August 2020

PhD Dissertation

Efficient Image Cryptosystem based on Double Random Phase Encoding and Dynamic Chaotic Maps

Graduate School of Chosun University

Department of Computer Engineering

Samaneh Gholami

Efficient Image Cryptosystem based on Double Random Phase Encoding and Dynamic Chaotic Maps

이중 무작위 위상 부호화와 동적 혼돈지도에 기반한 효율적인 영상 암호 시스템

2020 년 8 월 28 일

Graduate School of Chosun University

Department of Computer Engineering

Samaneh Gholami

Efficient Image Cryptosystem based on Double Random Phase Encoding and Dynamic Chaotic Maps

Advisor: Shin Seok-Joo

This dissertation is submitted to the Graduate School of Chosun University in partial fulfillment of the requirements for the award of a PhD degree

2020 년 5 월

Graduate School of Chosun University

Department of Computer Engineering

Samaneh Gholami

This certifies that the degree of Doctor of Philosophy of Samaneh Gholami is approved by:

강문수 (chair of the committee)

이충규 (committee member)

권구락 (committee member)

신석주 (committee member)

문인규 (committee member)

Graduate School of Chosun University

사마네의 박사학위논문을 인준함

위원장	조선대학교	교 수	강문수(인)
위 원	조선대학교	교 수	이충규 (인)
위 원	조선대학교	교 수	권구락 (인)
위 원	조선대학교	교 수	신석주(인)
위 원	대구경북과학기술원	교수	문인규(인)

2020 년 7 월

조선대학교 대학원

Dedication

To the kindest spouse I know: Keyvan

For his advice, his patience, and his faith.

Without you, none of this would have happened.

Acknowledgments

Going abroad and studying on a new topic, from where I decided to do this, is a tough decision. Defiantly, passing this difficult path and reaching the goal without the help and support of others is impossible. I am glad to have this opportunity to thank those who helped me.

I would like to express my sincere gratitude to my previous advisor Prof. Moon for providing me invaluable guidance and comments throughout the course of the Ph.D. I would specially thank current advisor Prof. Shin For his generous support and help. My specials thanks to Prof. 강문수, 이충규 and권구락 for supporting me to finalize this dissertation.

Every challenging work needs the support of friends and family, especially those who are very close to your heart. My deepest gratitude extends to my mother, Farideh and my father Hossein for inspired me to be diligent to achieve my goals. Also, I extend my sincere appreciation to my beloved family members, Morteza my brother, Sara my sister, Ahmad my brother-in-law, and my parents-in-law.

To all my friends in Korea especially my lab mates and my kindly friends in Iran, thank you for your understandings and encouragement in my moments of crisis. I cannot list all the names here, but you are always on my mind.

My wish for you all is you get success in every step of career and life.

تقدیر

برای من آمدن به خارج از کشور و تحصیل در مقطع دکترا، تصمیم سختی بود. بی تردید عبور از چنین مسیر دشواری و دستیابی به هدفم بدون کمک و حمایت دیگران غیر ممکن بود. من خوشحالم که این فرصت را دارم تا مراتب تشکرو قدردانی خودم رو نسبت به کسانی که دراین راه من رایاری کردن ابراز نمایم.

برخود واجب می‌دانم قدردانی صمیمانه خود را نسبت به استاد محترم Prof. Moon برای ارائه راهنمایی ها و نظرات ارزشمندشان در طول دوره دکترا اعلام نمایم. همچنین از Prof. Shin برای پشتیبانی و حمایت ها سخاوتمندانه شان تشکر می کنم. مراتب تشکر خود را نسبت به Prof. Lee, Prof. Gwan و Prof. Kang به خاطر حضور در جلسه دفاع اعلام می نمایم.

هر کار چالش برانگیزی نیاز به حمایت دوستان و خانواده دارد، به ویژه افرادی که قلباً به شما خیلی نزدیک هستند. عمیق ترین قدردانی من نسبت به مادرم **فریده** و پدرم **حسین** است که برای من در سخت کوشی الهام بخش بوده اند. همچنین از خانواده عزیزم در ایران، **مرتضی** برادرم، **سارا** خواهرم، **احمد** همسر خواهرم و پدر و مادر همسرم بسیار سپاسگذارم. از همه دوستانم در کره جنوبی و دوستان مهربانم در ایران، بخاطر حضورو دلگرمی هایشان در لحظات بحرانی تشکر می کنم. من نمیتوانم همه نامها را در اینجا فهرست کنم، اما همیشه در ذهن من هستند.

آرزوی من برای همه شما موفقیت در تمامی مراحل زندگی است.

Table of Contents

List of Tables

List of Figures

Abbreviations

DRPE: Double Random Phase Encoding

JPEG: Joint Photography Experts Group

CPM: Chaotic Phase Masks

PCI: Photon Counting Imaging

RPM: Random Phase Masks

FT: Fourier Transform

IFT: Inverse Fourier Transforms

PCE: Peak-to-Correlation Energy

2D: 2-dimensional

DCT: Discrete Cosine Transform

DWT: Discrete Wavelet Transform

NCC: Nonlinear Cross-Correlation

CR: Compression Ratio

MO: Microscope Objective

PC: Personal Computer

PD: Propagation Distance

RBC: Red Blood Cell

Abstract

Efficient Image Cryptosystem Based on Double Random Phase Encoding and Dynamic Chaotic Maps

By: Samaneh Gholami

Advisor: Shin Seok-Joo

Department of Computer Engineering

Graduate School of Chosun University

This dissertation introduces novel image encryption techniques with the integration of double random phase encoding (DRPE) and chaotic-based cryptography approaches. The primary goal of this study is to propose efficient encryption techniques that reduce the required storage space and enhance the security of digital images and holograms. In the first study, due to that encrypted images obtained through DRPE occupy considerable storage space, efficient compression schemes are proposed and the effect of compression on the encrypted data is analyzed. In the proposed scheme, the Joint Photography Experts Group (JPEG) and JPEG2000 (JP2K) compression techniques are applied to the quantized encrypted phase images obtained by combining the DRPE algorithm with the virtual photon-counting imaging technique. We compute the nonlinear cross-correlation between the registered reference images and the compressed input images to verify the performance of the compression of DRPE images. Indeed, we show quantitatively through experiments that compressed encrypted image data can be achieved while security and authentication factors are completely preserved.

In the second study, the primary objective is to reduce the key size in the numerical implementation of the DRPE method. This can be achieved by replacing random phase masks (RPM) with chaotic phase masks (CPM). Additionally, by using CPMs the security of conventional DRPE in different attacks can be completely preserved. By iterating the

Lorentz chaotic function certain times using keys and plaintext image, uniform random numbers are obtained that can replace RPM. The experiments revealed that the proposed scheme is highly sensitive to the key changes and good resistance against statistical attacks.

The last work introduces a new technique for the encryption of holograms obtained by digital holographic in the microscopic configuration. The hologram is optically recorded in off-axis configuration with a CCD camera and the zero-order and twin-image noises are eliminated by spatial filtering technique in the Fourier domain. Then, the filtered hologram in the Fourier domain is distorted by the one-time chaotic phase mask generated by chaotic dynamic mapping with the non-secret salt value and the secret key. The combination of non-secret salt value and private chaotic keys can guarantee a perfect forward secrecy scheme. Eventually, the numerical Fresnel propagation on an arbitrary plane and a given wavelength encodes the distorted hologram into white noise. By using one-time CPM and perfect forward secrecy scheme we can enhance the security of conventional optical encoding technique. Additionally, the size of the secret key for the encryption-decryption scheme is significantly reduced since we only need a very small size of the chaotic key. Different experimental results reveal that the proposed scheme is highly sensitive to the key changes and withstands against chosen-plaintext, chosen-cipher text attacks, and blind decryption without knowing the exact chaotic keys, correct propagation distance, and wavelength.

[KEYWORDS]: Double Random Phase Encoding, Compression technique, Chaotic method, Perfect Forward Secrecy, Digital Holographic Microscopy, Red Blood Cell

초록

이 논문은 DRPE (Double Random Phase Encoding)과 혼돈 기반 암호화 기법을 통합 한 새로운 이미지 암호화 기술을 소개합니다. 이 연구의 주요 목표는 필요한 저장 공간을 줄이고 디지털 이미지 및 홀로그램의 보안을 강화하는 효율적인 암호화 기술을 제안하는 것입니다. 첫 번째 연구에서는 DRPE를 통해 얻은 암호화 된 이미지가 상당한 저장 공간을 차지하기 때문에 효율적인 압축 방식이 제안되고 암호화 된 데이터에 대한 압축의 영향이 분석됩니다. 제안 된 방식에서, JPEG (Joint Photography Experts Group) 및 JPEG2000 (JP2K) 압축 기술은 DRPE 알고리즘과 가상 광자 계수 이미징 기술을 결합하여 얻은 양자화 된 암호화 된 위상 이미지에 적용됩니다. DRPE 이미지 압축 성능을 확인하기 위해 등록 된 참조 이미지와 압축 된 입력 이미지 간의 비선형 상호 상관을 계산합니다. 실제로 보안 및 인증 요소를 완전히 보존하면서 압축 된 암호화 된 이미지 데이터를 얻을 수 있다는 실험을 통해 정량적으로 보여줍니다.

두 번째 연구에서 주요 목표는 DRPE 방법의 수치 구현에서 키 크기를 줄이는 것입니다. 이는 랜덤 위상 마스크 (RPM)를 혼돈 위상 마스크 (CPM)로 교체하여 달성 할 수 있습니다. 또한 CPM을 사용하여 다른 공격에서 기존 DRPE의 보안을 완전히 유지할 수 있습니다. 키와 평문 이미지를 사용하여 Lorentz 카오스 기능을 특정 시간 반복하여 RPM을 대체 할 수있는 균일 한 난수를 얻습니다. 실험은 제안 된 체계가 주요 변화에 매우 민감하고 통계적 공격에 대한 우수한 저항성을 보여 주었다.

마지막 작업은 미세한 구성에서 디지털 홀로그램으로 얻은 홀로그램 암호화를위한 새로운 기술을 소개합니다. 홀로그램은 CCD 카메라를 사용하여 축외 구성으로 광학적으로 기록되며, 푸리에 영역에서의 공간 필터링 기술에 의해 0 차 및 트윈 이미지 노이즈가 제거됩니다. 그 후, 푸리에 도메인에서 필터링 된 홀로그램은 비-비밀 염 값 및 비밀 키를 갖는 혼돈 동적 매핑에

의해 생성 된 일회성 혼돈 위상 마스크에 의해 왜곡된다. 비 비밀 소금 가치와 개인 혼란 키의 조합은 완벽한 앞으로 비밀 체계를 보장 할 수 있습니다. 결국, 임의의 평면 및 주어진 파장에서의 수치 적 프레 넬 전파는 왜곡 된 홀로그램을 백색 잡음으로 인코딩한다. 일회성 CPM 및 완벽한 순방향 보안 체계를 사용하여 기존의 광학 인코딩 기술의 보안을 강화할 수 있습니다. 또한, 매우 작은 크기의 카오스 키만 필요하므로 암호화-암호 해독 체계의 비밀 키 크기가 크게 줄어 듭니다. 다른 실험 결과는 제안 된 체계가 주요 변경 사항에 매우 민감하고 정확한 혼란 키, 정확한 전파 거리 및 파장을 알지 못한 채 선택한 평문, 선택된 암호문 공격 및 블라인드 해독에 견딜 수 있음을 보여줍니다.

1 Introduction

In today's universe of internet and multimedia technologies, and with the rapid development of modern communication techniques, both information security and intellectual property protection are of great concern. No matter what kind of information you are storing or transferring, whether it is your private information or other data from your job or other materials that can affect your work, keeping your data safe should be a number one priority in your life. As a traditional security technique, cryptography has been widely studied for information security. Cryptography is the study of techniques to encrypt the original information into encoded information with the aim of protecting the content of the plaintext or plain image. More specifically, transferring and storing the images are growing dramatically, necessitating the design of effective methods to solve the problem of digital image cryptography. There are two main goals of image security: image authentication and image encryption.

Image authentication is the application of image science to determine if a particular image is an accurate representation of the original data based on a defined criterion. For developing the image authentication process, several approaches have been proposed. These approaches include optical information security methods that integrated with related encryption methods. Encryption algorithms provide a more secure type of cryptography that any unauthorized user cannot obtain the encrypted data. Only the authorized user who has the secret key can obtain the original data. Among the classical optical encryption techniques, the DRPE has been receiving much interest because of its high-level data security [1-12]. For the decryption process, we need the exact keys that have been used while the encryption process. Due to its high-security characteristic, the DRPE technique can be applied in many fields, such as in optical security, image encryption, information authentication, secure storage, and secure data transmission [13-20]. In [13-15] the encryption methods are proposed by fusion of the DRPE and photon counting to enhance the security of the encrypted images. In order to investigate security in the optical system, several works and enhancements are proposed to evaluate information security against popular attacks [16-18].

Although conventional DRPE processes are robust to many attacks, they are still vulnerable to specific attacks. It has been determined that DRPE is weak and vulnerable against impulse attacks [21, 22]. Recently, the photon-counting imaging (PCI) technique has been integrated into the DRPE method to enhance the security of conventional DRPE [13-15, 23-26]. Photon-counting imaging generates distributions with far fewer photons than conventional imaging and provides substantial bandwidth reduction by generating sparse encrypted data. An authentication system that combines DRPE with PCI (DRPE-PCI) can safeguard the encrypted data from unauthorized attacks and enhance its security to the desired level [13-15, 23-26]. This dissertation focus on improving the optical image encryption by combining DRPE, PCI, compression method and chaotic random generator method. In the first study, an attempt has been to reduce the encrypted image size by combining compression methods and DRPE. JPEG and JP2K compression techniques are examined in this study. These compression techniques have been widely used for reducing the size of images, storing full-color information, and automatic error recovery. These methods are the most popular lossy compression techniques that reduce the original image size by removing non-vital information. These two techniques are explained briefly in the next section.

Besides of the vulnerability of DRPE in some attacks, there is an unwanted property in the numerical implementation of DRPE. The storage space of random phase masks (RPM), regarded as the keys that contribute to convert an image to white noise, and is equal to the size of the original image. Therefore, as shown in Table 1.1 the key size for big images is significantly large. Key transfer and storage are other issues that are still to be addressed in numerical implementations of DRPE. Additionally, the key size is dependent upon the image size. It is well known that RPM has maximum entropy with the statistically independent property. RPMs (first and second RPMs) are uniformly distributed between {0, 2π}. The question that arises here is whether it is possible to generate RPM by a small number of keys independent of the image size. One way to circumvent this issue is by using another method to generate phase masks that can meet all the properties of RPM. Previously, pixel scrambling methods have been applied to enhance the security of the conventional DRPE technique [27-30]. As mentioned earlier, RPMs are uniformly distributed. Therefore, replacing RPM generations with any other method should follow the properties of a uniform distribution. In the second work, the effects of using a chaotic-based image encryption algorithm on DRPE outputs will be examined.

Table 1.1: Size of image and keys in DRPE

Image size	Key size
50×50	$2 \times 50 \times 50 floats$
256×256	$2 \times 256 \times 256 floats$
512×512	$2 \times 512 \times 512 floats$
1024×1024	$2 \times 1024 \times 1025 floats$

A. Motivations

By using the encryption algorithms the file is translated into a meaningless ciphertext and then transferred in this configuration; the receiving computer uses a key to translate the cipher into its original form. So if the message or file is intercepted before it reaches the receiving computer it is in an unusable (or encrypted) form. So, as expected, attackers are also being active to break those encryption systems so that they can get confidential information. The goal of these studies is to propose the encryption system that has the ability to encrypt data in a way that it is really hard for an intruder to break the code. One of the ways, in order to make the encryption system more strong, enhances the security of encryption keys.

Image authentication methods check the validity of the image whether it is still unchanged or already corrupted by any third party attacker in the midway of transmission. There are many ways to perform that transformation, some straightforward and some very complex. In order to smooth the transmission process, the image data is needed to be compressed then it can be easily sent on the other side. Otherwise, it usually takes a huge amount of bandwidth to go to the receiver’s side. Therefore, to decrease the size of an image, the compression algorithm is used.

Moreover, most of the image transmission involved the DRPE-PCI methods to keep the image safe from the outside attacker. In this way, it will be protected and even though it has been changed for transmission, on the receiving end by authentication method it can be retrieved easily. So, for decreasing the size of the encrypted image we will propose efficient compression schemes to reduce the size of the encrypted data by combining the DRPE-PCI method and compression methods (see Fig.1.1).

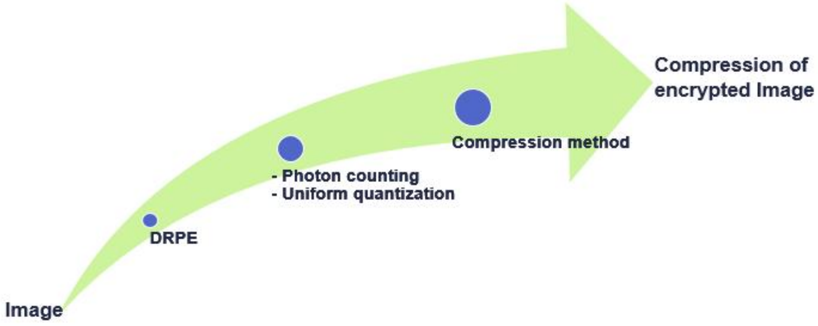


Figure 1.1: general scheme of DRPE-PCI and compression methods

The second property of DRPE that has been discussed in this thesis is the size of RPM as keys in the encryption method. For decreasing the size of RPM, chaotic method will be proposed as generating chaotic random phase mask. The chaotic-based image encryption algorithm was first reported by Matthews [31]. There are several advantages of chaotic random generators. It is neither periodic nor convergent and it is sensitive to the initial condition (image) and the control parameters (keys). It may seem chaotic due to the random and disorganized nature, but because of the determining mathematical equations, chaos-based random generators are deterministic [32-34]. Another advantage of using chaotic random generators is that it is easy to implement using microprocessors and personal computers. The highly unpredictable and random-looking nature of the chaotic output is the most attractive feature of the deterministic chaotic system that may lead to various novel applications. Chaotic random generators have been widely used for image security, encryption, and watermarking purposes. Following to increase the tendency to use chaotic; the development of cryptosystems chaos has been the interest of many researchers [31-37].

Due to the concept has been discussed above, developing an image encryption system, became the strong motivation to come forward with this dissertation.

B. Previous Achievements in Image Authentication Field

Cryptography became more popular during the Middle Ages with converting information (plain text) into unreadable figures (ciphertext) to protect the information content during the transport time. As shown in Fig.1.2 encryption key apply for encoding the original information to ciphertext and for decoding we need the decryption key. If these keys are the same, the encryption process is symmetric otherwise it is asymmetric. DRPE is an optical encryption technique that applies the same keys for encryption and decryption. In order to improve the DRPE efficiency, lots of encryption approaches were researched [1-25]. For example, Zhao et al. [19] proposed an image encryption system based on DRPE and RSA public-key algorithm which can be implemented for fingerprint applications with high robustness against the existing attacks. Suzuki [20] suggested the fingerprint verification system based on DRPE.

