12 (b) and (c). Figure 4.12 (d) shows that no meaningful data can be obtained if one of the keys is correct but a part of the other key is incorrect. Figure 4.13 (a) shows that the phase masks are correct, but the carrier key is incorrect, and in Figure 4.13 (b), no significant data is obtained in the case that only a pixel block of size 10×10 in the carrier is wrong. In the data hiding algorithm, a test was performed to measure the sensitivity of “ax” and “ay” values representing row and column shift operators respectively. For example, when the encrypted data is distributed to carrier, “ax” = 25 and “ay” = 20 were used, while “ax” =

24 and “ay” = 19 were used during decryption. Accordingly, as shown in Figure 4.13 (c), even a small change in “ax” and “ay” values prevented access to the encrypted data.

4.6.6 Robustness of Hybrid Method to Known-plaintext and Chosen-plaintext Attacks

Known-plaintext and chosen-plaintext attacks were performed on the method in order to measure the robustness of the hybrid method to plaintext attacks. The plaintext and the cipher-text are assumed to be captured when performing the known-plaintext and

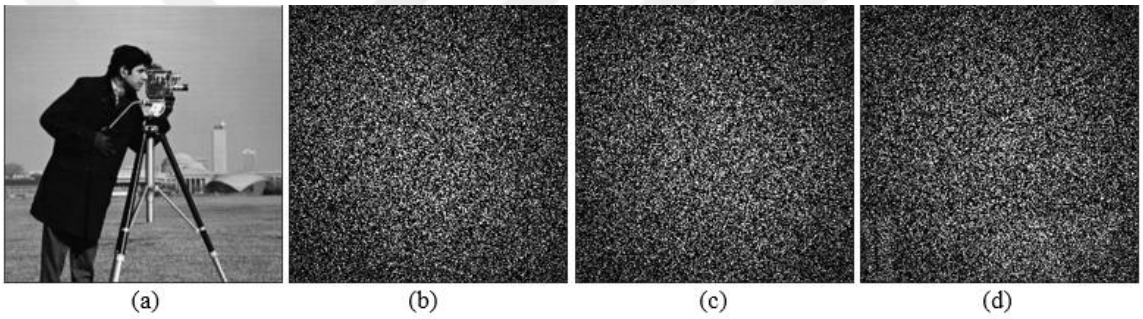


Figure 4.12 (a) Image of the message (Cameraman), (b) decrypted image when RPM2 is correct but RPM1 is incorrect, (c) decrypted image when RPM1 is correct but RPM2 is incorrect and (d) decrypted image when RPM2 is correct but some part of RPM1 is correct

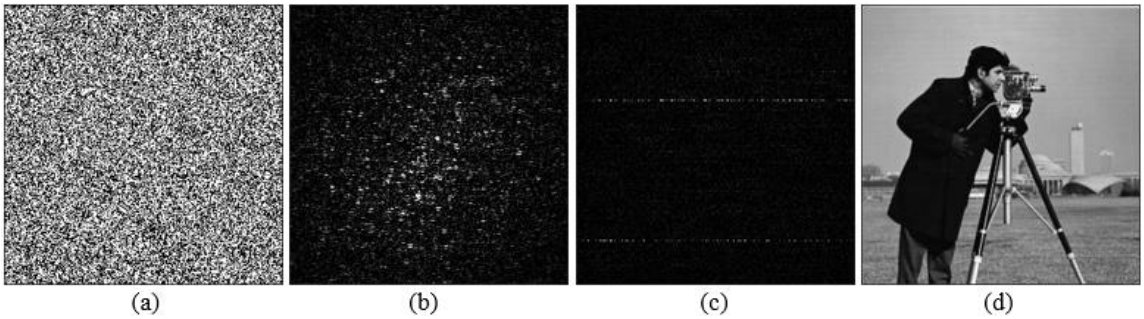


Figure 4.13 (a) Decrypted image when RPM1 and RPM2 is correct but noisy carrier is incorrect, (b) decrypted image when the all keys are correct but only 10×10 size block is incorrect in the noisy carrier, (c) decrypted image obtained from the case where “*ax*” and “*ay*” are reduced by 1 when all keys are correct, (d) decrypted image obtained from the case where all keys are correct

chosen-plaintext attacks without the hiding step. A copy of the plaintext has been redesigned so that Dirac Delta function (Δ) can be obtained when the redesigned plaintext is subtracted from its original. Subtracting the plaintext from the edited copy (P2) of itself (P1) can be found as:

$$P1(a,b) - P2(a,b) = \Delta. \quad \textbf{(4.9)}$$

While the cipher text $C1(a,b)$ corresponding to known plaintexts for the encryption methods having a linear structure can be calculated as follows:

$$C1(a,b) = \delta \cdot P1(a,b), \quad \textbf{(4.10)}$$

$C2(a,b)$ can be calculated as follows:

$$C2(a,b) = \delta \cdot P2(a,b), \quad \textbf{(4.11)}$$

In Equations, while $C1(a,b)$ and $C2(a,b)$ represent cipher texts, δ represent the encryption function. If the system is linear, the difference between the cipher texts $C1(a,b)$ and $C2(a,b)$ should give us the diagonal matrix (phase mask) in which used for phase retrieval algorithm. In this case, the phase mask $C1(a,b) - C2(a,b)$ in a linear encryption system can be found as follow:

$$C1(a,b) - C2(a,b) = \delta \cdot \left(P1(a,b) - P2(a,b)\right), \quad \textbf{(4.12)}$$

$$C1(a,b) - C2(a,b) = \delta \cdot \Delta, \quad \textbf{(4.13)}$$

In Figure 4.11 (a) - (d), it is given plain texts (P1 and P2) and corresponding cipher texts (C1 and C2), respectively. The subtraction Figure 4.14 (c) from (d) in a linear system according to Equation (4.1) should give us the phase key. The incorrect mask obtained and its correct version is shown in Figure 4.14 (e) and (f) respectively. It can be seen from the figure that the mask obtained is different from the actual mask, and the

encrypted data cannot be reached with the use of this mask in the decryption step. In addition, in a linear system like equation (4.1), the encrypted delta function and subtraction C2 from C1 should be similar. However, in Figure 4.14 (h), the encoded delta function is seen and it is understood that both the image and the correlation coefficient are very small (C = -0.0012), which is quite different from Figure 4.14 (e).

Since the developed method has a nonlinear structure, the cipher-text only attack proposed in accordance with DRPE in linear form is not effective on our method. For the implementation of another cipher-text only attack proposed for non-linear Phase Truncated Fourier Transform (PTFT) based optical encryption, one or both of the phase masks used during encryption must be known [15]. If one of the phase masks is wrong for the hybrid method, it can be seen that the plaintext cannot be obtained in Figure 4.12. If both phase masks are known by the attacker, the plaintext is reached by using phase

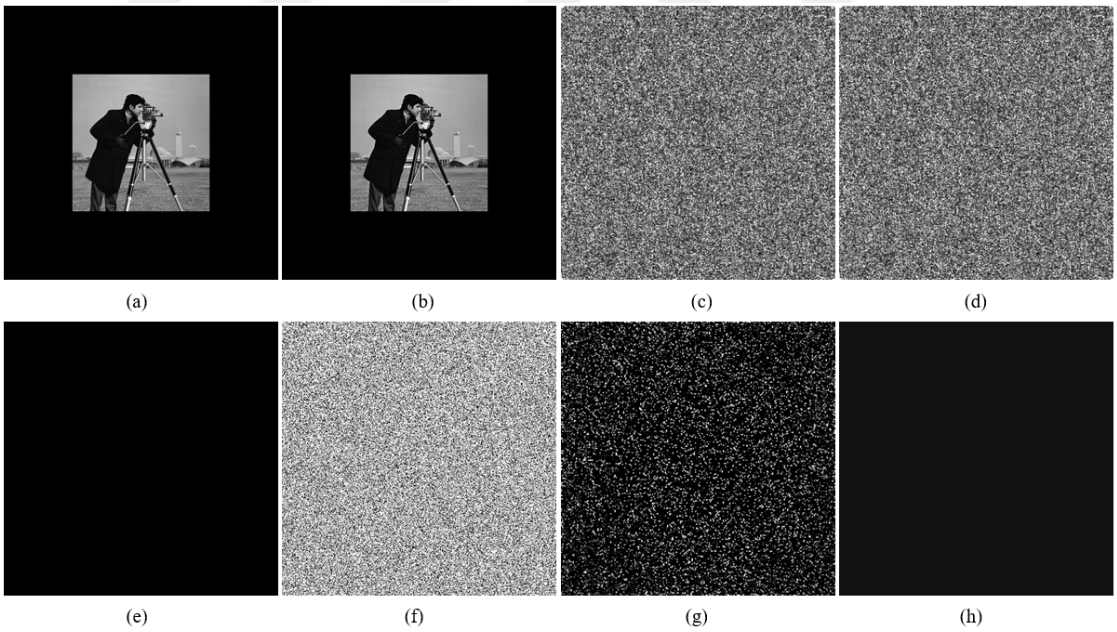


Figure 4.14 Robustness of the developed method against plaintext attacks. (a) Plain text P1. (b) Plain text P2. (c) Cipher text C1. (d) Cipher text C2. (e) Difference between cipher texts C1 and C2. (f) The actual random phase mask used for encryption. (g) Decrypted image with mask obtained from the difference of C1 and C2: CC= -0.0010. (h) Encrypted Dirac Delta function using the proposed method

retrieval algorithm. For a 256×256 matrix sized image, the total number of probabilities to be tried to obtain correct masks used for diffractive coding step is $256^{2\times512\times512}$.