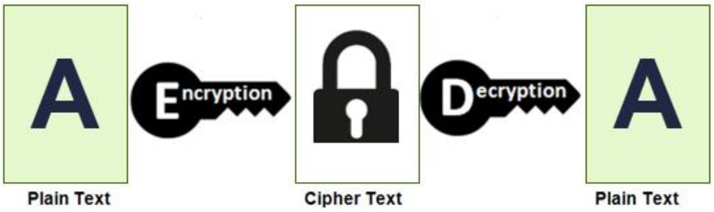


Figure 1.2: Cryptography (encryption, decryption)

Furthermore, the researchers have investigated the security of DRPE against a variety of attacks [38, 39]. The first one of these attacks is the chosen plaintext attack, where the attacker has full access to the cryptosystem and can introduce specially tailored plaintexts to be encrypted in order to deduce the encryption key [40, 22]. The next attack is the known-plaintext attack, where one or more plaintext-cipher text pairs are in possession of the attacker

[41]. In this case, the attacker cannot access the plaintexts, and his target is to deduce the encryption key from the available information. Depending on the number of plaintexts–ciphertext pairs available to the intruder, there are several different implementations of known-plaintext attack against optical cryptosystems. The cipher text-only attacks [21] is the critical attack that any cryptosystem must resist against it. In this attack, the intruder can retrieve the plaintext directly from the ciphertext, without the need for the encryption key.

To solve this problem the PCI technique has been one of the proposed methods to enhance the security of DRPE [13-15, 23-26]. Pérez-Cabré et al. [23] have established a method where he integrated a photon-counting imaging method with the original DRPE system. In other work [24] he introduced two different methods that both procedures allow us to increase the security of the encryption system against intruders. Also, it is shown that chaotic map and pixel scrambling methods could be used with light interference methods to have high robustness against noise perturbation and known attacks [27-30]. For example, Chen [27] showed that by integrating Arnold map (Cat map) with light interference methods, authentication can still be preserved and keys can be extended to enhance the security of the system.

C. Objectives of Research

As discussed earlier the main idea of this work is to decrease the size of the encryption image and enhance the security in the DRPE method. Also, propose the new encryption method for biological sample hologram. The objectives can be listed as:

- To study the compression method applied in the area where DRPE and photon-counting methods are of interest.
- To propose a new technique for decreasing the size of the key of DRPE in image

authentication studies.

◦ To study perfect forward secrecy.

◦ To propose a new method to enhance the security of biological hologram.

D. Organization of Research

The organization of this thesis is as follows. Chapter 2 gives an overview of the methods we have utilized in this study. Chapter 3 provides a brief description of the proposed scheme and discusses the experiments for image authentication schemes. Chapter 4 discusses the robust encryption of off-axis hologram by a one-time random phase mask generation. Eventually, chapter 5 provides the conclusions of the thesis and future research opportunities.

2 Background

Before describing the proposed approaches, we first briefly review the basic techniques that we have used in image authentication for efficient compression of DRPE or chaotic-DRPE methods.

A. Double Random Phase Encoding (DRPE)

In the DRPE encryption method, by introducing random phase-encoding in both the input and the Fourier planes, it is able to encode an input image to a complex-amplitude encoded image, whose real and imaginary parts can be regarded as independent stationary white noise that does not resemble the original image. The original image can be decoded only when the exact keys are given. A two-dimensional (2D) input image *f*(*x,y*) is converted into stationary encrypted white noise image labeled $f_c(x,y)$. Otherwise reconstructing the encrypted image without introduced white noise will be possible by using only the amplitude or the phase spectral information. To accomplish the stationary encrypted white noise image, a uniform white noise is produced by applying two random phase masks $\varphi_1(x,y)$ and $\varphi_2(u,v)$. These two-phase masks are in the spatial and frequency domains, $\exp(j2\pi\varphi_1(x,y))$ and $\exp(j2\pi\varphi_2(u,v))$, respectively, and are statistically independent and uniformly distributed over {0,2π}. Consequently, the encrypted image obtained from the DRPE method can be represented as follows [1, 14, and 17]:

$$f_c(x,y) = \Im^{-1}[\Im[f(x,y)\exp(j2\pi\varphi_1(x,y))]\exp(j2\pi\varphi_2(u,v))], \quad (1)$$

Where $\Im$ and $\Im^{-1}$ denote the 2D Fourier transform (FT) and the inverse Fourier transforms

(IFT), respectively. Also, *exp(x)* stands for e^x and j satisfies $j^2=-1$. The decryption process in DRPE is the reverse process of the encryption shown in Eq. (1). The Optical implementation of the DRPE encryption-decryption system shown in Fig.2.1(a) and (b). In the encryption process, the original image multiply by the first random phase mask then is illuminated by laser light. Then, the output of the previous part is multiplied by the second random phase mask and finally light passes through the second lens. The second lens, which acts like an IFT, converts the image back to the spatial domain. In the DRPE scheme, pixel values are converted to complex numbers with amplitude and phase information. The decryption process is the reverse of the encryption process.

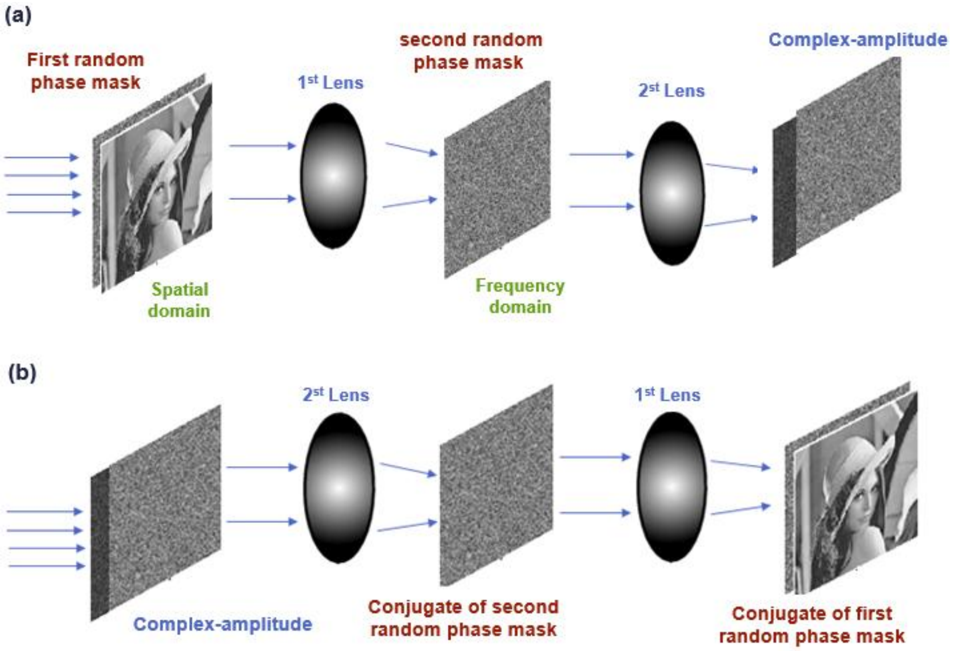


Figure 2.1: Optical implementation of encoding-decoding the DRPE algorithm in the Fourier domain (a) encoding and (b) decoding.

B. PCI

PCI is a special class of optical imaging techniques that was designed for low-light conditions or night vision imaging systems. PCI can also be computationally simulated by changing a limited number of photons based on the expected number of incident photons in the entire scene. In the virtual PCI scheme, the probability of counting photons (p_j) at an arbitrary pixel (x_j) in an image can be modeled as a Poisson distribution, as shown in Eq. (2):

$$Poisson(p_j;\lambda_j)=\frac{\lambda_j^{\,p_j}e^{-\lambda_j}}{p_j\,!}, \tag{2}$$

where λ_j is the Poisson parameter that is computed by $\lambda_j = N_p f_j$, N_p is the expected number of incident photons, and f_j is the normalized irradiance at pixel (x_j) such that $\sum_{j=1}^{M} f_j = 1$, with M being the total number of pixels in the image. In the proposed compression scheme, PCI is virtually applied to the amplitude portion of the encrypted complex amplitude image $f_c(x,y)$ obtained from DRPE [15,23].

C. Compression methods

As mentioned earlier, the output of the DRPE technique is very large. Thus, efficient compression techniques are crucial for storage and transmission purposes. Because the JPEG and JP2K compression techniques have superior performance compared to existing standards [42, 52], these two techniques have been used in this work and are explained briefly in this section.

a. JPEG:

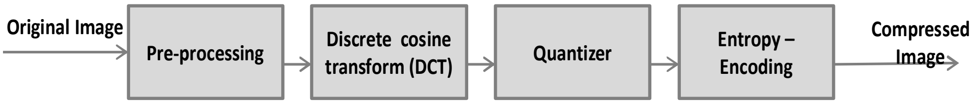


Figure 2.2: JPEG fundamental building blocks

JPEG is a well-known standardized image compression technique. It has been widely used for several purposes, including reduction of the size of image files, storage of full-color information, and automatic error recovery [42]. This technique is the most popular compression technique and supports lossy coding. Lossy compression reduces the original image size by removing non-vital information. In the baseline model (See Fig.2.2), the image is divided into 8×8 blocks and each block is transformed using the discrete cosine transform (DCT). The DCT is typically applied to reduce spatial redundancy to achieve good compression performance. The transformed blocks are quantized using a uniform scalar quantization, zig-zag scanned, and eventually, entropy coded using Huffman coding. The quantization step size for each of the 64 DCT coefficients is specified in a quantization table, which remains the same for all blocks [42].

b. JPEG2000

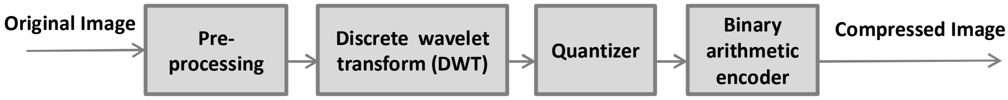


Figure 2.3: JPEG 2000 fundamental building blocks

JP2K is based on a discrete wavelet transform (DWT), scalar quantization, context modeling, arithmetic coding, and post-compression rate allocation. The fundamental building block of a JP2K encoder is shown in Fig.2.3. Preprocessing steps include tile component partitioning, DC shifting, and component transformation. During preprocessing, each slice of the original image block is partitioned into one or more disjoint rectangular regions called tiles. In terms of coding, these tile components are independent. DC shifting converts the input unsigned sample values of the image tile components into signed sample values with zero-point symmetry. Thus, the relationships between the image tile components are decreased through component transformation. JP2K uses a DWT for transformation as its core coding technology. A DWT can support the transmission of multi-resolution images by using an image multi-resolution representation and decrease the correlation between pixels in the full-frame to reduce the blocking effect in the codec process. After the entire image is transformed, the resulting coefficients are quantized and different levels of image quality are acquired based on the minimal precision required. The quantizer assigns different quantization levels for different sub-bands by using a scalar quantization method with a dead zone. The final step of encoding is called entropy encoding. The entropy encoder divides the wavelet sub-band into code blocks. DWT coefficients are then organized into binary bit planes. The entropy encoder uses context modeling and bit-plane arithmetic coding to encode the binary bit planes [43-50]

D. Chaotic method

As mentioned earlier, chaos is found to be very useful and has been used for the development of cryptosystems. Chaos is a sort of deterministic but random-like process that occurs in nonlinear dynamic systems. This dissertation proposes a chaotic map based on a Lorenz system as shown in Eq. (3). The Lorenz system is an autonomous system that can be applied as a chaotic system [33, 35].

$$\begin{cases} x' = a(y-x) \\ y' = cx - xz - y. \\ z' = xy - bz \end{cases} \tag{3}$$

If *a* = *10*, *b* = *8/3*, and *c* = *28*, the system is in chaotic state. Figure 2.4 shows iterating a Lorentz chaotic system with the initial values of *x* = *0.53*, *y* = *0.18*, *z* = *0.5* and *R* = *23* that is solved by the Runge-Kutta method. Parameter *R* defines the iteration number of the system.

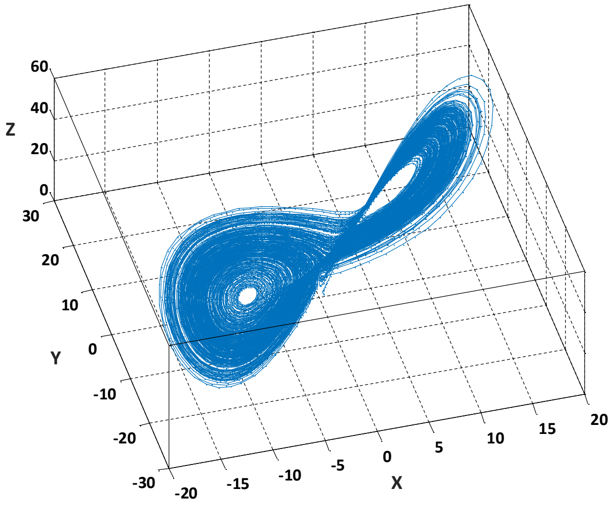


Figure2.4: A general Presentation of Digital Holographic Microscope

The generation of the chaotic random maps mainly depends on the initial values of *(x,y,z)* and the iteration number *R*. The generation of new values depends on the previous ciphered image pixel and the previous iteration values. In this way, the mask value for every pixel depends on the external keys and the pixel value itself. The mask generation process is shown in Fig.2.5 [35]. The procedure initiates by using the keys to generate the initial values (mainly x, y, z and the iteration number R_1) for running the chaotic system mentioned in Eq. (3). This the first run of the chaotic system provides another set of values for the actual generation of the CPM at the next run. The first run generates distinct values from the keys to start the actual generation of the chaotic phase masks. To be more specific, the first run maps the keys to a point in the *3D* space shown by Fig.2.5. The other runs, that is equal to the number of pixels in the image, with the contribution of the pixel value and the previously generated numbers (x, y, z, and the new iteration number R_i) produce the chaotic phase maps for the DRPE scheme. As it is shown in the scheme the Lorenz chaotic dynamic system is in common since it is the motor of random generation.

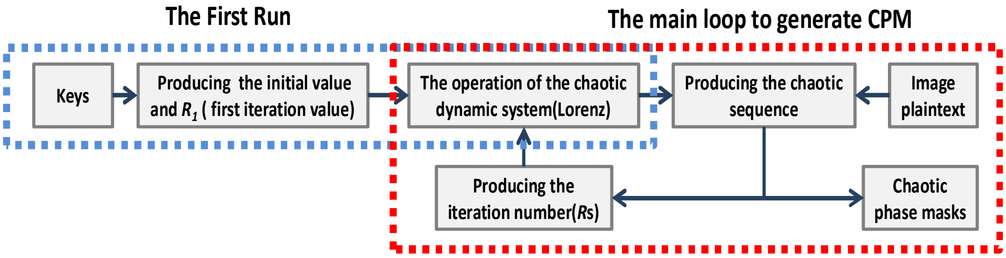

The First Run
The main loop to generate CPM
Keys
Producing the initial value and R_1 (first iteration value)
The operation of the chaotic dynamic system(Lorenz)
Producing the chaotic sequence
Image plaintext
Producing the iteration number(*Rs*)
Chaotic phase masks

Figure 2.5: Scheme of the proposed chaotic system for the generation of chaotic phase masks; the first ru n with the contribution of keys generate another set of values (x, y, z, and R_1); the main loop generates CPM by the use of values in the first run.

Figure 2.6 presents the workflow diagram for the chaotic random mask generation for an image with $n=M\times N$ pixels and $K=K_1K_2...K_{16}$, where the "K"s are 16 eight-bit keys. Three real numbers $x, y, z \in [0, 1]$ are acquired by the first step in Fig.2.6. R_1 is the first iteration of the mixed chaotic dynamic systems. As can be seen, x, y, and z are the initial values. The four-rank

Runge-Kutta method is used to iterate the Lorenz system T_1 times (Step #2). We set (x_0, y_0, z_0) as the real initial values of the chaotic dynamic system. In the next step (Step #3), depending on the value of R_1 and the values (x_0, y_0, z_0), we acquire (x_1, y_1, z_1), which are the initial values for the next iteration in the chaotic dynamic system. In Step #4, the following operation is performed in order to obtain A_1, which is the first chaotic value for the CPM corresponding to the first pixel. To calculate the value of A_i, the x value of the chaotic system is used. Our experimental results show that the y and z value can also be used but the performance of the proposed chaotic-DRPE does not change (results not shown). In the last step, Step #5, based on the values generated for (x_1, y_1, z_1) in Step #3 and on the C_1 value, we can calculate the next iteration time R_2 by incorporating the intermediate variable B_1. The pixel values are incorporated into the system by subtracting P_i from A_i. This can relate to the CPM generation system to the input image. Therefore, removing the pixel value of P from the system will generate CPMs that are identical for all images having the same input keys (independent of the input image). We then set (x_1, y_1, z_1) as the next initial values of the corresponding chaotic dynamic system. Steps #3 to #5 are then repeated to generate all CPM values motivated by the method presented by P. Fei [35].

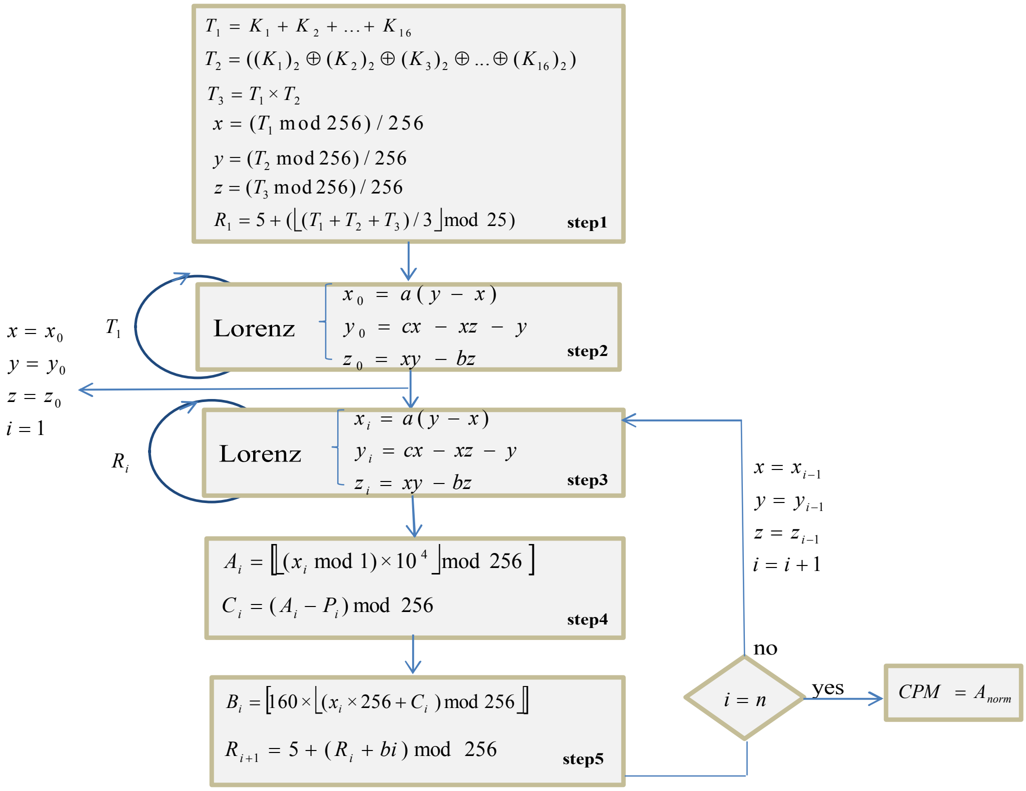

$T_1 = K_1 + K_2 + \ldots + K_{16}$
$T_2 = ((K_1)_2 \oplus (K_2)_2 \oplus (K_3)_2 \oplus \ldots \oplus (K_{16})_2)$
$T_3 = T_1 \times T_2$
$x = (T_1 \bmod 256) / 256$
$y = (T_2 \bmod 256) / 256$
$z = (T_3 \bmod 256) / 256$
$R_1 = 5 + (\lfloor (T_1 + T_2 + T_3) / 3 \rfloor \bmod 25)$
step1
Lorenz
$x_0 = a(y - x)$
$y_0 = cx - xz - y$
$z_0 = xy - bz$
step2
T_1
$x = x_0$
$y = y_0$
$z = z_0$
$i = 1$
Lorenz
$x_i = a(y - x)$
$y_i = cx - xz - y$
$z_i = xy - bz$
step3
R_i
$x = x_{i-1}$
$y = y_{i-1}$
$z = z_{i-1}$
$i = i + 1$
$A_i = [\lfloor (x_i \bmod 1) \times 10^4 \rfloor \bmod 256]$
$C_i = (A_i - P_i) \bmod 256$
step4
$B_i = [160 \times \lfloor (x_i \times 256 + C_i) \bmod 256 \rfloor]$
$R_{i+1} = 5 + (R_i + bi) \bmod 256$
step5
no
$i = n$
yes
$CPM = A_{norm}$

Figure 2.6: Workflow of chaotic generation. K_n: ASCII value of the nth key. $(K_n)_2$: a binary form of the ASCII value of the nth key. ⊕: *XOR* operation [18].