With the additional key space provided by data hiding step, the robustness of the method to cipher-text only attacks is significantly increased. Figure 4.13 (b) shows that the correct Fourier amplitude cannot be obtained from the carrier even if a block size of only 10×10 matrix from the 16-bit carrier used for data hiding is incorrect. The number of possible combinations required to obtain correct noisy carrier with a tolerance of a pixel block of 10×10 size is $65536^{4598\times3860}$. Similarly, the correct amplitude matrix must be available for the application of the phase retrieval attack against the diffractive imaging-based optical encryption to the hybrid method. For this reason, it is almost impossible to find correct carrier matrix by using brute force attack.

CHAPTER 5

HYBRID MULTIPLE-IMAGE ENCRYPTION BASED ON COMPRESSIVE SENSING AND PHASE RETRIEVAL TECHNIQUE

The symbols used in this chapter are specific to this chapter, not general expressions. In the proposed many algorithms for multiple-image encryption systems such as wavelength multiplexing [19], position multiplexing [20] and interference-based position multiplexing [21], there are noise problems caused by “cross-talk” due to the simple addition of the images. In addition, the limited capacity of the images to be encrypted at the same time is one of the common problems. Iterative phase retrieval based algorithms have been proposed to minimize cross-talk effect and obtain less noisy images in the decryption [22, 23, 56]. Cascaded phase retrieval and 4-f-based optical image encryption systems [24, 73] have been proposed to eliminate the problem of the number of images to be encrypted at the same time. However, these systems have a structure that cannot decrypt the image before decrypting the previous image because of their hierarchical order. This makes users dependent on each other at the authorization stage.

Sampling is often used in the field of signal and image processing, and when transferring the signal or image to digital media, it is called processing, taking a certain number of samples instead of taking the entire data [39]. Nyquist sampling criterion is taken into account to avoid aliasing on the signal or image to be reconstructed when sampling is normally performed [39]. According to the Nyquist sampling criterion, the sampling frequency of the signal must be at least twice the frequency of the signal. However, there have been recent studies on Compressive Sensing (CS) technique in which the original signal is able to reconstruct at the excellent level from the signal that is sampled with a

much lower rate than the Nyquist sampling criteria [39, 74, 75]. Because the CS method can sample images at low rate, there is free space for extra image encryption [76].

Providing independent and noiseless access to the transmitted images does not make sense if there is no strong encryption algorithm against attacks. Therefore, in this study, a hybrid multiple-image encryption algorithm for satisfying all of the aforementioned criteria has been developed by using a CS method, phase retrieval based modified diffractive imaging method, space multiplexing and a method of reducing the matrix size of the image to be sent. The important advantages of the hybrid method are determined by experimental studies and security tests.

5.1 Techniques Used For Hybrid Method

In this study, the hybrid method consists of four main techniques. The first technique is the CS method in which images are sampled at low rate. The second technique is the phase retrieval algorithm used in the last step for decrypting each sampled image which is modulated with a separate phase mask using the diffractive imaging method. The third technique is an algorithm known as space multiplexing for laying a series of images into a plane in blocks. The fourth and final technique is the algorithm that separates the plane containing the encoded images firstly into two different parts and then creates a complex new matrix plane with a lower matrix size by synthesizing these parts as phase and amplitude.

5.1.1 Compressive Sensing

According to the Nyquist sampling criterion, more samples are taken than the number of samples in which the detail information of the signal is carried when a signal is sampled. However, when these signals are transmitted or stored in memory, only large values of different spaces (such as Wavelet space, Fourier transform and Cosine transformation) are recorded [39]. Compressive sensing (CS) method uses two principles as sparsity and incoherence in sampling [39]. Sparsity takes advantage of the fact that a signal can be separated in the input space or in different transformation spaces such as Wavelet,

Fourier and Cosine. According to the sparsity principle, the information contained in the continuous or discrete time signals may in fact be smaller than their respective bandwidths or lengths. According to the Incoherence principle, the information in the signal is recorded by, Ω which is a signal-independent sensing operator. In the CS method, as the inconsistency between Ω and the sparsity operator increases, the signal can be better reconstructed by sampling at lower rates. Sampled signal using CS method can be found as z:

$$z = \Omega \bullet FT(x). \qquad \textbf{(5.1)}$$

In the Equation, Ω represents sensing operator, $FT(\ )$ represents Fourier transform, x represents the image with "*n*" pixels and z represents the sampled image with "*m*" pixels. Note that the sampled image has much less pixels than the original $(m << n)$. In the equation (5.1), since the image x is discrete in the frequency domain, the Fourier transform is used as the sparsifying operator. Since equation (5.1) is an ill-condition problem, the CS method can reconstruct x iteratively from the sampled image z by minimizing $\|\hat{x}\|_{\ell 1}$, $\|z - \Omega \bullet FT \bullet \hat{x}\|_{\ell 2} < \delta$,where δ represents the error rate tolerated to compensate for the noise ratio in the signal, while $\|\ \|_{\ell 1}$ and $\|\ \|_{\ell 2}$ represent the norms $\ell 1$ and $\ell 2$, respectively. In general, the expression of a norm in which p represents the norm is defined as $\ell_p : \|x\|_p = \sqrt[p]{\sum_i |x_i|^p}$.

The sensing operator Ω is very important in order to reconstruct almost the original of the sampled signal. The sensing operator Ω consists of signal-independent values when applied in the signal acquisition stage, while the signal is composed of signal-dependent or signal independent values when applied in a state where the signal is present. In this study, the Ω operator is generated as in Wang's study [76]. The image with an "*M*" number of pixels is reordered depending on the values in the frequency domain. The largest "*N*" number of samples is taken from the rearranged matrix $(N < M)$, and Ω is

an index that represents the coordinates of these selected "*N*" pixels in the matrix. Because each image has unique values in the frequency domain, the Ω operator varies depending on the image to be encrypted. Thus, the Ω operator provides an additional key space robust to attacks for the hybrid method. The sampling ratio R can be written as follows:

$$R = (m / n) \times 100. \quad \textbf{(5.2)}$$

If the sampling ratio becomes larger, the quality of the reconstructed images and the correlation value increases. Similarly, if the sampling ratio becomes smaller, the quality of the reconstructed images decreases, but the number of images to be encrypted at the same time increases. For this reason, a sampling ratio of optimum value should be selected by considering the correlation value and the number of images to be encrypted.

5.1.2 Diffractive Imaging and Phase Retrieval Algorithm

Since this study was prepared based on the method of optical image encryption in section 4, the hybrid method developed here uses the same framework as the method in Chapter 4, namely the Fourier transform based diffractive imaging structure [77, 78]. However, in this study, Hybrid Input Output / Error Reduction (HIO / ER) phase retrieval algorithm, which is given in Chapter 3, is used to reconstruct the image modulated by diffractive imaging [69]. HIO / ER has two major advantages according to the ER algorithm. First, because the oversampling method is required for the ER algorithm, the matrix size of the image is increasing, but the matrix size of the image does not change as no oversampling method is required for HIO / ER. This allows the efficient use of bandwidth in the hybrid method that has been developed and the ability to encrypt more images at the same time. The second advantage of HIO / ER is that it achieves a phase of an image more accurately and noiseless than ER as seen in Chapter 3. Thus, the resistance of the hybrid method is increased against the noise in the transmission line. The diffractive imaging method used for the developed hybrid method is given in Figure 4.1. The Fourier amplitude G of the image obtained by modulating

the image $z(a,b)$ sampled by the CS technique with two random phase masks $(RPM1, RPM2)$ according to the design given in Figure 4.1 can be calculated as follows:

$$G = \left|\mathrm{FT}\left\{\lambda z(a,b)\right\}\right|, \quad \lambda = RPM1 \times RPM2 \tag{5.3}$$

In the equation, FT and λ represent the Fourier transform and the diagonal matrix formed by the multiplication of phase masks, respectively.

5.1.3 Space Multiplexing and Pixel Scrambling

Space multiplexing is a simple way to synthesize images on a single plane [76]. First, in this stage, a 724×724 zero matrix is generated as a plane in which images are synthesized. The single plane S, where the images are placed in certain regions so that they do not overlap, can be calculated as follows:

$$S = B(a,b) + A_i(a,b) \tag{5.4}$$

From the variables in the equation, $B(a,b)$ and $A(a,b)$ represent the zero matrix and the Fourier amplitude of each encrypted image, respectively, while the sub-index i represents the number of images. From the other variables in the equation, (a,b) represents the number of rows and columns of the images to be added, and thus it represents the number of rows and columns which the images will occupy in the zero matrix. In the space multiplex based multiple-image encryption methods, the images are placed on the plane so that they do not overlap with each other to avoid crosstalk effect. In this study, space multiplexing method is used to eliminate both cross-talk effect and to authorize different users to access different images. Images are subjected to simple pixel scrambling after they have been synthesized in a single plane, in order to prevent unaware of their location on the plane and to avoid regional losses against possible occlusion attacks. Scrambling order required to solve the mixing process and including

the location of images on the plane are sent to authorized persons. If the c number of images need to be encrypted with a fixed sampling ratio R, the relationship between the number of images to be sent and the sampling ratio can be defined as follows:

$$c \times \mathrm{R} \leq 800, \tag{5.5}$$

where c represents the total number of images to be encrypted. If c number of images with m pixels need to be synthesized on a plane with n pixels, total pixels of c number of images should be less than n. ($c \bullet m \leq n$)

5.1.4 Rebuilding the Image as Amplitude and Phase

In order to reduce the matrix size of the plane to which the images are combined with the space multiplexing, a method has been developed that removes certain parts from the image itself and records it as the phase of that image. As seen from Figure 5.1, the matrix of 724×724 size is divided into four regions. The number one region is the matrix with size of 512×512, which represents the amplitude of new matrix, and the phase in the remaining regions. One of the points to be considered when creating the phase information is that the number two region in size 512×212 is placed in the new matrix by taking transposing. Another point to be considered is that the number four region in matrix size 212×212 is divided into 88×510 and 32×2 matrix sized pieces, respectively, when it is inserted into the 88×512 matrix size region of the new matrix. After obtaining the phase information, the new matrix is a 512×212 pixel size complex matrix with both amplitude and phase information. This results in both a smaller pixel size and a more complex image.