E. Correlation of two adjacent pixels

In consideration of the intrinsic characteristics of adjacent pixels in the digital image, we found that analyzing the correlation between each pixel is the best statistical analysis for finding the correlation coefficients. Because of the high correlation between the pixels of an image, the secure encryption scheme should remove the correlation in order to improve the resistance against statistical analysis [33, 35-36]. To test the correlation between horizontally, vertically, and diagonally adjacent pixels, we calculate the correlation coefficient of each pair by using the following formulas:

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{4}$$

where *E(x)* is the estimation of the mathematical expectations of *x, D(x)* is the estimation of the variance of x and cov(*x,y*) is the estimation of covariance between *x* and *y. x* and *y* are gray-scale values of two adjacent pixels in the image.

F. Peak-to-correlation energy

The authentication between the reference image and the input image is evaluated by the peak-to-correlation energy (PCE), which is defined as:

$$PCE = \frac{\max\{|ncc(x,y)|^2\}}{\sum_{i=1}^{M}\sum_{j=1}^{N}|ncc(x_i,y_j)^2|}, \tag{5}$$

where *M* and *N* are the image size along the x and y-axes. *ncc(x,y)* is given as:

$$ncc(x,y) = \Im^{-1}\{|A^r(u,v)A^i(u,v)|^k \exp\left[j(P^r(u,v) - P^i(u,v))\right]\}, \tag{6}$$

where *A* is the amplitude and *P* is the phase value of the encrypted image (*r* superscripts stand for the registered reference image and *i* superscript stands for an input image). In addition, *k* defines the density of the applied nonlinearity [13, 53]. In the following study, chaotic-DRPE is tested for various values of *k*.

3 Efficient Image Cryptosystem based on Double Random Phase Encoding and Dynamic Chaotic Maps:

This chapter, provide efficient authentication methods that will address the weakness of conventional authentication technique and provide optimum required space and security. In the following chapters, proposed algorithms are described and we focus on their different experimental results. Methods are classified according to the service they provide, that is combining the compression method and DRPE to reduce the size of the encryption image in section (A), using chaotic method to decrease the size of the key in section (B). To verify the validity of the proposed methods, numerical simulation experiments are performed on a gray-scale version of the images shown in Fig.3.1. The two images are among the benchmark images for image processing studies [54]. The following simulations were performed on a PC with a 32-bit Windows 7 Enterprise OS, Intel(R) Core(TM) i5-2500K 3.30 GHz processor, 4 GB of RAM. All the simulations are implemented in MATLAB 2016.

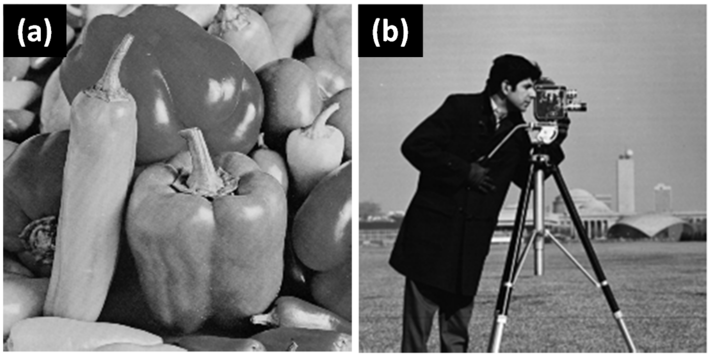


Figure 3.1: Images used in our numerical experiments: (a) Peppers, (b) Cameraman.

A. Efficient compression schemes for double random phase-encoded data for image authentication

a. Abstract:

In this section, we propose efficient compression schemes to reduce the size of the encrypted image data from the fusion of the DRPE algorithm, the virtual PCI technique, and conventional compression algorithms. The compression method is applied to the sparse encrypted data of the PCI technique. We compute the nonlinear cross-correlation between the registered reference images and the compressed input images to verify the performance of the compression of double random phase-encoded images. This section shows quantitatively through experiments that considerable compression of the encrypted image data can be achieved while security and authentication factors are completely preserved.

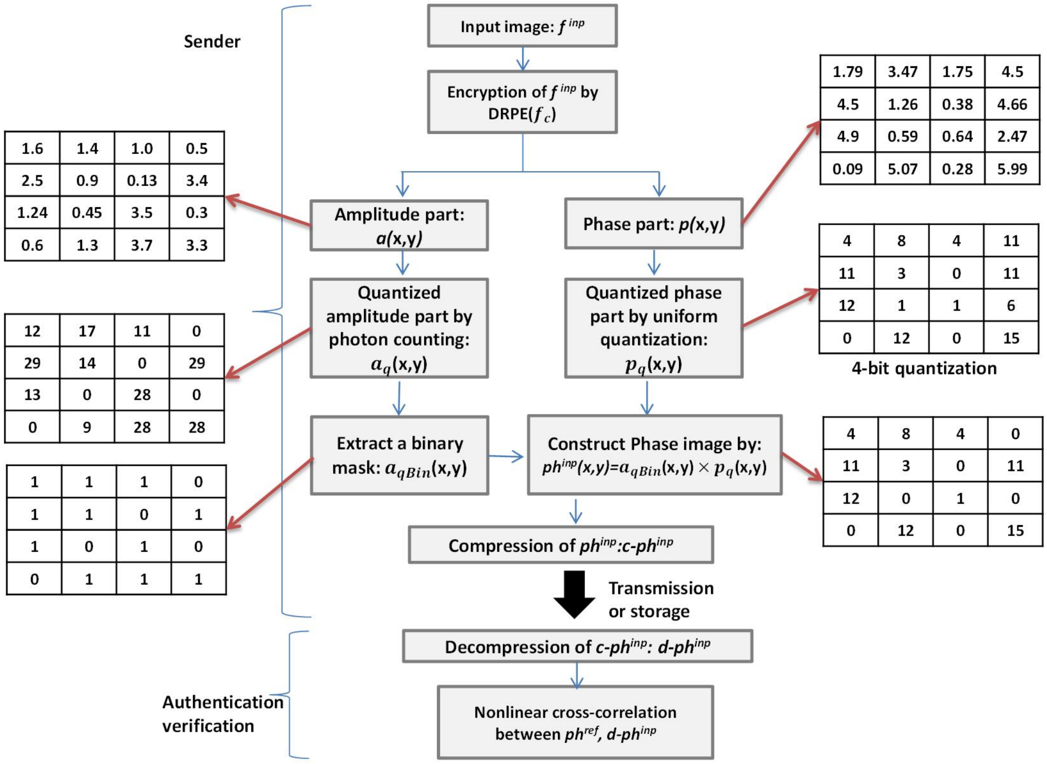
b. Motivations:

Referring to the DRPE concept, the input image is transformed into phase and amplitude objects. The storage space or transmission time required for these objects makes the DRPE method unsuitable for practical applications. Therefore, developing efficient compression schemes is essential for speeding up transmission time and decreasing the storage size of DRPE results. For compression methods, the JPEG has proposed many successful standards. The JPEG proposed many popular compression techniques for imaging applications. These techniques are used in applications ranging from the internet to digital photography and show good performance for the storage of many images in storage media elements [42-52].

The proposed method has several advantages. First, the complex images yielded by the proposed authentication procedures cannot be visually recognized because they contain photon-limited encrypted data, obtained by combining the DRPE and PCI methods. Second, by applying the proposed compression methods, the size of the encrypted images is reduced significantly without affecting authentication results. Finally, the photon-limited input phase image can be authenticated using a nonlinear cross-correlation metric.

c. Proposed compression scheme

In the proposed method, a quantization method based on the PCI technique is applied to the amplitude portion of the encrypted image (labeled as $a(x, y)$), $f_c(x,y)$ obtained from DRPE. The virtual PCI technique changes the pixel values in $a(x, y)$ to zero or very small values. The phase portion $p(x, y)$ obtained from DRPE contains real value in the range $[-\pi, \pi]$. Thus, $p(x, y)$ is converted into quantized values through a uniform quantization method similar to that used in [15]. The number of bits used for the uniform quantization process determines the quantized integer range. In this study, two-bit and four-bit quantization processes are considered. To construct a phase image, a binary mask of the photon-limited amplitude portion can be directly multiplied by the quantized phase values. The entry for each binary mask is unity if the corresponding photon limited amplitude portion is a nonzero value; otherwise, the entry is zero. Finally, the JPEG and JP2K compression techniques are applied to the new phase image obtained by using the binary mask and uniform quantization [see Fig.3.2].


Sender
Input image: f^{inp}
Encryption of f^{inp} by DRPE(f_c)
Amplitude part: a(x,y)
Phase part: p(x,y)
Quantized amplitude part by photon counting: a_q(x,y)
Quantized phase part by uniform quantization: p_q(x,y)
4-bit quantization
Extract a binary mask: a_{qBin}(x,y)
Construct Phase image by: ph^{inp}(x,y)=a_{qBin}(x,y) × p_q(x,y)
Compression of ph^{inp}:c-ph^{inp}
Transmission or storage
Decompression of c-ph^{inp}: d-ph^{inp}
Authentication verification
Nonlinear cross-correlation between ph^{ref}, d-ph^{inp}

1.6	1.4	1.0	0.5
2.5	0.9	0.13	3.4
1.24	0.45	3.5	0.3
0.6	1.3	3.7	3.3

12	17	11	0
29	14	0	29
13	0	28	0
0	9	28	28

1	1	1	0
1	1	0	1
1	0	1	0
0	1	1	1

1.79	3.47	1.75	4.5
4.5	1.26	0.38	4.66
4.9	0.59	0.64	2.47
0.09	5.07	0.28	5.99

4	8	4	11
11	3	0	11
12	1	1	6
0	12	0	15

4	8	4	0
11	3	0	11
12	0	1	0
0	12	0	15

Figure 3.2: The conceptual scheme of the proposed method. The method is composed of two main steps: the DRPE-based encrypted image compression and image authentication verification.

Although the amplitude portion *a(x, y)* of the input image is not sent during the transmission, the new phase image can still be verified in the authentication step. It should be mentioned that authentication verification rejects false input images when their PCE is smaller than 0.1. The authentication system or receiver decompresses the compressed phase images for the performance evaluation of the proposed compression schemes. Because the decrypted images from the proposed procedure are not visually recognizable, it is necessary to adopt a comparison scheme to authenticate the retrieved images. In this study, nonlinear cross-correlation (NCC) is used to compare the reference image to the input image, which has a different photon-limited amplitude mask from that of the reference image (see Fig. 3.2) [15, 23].

Our proposed image authentication schemes efficiently compress the DRPE-encrypted images, store the compressed images in the authentication system, and utilize the decompressed images for private user image verification. It should be noted that it is likely a bad idea to directly store original images as a reference in a system for verifying personal user images because these images would be prime targets for attackers or malicious system administrators. Therefore, another advantage of the proposed approach is that, even if attackers or malicious administrators invade the system, they cannot obtain the original user images because our method utilizes efficiently compressed DRPE-encrypted images, rather than storing raw images (or original images) for user image verification.

d. Numerical simulation

The test images (256×256 pixels) shown in Fig. 3.1 are used to evaluate the proposed image authentication schemes. In the following experiments, the reference image is “Peppers”. Two input images are selected to be authenticated. For the true input image, “Peppers” is selected and for the false input image, “Cameraman” is considered. There is a full implementation of JP2K available in a low-level C API under a BSD 2-clause license (Version 2.1.0). We downloaded and used this source code with some minor changes based on our data types and the experiments we wished to perform.

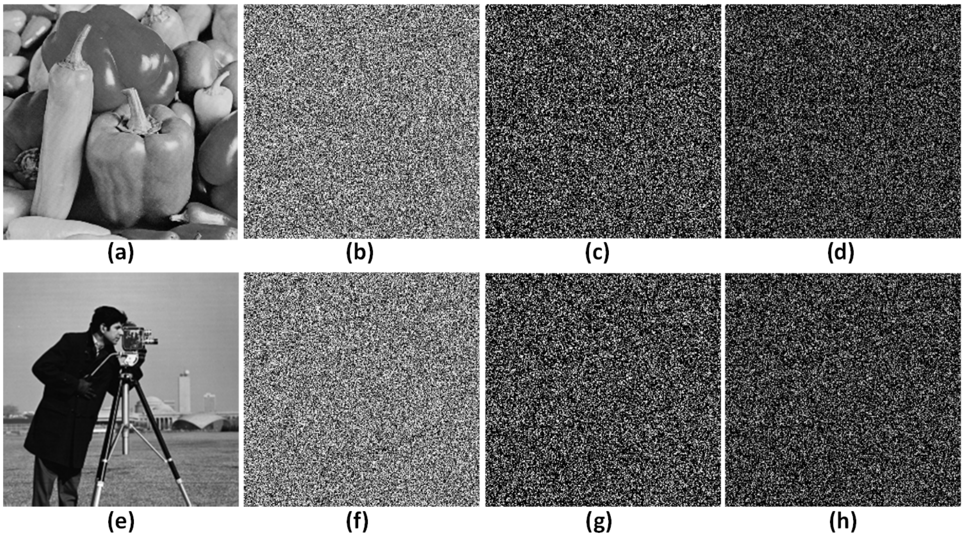


Figure 3.3: Two test images used in our numerical experiments: (a) Peppers (reference image and true input image), (b) phase values after DRPE, (c) phase image obtained by the proposed method, (d) phase image after compression and decompression (JP2K technique; CR = 64), (e) Cameraman (false input image), (f) phase values after DRPE, (g) phase image obtained by the proposed method, (h) phase image after compression and decompression(JP2K technique; CR=64).

In the following simulation, the lossy compression of JPEG and JP2K are tested on phase images from the DRPE-PCI scheme with various N_p and quantization bit sizes (n_k= 2 and n_k = 4 bits). We attempt to obtain the highest possible compression ratio without losing authentication efficiency. The compression ratio (CR) in this research is defined as:

$$CR = \frac{Size\ of\ \ the\ unquantized\ \ phase\ image}{Size\ of\ \ the\ compressed\ \ phase\ image}. \tag{1}$$

Figure 3.3 (b) shows the phase portion (*p(x, y)*) of the encrypted Peppers image (Fig. 3.3 (a)) from DRPE. The phase image of Peppers, as it has been explained previously, is shown in Fig. 3.3 (c). Figure 3.3 (d) shows the phase image after applying compression and decompression using JP2K. Based on the properties of PCI, it is difficult to reconstruct a reference image after applying the PCI algorithm. Therefore, PCE is used for authentication between the reference image and input image.

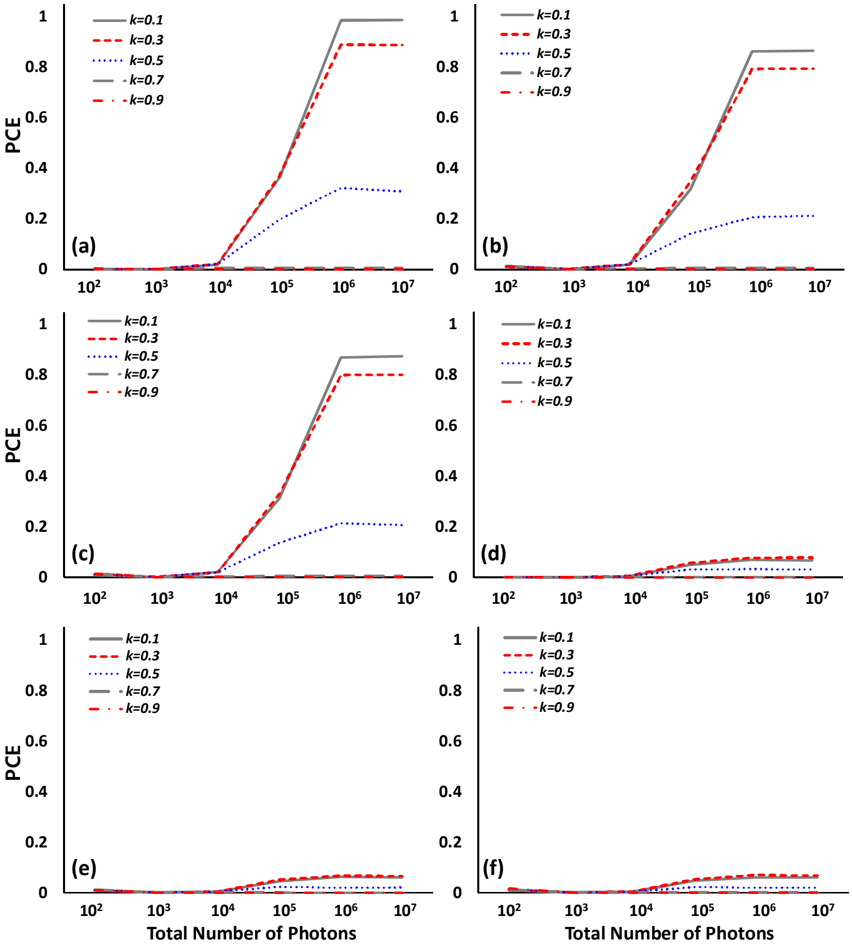


Figure 3.4: PCE with various k and N_p values: (a) without compression for the true class (Peppers). (b) applying JPEG compression for the true class (Peppers), (c) applying JP2K compression for the true class (Peppers), (d) without compression for the false class (Cameraman), (e) applying JPEG compression for the false class (Cameraman), (f) applying JP2K compression for the false class (Cameraman, CR is approximately 64 for the case of N_P>=10^5; n_k=2).

Figure 3.4(a), (b), and (c) plot the PCEs of non-compressed images and compressed phase images using the JPEG and JP2K methods, respectively. It has been demonstrated that PCE increases with an increase in the expected number of photons for the true class, particularly when $N_p > 10^5$. As expected, PCE values are near 1 when the parameter k is equal to 0.1. It can be seen in Figs. 3.4 (d), (e), and (f) that PCE is less than 0.1 in false input images, even when increasing the total number of photons. We observe from Fig. 3.4 that PCE values have nearly the same trends in non-compressed and compressed images. In this case, the quantization bit size for the phase value is set to 2 bits.