5.1.5 Encryption and Decryption Process

The process to be applied for each image to be encrypted is given in Figure 5.2 (a). In this process, the image $\left(x_{m,n}\right)$ to be encrypted is sampled with the CS method given in

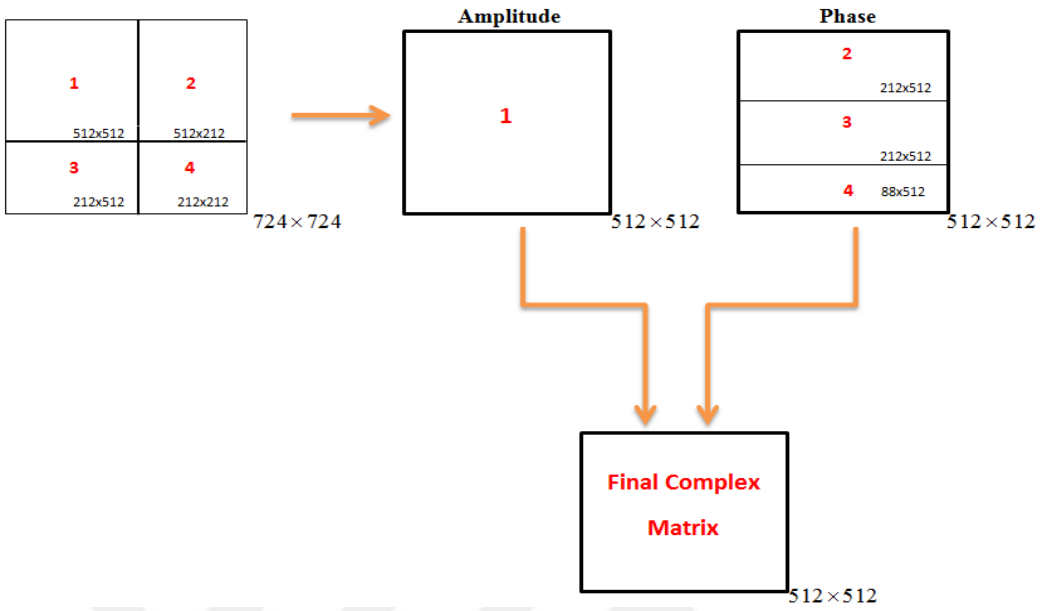


Figure 5.1 Redesign the image as amplitude and phase information

equation (5.1) and the image $(z_{a,b})$ with smaller pixel size is obtained. Note that the point is $(a \times b) < (m \times n)$. The Fourier amplitude of the matrix obtained after modulating the sample with λ according to the equation (5.2) is defined as G. $RPM1$ is a mask that is fixed at the receiver and transmitter side, whereas $RPM2$ is a mask which changes at each encryption and has different values for different receivers. In this way, each user can only access the information they are allowed. The reason for using two masks is to increase the robustness of the masks against known-plaintext attacks. Since the diagonal matrix is used in the equation (5.2) during the encryption, the projection operator in the HIO / ER algorithm to be used for decryption is required to use the diagonal matrix. According to this, the projection operator ρ_f in the third step of the Algorithm-1 given in Chapter 3 is changed as follows:

$$\rho_f = \frac{FT^{-1}(y'_s)}{\lambda} \qquad \textbf{(5.6)}$$

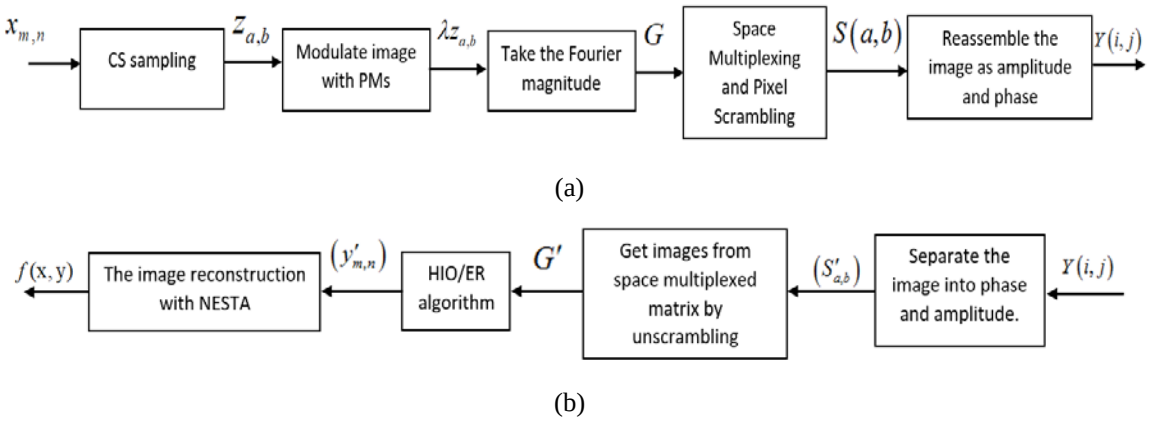


Figure 5.2 (a) Encryption, (b) Decryption processes

Each amplitude matrix obtained in Equation (5.2) is placed on a single plane with the space multiplexing method given in equation (5.3) and the pixels of the images are scrambled. The plane matrix obtained by synthesizing the images and scrambling all the pixels is $S(a,b)$ as shown in Figure 5.2 (a). By applying the method developed for reducing the matrix size to the $S(a,b)$ plane, both the size of the matrix is reduced and the complexity of the matrix is increased. Thus, the encrypted image matrix to be sent at the end is $Y(i,j)$ as shown in Figure 5.2 (a). The decryption process of the encrypted images is shown in Figure 5.2 (b). During decryption, the phase information of $Y(i,j)$, which contains all the images, is extracted and re-combined with the amplitude of the image with the correct indexes to reach space multiplexed image matrix $S'_{a,b}$, which has mixed pixels. In the second stage of the decryption, after the space multiplexed plane is descrambled with the scrambling order, each author which is authorized with the indices given to it, reaches the Fourier amplitude of the image (G'). The sampled image $y'_{m,n}$ is obtained from Fourier amplitudes of images by using the HIO / ER algorithm with defined random phase masks for each authority. In the last step of decryption process, the original $f(x,y)$ of each image can be reconstructed from $y'_{m,n}$ by minimizing $\left\|\hat{f}_{x,y}\right\|_{\ell 1}$ *subject to* $\left\|y'_{m,n} - \Omega \bullet FT \bullet \hat{f}_{x,y}\right\|_{\ell 2} < \delta$. Since this is a $\ell 1$ minimizing problem, in

this study, it is preferred to solve this problem by using NESTA algorithm [79]. NESTA uses Nesterov's minimizing nonsmooth convex functions to solve such problems [79]. Nesterov has developed an algorithm that minimizes any smooth convex function. The algorithm has solved $\ell 1$ minimizing problems by calculating the gradient of smooth convex function over three consecutive sequences (y_k, z_k, x_k). The algorithm of NESTEROV is given by Algorithm-2.

Algorithm-2 (NESTEROV)

Inputs: x_k, k

x_k - Sampled image with CS method.

k - Number of iterations.

Output: x_k - The latest updated matrix at the end of all steps.

Start. First iteration starts with x_0.

General Steps (k =0, 1, 2, …) **:**

1) $\nabla f\left(x_k\right)$
2) $y_k = \arg\ \min_{x\in Q_p} \frac{L}{2}\left\|x - x_k\right\|_{\ell 2}^2 + \left\langle \nabla f\left(x_k\right), x - x_k \right\rangle,$
3) $z_k = \arg\ \min_{x\in Q_p} \frac{L}{\sigma_p} p_p\left(x\right) + \sum_{i=0}^{k} \alpha_i \left\langle \nabla f\left(x_k\right), x - x_k \right\rangle,$
4) $x_k = \tau_k z_k + \left(1+\tau_k\right) y_k,$
5) Return step 1.

Up to: *Total number of iterations* $= k$

In the Algorithm-2, L represents the Lipschitz constant, Q_p represents feasible set, $\alpha_k = 1/2\left(k+1\right)$ and $\tau_k = 2/\left(k+3\right)$. In the third step, the prox-function $p_p\left(x\right)$ used for the feasible set is strongly convex when used with the parameter σ_p. This increases the convergence rate of the algorithm. According to the NESTEROV algorithm, firstly, after calculating the gradient of x_k, y_k and z_k are calculated respectively. Then, x_k continues

to be updated until the number of steps is completed. The first optimal solution during the iterations is y_k and the following z_k which keeps the memory of previous iterations, is calculated by the weighted sum of all previously calculated gradient values. Thus, with the calculation of the z_k, a much better solution than y_k has been introduced to minimizes any smooth convex function.

5.2 Experimental Studies

The hybrid method synthesizes 31 images with 256×256 pixel size in a single carrier with a sampling rate of %25. However, for ease of expression, 6 images selected from 31 images are shown in Figure 5.3(a1)-5.3 (a6). The images sampled by the CS method to the size of 128×128 pixels are shown in Figure 5.3(b1)-5.3(b6). Fourier amplitudes calculated after modulating each sampled image with random phase masks are given in Figure 5.3(c1)-5.3(c6). The matrix obtained by scrambling the Fourier amplitudes in a single plane having a matrix size of 724×724 is given in Figure 5.3 (d). The created plane is reduced to 512×512 matrix size by the hybrid method. Thus, both a complex and a reduced pixel-size image are obtained as seen in Figure 5.3 (e). The encrypted images are decrypted as in Figure 5.3(f1)-5.3(f6) following the process in Figure 5.2 (b). In the last stage of the decryption process, NESTA does not recover the originals of the sampled images but obtains very good quality. All of the correlation values between the original images and the reconstructed images are greater than 0.9930. The effectiveness of the hybrid method can be understood by the fact that the images obtained with a 25% lower sampling ratio have a very good correlation coefficient.

5.3 Security Tests

In order to measure the reliability of the hybrid method, it has been subjected to different security tests. Correlation coefficient (CC) and peak signal to noise ratio (PSNR) parameters are used for the test results.

5.3.1 Occlusion Attacks

In order to measure the resistance of the hybrid method to occlusion attacks, some regions of the single plane is removed in Figure 5.3 (e). Occlusion attacks applied to different regions with different ratios are given in Figure 5.4(a)-5.4(d) and corresponding decrypted images are given in Figure 5.4(e)-5.4(g). Figure 5.4 shows that noises occur in decrypted images but the details of the images are still presented. Since the occlusion attack on different parts of the encrypted image has no effect on the decoded images, it is understood that the effect of occlusion is independent of the regions. However, as the occlusion rate increases, the quality of the decoded images decreases.

5.3.2 Noise Attacks

In order to test the robustness of the hybrid method against noise attacks, Gaussian noise is added to the encrypted image in different variance values. It is understood from the decrypted images given in Figure 5.5 that the method is highly robustness to noise. However, as the variance value of the added noise increases, the obtained image quality and correlation coefficient decrease.

5.3.3 Robustness of Algorithm to Wrong Phase Retrieval Keys

The random two phase masks used during encryption with the hybrid method is required for the phase retrieval algorithm in the decryption process. If these two masks are not used in the phase retrieval algorithm or different randomly generated masks are used, decrypted images are not correct. The decrypted images are given in Figure 5.6 (a1) - 5.6 (a6) when the first phase masks are incorrect, while the decrypted images are given in Figure 5.6 (b1) - 5.6 (b6) when the second phase masks are incorrect. Figure 5.6 shows that both phase masks must be correct for decrypting the correct images.

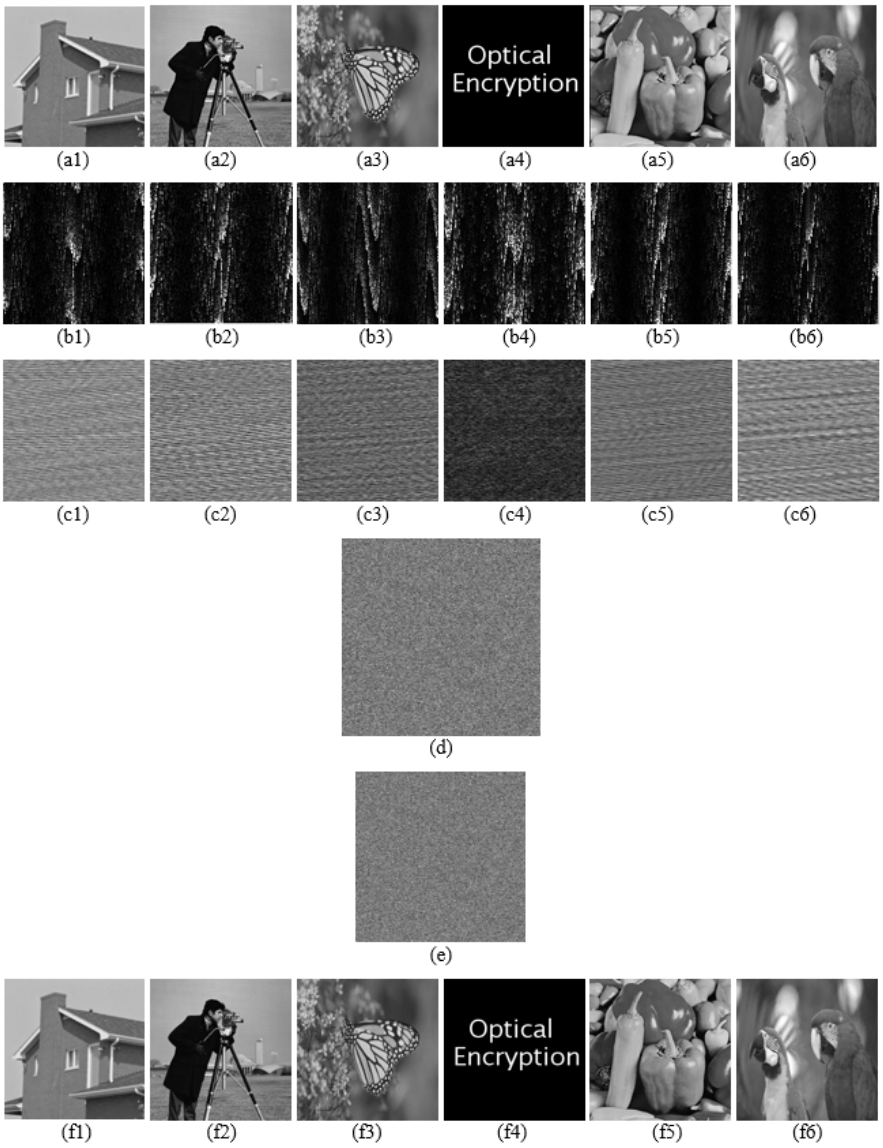


Figure 5.3 The experimental results using the hybrid method. (a1)-(a6) Images to be encrypted (256×256). (b1)-(b6) The sampled images with compressive sensing method (128×128). (c1)-(c6) Fourier amplitudes of images modulated with different phase masks (128×128). (d) Single synthesized image after pixel scrambling and space multiplexing (724×724). (e) Encrypted image with reduced size by redesigning as a phase of a part of the single plane (512×512). (f1)-(f6) Decrypted images (256×256) with (f1) CC= 0.9963; (f2) CC= 0.9979; (f3) CC= 0.9938; (f4) CC= 0.9992; (f5) CC= 0.9960; and (f6) CC= 0.9981

5.3.4 Robustness of Algorithm to Wrong Scrambling Order

In the hybrid method, the scrambling order matrix must be on the receiver side to descramble pixels after the space multiplexing process. If the receiver tries to descramble using an incorrect scramble order matrix, the images reconstructed by using CS will be incorrect in the last stage, since the pixels of different images will be confused with each other. The images obtained in the decryption section using the wrong scrambling order are shown in Figure 5.7 (a) - 5.7 (e). As a result, the scrambling order provides an additional key space.

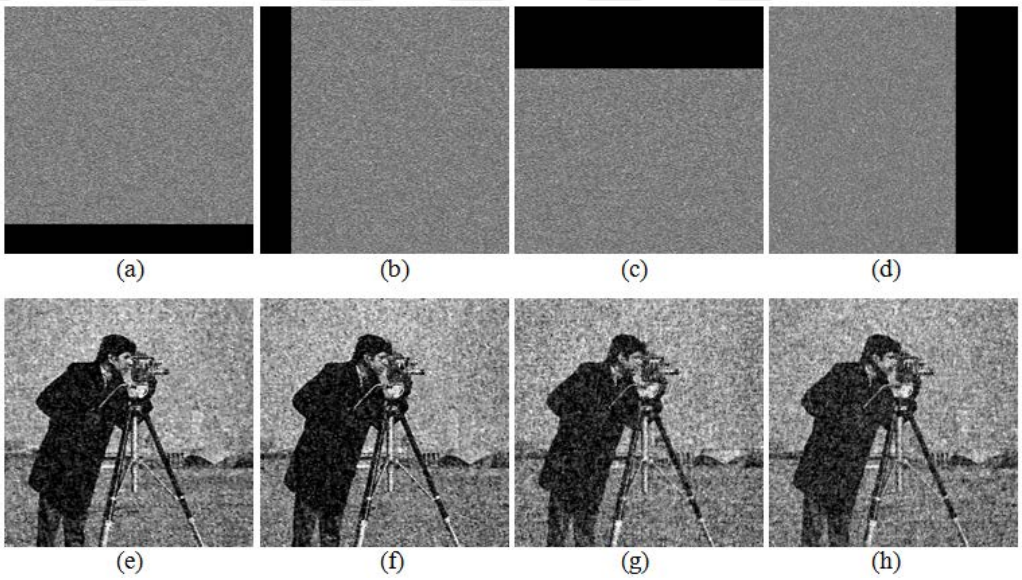


Figure 5.4 Measurement of resistance to occlusion attacks. (a) 1/8 image occluded (lower rectangular region). (b) 1/8 image occluded (left rectangular region). (c) 1/4 image occluded (upper rectangular region). (d) 1/4 image occluded (right rectangular region). (e) Decrypted image from (a) CC= 0.8857, PSNR=18.1963. (f) Decrypted image from (b) CC= 0.8299, PSNR=17.7489. (g) Decrypted image from (c) CC= 0.7608, PSNR=16.5579. (h) Decrypted image from (d) CC= 0.7620, PSNR=16.8155