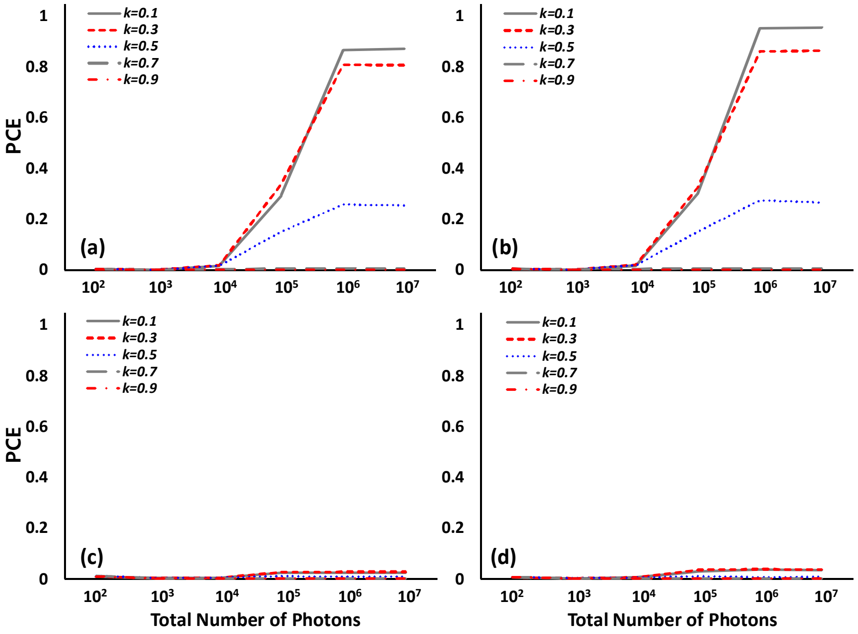


Figure 3.5: Experimental results (PCE) with various k and N_p values: (a) applying JPEG compression for the true class (Peppers), (b) applying JP2K compression for the true class (Peppers), (c) applying JPEG compression for the false class (Cameraman), (d) applying JP2K compression for the false class (Cameraman, CR is approximately 64 for the case of $N_P >= 10^5$; $n_k=2$).

According to Figs.3.5(a) and (b) (the results of 4-bit quantization), when increasing the total number of photons ($N_p >= 10^5$), the PCEs of the compressed phase images using the JPEG and JP2K methods increase similar to Figs. 3.4(b) and (c). Additionally, one can see from Figs. 3.5(c) and (d) that both JPEG and JP2K yield similar PCE results in cases with a false input image. Furthermore, PCE in JP2K is marginally larger than the same value in JPEG in the case of true class input. It specifies that JP2K has less information lost comparing with the JPEG method.

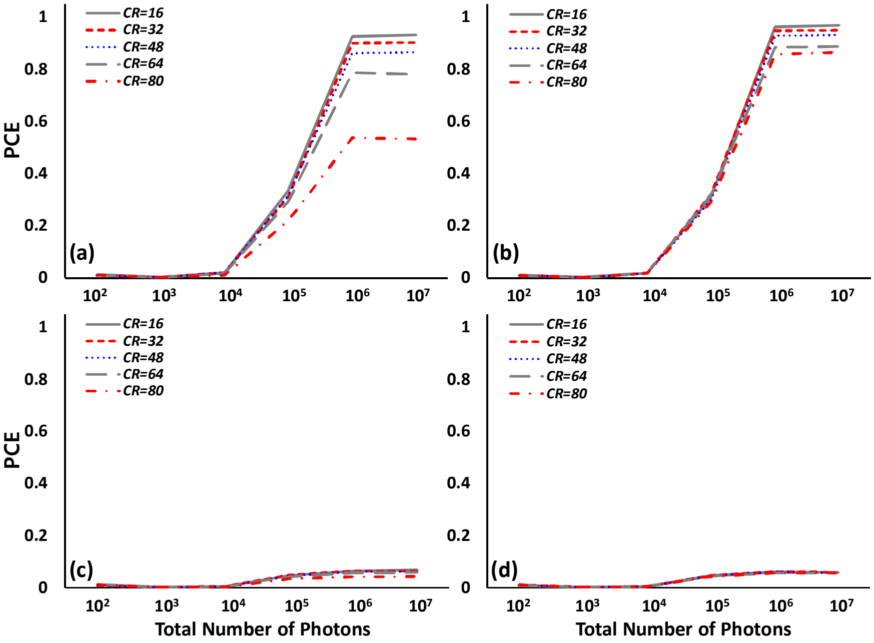


Figure 3.6: Experimental results (PCE) with various CR and Np values: (a) applying JPEG compression for the true class (Peppers), (b) applying JP2K compression for the true class (Peppers), (c) applying JPEG compression for the false class (Cameraman), (d) applying JP2K compression for the false class (Cameraman, $n_k = 2$, k is 0.1).

Figures 3.6(a) and (b) show the PCE changes when applying JPEG and JP2K with various CR and N_p values when n_k = 2. It is observed that by increasing N_p, PCE is also increased in both graphs. Also, the authentication strategy rejects false input images because PCE is far below 0.1, as shown in Figs. 3.6(c) and (d). It is worth noting that throughout the experiments, the random phase values (keys) used for encryption of the input images are assumed to be equal to those used for the reference images. Otherwise, the PCE value falls dramatically.

Additionally, we tested the true input image with a photon-limited amplitude mask equal to that of the reference image in two cases of non-compressed (Fig.3.7(a)) and compressed ones (Fig.3.7(b)). As has been expected, PCE values are around 1 when the parameter k value is equal to 0. The trend in both figures is similar and shows that applying compression does not degrade the phase image significantly.

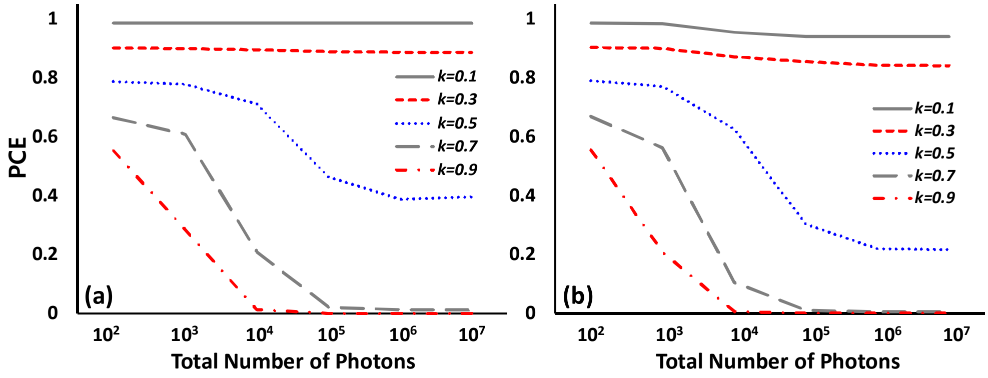


Figure 3.7: Experimental results (PCE) with various k and Np values: (a) without compression for the true class (Peppers), (b) applying JP2K compression for the true class. (Reference and true input images have the same photon-limited amplitude mask, CR is approximately 64 for the case of $N_P >= 10^5$; $n_k = 2$).

We are also interested in measuring the size of phase images compared to original gray-scale images (without applying any image encryption or compression techniques) to determine the compression gain (we call it true compression gain or TCG) of the proposed technique. The true compression gain can be obtained by:

$$TCG = \frac{Size\ of\ \ gray\ scale\ image}{Size\ of\ \ the\ compressed\ \ phase\ image}, \qquad (2)$$

Figure3.8 shows PCE, CR, and TCG values for n_k = 1, 2, and 4 in black, blue, and red lines, respectively. TCG values are indicated by the labels on the graph. The test image was

Peppers. Various CR values were evaluated. The y-axis of the graph shows PCE changes and the x-axis represents various CR values (calculated using Eq.1). We can see that 4-bit quantization has the highest PCE values, but the lowest TCG values due to the usage of 4 bits.

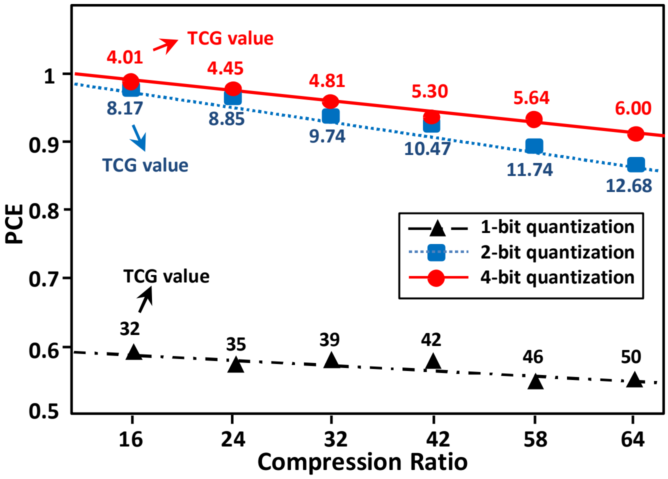


Figure 3.8: PCE after applying JP2K compression for the true input image (Peppers) with $N_p = 6 \times 10^6$ and various CRs, $n_k = 1$, 2, and 4.

It can be observed that by using the compression methods the PCE is marginally similar to the non-compressed scheme. Indeed, we can claim that JP2k marginally outperforms JPEG if PCE is the main concern. Also, it worth to mention the proposed authentication system, not only resist against unauthorized attacks but also has influenced to decrease the size of the encrypted image by combining the compression method and PCI.

e. Conclusion

This study aimed to provide a comparative evaluation and assessment of JPEG and JP2K compression algorithm performance on the quantized phase images from DRPE-PCI using various numbers of photons from the perspective of authentication efficiency. The proposed technique considers not only quantized phase values but also a binary mask of photon-counted amplitude values. This study demonstrated that as far as lossy compression is concerned, JP2K seems to perform reasonably well in terms of its ability to efficiently handle various CRs. The results for the JP2K method showed that phase images can be compressed several times while still allowing images to be verified using a nonlinear cross-correlation technique.

B. Double Random Phase Encoding Scheme based on Dynamic Chaotic Map for Efficient Image Cryptography

a. Abstract:

In this section, chaotic dynamic mapping and DRPE are combined to not only decrease key size but also enhance the security in the numerical implementation of the conventional DRPE technique. To accomplish this, a Lorenz system and 32 eight-bit external keys (16 keys for each phase mask) are used to generate chaotic random phase masks. The initial condition of the Lorenz system is the plain text itself. Then, the CPMs replace the original RPMs in the DRPE scheme. The PCE between the encrypted input image and the encrypted reference image in the database can verify the permission. The experiments reveal that the proposed scheme is highly sensitive to the key changes and good resistance against statistical attacks.

b. Motivation:

The main motivation of the proposed method is to generate a differentiable phase mask to be used in conventional DRPE. This has led us to propose Chaotic-DRPE in which some fixed keys along with the content of the image can produce different phase masks for different images. Therefore, even by decreasing the size of keys the security of the conventional DRPE encryption method is not disturbed due to that encryption scheme is still the same though RPMs are generated dynamically by the chaotic method. One major advantage of chaotic-DRPE is that the key size is independent of the input image size. Secondly, the key size is always fixed and is far smaller than that of the conventional DRPE method. Thirdly, cracking or hacking the keys become infeasible even though DRPE is vulnerable against attacks of chosen-ciphertext and known-plaintext attacks [37, 39]. The introduced phase masks generated by the chaotic system can assure the security of the system.

c. Chaotic-DRPE

As can be seen in Eq. (3), during the implementation of DRPE, the chaotic method was applied for generating the CPMs. In this method, the input image first passes through the first chaotic mask and then passes through the 2D FT that is achieved by the first lens. In the next step, the output of the previous part is multiplied by the second chaotic mask. Finally, a second lens, which acts like an IFT, converts the image back to the spatial domain. In the proposed scheme, pixel values are converted to complex numbers with amplitude and phase information.

$$f_c(x,y) = \Im^{-1}[\Im[f(x,y)\exp(j2\pi CPM_1(x,y))]\exp(j2\pi CPM_2(u,v))], \qquad (3)$$

To apply the proposed encryption, *CPM₁* and *CPM₂* are extracted from the initial condition (the input image) and from the 16 eight-bit keys (shown in Fig. 2.3). Figure 3.9 shows the overall scheme of the proposed chaotic-DRPE system.

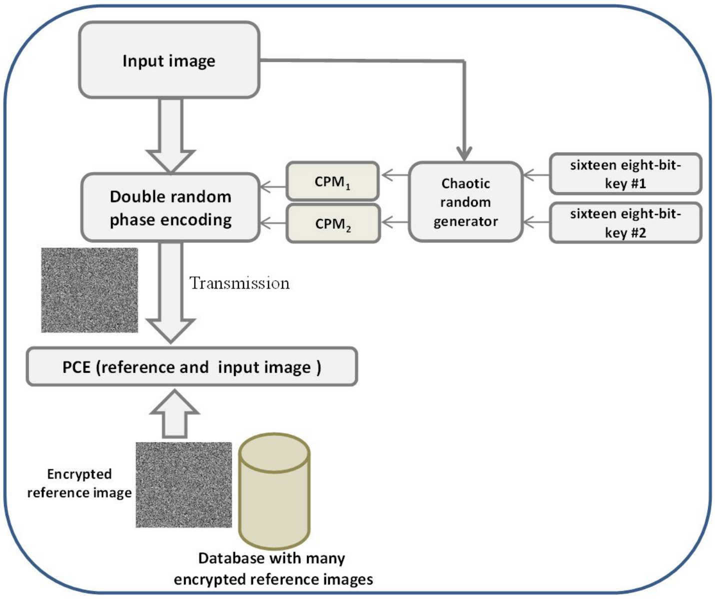

Input image
Double random phase encoding
CPM_1
CPM_2
Chaotic random generator
sixteen eight-bit-key #1
sixteen eight-bit-key #2
Transmission
PCE (reference and input image)
Encrypted reference image
Database with many encrypted reference images

Figure 3.9: Scheme of the proposed compact authentication scheme. The reference images are encrypted and then stored in the database with the chaotic keys given the first time to the newly defined user in the system.

To generate encrypted reference images, one image of the authorized user is taken once he is introduced into the system. This image and one chaotic key, which will be used with this user for future verification, are fed into the encryption system. Eventually, the encrypted content is stored in the database. Therefore, the database does not require to keep input image and chaotic key.

d. Experimental Result and Discussion

To verify the validity of the proposed method, two versions of the images shown in Fig. 3.1 are used; 50×50 and 256×256 pixels. The authentication between the reference image and the input image is evaluated by PCE for various values of *k*. The reference images are encrypted and stored in a secure database with the chaotic keys that are given to the user. Thus, by applying PCE, the input image can be verified without decoding. One main advantage of the authentication method is that the encrypted image is dependent on both the input image and the chaotic keys (initial seeds). Any changes in the input image or chaotic keys alter the content of encrypted data. Figure. 3.10 shows the results of the proposed efficient cryptography system.

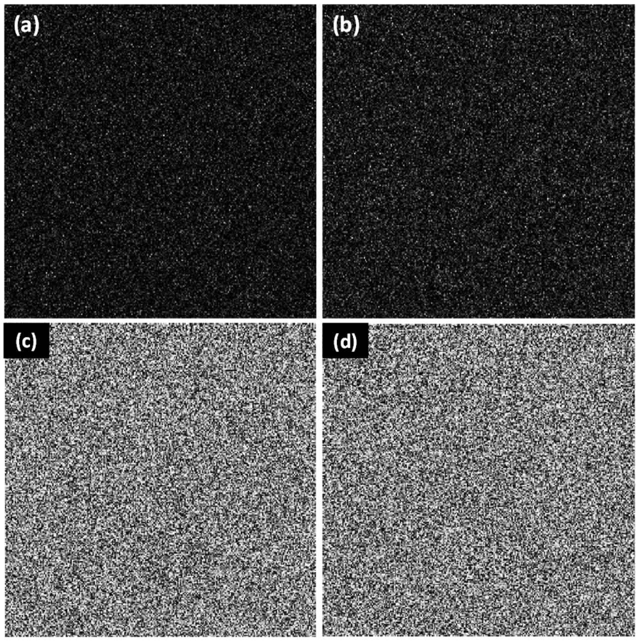


Figure 3.10: Amplitude part of encrypting image by the chaotic-DRPE method: (a) Peppers, (b) Cameraman and (c) and (d) respectively show the phase part of Peppers and Cameraman.

Table.3.1 shows the PCE results of the chaotic-DRPE for the Peppers image for both true (Peppers) and false input (Cameraman) images. From examining the results, it turns out that the PCE in the true input image is about 0.94 for *k* = 0.2 while this value decreases near 0.17 in the false input image (see Table 3.1). Furthermore, when the size of the image is 256×256, the size of the key in the RPM is a 2×256×256 float-value while the size of the key in chaotic-DRPE is 2×16 bytes. Using the chaotic method in DRPE has several advantages but the most important one is that we only need to store 32 eight-bit keys. As compared to the RPM that needs 2×256×256 float-value keys (depending on the size of the image), it is significantly better in terms of saving memory while being independent of the image size.

Table 3.1: PCE results by applying CPM and RPM in DRPE for the true and false input image for various *k*.

Image size	Input type	Random phase generation technique	PCE *k*=0	PCE *k*=0.2	Key size
50×50	PCE (true input)	Chaotic	1	0.94	2×16 bytes
	PCE (false input)	Chaotic	0.17	0.17	2×16 byte
	PCE (true input)	RPM	1	0.94	2×50×50 floats
	PCE (false input)	RPM	0.15	0.14	2×50×50 floats
256×256	PCE (true input)	Chaotic	1	0.94	2×16 byte
	PCE (false input)	Chaotic	0.15	0.18	2×16 byte
	PCE (true input)	RPM	1	0.94	2×256×256 floats

To verify the method, histograms are obtained and correlation coefficients are measured. Figure 3.11 depicts the histograms of the original image and two CPMs. As shown, the histogram of the original image is significantly different from the CPMs' histogram. The CPM histograms are nearly uniformly distributed, which indicates that they can protect well the information of the image from a statistical attack.

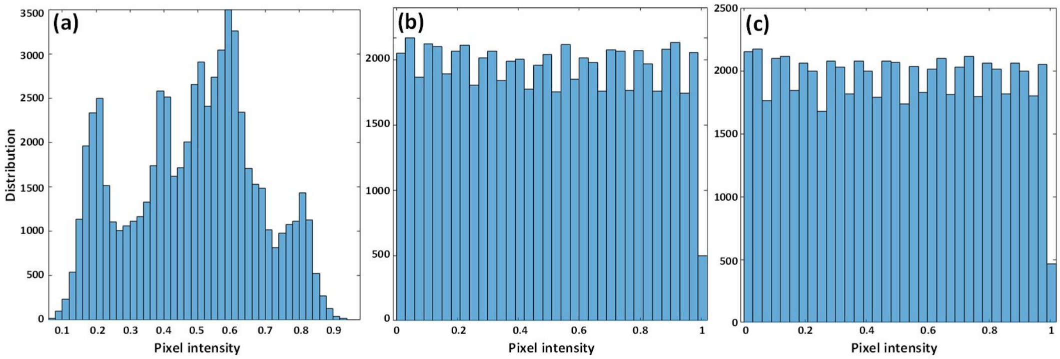


Figure 3.11: (a) Histogram of the plaintext image, (b) histogram of the first chaotic mask, (c) histogram of the second chaotic mask.

The correlation coefficient of the pixel pair of Peppers image and CPMs with the two secret keys 'A1C2B4M9$#*-OP2/' and 'MNO123+-/][ABD>1' in the horizontal, vertical, and diagonal directions are calculated. The correlation coefficient results are listed in Table.3.2. It is evident that two adjacent pixels from the CPM have a negligible correlation while two adjacent pixels in the plain image have a high correlation. Fig.3.12 displays correlation analysis figures of the plain image as well as both CPM. These figures provide additional evidence for the claim that neighboring pixels of CPM do not have a relationship.