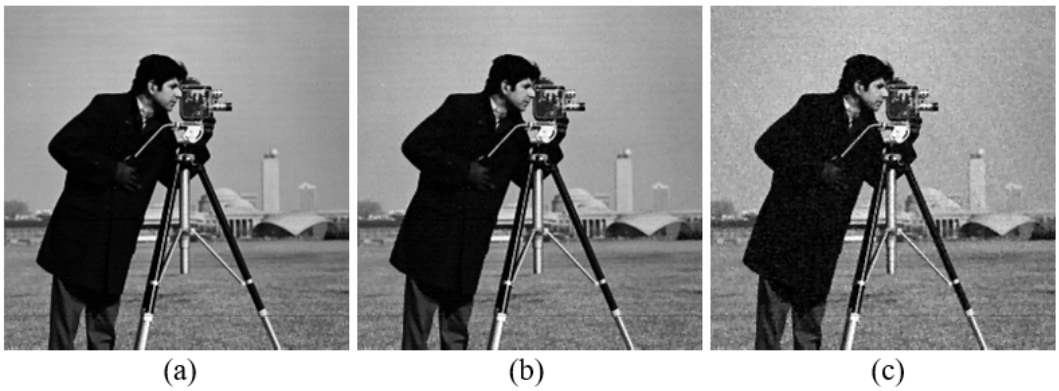


Figure 5.5 Measurement of resistance to noise attacks. (a) Decrypted image with Gaussian noise of 0.1 variance, CC= 0.9979, PSNR= 33.8685. (b) Decrypted image with Gaussian noise of 1 variance, CC= 0.9972, PSNR= 33.3373. (c) Decrypted image with Gaussian noise of 5 variance, CC= 0.9892, PSNR= 27.6478

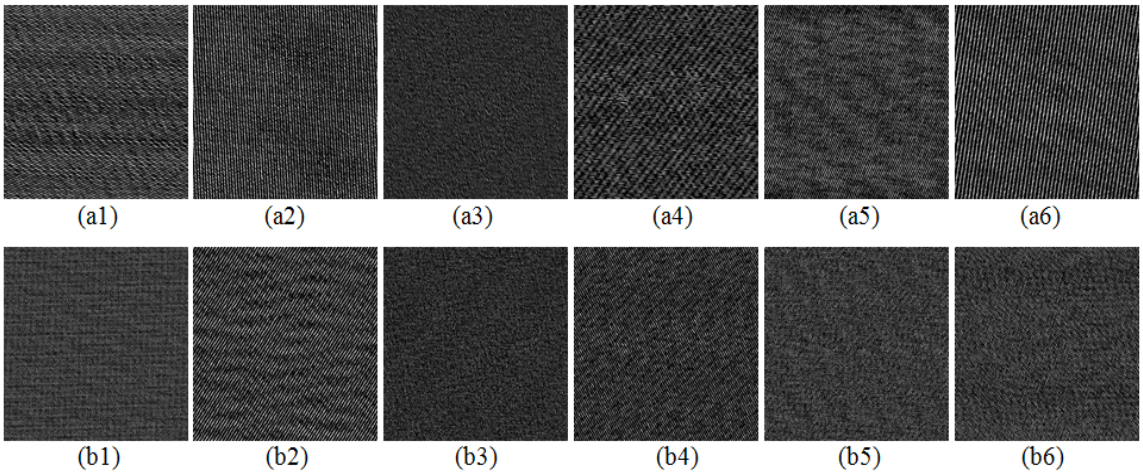


Figure 5.6 Measuring the resistance of the hybrid method to the use of wrong phase masks. (a1)-(a6) Decrypted images with wrong first phase mask: (a1) CC= -0.0177; (a2) CC= 0.0026; (a3) CC= 0.0722; (a4) CC= 0.0918; (a5) CC= -0.0149; and (a6) CC= 0.0210. (b1)-(b6) Decrypted images with wrong second phase mask: (b1) CC= 0.0252; (b2) CC= -0.0138; (b3) CC= 0.0641; (b4) CC= 0.0223; (b5) CC= -0.0297; and (b6) CC= -0.0241

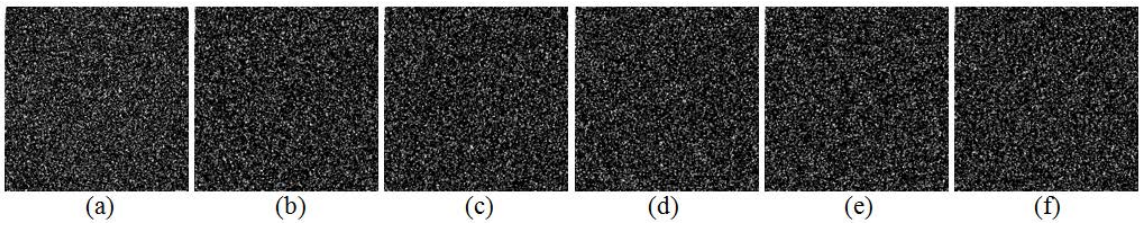


Figure 5.7 Decrypted images with wrong scrambling order. (a) CC= -0.0167; (b) CC= -0.0075; (c) CC= 0.0039; (d) CC= -0.0401; (e) CC= 0.0185; and (f) CC= 0.0159

5.3.5 Robustness of Algorithm to Wrong Sampling Operator

The CS method used in the initial step of the encryption process requires both the sampling operator and the sampled data to reconstruct the original images from the sampled images. Figure 5.8 (a) - 5.8 (g) show that images cannot be obtained by using a wrong sampling operator.

5.3.6 Effect of Sampling Ratio

The sampling rate R determines the total number of images to be sent at the same time. A total of 31 images are encrypted in the experimental studies with a sampling rate of 25%. For ease of expression, 6 images selected from these images are encrypted here with sampling ratios of less than 25% as shown in Figure 5.9 (a1)-(c6). As a result, although the sampling ratio is decreased, the detail information is preserved, but the decrease in the sampling ratio decreases the PSNR and CC values. For images with a sampling ratio of greater than 16.18%, the CC value is greater than 99% and a total of 49 images are encrypted. When the sampling ratio is 9, 76%, a total of 81 images can be encrypted with 97% CC values and a total of 121 images can be encrypted in 95-97% CC values with the sampling ratio 6, 44%.

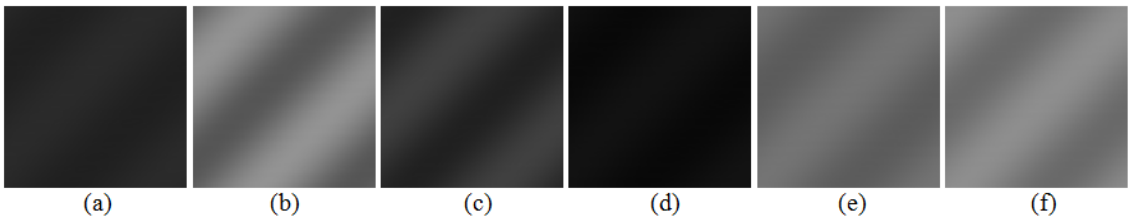


Figure 5.8 Measuring the robustness of the hybrid method to the wrong sampling operators. (a)-(f) Decrypted images with wrong sampling operators: (a) CC= 0.0885; (b) CC= 0.2550; (c) CC= 0.0856; (d) CC= 0.1881; (e) CC= 0.2101; and (f) CC= 0.0520

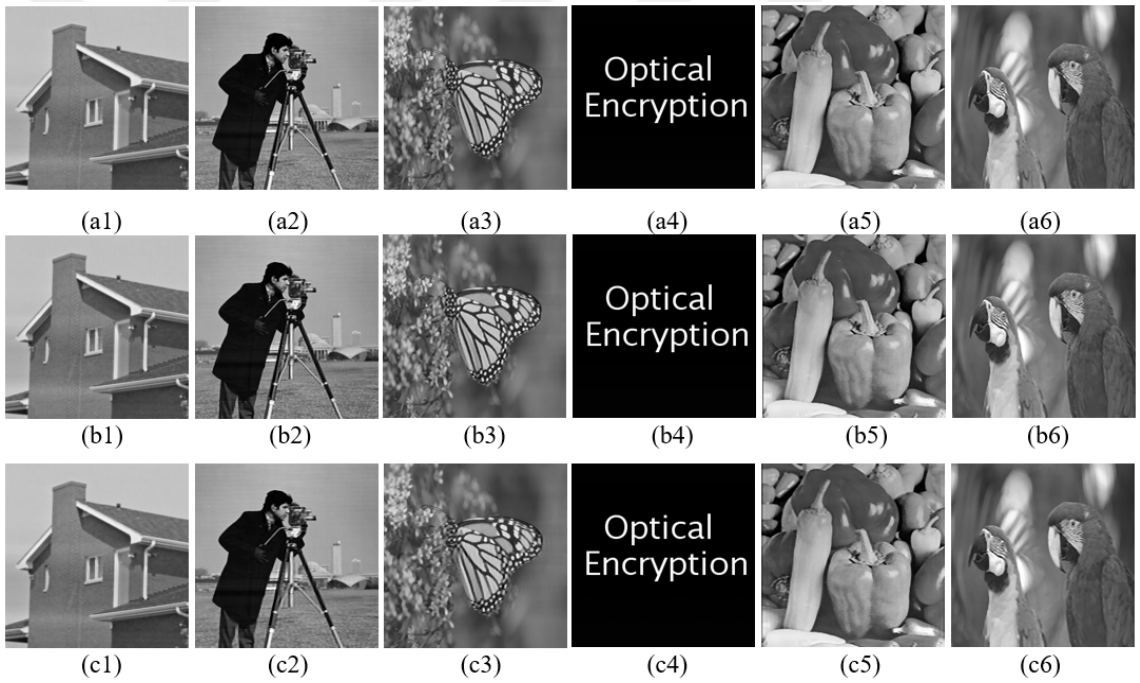


Figure 5.9 The effect of the sampling ratios on the decrypted images. (a1)-(a6) Decrypted images for sampling ratio %16,18 (b1)-(b6) Decrypted images for sampling ratio %9,76: (c1)-(c6) Decrypted images for sampling ratio %6,44