Table 3.2: Correlation coefficients for two adjacent pixels in plain image, first and second chaotic maps.

Direction	Plain image (Peppers)	First key	Second key
Horizontal	0.8907	0.0002	0.0015

Vertical	0.7252	0.0072	0.0018
Diagonal	0.5728	0.0123	0.0173

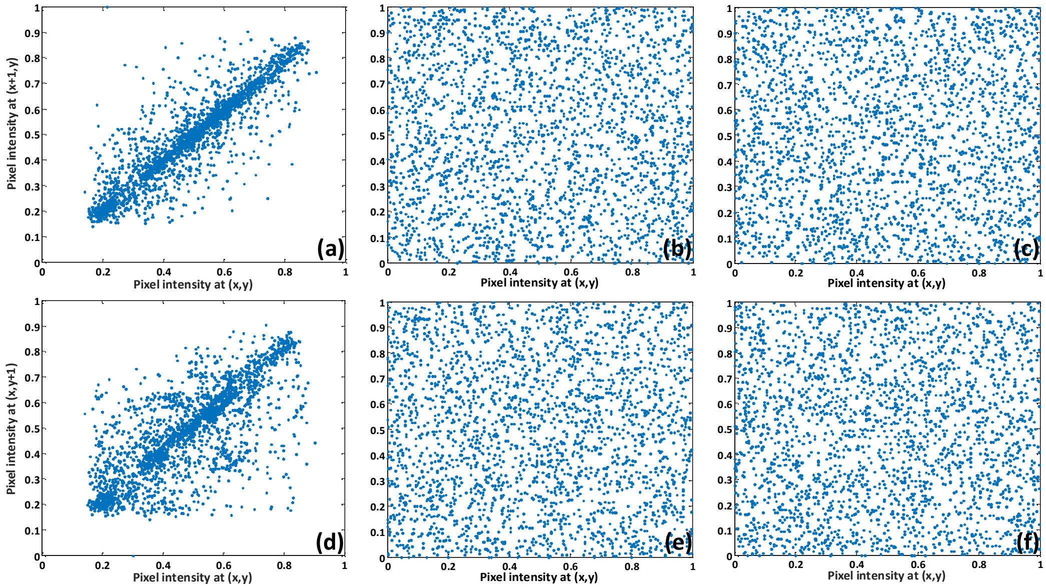


Figure 3.12: Correlation analysis (a) between plain image (pixels located at (x, x+1)), (b) between first chaotic mask (pixels located at (x, x+1)), (c) between second chaotic mask (pixels located at (x, x+1)), (d) between plain image (pixels located at (y, y+1)), (e) between first chaotic mask (pixels located at (y, y+1)), (f) between second chaotic mask (pixels located at (y, y+1)).

As mentioned, we believe that the cipher image is too sensitive to the keys. As can be seen in Fig. 3.13(a), by using a different key or a false input image, the PCE drops dramatically. Furthermore, for proving the relationship between keys and the cipher image, the avalanche effect can measure the dependency between cipher image and keys. Usually, the avalanche effect is applied to show the difference between two plain images and their corresponding cipher image. From the point of view of an encryption algorithm, an avalanche effect is evident if a small change in the plaintext or key causes a large change in the cipher-text [36]. According to the avalanche effect concept, low avalanche value represents that the designed algorithm suffers from poor randomization hence could be considered insecure. Due to this weakness, the algorithm cannot endure statistical attacks [55]. If we take the Hamming distance between the original text *f(x, y)* and the ciphertext *f′(x, y)* (which we obtain by encrypting after changing some bits of the original plaintext or key) to be *H*(*f(x, y)*, *f′(x, y)*), then the avalanche effect can be calculated from the following equation:

$$Avalanche = \frac{H(f(x,y), f'(x,y))}{Num(Y)}, \tag{4}$$

where *Num(Y)* denotes the total number of binary bits of the ciphertext. According to the avalanche property, a desirable aspect of the chaotic method should be one wherein a small change in either the plaintext or the key produces a significant change in the ciphertext [36, 55-56]. In the following avalanche evaluation, CPMs are generated by changing bits of the key from 1 to 128 bits (16 bytes). As can be seen in Fig. 3.13(b), the minor change in the secret keys results in significant changes in the cipher image.

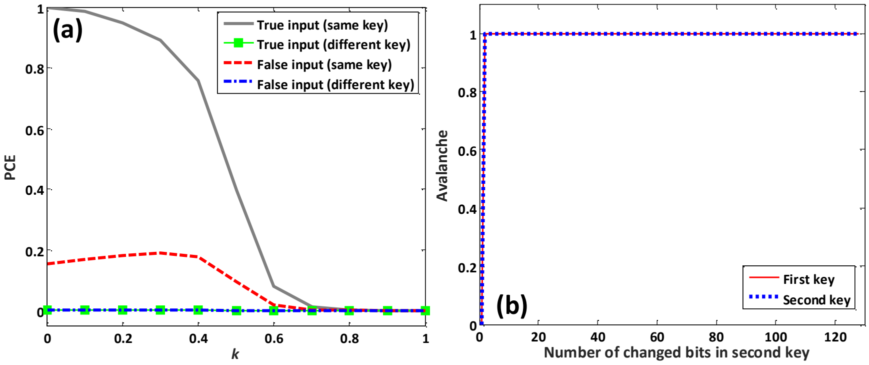


Figure 3.13: (a) PCE for different *k* values (b) avalanche between reference and input image by varying bits of the keys (first and second key) from 1 to 128 bits for the first CPM.

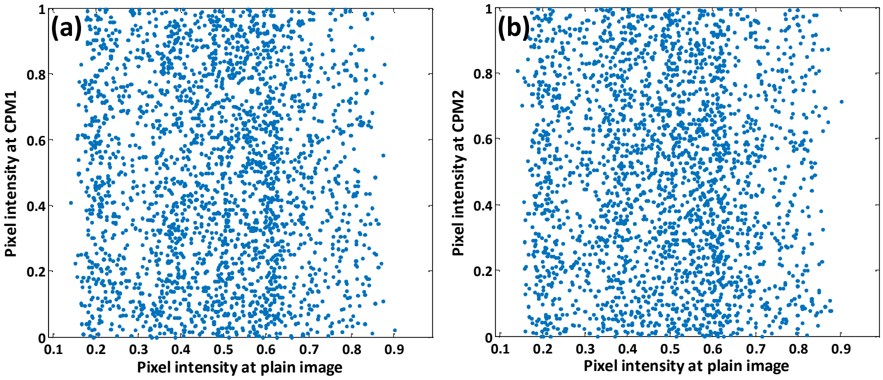


Figure 3.14: (a) Correlation analysis of plain image and CPM_1 (correlation coefficient is 0.011), (b) Correlation analysis of plain image and CPM_2 (correlation coefficient is 0.015).

In addition, the correlation analysis results between the plain image and both CPMs are shown in Fig.3.14. As can be seen, the plain image and the CPMs have a negligible correlation. We also analyzed the statistical properties of the chaotic phase mask itself. Since the conventional random numbers utilized in DRPE are uniformly distributed, we evaluated the properties of the CPM and compared it with those of the conventional random generator. Table.3.3 shows the results of the analysis.

Table 3.3: Statistical properties of the conventional random distribution, CPM1 and CPM2 (n=256×256, mean and variance values for uniform distribution are 0.5, the variance is 0.0833, skewness is close to zero, and entropy for CPM should be close to 8 bits)

	Mean	Median	Variance	Skewness	Entropy
Conventional Random Generator	0.49	0.49	0.083	0.006	Nan
CPM_1	0.49	0.49	0.084	0.031	7.99
CPM_2	0.49	0.49	0.084	0.018	7.93

e. Attack Resistance

Chosen-ciphertext attack

In DRPE, the second lens cannot provide any security contribution and, having the final ciphertext, it is always possible to compute an FT to reverse this operation. Accordingly, we can retrieve the second phase mask by chosen-ciphertext attack [39,40] as follows:

$$\begin{aligned} f_c[\delta(x,y)] &= \exp(j2\pi\varphi_2(u,v))\Im[\delta(x,y)\exp(j2\pi\varphi_1(x,y)] \\ &= \exp(j2\pi\varphi_2(u,v))\Im[\delta(x,y)\exp(j2\pi\varphi_1(0,0)] \\ &= \exp(j2\pi\varphi_2(u,v))\exp(j2\pi\varphi_1(0,0)), \end{aligned} \tag{5}$$

where *(x, y)* are the spatial coordinates and *δ(x, y)* is the impulse distribution that is equal to 1 in (0, 0) and 0 in other pixels. Also, $R_1(0, 0)$ is the central value of the first CPM and *(u, v)* represents the coordinates in the Fourier domain. It demonstrates that the ciphertext of an impulse image in the Fourier domain is equal to the second key. Therefore, the opponent can easily recover the second key by encrypting an impulse image [39, 40]. The generated CPM according to the chaotic scheme can be mentioned as one effective means to protect the DRPE scheme. In this case, even if an intruder reveals the second phase mask according to Eq. (11), he is not able to use this phase mask to decode other encrypted images. The reason is nothing but the phase masks are generated by both plain text and user keys. Thus, knowing the phase mask of the impulse response cannot help the attacker to decode or encode other images. Since an attacker has access to the CPM, it must be computationally infeasible to determine the chaotic keys. In addition, this leaked CPM is not valid because CPM generation products different phase masks for different plaintexts as explained in Section 2.D. In hence, with access to the CPM, there isn't actually any useful information for an attacker to encrypt other images. They will still have to break each individual CPM for each individual encryption, which, as it stands right now, is an insurmountable task.

Resistance against different noise

To further evaluate the vulnerability of the proposed image cryptography scheme against different conditions, the performance of the chaotic-DRPE method is evaluated while the input image is distorted by adding different types of noises (Gaussian noise, salt-pepper noise, zeroing a portion of the image and compressing the image by JPEG compression). Figure 3.15-3.18 demonstrate the effects of different type of noises applied to the input image for *k*=0. These figures show the effects of Gaussian noise in the input image with different variance values (defines the strength of the noise), salt-pepper noise with different density values, zeroing portion of the image with different sizes and compressing the input image with different compression ratios, respectively. Figures 3.16 and 3.18 represent the PCE value against two parameters of *k* value which defines the density of the applied nonlinearity in the y-axis and noise parameter which is shown in the x-axis. As can be seen in all of the graphs, PCE is 1 for *k*=0 when the image is not exposed to any noise. We can see that, for all cases the PCE declines while the noise values or *k* value increase but the input image still can be verified since the PCE value for the false input image is around 0.2 (See Fig. 3.13(a)).

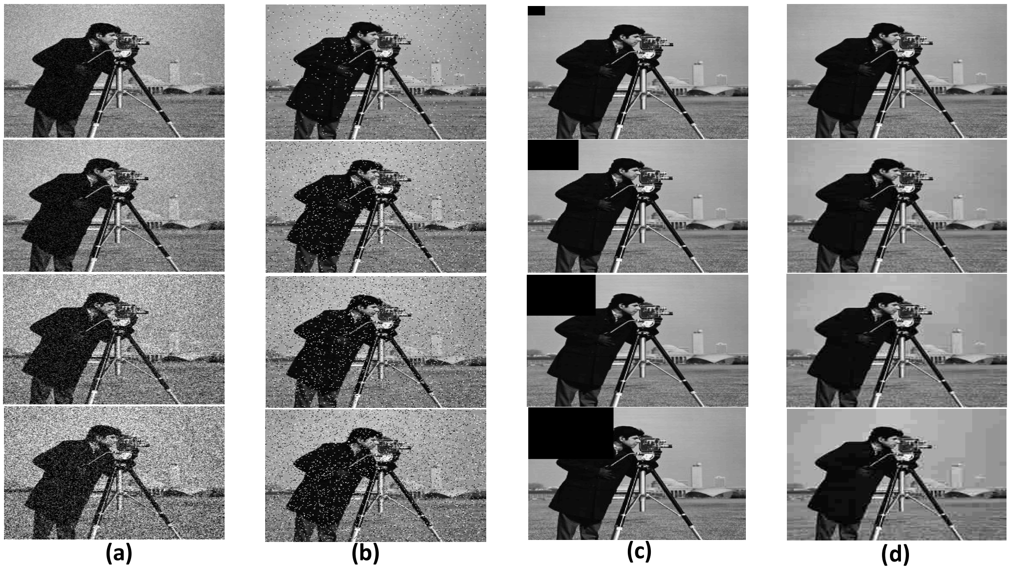


Figure 3.15: Input image distorted by different types of noise (a) Gaussian noise (mean value=0 and variance=0.005, 0.01, 0.03, 0.05), (b) Salt-pepper noise (density=0.02, 0.06, 0.08, 0.1), (c) zeroing image (area size=20×20, 60×60, 80×80, 100×100), (d) compression ratio (CR= 9.79, 24.64, 64.64, 83).

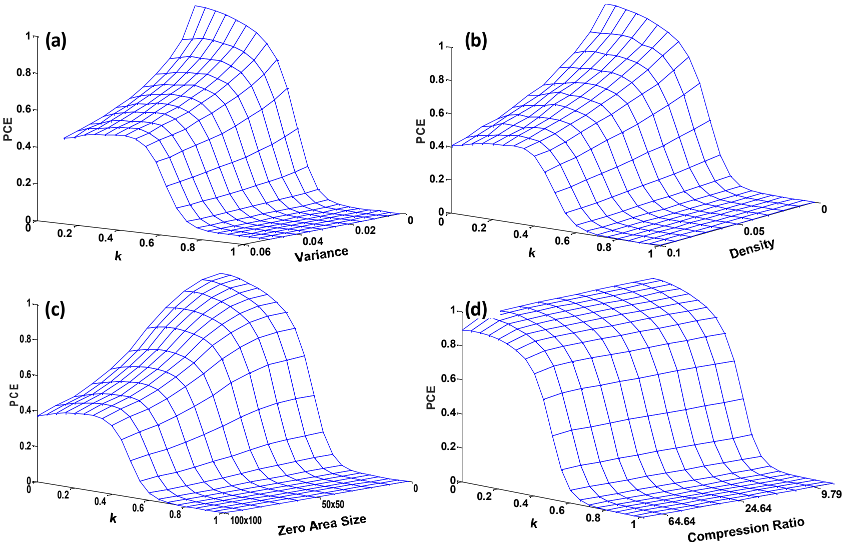


Figure 3.16: Simulation results for PCE between two chaotic-DRPE and input image(Cameraman) distorted by (a) Gaussian noise, (b) Salt and pepper noise, (c) Zeroing an area of the input image, (d) Applying JPEG compression

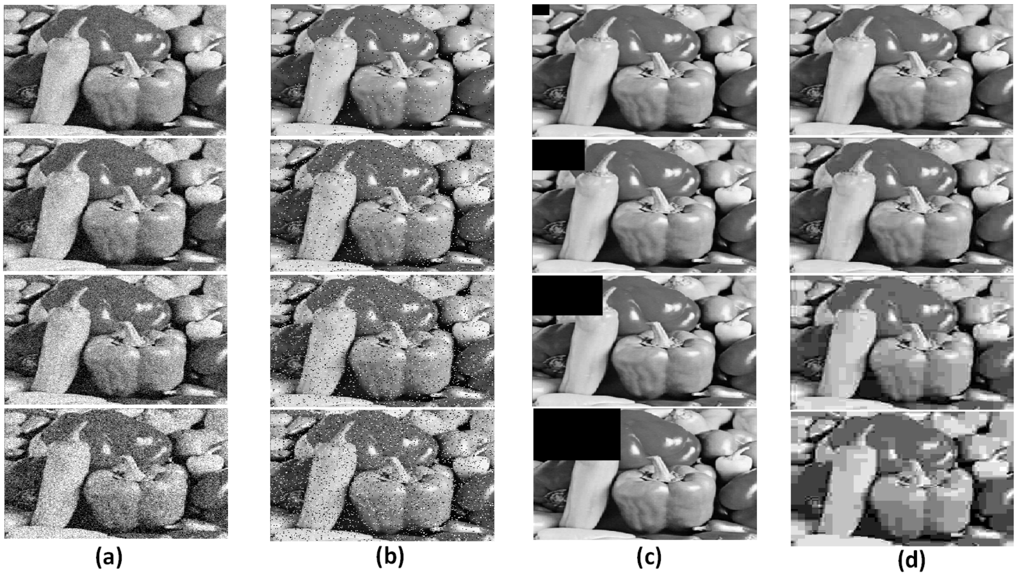


Figure 3.17: Input image distorted by different types of noise (a) Gaussian noise (mean value=0 and variance=0.005, 0.01, 0.03, 0.05), (b) Salt-pepper noise (density=0.02, 0.06, 0.08, 0.1), (c) zeroing image (area size=20×20, 60×60, 80×80, 100×100), (d) compression ratio (CR=11.1, 16.16, 38.8, 53.09).

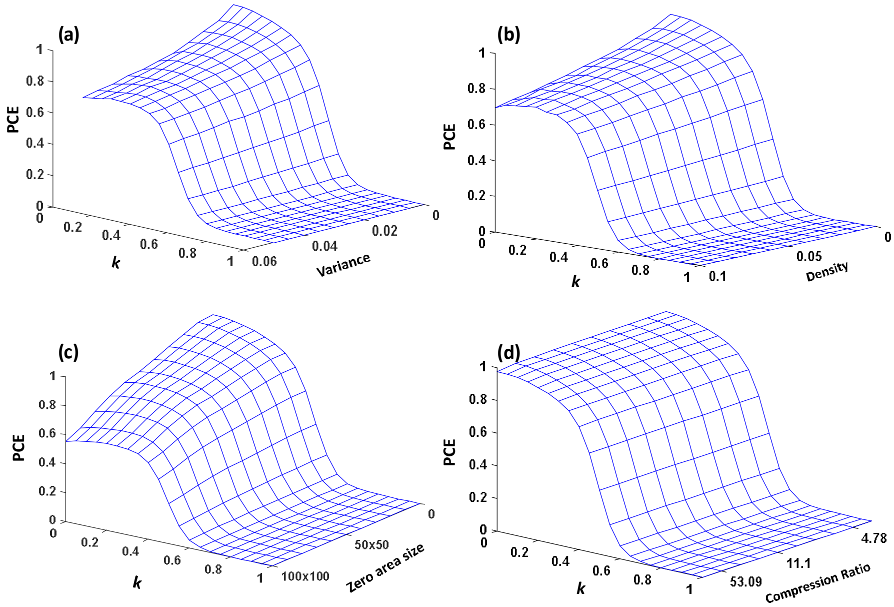


Figure 3.18: Simulation results for PCE between two chaotic-DRPE and input image(Peppers) distorted by (a) Gaussian noise, (b) Salt and pepper noise, (c) Zeroing an area of the input image, (d) Applying JPEG compression.

According to the results, the proposed method in comparison with the conventional DRPE algorithm requires less key and less space to store them. The conventional DRPE scheme for an image with a size of 256×256 requires 2×256×256 float value for the storage of keys. In comparison, the proposed method only requires 2×16 bytes of memory for saving the keys.

f. Conclusions

This study aims at modifying the DRPE method and introducing an efficient method under the objective of saving memory and enhancing the security of conventional DRPE. The results of the proposed method show that the chaotic method can be suitable for generating phase masks in DRPE. Introduced CPM not only can satisfy all of the properties of RPM but also it can overcome needing big RPM storage and secure transfers. With the help of chaotic mapping, the key size for generating the two random masks can be independent of the size of the image and can be constant for the entire images. In addition, DRPE is not vulnerable to chosen-ciphertext or known-plaintext attacks by using the dynamic chaos maps. The biggest advantage of the proposed method in authentication is that the encrypted content is dependent on both chaotic keys and the input image. Therefore, any changes in the input image or chaotic keys will alter the encrypted content and PCE value drops significantly.