5.3.7 Robustness of Algorithm to Plaintext Attacks

In order to prove that the hybrid method has a nonlinear structure and to measure its resistance to attacks, the same method as the chosen-plaintext attack in Chapter 4 is

Table 5.1 Correlation (CC) and PSNR analysis results according to the sampling ratios of the images given in Figure 5.9

Images / **Sampling Ratios**	***%16,18***	***%9,76***	***%6,44***
First image	**CC**= 0.9971, **PSNR**=28.41 dB	**CC**= 0.9894, **PSNR**=28.55 dB	**CC**= 0.9766, **PSNR**=27.52 dB
Second image	**CC**= 0.9932, **PSNR**=29 dB	**CC**= 0.9877, **PSNR**=29 dB	**CC**= 0.9792, **PSNR**=26.18 dB
Third image	**CC**= 0.9902, **PSNR**=28.46 dB	**CC**= 0.9723, **PSNR**=28.02 dB	**CC**=0.9667, **PSNR**=22.18 dB
Fourth image	**CC**= 0.9996, **PSNR**=35.28 dB	**CC**= 0.9990, **PSNR**=32.15 dB	**CC**= 0.9962, **PSNR**=31.47 dB
Fifth image	**CC**= 0.9923, **PSNR**=25.36 dB	**CC**= 0.9706, **PSNR**=24 dB	**CC**= 0.9609, **PSNR**=20.06 dB
Sixth image	**CC**= 0.9935, **PSNR**=31.02 dB	**CC**= 0.9838, **PSNR**=29.49 dB	**CC**= 0.9701, **PSNR**=21.36 dB

applied on the method. Firstly, Dirac Delta function is determined by taking the difference $P1(a,b)-P2(a,b)$ of two plaintexts (P1 and P2) as in equation (4.14). Cipher texts $C1(a,b)$ and $C2(a,b)$ corresponding to known plaintexts for the encryption methods having a linear structure can be calculated as in equations (4.10) and (4.11), respectively. It is necessary to pay attention to the fact that the difference between the cipher texts $C1(a,b)$ and $C2(a,b)$ should give us the diagonal matrix (phase mask) in which used for phase retrieval algorithm. . In this case, the phase mask $C1(a,b)-C2(a,b)$ in a linear encryption system can be found as in equations (4.12) and (4.13). For ease of expression, the space multiplexing stage and the stage redesigned the portions of the image as its amplitude and its phase are removed and the attack is carried out with a single image. It is assumed that both message image and encrypted images were captured when attack is applied. Figure 5.10 (a) - (d) shows plain texts (P1

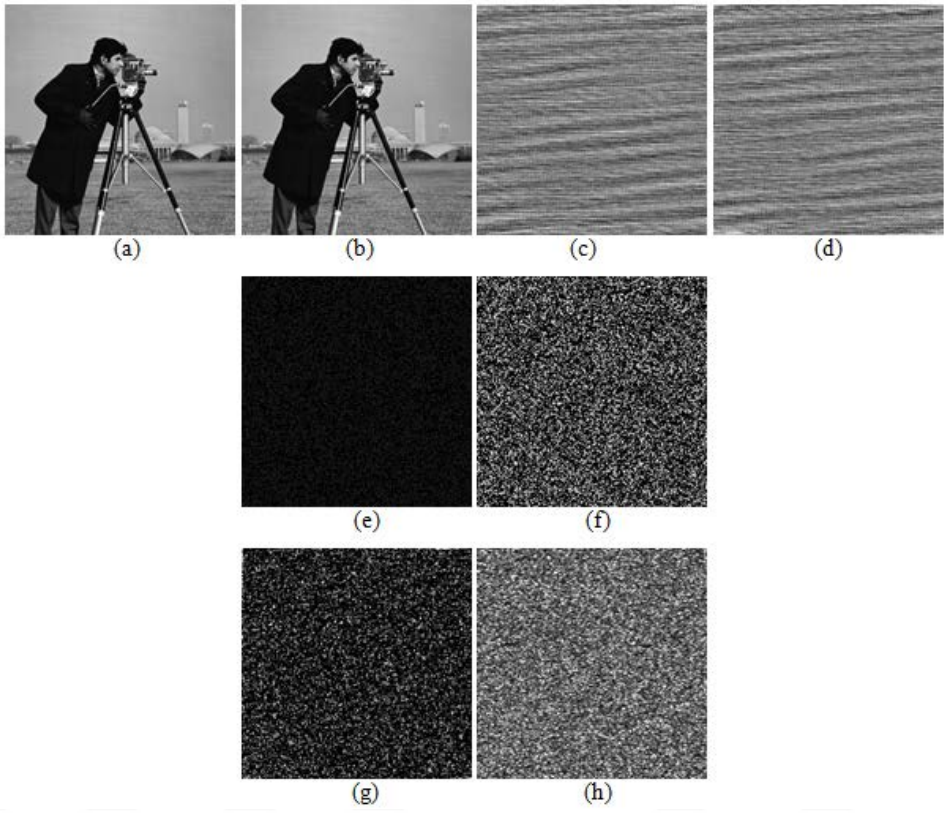


Figure 5.10 Measuring the resistance of the hybrid method to plaintext attacks. (a) Plain text P1. (b) Plain text P2. (c) Cipher text C1. (d) Cipher text C2. (e) The difference between C1 and C2. (f) The actual diagonal matrix used for encryption. (g) Decrypted image with mask derived from the difference of C1 and C2: CC= -0.0040. (h) The encrypted Dirac Delta function with the hybrid method

and P2) and corresponding cipher texts (C1 and C2) respectively. The difference between Figure 5.10 (c) and (d) in a linear system according to Equation (4.13) should reveal the diagonal matrix. The incorrect mask obtained and its accurate version is shown in Figure 5.10 (e) and (f) respectively. It can be seen from the Figure 5.10 (g) that the mask obtained is different from the accurate mask and the encrypted image cannot be decrypted with the use of this mask. Again, in a linear system like equation (4.13), the difference of the encrypted delta function and cipher text should be similar. However, it is understood that the encrypted delta function given in Figure 5.10 (h) is quite different from Figure 5.10 (e) and the correlation coefficient is very small (CC = -0.0089). In addition, the sensing operator to be used for sampling is not possible to obtain randomly because it changes depending on the image to be encrypted. For

example, when an image of 256×256 matrix size is sampled to a 128×128 matrix size, the total number of probabilities to be tried to obtain the correct sensing operator is $256^{128\times128}$. As a result, it is almost impossible to find the correct sensing operator without the image itself being known. The scrambling operator for the system and the two random phase masks required for diffractive imaging also increase the reliability by providing additional key space. For a 256×256 matrix sized image, the total number of probabilities to be tried to obtain correct phase masks used for diffractive coding step is $256^{2\times256\times256}$. In addition, both compressive sensing and diffractive imaging provide a nonlinear structure in the hybrid method, making the system resistant to attacks such as known-plaintext and chosen-plaintext, in which linear optic encryption systems are weak. With the structure reuniting the phases and amplitudes of the images, the matrix size of the carrier is further reduced.

CHAPTER 6

CONCLUSIONS AND FUTURE WORKS

The aim of this thesis is to develop a new optical image encryption method considering the weaknesses of linear optical encryption systems and to develop a new optical multiple-image encryption method which can use the bandwidth efficiently while eliminating security vulnerabilities due to the rapid increase of data. The results of the studies;

1. A hybrid method has been developed by using modified diffractive imaging and image-hiding algorithms to design a more robust method to attacks in which DRPE based methods (LCT, FrT, FsT, FFT), PTFT-based asymmetric encryption systems and diffractive imaging-based optical image encryption systems are weak. Using modified diffractive imaging method, the image to be encrypted is first encoded by two phase masks, one fixed on both the receiving and transmitting sides, and the other changing at each encryption. Note that both phase masks must be on the receiving side in order to decrypt images. Then the phase information of the modulated images is subtracted and their Fourier amplitudes which are noise-like images are subjected to the hiding step. The image that will be in the carrier is obtained by converting a photograph taken in the dark into a 16-bit depth gray scale and transforming it into a completely noisy image by subjecting it to a contrast enhancement method. The Fourier amplitude which is noise-like image of the modulated image with the phase masks is hidden by a hiding algorithm using "*ax*" and "*ay*" parameters in this carrier. In the developed hybrid method, the carrier noisy image and *ax* - *ay* parameters has increased the reliability of the method by providing additional key space, while the image capacity that can be hidden at the same time according to the matrix size of the carrier has also been increased. For a 256×256 matrix sized image,

the total number of probabilities to be tried to obtain correct masks used for diffractive coding step is $256^{2\times512\times512}$.