4 Robust Encryption of Off-Axis Hologram by one-time Double Random Phase Mask Generation

a. Abstract and Motivations:

One of the most sought ways to take and record biological image is digital holographic in the microscopic configuration. Holography in the microscopic configuration by recording both the amplitude and phase of the interference light can reconstruct the shape of flat cells or semi-transparent internal subcellular structures. It is one of the most useful techniques with non-invasive and non-destructive capability in studying biological samples. Specifically, the off-axis holographic microscopy technique can be used to perform a quantitative analysis of the different types of cells since we can separate virtual image, real image and zero-order noise [57-62].

The security of biomedical images is an important issue in the field of image transmission, data storage since the donor or patient's private information should be kept secure regarding the privacy concerns. These images are the most important items in the area of studying sample, drug-delivery assess, healthcare diagnostic or procedures since they are used to observe the success of drug delivery, features of donors or patients such as cells, internal organs, and tissues. In addition, they are used to evaluate the patient and check the effects of the treatment or drug adversary effects on the sample. Therefore, protecting biomedical images from unauthorized access is essential. Among the classical optical encryption techniques, combining the DRPE method with the different chaotic methods and pixel scrambling techniques are suggested in different works [27-31]. The main reason to use a chaotic method is that it is free from statistical or mathematical weakness. Therefore, it has indirectly assisted in the development of encryption structures. DRPE combined with chaotic methods typically proposes replacing the ordinary phase values with another set of random values generated by a chaotic generator. By varying the keys (parameters of the chaotic system) related to the chaotic system, different random sequenced can be created. Although replacing ordinary RPM with chaotic-based phase mask (CPM) might be able to protect the encrypted image, still compromising private keys allows an attacker to build midway attacks to intercept and decrypt any encrypted image. Unfortunately, the attacker could also have recorded past encrypted image afterward, he can decrypt them by compromised key.

The principal motivation of this study is to extend the DRPE model for encrypting the hologram sample in order to protect them from long-term private key compromise attacks. Our encryption model is defined in the spirit of perfect forward secrecy (PFS [63-66] by limiting the adversary effects of breaking CPM. Historically, the term "perfect forward secrecy" was coined by C.G. Günther in 1989 to eliminate the cryptographic key problem [63]. Further, the PFS concept has been discussed in common method involved the key agreement protocols, user authentication, key authentication, e-mail system [64-69]. To the best of our knowledge, this is a first work that surveys the PFS to enhance the security of DRPE-based encoded biological hologram.

Several techniques are proposed to secure the holographic data [70-73]. In [73] it is shown that if an RPM virtually is attached to a 3-D object's hologram and then forced to be propagated by the Fresnel domain the result is completely white noise. Todays because of the vital importance of biomedical holograms, a robust and secure mechanism to exchange the holograms over the internet or safe storage is challenging and needs to be addressed. Most encryption techniques in the literature are dealing with two RPMs in the Fourier domain. In this work, we introduce a new method in which it uses only one phase mask but two times to encode the input hologram. This phase mask is generated by running a chaotic system with two input parameters of the secret key (we use secret chaotic key interchangeably) and a single salt value that is open to the public. Our proposed configuration provides maximum protection in terms of PFS. To enable PFS in the encryption-decryption scheme, the proposed method has to be able to use ephemeral keys which are erased from memory as soon as the generated the CPM is complete. This means during the encryption, new CPMs are constantly generated by a new set of keys for each and every new input hologram. Therefore, the compromise of a single CPM will not affect another encrypted hologram. If an intruder steals or reveals one set of key parameters, he is not successful in decrypting all holograms. The latest hologram gets compromised, but any encrypted hologram prior or after it can't be retrieved. This is due to that the phase generation parameters are never reused and should never be stored which offers the protection going forwards. This can boost the security of the classical optical encryption technique in different ways especially against chosen-plaintext or chosen-ciphertext attacks. Additionally, the new scheme, due to using keys with smaller sizes, is easier for key management, key transferring schemes. A value is assigned to the salt value and it is shared publicly to all users. This salt value defines a state of the chaotic system and the secret key will contribute to the randomization of the output values. This can implement forward secrecy to its full benefits. To decode the hologram authorized person uses the secret chaotic key and the shared salt value to generate the correct CPM.

In this work, after recording the biomedical sample in off-axis configuration by a CCD camera, the hologram is filtered in the frequency domain. The filtering allows us to keep the real image and rid of the zero-order noise and twin image in the reconstruction plane. Then, the real part of the Fourier-transformed hologram is distorted by the CPM generated by chaotic dynamic mapping with the non-secret salt value and the secret key. To accomplish chaotic mapping, one chaotic map and one secret key (16 eight-bit keys) are used to generate CPM. Thereupon, the CPM replaces the original RPM and inverse Fourier transformed applied on the phase-distorted hologram and is multiplied by the same CPM for the second time. Finally, the distorted image is forced by the Fresnel propagation to an arbitrary plane and a given wavelength encodes the distorted hologram into white noise.

The proposed method has several advantages. First and foremost the encrypted hologram can only be decrypted if the exact chaotic parameters, wavelength and propagation distance (related to the Fresnel propagation) are provided. This can enhance the security of the conventional optical encoding technique. The reason is nothing but the phase mask is generated according to the single salt value and secret chaotic key. Only those users with the knowledge of these values can generate correct CPM to decode the hologram. In many different cases, the hologram will be decoded wrongly and will not resemble the original hologram as will be shown in the following sections. Also, if at any case attacker obtains the random phase values by chosen-plane-text or chosen-ciphertext attacks, he will not be able to decode any other hologram since different phase mask is generated for different images. On top of these advantages, our proposed method can achieve PFS by using the initial salt value and secret interchangeably key in CPM generating process.

b. Background

Off-axis digital holography for biological sample recording:

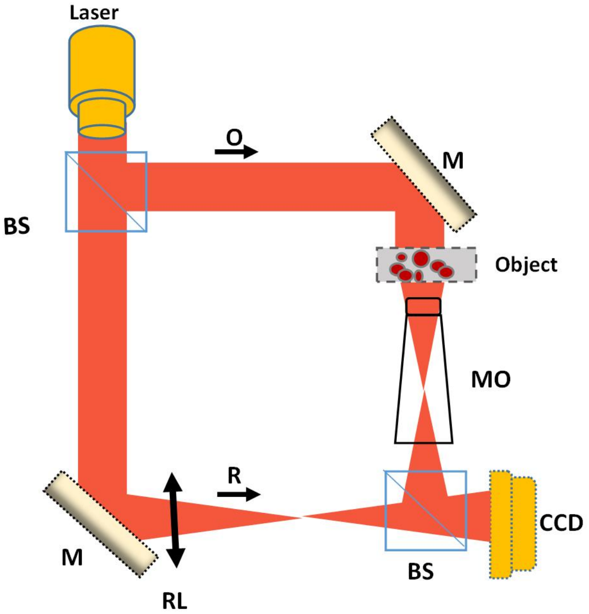


Figure 4.1: Simple representation of the off-axis digital holographic in the microscopic configuration used in this experiment to acquire biological hologram.

In this study, the off-axis device is based on a Mach–Zehnder interferometer, in which the coherent laser source is divided into an object and reference beams using a beam splitter (Fig. 4.1) with a small tilt angle between the two beams. The object beam illuminates the specimen and creates the object wavefront. A microscope objective (MO) magnifies the object wavefront, and the object and reference wavefronts are joined by a beam collector to create the hologram. The interferograms are recorded by a CCD camera (Fig.4.2a), to be transferred to a personal computer (PC) for numerical reconstruction. In the hologram plane *(x, y)*, interference between the object wave O and the plane reference wave R produces an intensity distribution, which is generally written as the sum of four terms:

$$I_H = I_r + I_o(x,y) + R^*O + O^*R, \tag{1}$$

where I_r is the intensity of the reference wave and I_o (x, y) is the intensity of the object wave. R^*O and RO^* represent the interference terms, with R^* and O^* denoting the complex conjugates of the two waves. Figure 4.2(b) shows that the small tilt angle between O and R that allows us to separate the real image, twin image, and zero-order noise with a proper spatial filter in the Fourier domain by following:

$$I_H^F = IFFT\left\{FFT(I_H)\times Filter\right\} = R^*O \tag{2}$$

Where FFT and IFFT respectively are Fourier and inverse Fourier transforms. The reconstruction of the complex amplitude image can be expressed by the Fresnel approximation, as follows:

$$\begin{aligned}\Psi\left(m,n\right) = A\Phi(m,n)\exp\left[\frac{i\pi}{\lambda d}\left(m^2\Delta\xi^2 + n^2\Delta\eta^2\right)\right]\times \\ FFT\left\{R_D\left(k,l\right)I_H^F\left(k,l\right))\times\exp\left[\frac{i\pi}{\lambda d}\left(k^2\Delta x^2 + l^2\Delta y^2\right)\right]\right\}_{m,n} ,\end{aligned} \tag{3}$$

Where A is complex constant factor, k, l, m, and n are integers ($-N/2 \le k, l, m, n \le N/2$; $N \times N$ is the number of pixels in the CCD camera, 1024 × 1024), R_D is the digital reference plane wave and $\Phi(m, n)$ is the digital phase mask calculated by [74-77]:

$$\Phi(m,n) = \exp\left[\frac{-i\pi}{\lambda D}\left(m^2\Delta\xi^2 + n^2\Delta\eta^2\right)\right], \tag{4}$$

The digital phase mask can resolve the phase aberrations caused by the MO in the object wave arm. Moreover, $\Delta\xi$ and $\Delta\eta$ are the sampling intervals in the observation plane, expressed by:

$$\Delta\xi = \Delta\eta = \frac{\lambda d}{N\Delta x}, \tag{5}$$

d is the distance between the camera plane and the observation plane or so-called digital propagation distance, and Δx is the pixel size in x direction. The adjustment of k_x, k_y, and D can be performed in the absence of fringes by removing the residual gradients or curvature of the reconstructed phase distribution in some areas of the image, i.e., where a constant phase is presumed. Since Ψ is in the form of a complex value, the phase image (Fig.4.2(c)) can be obtained by:

$$\phi(m,n)=\tan^{-1}\left\{\frac{\mathrm{Im}\left[\Psi(m,n)\right]}{\mathrm{Re}\left[\Psi(m,n)\right]}\right\}, \tag{6}$$

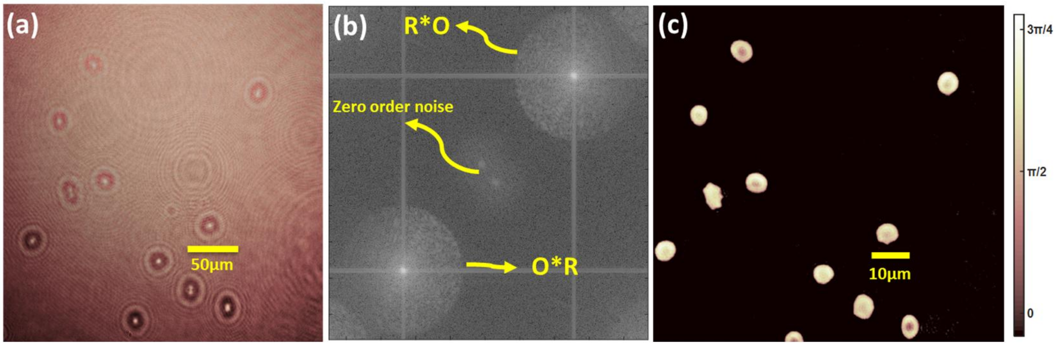


Figure 4.2: (a) A recorded hologram of human red blood cell by off-axis Digital holography configuration, (b) Fourier transform of the off-axis hologram, (c) phase image after numerical reconstruction.

CPM generation in PFS

Owing to chaotic features, including sensitivity to the initial conditions and control parameters it is a suitable and adaptable method in cryptography [33, 35]. The mathematical definition of a map is expressed below:

$$\begin{cases} x' = a(y-x) \\ y' = cx - xz - y, \\ z' = xy - bz \end{cases} \tag{7}$$

The Lorenz attractor should be set with specified values of $a = 10,\ b = 8/3,\ c = 28$ to be in the chaotic state. Figure. 4.3 illustrates the mask generation process by using the Lorenz map with a secret key and salt value. The generation of the chaotic random maps principally depends on the initial values of *(x,y,z)* and the iteration number *R*. The procedure initiates by using the new secret keys (for each CPM generation) to generate the initial values (*x, y, z* and the iteration number R_1) for running the chaotic system mentioned in Eq. (7). The generation of new CPM values depends on the previously generated CPM value and the iteration values except for the first CPM value. The first CPM value is produced by the salt value that will be explained more in the following. The other runs, that is equal to the number of pixels in the image, and the previously generated numbers (*x, y, z*, and the new iteration number R_i) produce the chaotic phase maps for the DRPE scheme.

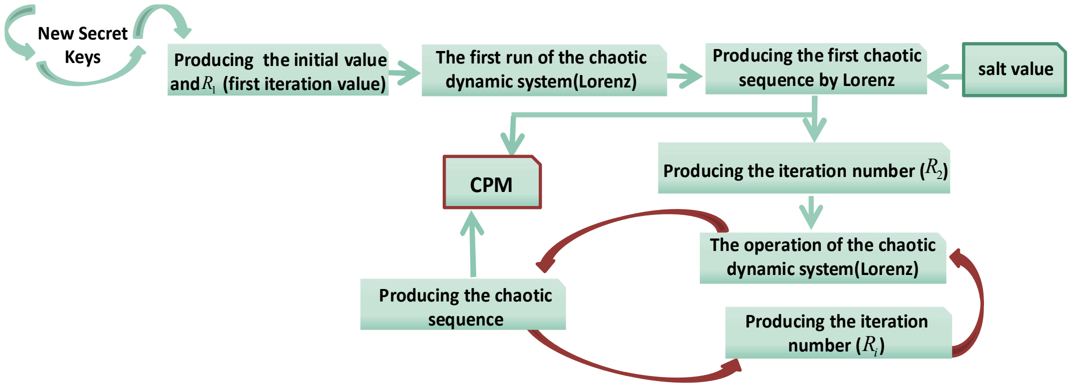

New Secret Keys
Producing the initial value and R_1 (first iteration value)
The first run of the chaotic dynamic system(Lorenz)
Producing the first chaotic sequence by Lorenz
salt value
CPM
Producing the iteration number (R_2)
The operation of the chaotic dynamic system(Lorenz)
Producing the chaotic sequence
Producing the iteration number (R_i)

Figure 4.3: Scheme of the proposed chaotic system for the generation of chaotic phase masks.

For making a process easier to understand, Fig. 4.4 presents a step by step diagram for CPM generation with the non-secret salt value. The secret key is specified by the red rectangle in the first step that is $K=K_1K_2\ldots K_{16}$, where the "*K*"s are 16 eight-bit keys. In this phase mask generation strategies, the secret key is unique for each time the process starts. Three real numbers $x, y, z \in [0, 1]$ are acquired by the first step. Also, R_1 is the first iteration of the mixed chaotic dynamic systems. In Step#2, the Lorenz system iterates T_1 times and procreate x_0, y_0, z_0 is the real initial values of the chaotic dynamic system. In Step #3, depending on the value of R_1 and the values (x_0, y_0, z_0), we acquire (x_1, y_1, z_1), which are the initial values for the next iteration in the chaotic dynamic system. In the following to present the main loop, the steps that should be repeated for generating CPM, placed on a red circle. Before the next step, the condition for determining the *"M"* value is checked. "*M"* value is a variable that plays a significant role in determining the next iteration time. Base on the number of the loop, *"M"* can be salt value otherwise it should be the previous CPM value. In Step #4, the following operation is performed in order to obtain A_1, which is not only set the first chaotic value for the CPM but also indirectly contributing to the producing the next iteration number by setting *"M"*. To calculate the value of A_i, the x value of the chaotic system is used. Our experimental results show that the y and z value can also be used but the performance of the proposed system does not change (results not shown). In the last step, Step #5, based on the values generated for (x_1, y_1, z_1) in Step #3 and on the C_I value, we can calculate the next iteration time R_2 by incorporating the intermediate variable B_1. We then set (x_1, y_1, z_1) as the next initial values of the corresponding chaotic dynamic system. Steps #3 to #5 are then repeated to generate all CPM values motivated by the method presented by P. Fei [35].

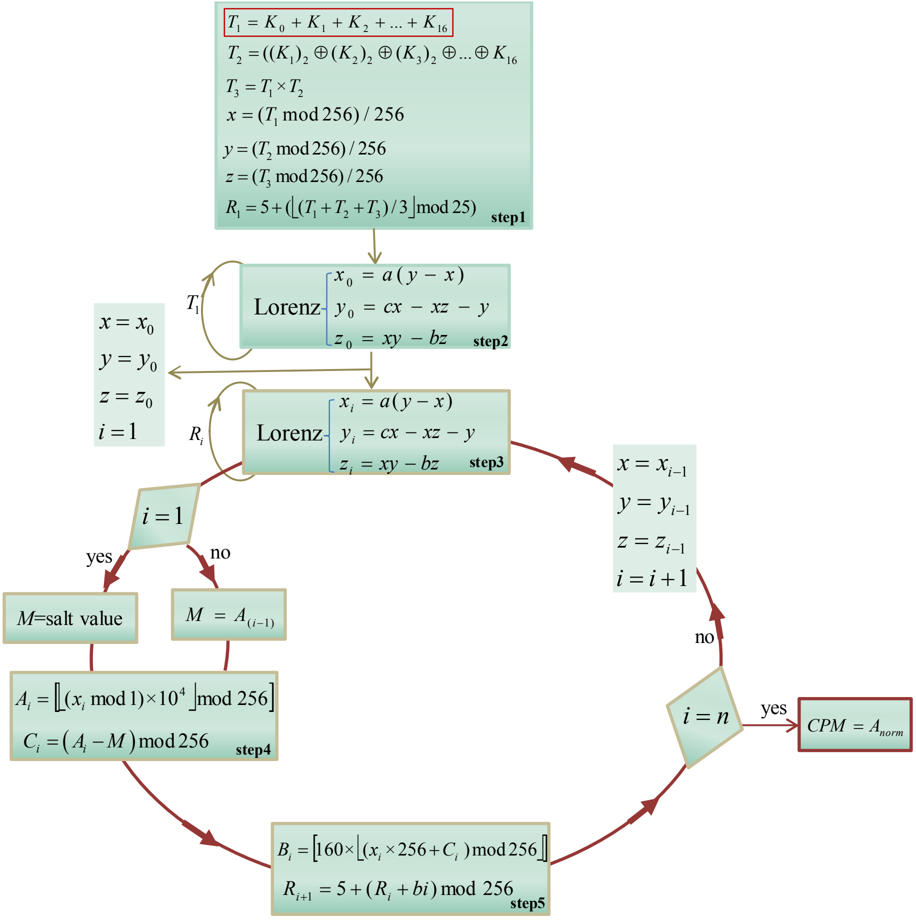

$T_1 = K_0 + K_1 + K_2 + ... + K_{16}$
$T_2 = ((K_1)_2 \oplus (K_2)_2 \oplus (K_3)_2 \oplus ... \oplus K_{16}$
$T_3 = T_1 \times T_2$
$x = (T_1 \bmod 256)/256$
$y = (T_2 \bmod 256)/256$
$z = (T_3 \bmod 256)/256$
$R_1 = 5 + (\lfloor (T_1 + T_2 + T_3)/3 \rfloor \bmod 25)$
step1
T_1
Lorenz
$x_0 = a(y - x)$
$y_0 = cx - xz - y$
$z_0 = xy - bz$
step2
$x = x_0$
$y = y_0$
$z = z_0$
$i = 1$
R_i
Lorenz
$x_i = a(y - x)$
$y_i = cx - xz - y$
$z_i = xy - bz$
step3
$x = x_{i-1}$
$y = y_{i-1}$
$z = z_{i-1}$
$i = i + 1$
$i = 1$
yes
no
M=salt value
$M = A_{(i-1)}$
$A_i = \lfloor \lfloor (x_i \bmod 1) \times 10^4 \rfloor \bmod 256 \rfloor$
$C_i = (A_i - M) \bmod 256$
step4
no
$i = n$
yes
$CPM = A_{norm}$
$B_i = [160 \times \lfloor (x_i \times 256 + C_i) \bmod 256 \rfloor]$
$R_{i+1} = 5 + (R_i + bi) \bmod 256$
step5

Figure 4.4: Workflow of chaotic generation. K_n: ASCII value of the n^{th} key. $(K_n)_2$: a binary form of the ASCII value of the n^{th} key. $\oplus$: *XOR* operation.

c. Hologram encoding by Fresnel propagation

The hologram is recorded by an off-axis configuration. The hologram should be filtered since the unwanted data of zero-order noise and conjugate image are also stored into hologram content. Filtering also reduces the size of a hologram for the encryption-decryption scheme. Next, the filtered hologram is distorted (by multiplying *CPM*) and the inverse Fourier transform is applied. The distorted filtered hologram is again multiplied by the CPM. Eventually, it is encrypted into stationary white noise by doing numerical Fresnel propagation as follows:

$$U_{Enc} = Fr\left\{\Im^{-1}\left\{I_H^F \times \exp(j2\pi \times CPM)\right\} \times \exp(j2\pi \times CPM)\right\}, \tag{8}$$

Where Fr is the numerical Fresnel propagation and $\Im^{-1}$ is the inverse Fourier transformation. The wavelength (λ) and propagation distance (PD) of the Fresnel propagation are other keys to this scheme. The λ can be similar to the one used by off-axis configuration or can be set differently since this step is executed on a computer. The schematic diagram of the proposed encryption-decryption system in the Fresnel domain is given in Fig. 4.5. As shown in both equation 8 and Fig. 4.5, the same CPM is applied two times. For generating CPM, the non-secret salt value is shared among all users and the sixteen-eight-bit key is the ephemeral secret key that can be used for each encryption process. After CPM is generated, the ephemeral secret key is deleted from the server because it cannot be used more than once. Only the user with exact same the salt value and chaotic keys that are used for encryption can generate correct CPM to decode the hologram. In any other case, the decoded hologram is invalid and no useful information about the biological sample can be revealed. To decrypt the hologram, the inverse of the encryption process is used. The inverse Fresnel propagation of U_{Enc} is taken. It is then multiplied by the complex conjugate of the CPM and the Fourier transform is applied. Thereupon, multiplied by the complex conjugate of the CPM once more bringing this back to the decrypted filtered hologram.

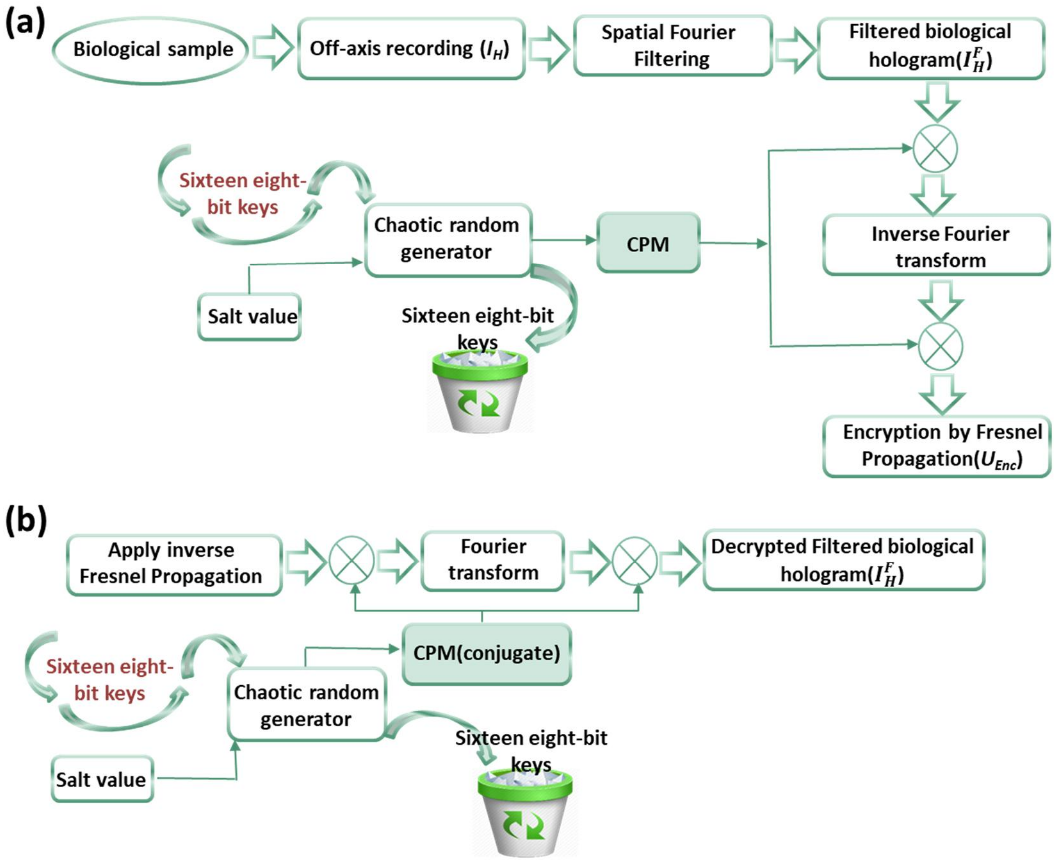

(a)
Biological sample
Off-axis recording (I_H)
Spatial Fourier Filtering
Filtered biological hologram(I_H^F)
Sixteen eight-bit keys
Chaotic random generator
CPM
Inverse Fourier transform
Salt value
Sixteen eight-bit keys
Encryption by Fresnel Propagation(U_{Enc})
(b)
Apply inverse Fresnel Propagation
Fourier transform
Decrypted Filtered biological hologram(I_H^F)
CPM(conjugate)
Sixteen eight-bit keys
Chaotic random generator
Sixteen eight-bit keys
Salt value

Figure 4.5: Proposed biological encoding-decoding scheme; (a) Encoding and (b) Decoding.

d. Results and discussions

Experiments are performed on images shown in Fig.4.6 (a, b), (holograms of red blood cells and skeleton muscle cells, respectively). All the simulations are implemented in MATLAB 2016. The original hologram is 1024×1024 pixels (8 bit) and after applying FFT and spatial filtering we deal with 512×512 complex pixel values. The laser source's wavelength for off-axis hologram recording is 666 nm, the wavelength and distance for encryption by Fresnel propagation is 533 nm and 0.4 meters respectively. The amplitude, phase parts and autocorrelation of the encrypted red blood cells (RBC) and skeleton muscle cells by the proposed method are shown in Fig.4.6(c-h). The similarity between the decrypted hologram and the original hologram is evaluated by the PCE.

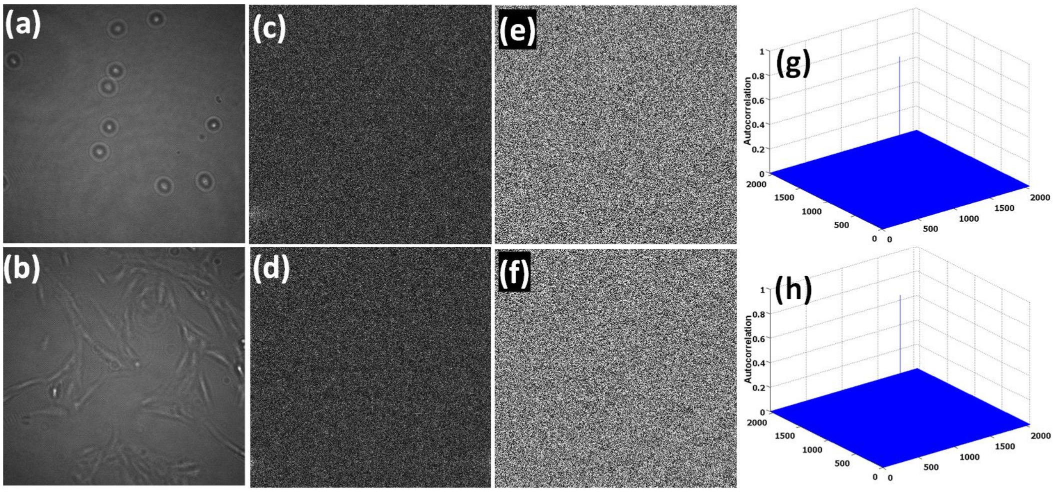


Figure 4.6: Recorded holograms of (a) RBC and (b) skeleton muscle cells. Amplitude part of the encrypted image: (c) RBC, (d) skeleton muscle cell, phase of encrypted image: (e) RBC, (f) skeleton muscle cells, Autocorrelation of encrypted image (g) RBC and (h) skeleton muscle cells.

Figure 4.7 depicts the histograms of the real, imaginary, amplitude and phase part of encrypted RBC hologram and the corresponding's CPM. The encrypted phase part and CPM histograms are nearly normally distributed, which indicates that they can protect well the information of the hologram from a statistical attack.

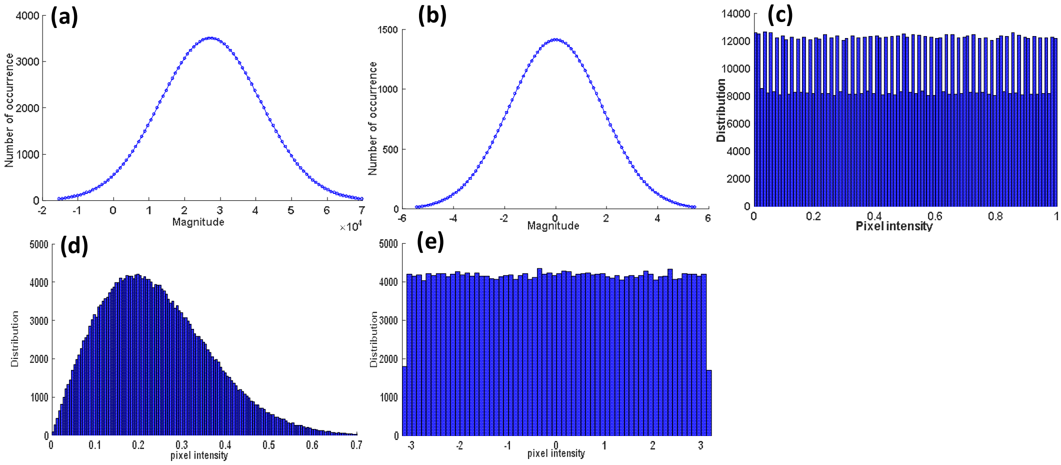


Figure 4.7: Histogram of the encrypted RBC hologram (a) real part, (b) imaginary part, (c) CPM, and encrypted RBC hologram (d) amplitude, (e) phase.

To examine the relationship between two adjacent pixels of RBC sample hologram and CPM with the secret keys ‘A1C2B4M9$#*-OP2/’, the correlation coefficient was employed. The correlation coefficient results in the horizontal, vertical, and diagonal directions are listed in Table 4.1. It can be seen the larger coefficient indicates the stronger relationship in the plain image. In contrast, the smaller coefficient is evident that two adjacent pixels from the CPM have a negligible correlation. Fig.4.8 displays a correlation analysis of the biological sample holograms and their CPMs. These figures provide additional evidence for the claim that neighboring pixels of CPM do not have a relationship.

Table 4.1: Correlation coefficients for two adjacent pixels in hologram and chaotic map

Direction	**Plain image (RBC sample)**	**Chaotic key**
Horizontal	0.9205	0.0017
Vertical	0.9127	-0.0585
Diagonal	0.7273	-0.0550

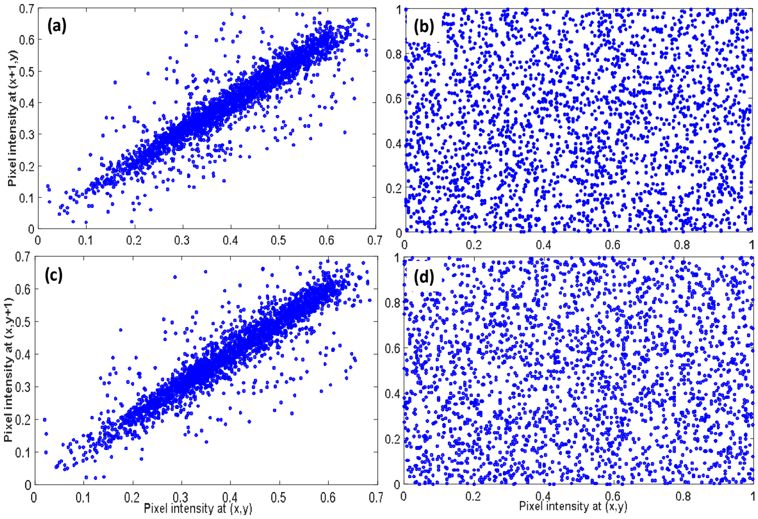


Figure 4.8: Correlation analysis between pixels located at position (x,x+1) (a) in RBC sample hologram, (b) in a chaotic mask and correlation analysis between pixels located at position (y,y+1) (c) in RBC sample hologram, (d) in the chaotic mask.

As mentioned previously the proposed scheme is sensitive to the chaotic key changes. Fig.4.9 (a) shows PCE of the proposed method for RBC for true input hologram and correct CPMs keys (RBC) and false input hologram and false CPMs keys (skeleton muscle cell). It turns out that by using a different key or a false input image, the PCE drops dramatically (See Fig.4.9 (a)). Since the avalanche effect is an attractive property to verify the security of the system, in the following avalanche effect is measure between the encrypted biological hologram and key. Referring to the avalanche effect concept, for satisfying the avalanche criterion the small change in keys should lead to a large number of differences in encrypted hologram [36, 78]. If we take the Hamming distance H between the $U_{ENC}(x,y)$ encoded by specific chaotic keys and the $U'_{ENC}(x,y)$ which we obtain by encoding with some bits changes of that specific chaotic keys, then the avalanche effect can be calculated from the following equation:

$$Avalanche = \frac{H(U_{ENC}(x,y), U'_{ENC}(x,y))}{Num(Y)}, \tag{11}$$

where $Num(y)$ denotes the total number of binary bits of the hologram. In the Fig.4.9 (b), CPM is generated by changing bits of the key from 1 to 128 bits (16 bytes). In consonance with avalanche definition, Fig.4.9 (b) proves the relationship between keys and the ciphered holograms. As can be seen, the minor changes in the chaotic keys result in significant changes in the cipher image.

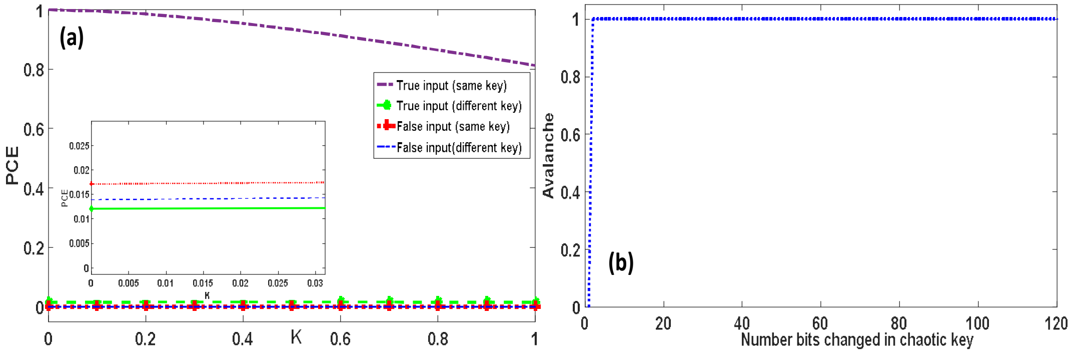


Figure 4.9: (a) PCE for different k values in different conditions; inset shows the scenarios of PCE dropping dramatically (b) amplitude value's avalanche by varying bits of the key from 1 to 128 bits (8×16 bits).

e. Attacks, Parameters Selection and Perfect Forward Secrecy of the Proposed Method

Varying propagation distance and wavelength

To evaluate the vulnerability of the proposed scheme against different conditions, the performance of the method is evaluated while the biological sample hologram is decrypted by propagation distance and wavelength values different from ones used by encryption. Figures.4.10 (a-b) represents the PCE value against two parameters of k value which defines the density of the applied nonlinearity in the *y-axis* and propagation distance or wavelength values which are shown on the *x-axis*. As can be seen in both graphs, PCE is 1 for *k=0* when decryption is done by correct propagation distance and wavelength same as encryption values. We can see that, by a small change in the propagation distance and wavelength PCE sharply falls.

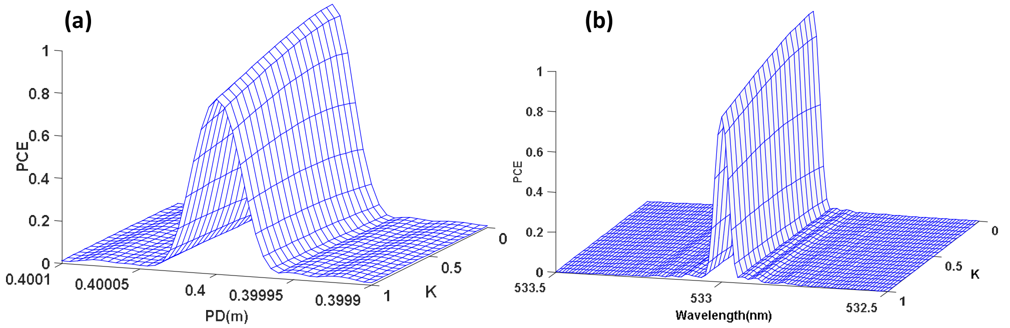


Figure 4.10: PCE for the decrypted RBC hologram with different (a) Propagation distance (PD), (b) and Wavelength (nm).

Varying propagation distance and wavelength

The amplitude and phase of the encoded hologram after decoding by the correct key and numerical reconstruction parameters are shown in Fig 4.11(a,b), respectively. If an attacker decides to record only the amplitude of the encoded data (Fig 4.6(c)) and reconstruct the image, the results are not resembled the correct images (See Fig 4.11(c,d)). These figures provide additional evidence for the claim that it is not possible an attacker reconstruct hologram only by the amplitude part.