2. A new hybrid multiple-image encryption method has been developed in order to eliminate the difficulties experienced by the optical multiple-image encryption methods which are associated with the increasing amount of data. Firstly, images are compressed at very small sampling rates and subjected to diffractive imaging system. The diffractive coding used herein is the same as the method used in the first hybrid method. Fourier amplitudes obtained from compressed and phase masks modulated images are subjected to a simple pixel mixing process and then combined in a single plane. In order to further reduce the matrix size of the plane to be transmitted, an algorithm that separates the image into phase and amplitude information and then reuniting them is used. The CS technique allows increasing the number of images to be encrypted at the same time in the single carrier while the diffractive imaging method increases the reliability of the hybrid method by providing a non-linear structure. The space multiplexing method for combining images in a single plane allows different images to be authorized to different users, and also prevents the cross-talk-related noise from being obstructed by overlapping the images. Pixel scrambling prevents data loss from being regional against possible occlusion attacks. The hybrid method developed allows the simultaneous encryption of the total of 121 gray-tone images in the single carrier with correlation coefficients at acceptable levels. This result also shows that the total of 40 different color images can be encoded at the same time by using the hybrid method. In this hybrid method, for a 256×256 matrix sized image, the total number of probabilities to be tried to obtain correct masks used for diffractive coding step is $256^{2\times256\times256}$. The reason that the number of probability in this method is different from the first method is that oversampling is used in the first method. In addition, each algorithm used is further enhanced by providing additional key space for the system.

In this study, an alternative and more reliable method has been developed for optical image encryption methods. In addition, another hybrid optical multiple-image encryption method has been developed to address the problems of existing multiple-image encryption systems. These studies are still open to improvement. The aspects that can be improved are;

1. When the pixel size of the carrier used for the diffractive imaging and image-hiding algorithm is large, it takes up more space in the bandwidth of the communication line. A new method can be developed by subjecting the carrier to the compression processes used in the concealing stage in order to make it suitable for use in practice.
2. By combining the cloaking process with different optical encryption systems (DRPE, PTFT, Ghost imaging and Photon Counting), reliability can be increased while simultaneously encrypting more than one image.
3. The method of reducing the matrix size of the carrier in the hybrid multiple-image encoding system can be further improved. For example, for this method, which separates and reassembles the image as phase and amplitude, CS technique can be applied again to make more efficient use of bandwidth.

REFERENCES

[1] Zeghid, M., Machhout, M., Khriji, L., Baganne, A., & Tourki, R. A modified AES based algorithm for image encryption. International Journal of Computer Science and Engineering, (1), 1, 70-75. 2007

[2] Yun-Peng, Z., Wei, L., Shui-ping, C., Zheng-jun, Z., Xuan, N., & Wei-di, D. Digital image encryption algorithm based on chaos and improved DES. In Systems, Man and Cybernetics, 474-479. 2009

[3] El-Deen, A., El-Badawy, E., & Gobran, S. Digital image encryption based on RSA algorithm. Journal of Electronics and Communication Engineering, (9), 1, 69-73. 2014

[4] P. Refregier & B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, Optics Letters, (20), 767-769, 1995.

[5] Qin, W., & Peng, X. Asymmetric cryptosystem based on phase-truncated Fourier transforms. Optics Letters, (35), 2, 118-120. 2010

[6] Liu, S., Guo, C., & Sheridan, J. T. A review of optical image encryption techniques. Optics & Laser Technology, (57), 327-342. 2014

[7] Rajput, S. K., & Nishchal, N. K. Image encryption based on interference that uses fractional Fourier domain asymmetric keys. Applied Optics, (51), 10, 1446-1452. 2012

[8] Clemente, P., Durán, V., Tajahuerce, E., & Lancis, J. Optical encryption based on computational ghost imaging. Optics letters, (35), 14, 2391-2393. 2010

[9] Cai, J., Shen, X., Lei, M., Lin, C., & Dou, S. Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition. Optics letters, (40), 4, 475-478. 2015

[10] Chen, W., Chen, X., & Sheppard, C. J. Optical image encryption based on diffractive imaging. Optics letters, (35), 22, 3817-3819. 2010

[11] Carnicer, A., Montes-Usategui, M., Arcos, S., and Juvells, I. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. Optics letters, (30), 13, 1644-1646. 2005

[12] Peng, X., Zhang, P., Wei, H., & Yu, B. Known-plaintext attack on optical encryption based on double random phase keys. Optics Letters, (31), 8, 1044-1046. 2006

[13] Peng, X., Wei, H., & Zhang, P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. Optics letters, (31), 22, 3261-3263. 2006

[14] X. Wang & D. Zhao, A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms, Opt. Commun. (285), 1078–1081. 2012

[15] X. Wang, Y. Chen, C. Dai & D. Zhao, Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform, Applied Optics, (53), 208–213. 2014

[16] Y. Wang, C. Quan, & C. J. Tay, New method of attack and security enhancement on an asymmetric cryptosystem based on equal modulus decomposition, Applied Optics, (55), 679–686. 2016

[17] Cai, J., & Shen, X. Modified optical asymmetric image cryptosystem based on coherent superposition and equal modulus decomposition. Optics & Laser Technology, (95), 105-112. 2017

[18] Li, T., & Shi, Y. Security risk of diffractive-imaging-based optical cryptosystem. Optics express,(23), 16, 21384-21391. 2015

[19] Situ, G., & Zhang, J. Multiple-image encryption by wavelength multiplexing. Optics letters, (30), 11, 1306-1308. 2005

[20] Situ, G., & Zhang, J. Position multiplexing for multiple-image encryption. Journal of Optics A: Pure and Applied Optics,(8), 5, 391. 2006

[21] Qin, Y., & Gong, Q. Interference-based multiple-image encryption with silhouette removal by position multiplexing. Applied optics, (52), 17, 3987-3992. 2013

[22] Hwang, H. E., Chang, H. T., & Lie, W. N. Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain. Optics letters, (34), (24), 3917-3919. 2009

[23] Chen, W., & Chen, X. Optical multiple-image encryption based on multiplane phase retrieval and interference. Journal of Optics, (13), (11), 115401. 2011

[24] Yong-Liang, X., Xin, Z., Sheng, Y., Qiang, L., & Yang-Cong, L. Multiple-image optical encryption: an improved encoding approach. Applied optics, (48), 14, 2686-2692. 2009

[25] Unnikrishnan, G., Joseph, J., & Singh, K. Optical encryption by double-random phase encoding in the fractional Fourier domain. Optics letters, (25), 12, 887-889. 2000

[26] Situ, G., & Zhang, J. Double random-phase encoding in the Fresnel domain. Optics Letters, (29), 14, 1584-1586. 2004

[27] Qin, W., & Peng, X. 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, (11), 7, 075402. 2009

[28] Cheng, X. C., Cai, L. Z., Wang, Y. R., Meng, X. F., Zhang, H., Xu, X. F., ... & Dong, G. Y. Security enhancement of double-random phase encryption by amplitude modulation. Optics letters, (33), 14, 1575-1577. 2008

[29] He, W., Peng, X., & Meng, X. A hybrid strategy for cryptanalysis of optical encryption based on double-random phase–amplitude encoding. Optics & Laser Technology, (44), 5, 1203-1206. 2012

[30] Kumar, P., Kumar, A., Joseph, J., & Singh, K. Vulnerability of the security enhanced double random phase-amplitude encryption scheme to point spread function attack. Optics and Lasers in Engineering, (50), 9, 1196-1201. 2012

[31] Pérez-Cabré, E., Cho, M., & Javidi, B. Information authentication using photon-counting double-random-phase encrypted images. Optics letters, (36), 1, 22-24. 2011

[32] Pérez-Cabré, E., Abril, H. C., Millán, M. S., & Javidi, B. Photon-counting double-random-phase encoding for secure image verification and retrieval. Journal of Optics, (14), 9, 094001. 2012

[33] Rajput, S. K., Kumar, D., & Nishchal, N. K. Photon counting imaging and phase mask multiplexing for multiple images authentication and digital hologram security. Applied Optics, (54), 7, 1657-1666. 2015

[34] Guillaume, M., Melon, P., Réfrégier, P., & Llebaria, A. Maximum-likelihood estimation of an astronomical image from a sequence at low photon levels. JOSA A, (15), 11, 2841-2848. 1998

[35] Morris, G. M. Image correlation at low light levels: a computer simulation. Applied optics, (23), 18, 3152-3159. 1984

[36] Hiskett, P. A., Buller, G. S., Loudon, A. Y., Smith, J. M., Gontijo, I., Walker, A. C., ... & Robertson, M. J. Performance and design of InGaAs/InP photodiodes for single-photon counting at 1.55 μm. Applied Optics, (39), (36), 6818-6829. 2000

[37] Lange, K., & Carson, R. EM reconstruction algorithms for emission and transmission tomography. J Comput Assist Tomogr, (8), (2), 306-16. 1984

[38] Guillaume, M., Melon, P., Réfrégier, P., & Llebaria, A. Maximum-likelihood estimation of an astronomical image from a sequence at low photon levels. JOSA A, (15), (11), 2841-2848. 1998

[39] Mahalanobis, A., & Muise, R. Object specific image reconstruction using a compressive sensing architecture for application in surveillance systems. IEEE transactions on aerospace and electronic systems, (45), (3), 1167-1180. 2009

[40] Kishk, S., & Javidi, B. Watermarking of three-dimensional objects by digital holography. Optics letters, (28), (3), 167-169. 2003

[41] Chen, W., Chen, X., Anand, A., & Javidi, B. Optical encryption using multiple intensity samplings in the axial domain. JOSA A, (30), (5), 806-812. 2013

[42] Qin, Y., Wang, Z., & Gong, Q. Diffractive-imaging-based optical image encryption with simplified decryption from single diffraction pattern. Applied optics, (53), (19), 4094-4099. 2014

[43] Qin, Y., Gong, Q., & Wang, Z. Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme. Optics express, (22), (18), 21790-21799. 2014

[44] Wang, X., & Zhao, D. Security enhancement of a phase-truncation based image encryption algorithm. Applied optics, (50), (36), 6645-6651. 2011

[45] Ding, X., Deng, X., Song, K., & Chen, G. Security improvement for asymmetric cryptosystem based on spherical wave illumination. Applied optics, (52), (3), 467-473. 2013