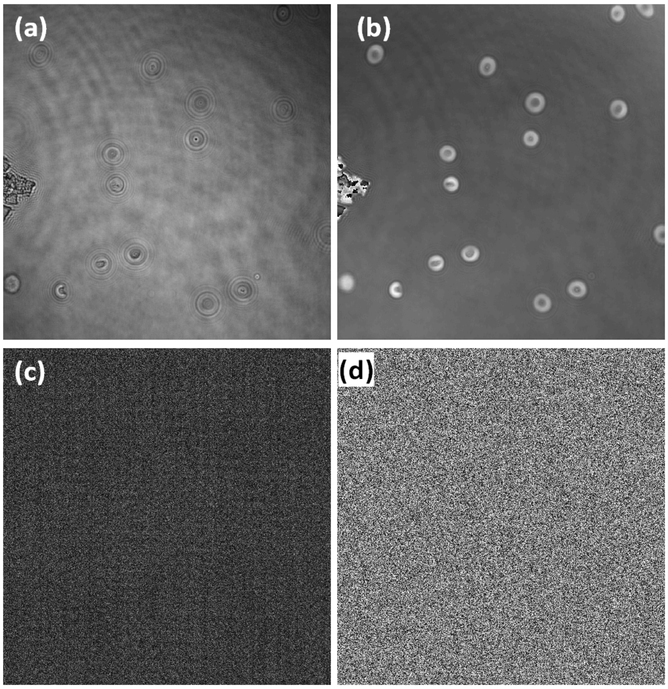


Figure 4.11: (a) Amplitude part and (c) phase part of the decoding image with the correct numerical hologram reconstruction, (b) Amplitude and (d) phase part of reconstructing hologram by only the amplitude part of the encoded image.

Resistance against chosen-plaintext and chosen-ciphertext attacks and security discussions

By given that CPM is derived from complex mathematical operations, it will be too difficult for an attacker to brute force the CPMs. Also, the attacker cannot use leaked CPM for decrypting another hologram because different CPM is used for the different holograms. This is due to that the phase mask is generated by a proposed method that is unique for each encryption process. So, the CPM for images differs and any information about the phase mask of one encrypted hologram cannot help decoding other encrypted holograms. Therefore, DRPE is not more vulnerable against chosen-plaintext, chosen-ciphertext attacks [22, 40]. From another point of view, using the long-term secret key will compromise the secrecy of all CPM. This is a major security threat that makes the long-term key extremely attractive for attackers. In this case, if the keys of the server get stolen, not only all future encrypted holograms are compromised but also an attacker can decrypt previously encrypted holograms with the stolen keys. Therefore, we need the technique to protect the security of CPM beyond their lifetime, such as the time that CPM used for hologram encryption [63]. The proposed method offers to benefits of PFS by using non-secret salt value and the secret chaotic key (interchangeably). PFS means that secret key is no longer used and is erased from memory, then there is no way for the attacker to find this key.

In the proposed encryption system automatically and frequently the secret keys are changed, such that if the latest key is compromised, it exposes only the latest encrypted information and the other holograms stay safe. Therefore, not only finding an expired key does not have value for the attacker to encrypted images in the future but also the encrypted images in past cannot be decrypted with compromised secret keys in the future. This valuable property of the proposed method comes from this principle that for decrypting each image we need both salt value and the secret chaotic key. The two keys generate a new CPM for every encryption process, even those sent consecutively by the same user. So, neither leaked CPM nor expired secret keys cannot help an attacker to decode the other holograms since they have their own secret key to generate the CPM.

f. Conclusion

This section suggests an efficient biological hologram encryption-decryption scheme under the objective of enhancing the security of the conventional optical encryption method by combining different concepts. The results of the proposed method show that the chaotic method can be suitable for generating phase masks for encryption by Fresnel propagation. Perfect forward secrecy is one of the most important considerations of designing biological hologram encryption-decryption to withstand different attacks. Also, less space is required since we only need to store secret keys. Additionally, it is shown in experiments that the proposed system is robust to blind decryption without knowing exact CPM as well as correct propagation distance, and wavelength that is used in the encoding step.

5 Conclusion and Future Research Opportunities

From past researches, scientists have created many methods to ensure the security of the images which are transmitted through insecure channels. In this thesis, we addressed the problem of security and unwanted property in numerical implementation of DRPE by using compression method and cryptography methods. One of the main contributions of our work is to reduce the size of the encrypted image by combining the compression methods (JPEG and JP2K) and DRPE. In particular, our proposed method considers not only quantized phase values but also a binary mask of photon-counted amplitude values [79]. As well as, numerical comparison of PCE behavior has been indicated the JP2K deal better in different compression ratios.

The main purpose of the second work was to reduce the size of keys and find a secure way to encrypt the images. Here, in this study, we have introduced a new encryption scheme by combining the chaotic-method and DRPE. The experiment results indicate that this proposed system can generate the CPM by a small number of keys independent of the image size [80]. Moreover, it is giving extra security to DRPE for increasing robustness against chosen-ciphertext or know-plaintext attacks.

Finally, another contribution relies on the biological hologram encryption-decryption scheme under the objective of enhancing the security of the conventional optical encryption method by combining different concepts. This contribution allows using perfect forward secrecy to solve long term secret keys compromise attacks. Furthermore, the experiments result to evaluate this method have proven that the proposed method to be a good one for hologram encryption by using perfect forward secrecy concept.

In future work, the current biological hologram encryption-decryption scheme can be improved by developing new asymmetric key generation architecture by combining the perfect forward secrecy. Also, the encryption algorithm can be used for information hiding and watermarking.

6 References

[1] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett 20, 767-769 (1995).

[2] I. Moon, F. Yi, Y. Lee, and B. Javidi, “Avalanche and bit independence characteristics of double random phase encoding in the Fourier and Fresnel domains,” J. Opt. Soc. Am. A 31, 1104-1111 (2014).

[3] R. Tao, Y. Xin, and Y. Wang, “Double image encryption based on random phase encoding in the fractional Fourier domain,” Opt. Express 15, 16067-16079 (2007).

[4] Z. Liu, Y. Zhang, S. Li, W. Liu, W. Liu, Y. Wang, and S. Liu “Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains,” Opt. Lasers Technol. 47, 152-158 (2013).

[5] G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain,” Opt. Lett 25, 887-889 (2000).

[6] W. Chen, “Multiple-wavelength double random phase encoding with CCD-plane sparse-phase multiplexing for optical information verification,” Appl. Opt 54, 10711-10716 (2015).

[7] F. Yi, Y. Jeoung, and I. Moon, “Three-dimensional image authentication scheme using sparse phase information in double random phase encoded integral imaging,” Appl. Opt 56, 4381-4387 (2017).

[8] X. Wang, W. Chen, and X. Chen, “Optical information authentication using compressed double-random-phase-encoded images and quick-response codes,” Opt. Express 23, 6239-6253 (2015).

[9] Y. Frauel, A. Castro, T. Naughton, and B. Javidi, “Security analysis of optical encryption,” Proc. of SPIE 5986 (2005).

[10] J.Chen, N.Bao, LY.Zhang, ZL.Zhu, “Optical information authentication using optical encryption and sparsity constraint”, Opt. Lasers Eng107, 352-63(2018).

[11] Z.Shao, Y.Shang, Q.Tong, H.Ding, X.Zhao, X.Fu, “Multiple color image encryption and authentication based on phase retrieval and partial decryption in quaternion gyrator domain”, Multimedia Tools and Applications77, 25821-40(2018).

[12] G.Luan, A.Li, D.Zhang, D.Wang, “Asymmetric Image Encryption and Authentication Based on Equal Modulus Decomposition in the Fresnel Transform Domain”, IEEE Photonics Journal11, 1-7(2019).

[13] F. Yi, I. Moon, Y. Lee, A Multispectral Photon-Counting Double Random Phase Encoding Scheme for Image Authentication. Sensors 2014, 14, 8877-8894.

[14] A. Markman, B. Javidi, Full-phase photon-counting double-random-phase encryption. J. Opt. Soc. Am. A 2014, 31, 394-403.

[15] I. Moon, F. Yi, M. Han, J. Lee, Efficient asymmetric image authentication schemes based on photon counting-double random phase encoding and RSA algorithms. Appl. Opt. 2016, 55, 4328-4335.

[16] T. Naughton, B. Hennelly, T. Dowling, Introducing secure modes of operation for optical encryption J. Opt. Soc. Am. A 2008, 25, 2608-2617.

[17] W. Chen, B. Javidi, X. Chen, Advances in optical security systems. Adv. Opt. Photon. 2014, 6, 120-155.

[18] O. Matoba, T. Nomura, E. Perez-Cabre, M. Millan, B. Javidi, Optical Techniques for Information Security. Proceedings of the IEEE 2009, 97, 1128-1148.

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

[20] H. Suzuki, M. Yamaguchi, M. Yachida, N. Ohyama, H. Tashima, Obi, T. Experimental evaluation of fingerprint verification system based on double random phase encoding. Opt. Express 2006, 14, 1755-1766.

[21] X. Liu, J. Wu, W. He, M. Liao, C. Zhang, and X. Peng, “Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding,” Opt. Express 23, 18955-18968 (2015).

[22] Y. Frauel, A. Castro, T. Naughton, and B. Javidi, “Resistance of the double random phase encryption against various attacks,” Opt. Express 15, 10253-10265 (2007).

[23] E. Pérez-Cabré, M. Cho, and B. Javidi, “Information authentication using photon-counting double-random-phase encrypted images,” Opt. Lett 36, 22-24 (2011).

[24] E. Pérez-Cabré, H. Abril, M. Millán, and B. Javidi, “Photon-counting double-random-phase encoding for secure image verification and retrieval,” J. of Opt 14, 094001 (2012).

[25] S. Rajput, D. Kumar, and K. Nishchal, “Photon counting imaging and phase mask multiplexing for multiple images authentication and digital hologram security,” Appl.Opt54, 1657-66 (2015).

[26] J.Lee, N.Sultana, F.Yi, I.Moon, “Avalanche and Bit Independence Properties of Photon-counting Double Random Phase Encoding in Gyrator Domain”, Current Optics and Photonics2, 368-77(2018).

[27] W. Chen, C. Quan, C. Tay, Optical color image encryption based on Arnold transform and interference method. Opt. Commun. 2009, 282, 3680-3685.

[28] N. Singh, A. Sinha, Gyrator transform-based optical image encryption, using chaos. Opt Lasers Eng 2009, 47-539-46.

[29] H. Khanzadi, MA. Omam, F. Lotfifar, M. Eshghi, Image encryption based on gyrator transform using chaotic maps. In Signal Processing (ICSP), 2010 IEEE 10th International Conference on, 2010, pp. 2608-2612.

[30] Jx. Chen, ZL. Zhu, C. Fu, H. Yu, Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains. Optics Communications. 2015, 341,263-70.

[31] R. Matthews, On the derivation of a Chaotic encryption algorithm. Cryptologia 1984, 8, 29-41.

[32] M. Mishra, P. Singh, C. Garg, A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping. International Journal of Information & Computation Technology 2014, 4, 0974-2239.

[33] J. He, Z. Li, H. Qian, Cryptography based on Spatiotemporal Chaos System and Multiple Maps. Journal of Software 2010, 5, 421-428.

[34] D. Socek, Shujun Li, S. S. Magliveras and B. Furht, Short Paper: Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption, First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Athens, 2005, pp. 406-407. doi: 10.1109/SECURECOMM.2005.39

[35] Peng Fei, Shui-Sheng Qiu and Long Min, An image encryption algorithm based on mixed chaotic dynamic systems and external keys, Proceedings. 2005 International Conference on Communications, Circuits and Systems, 2005. Hong Kong, China, 2005, pp. 1139. doi: 10.1109/ICCCAS.2005.1495308.

[36] A. Akhshani, S. Behnia, A. Akhavan, H. Hassan, Z. Hassan, A novel scheme for image encryption based on 2D piecewise chaotic. Opt. Commun. 2010, 283, 3259-3266.

[37] G. Ablay, A Chaotic Random Bit Generator with Image Encryption Applications. International Journal of Computing Academic Research 2016, 5, 207-214.

[38] AV.Zea, JF.Barrera, R.Torroba, Cryptographic salting for security enhancement of double random phase encryption schemes. J.Opt. 2017, 19,105703.

[39] Y. Frauel, A. Castro, T. Naughton, B. Javidi, Resistance of the double random phase encryption against various attacks. Opt. Express 2007, 15, 10253-10265.

[40] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Vulnerability to chosen cyphertext attacks of optical encryption schemes based on double random phase keys. Opt. Lett. 2005, 30, 1644-1646.

[41] X, Peng, P.Zhang, H.Wei, B.Yu, Known-plaintext attack on optical encryption based on double random phase keys. Opt.Lett. 2006, 31,1044-1046.

[42] Y. Wiseman, The still image lossy compression standard-JPEG in Encyclopedia of information science and technology, 3rd ed. (IGI Global, PA, 2015).

[43] P. Schelkens, A. Skodras, and T. Ebrahimi, The JPEG 2000 Suite (John Wiley & Sons, NY, 2009).

[44] D. Santa-Cruz, T. Ebrahimi, J. Askelöf, M. Larsson, and C. Christopoulos, "JPEG 2000 still image coding versus other standards," Proc. of SPIE 4115, 446-454 (2000).

[45] A. Skodras, C. A .Christopoulos, and T. Ebrahimi, "JPEG2000: The Upcoming Still Image Compression Standard," Pattern Recogn. Lett 22, 1337-1345 (2001).

[46] D. Santa-Cruz, R. Grosbois, and T. Ebrahimi, "JPEG 2000 performance evaluation and assessment," Signal Processing: Image Communication 17, 113-130 (2002).

[47] P. Pasumpon, S. Sivanandam, and R. Rani, "Lossy Still Image Compression Standards: JPEG and JPEG2000 - A Survey," International Journal of the Computer, the Internet and Management 17, 69-84 (2015).

[48] A. Skodras, C. Christopoulos, and T. Ebrahimi, "The JPEG 2000 Still Image Compression Standard," IEEE Signal Process Mag 18, 36-58 (2001).

[49] G. Wallace, "The JPEG Still Picture Compression Standard", IEEE Trans. Consum. Electron 38 xviii-xxxiv (1992).

[50] K. Jaferzadeh, S. Gholami, and I. Moon, "Lossless and lossy compression of quantitative phase images of red blood cells obtained by digital holographic imaging", Appl. Opt 55, 10409-16 (2016).

[51] P.Li, KY.Lo, “A content-adaptive joint image compression and encryption scheme”, IEEE Transactions on Multimedia20, 1960-72(2018).

[52] V.Itier, P.Puteaux, W.Puech, “Recompression of JPEG crypto-compressed images without a key”, IEEE Transactions on Circuits and Systems for Video Technology, (2019).

[53] J.Horner, Metrics for assessing pattern-recognition performance. Appl. Opt. 1992, 31, 165-166.

[54] http://www.imageprocessingplace.com/downloads_V3/root_downloads/image_databases/standard_test_images.zip.

[55] A. Alabaichi, R. Mahmod, F. Ahmad, Analysis of Some Security Criteria for S-boxes in Blowfish Algorithm. International Journal of Digital Content Technology and its Applications 2013, 7, 8

[56] W. Stallings, Cryptography and Network Security Principles and Practice, Prentice Hall: NY, USA, 2011.

[57] B. Kemper, G. V. Bally, “Digital holographic microscopy for live cell applications and technical inspection,” Appl. Opt. 47(4), a52-61 (2007).

[58] Jaferzadeh, K., and Moon, I., “Quantitative investigation of red blood cell three-dimensional geometric and chemical changes in the storage lesion using digital holographic microscopy,” J. Biomed. Opt, 20, 111218 (2015).

[59] Moon, I., et al., “Automated three dimensional identification and tracking of micro/nano biological organisms by computational holographic microscopy,” Proc. IEEE, 97, 990-1010 (2009).

[60] K.Jaferzadeh, I.Moon, “Human red blood cell recognition enhancement with three-dimensional morphological features obtained by digital holographic imaging,” J. Biomed. Opt., 21, 126015 (2016).

[61] B.Rappaz, I.Moon, F.Yi, B. Javidi, P.Marquet, and G. Turcatti, "Automated multi-parameter measurement of cardiomyocytes dynamics with digital holographic microscopy," Opt. Express 23, 13333-13347 (2015).

[62] P.Marquet, et al., “Digital holographic microscopy: a noninvasive contrast imaging technique allowing quantitative visualization of living cells with subwavelength axial accuracy,” Optics Letters, 30, 468-470 (2005).

[63] Günther CG. “An identity-based key-exchange protocol.” In Workshop on the Theory and Application of of Cryptographic Techniques 1989. Springer, Berlin, Heidelberg.

[64] Sun HM, Hsieh BT, Hwang HJ. “Secure e-mail protocols providing perfect forward secrecy”. IEEE Communications Letters. 2005 Jan;9(1):58-60.

[65] Van Tilborg HC, Jajodia S, editors. “Encyclopedia of cryptography and security”. Springer Science & Business Media; 2014 Jul 8.

[66] Xie Q, Zhao J, Yu X. “Chaotic maps-based three-party password-authenticated key agreement scheme”. Nonlinear Dynamics. 2013 74(4):1021-7.

[67] Sun HM, Yeh HT. ”Password-based authentication and key distribution protocols with perfect forward secrecy”. Journal of Computer and System Sciences. 200672(6):1002-11.

[68] Qi.M, Chen.J.“An enhanced authentication with key agreement scheme for satellite communication systems”. INT J SATELL COMM N. 36(3):296-304(2018).

[69] Asokan N, Ginzboorg P. “Key agreement in ad hoc networks. Computer communications. 2000, 23(17):1627-37.

[70] E.Tajahuerce, B.Javidi, “Encrypting three-dimensional information with digital holography.” Appl. Opt. 2000, 39, 6595-6601.

[71] Nomura, T.; Uota, K.; Morimoto, Y. Hybrid, “encryption of a 3-D object using a digital holographic technique.” Opt. Eng. 2004, 43, 2228-2232.

[72] Tajahuerce, Enrique, and Bahram Javidi. “Encrypting three-dimensional information with digital holography.” Appl. Opt.2000. 39, no. 35, 6595-6601.

[73] Kim, Hyun, Do-Hyung Kim, and Yeon H. Lee. “Encryption of digital hologram of 3-D object by virtual optics.” Optics express 12, no. 20 (2004): 4912-4921.

[74] P. Marquet, B. Rappaz, P. Magistretti, E. Cuche, Y. Emery, T. Colomb, and C. Depeursinge, “Digital holographic microscopy: a noninvasive contrast imaging technique allowing quantitative visualization of living cells with subwavelength axial accuracy,” Opt. Lett., 30(5), 468-470 (2005).20

[75] C. Etienne, P. Marquet, C. Depeursinge, "Simultaneous amplitude-contrast and quantitative phase-contrast microscopy by numerical reconstruction of Fresnel off-axis holograms," Appl. Opt. 38, 6994-7001 (1999).

[76] T.Colomb, F.Montfort, J.Kühn, N.Aspert, E.Cuche, A.Marian, F.Charrière, S.Bourquin, P.Marquet, and C.Depeursinge, "Numerical parametric lens for shifting, magnification, and complete aberration compensation in digital holographic microscopy," J. Opt. Soc. Am. A23, 3177-3190 (2006).

[77] Voelz,D. George. “Computational Fourier optics. a MATLAB tutorial.” Bellingham, WA: SPIE press,(2011).

[78] A.Alabaichi, R.Mahmod, F.Ahmad, “Analysis of Some Security Criteria for S-boxes in Blowfish Algorithm.” JDCTA, 7, 8(2013).

[79] S.Gholami, K.Jaferzadeh, S.Shin, I.Moon, “Efficient Compression Schemes for Double Random Phase-encoded Data for Image Authentication. Current Optics and Photonics,” 3(5):390-400(2019).

[80] S.Gholami, K.Jaferzadeh, S.Shin, I.Moon, “An efficient image-based verification scheme by fusion of double random phase encoding and dynamic chaotic map” Multimedia Tools Appl, 1-8(2019).