[46] Liu, W., Liu, Z., & Liu, S. Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang–Gu algorithm. Optics letters, (38), (10), 1651-1653. 2013

[47] Wang, Y., Quan, C., & Tay, C. J. Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask. Optics Communications, (344), 147-155. 2015

[48] Zhang, Y., Wang, B., & Dong, Z. Enhancement of image hiding by exchanging two phase masks. Journal of Optics A: Pure and Applied Optics, (11), (12), 125406. 2009

[49] Han, Y., & Zhang, Y. Optical image encryption based on two beams' interference. Optics Communications, (283), (9) 1690-1692. 2010

[50] Kumar, P., Joseph, J., & Singh, K. Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator. Applied optics, (50), (13) 1805-1811. 2011

[51] Chen, W., & Chen, X. Iterative phase retrieval for simultaneously generating two phase-only masks with silhouette removal in interference-based optical encryption. Optics Communications, (331), 133-138. 2014

[52] Yang, B., Liu, Z., Wang, B., Zhang, Y., & Liu, S. Optical stream-cipher-like system for image encryption based on Michelson interferometer. Optics express, (19), (3) 2634-2642. 2011

[53] Wang, X., & Zhao, D. Optical image hiding with silhouette removal based on the optical interference principle. Applied optics, (51), (6) 686-691. 2012

[54] Wang, Q. Optical image encryption with silhouette removal based on interference and phase blend processing. Optics Communications, (285), 21-22, 4294-4301. 2012

[55] Erkmen, B. I., & Shapiro, J. H. Ghost imaging: from quantum to classical to computational. Advances in Optics and Photonics, (2), (4) 405-450. 2010

[56] Huang, J. J., Hwang, H. E., Chen, C. Y., & Chen, C. M. Lensless multiple-image optical encryption based on improved phase retrieval algorithm. Applied optics, (51), (13) 2388-2394. 2012

[57] Chang, H. T., Hwang, H. E., & Lee, C. L. Position multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain. Optics Communications, (284), (18) 4146-4151. 2011

[58] Chang, H. T., Hwang, H. E., Lee, C. L., & Lee, M. T. Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in the Fresnel transform domain. Applied optics, (50), (5) 710-716. 2011

[59] Chen, W., Chen, X., & Sheppard, C. J. Optical image encryption based on phase retrieval combined with three-dimensional particle-like distribution. Journal of Optics, (14), (7) 075402. 2012

[60] Alfalou, A., & Brosseau, C. Optical image compression and encryption methods. Advances in Optics and Photonics, (1), (3) 589-636. 2009

[61] Alfalou, A., & Brosseau, C. Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption. Optics letters, (35), (11) 1914-1916. 2010

[62] Jiao, S., Gao, Y., Lei, T., Xie, Z., & Yuan, X. A Parallel Optical Image Security System with Cascaded Phase-only Masks. arXiv preprint arXiv:1902.07985. 2019

[63] Shechtman, Y., Eldar, Y. C., Cohen, O., Chapman, H. N., Miao, J., & Segev, M. Phase retrieval with application to optical imaging: a contemporary overview. IEEE signal processing magazine, (32), (3) 87-109. 2015

[64] Bianco, V., Memmolo, P., Leo, M., Montresor, S., Distante, C., Paturzo, M., ... & Ferraro, P. Strategies for reducing speckle noise in digital holography. Light: Science & Applications, (7), (1) 48. 2018

[65] Faulkner, H. M. L., & Rodenburg, J. M. Movable aperture lensless transmission microscopy: a novel phase retrieval algorithm. Physical review letters, (93), (2) 023903. 2004

[66] Fienup, C., & Dainty, J. Phase retrieval and image reconstruction for astronomy. Image Recovery: Theory and Application, (231), 275. 1987

[67] R. W. Gerchberg & W. O. Saxton, A practical algorithm for the determination of phase from image and diffraction plane pictures, Optik, (35), 237–250, 1972.

[68] Yang, G. Z., Dong, B. Z., Gu, B. Y., Zhuang, J. Y., & Ersoy, O. K. Gerchberg–Saxton and Yang–Gu algorithms for phase retrieval in a nonunitary transform system: a comparison. Applied optics, (33), (2) 209-218. 1994

[69] A. Fannjiang & W. Liao, Phase retrieval with random phase illumination, JOSA A, (29), 1847-1859, 2012.

[70] Candes, E. J., Li, X., & Soltanolkotabi, M. Phase retrieval via Wirtinger flow: Theory and algorithms. IEEE Transactions on Information Theory, (61), (4) 1985-2007. 2015

[71] Metzler, C., Schniter, P., & Veeraraghavan, A. prDeep: Robust Phase Retrieval with a Flexible Deep Network. In International Conference on Machine Learning 3498-3507. 2018

[72] A. S. A. Ghani & N. A. M. Isa, Underwater image quality enhancement through integrated color model with Rayleigh distribution, Applied soft computing, (27), 219-230, 2015.

[73] Li, X., Meng, X., Yin, Y., Yang, X., Wang, Y., Peng, X., ... & Chen, H. Hierarchical multilevel authentication system for multiple-image based on phase retrieval and basic vector operations. Optics and Lasers in Engineering, (89), 59-71. 2017

[74] Candes, E., & Romberg, J. Sparsity and incoherence in compressive sampling. Inverse problems, (23), (3) 969. 2007

[75] Candès, E. J., & Wakin, M. B. An introduction to compressive sampling [a sensing/sampling paradigm that goes against the common knowledge in data acquisition]. IEEE signal processing magazine, (25), (2) 21-30. 2008

[76] Deepan, B., Quan, C., Wang, Y., & Tay, C. J. Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique. Applied optics, (53), (20) 4539-4547. 2014

[77] Hazer, A., Ozen, I., & Yıldırım, R. Confidential Data Transport In Noise Image. Proceeding Book of the International Conference on Cyber Security and Computer Science (ICONCS 2018), 12 20181018, http://iconcs.org/home_files/ICONCS_proceeding.pdf

[78] Hazer, A., & Yıldırım, R. Multiple-Image Encryption with Phase Retrieval, 4th International Mediterranean Science and Engineering Congress (IMSEC 2019) 371-373, 2019 – Alanya.

[79] Becker, S., Bobin, J., & Candès, E. J. NESTA: A fast and accurate first-order method for sparse recovery. SIAM Journal on Imaging Sciences, (4), (1) 1-39. 2011

CURRICULUM VITAE

PERSONAL INFORMATION

Name Surname **:** Abdurrahman HAZER

Date of Birth **:** 02.05.1991

Phone **:** 05544931032

E-mail **:** hazerabdurrahman@gmail.com

EDUCATION

High School **:** Ankara Kalaba High School (2005-2009)

Bachelor **:**Abant İzzet Baysal University, Elecrical-Electronics Engineering (2009-2014)

Master Degree **:**Ankara Yıldırım Beyazıt University, Elecrical-Electronics Engineering (2016-)

WORK EXPERIENCE

2016 -2019 **Turkey Association of Municipalities - Directorate of Information Technology**

I worked as an ETL (Extract Transform Load) specialist in BELBİS project which is carried out Union of Municipalities of Turkey-Information Technologies Department. I have written SQL codes to execute ETL process.

2019 - … **Turkey Association of Municipalities - Directorate of Information Technology**

I have developed software using JAVA for BELBİS project which is carried out Union of Municipalities of Turkey-Information Technologies Department. I have written the Strategic Plan module for municipalities to use.

PROJECTS AND WORKS:

1. Undergraduate Thesis: Intervalometer Design and Implementation with Arduino.
2. EE525 ANTENNAS FROM THEORY TO PRACTICE

As a graduate course project, I designed and simulated an “L-band patch” antenna with HFSS. After the simulation I made the antenna and made measurements. (The relevant documents of the project are available.)

3. EE545 SATELLITE TECHNOLOGY

As a graduate course project, I designed a navigation satellite and conducted a study on finding the satellite location using MATLAB. In particular, pay load of the satellite was emphasized in the project. (The relevant documents of the project are available.)

4. EE563 PATTERN RECOGNITION

As a graduate course project, I made an Object Recognition project with MATLAB using the K-Nearest Neighbors algorithm. (The relevant documents of the project are available.)

5. REAL-TIME DIGITAL FILTERING

As a graduate course project, I have written VHDL codes with a small algorithm to do digital filtering using ALTERA QUARTUS. The codes were tested on FPGA. (The relevant documents of the project are available.)

6. COMPUTER BASED CONTROL SYSTEMS

As a graduate course project, I have completed a project that will enable three microprocessors to communicate simultaneously. For this project, I first designed a circuit in Proteus using 3 microprocessors (pic16f877a) and 3 different color (red, green and blue) leds and made the electronic board of this circuit. Then I designed an interface with C # and communicated 3 microprocessors (pic16f877a) simultaneously with the commands entered from this interface. I tested the circuit with RGB LEDs. (The relevant documents of the project are available.)

PUBLİSHED PAPERS:

1. Hazer, A., Ozen, I., and Yıldırım, R. (2018). Confidential Data Transport In Noise Image. *Proceeding Book of the International Conference on Cyber Security and Computer Science (ICONCS 2018), 12 20181018,* http://iconcs.org/home_files/ICONCS_proceeding.pdf
2. Hazer, A., and Yıldırım, R. "*Multiple-Image Encryption with Phase Retrieval*" 4th International Mediterranean Science and Engineering Congress (IMSEC 2019) 25-27, 2019 – Alanya

TOPICS OF INTEREST

- Optical Signal Processing
- Speckle Processing
- Digital Image Processing
- Phase Retrieval
- Signal Processing
- Cryptography