ap

Asian Journal of Physics Vol. 23, No 3 (2014) 473-490

Optical asymmetric cryptosystems: A Review

Sudheesh K Rajput and Naveen K Nishchal*
Department of Physics
Indian Institute of Technology Patna, Patliputra, Patna-800 013, India

From the cryptography point of view, symmetric encryption schemes suffer from several problems; such as, key distribution, management, delivery and various kinds of attacks. In order to overcome these problems, various asymmetric image encryption schemes have been reported in literature during past few years. In this paper, at first, we present an overview of some of the basic image encryption schemes and then we review all the optical asymmetric cryptosystems based on amplitude- and phase-truncation and phase retrieval approach in different encryption domains like Fourier, Fresnel, and fractional Fourier transform domains. The input image/data used are gray-scale and color patterns.

Keywords: Image encryption, optical asymmetric cryptosystems, Fourier transform, Fresnel transform, fractional Fourier transform, Phase retrieval algorithm.

1 Introduction

Confidential communication is one of the necessities of social life. In this context, some important issues have to be solved. The message should be transmitted secretly, so that no unauthorized user gets access to the original secured message. The sender should be ensured that the message received is exactly the same as it was transmitted. Also, the receiver should ensure that the message coming from right person is exactly the same as it was transmitted. There could be two ways to solve these issues; write message with invisible ink or to transmit via trustworthy person. Another way is a scientific approach, which is called cryptography.

Cryptography is an art of transforming information into something unintelligible for anyone but the intended recipient. Several cryptographic tools are being used to ensure security, integrity, and authentication of data. As an information carrier, image is widely used in many fields for its vivid expression. Consequently, securing image is an important issue in information security. There have been several studies on digital information security techniques [1, 2].

The process of transformation of a plaintext into a ciphertext is called **encryption** and the reverse process is called **decryption**. In encryption, a secret data (plaintext) is transformed into a noisy distribution (ciphertext) with an algorithm so that it is computationally infeasible to reveal it without knowledge of the exact keys [1,2]. But, advanced high speed computers are able to reduce the processing time required to decipher an encoded message, which are becoming easily available. When large amounts of information are to be encoded, digital techniques take longer time in processing. Various digital techniques have been developed for image encryption applications [1, 2]. However, these techniques are inherently one-dimensional and limited to serial processing; the ones and zeros denoting the presence or absence of a pixel have to be processed one bit at a time [3-5].

Optical techniques for information security have triggered much interest because of their unique advantages such as parallel processing; every pixel of two-dimensional images can be both relayed and processed at the same time [4, 5]. So, when a large volume of information is to be processed, parallel processing offers enormous advantages. These techniques also have multi-dimensional capability; information can be hidden in any of the several dimensions, such as phase, wavelength, spatial frequency, or polarization of light. Optical encryption techniques provide high level of security because two-dimensional (2-D) information can be encoded securely. The optical techniques can easily be extended to three dimensions using holography

Corresponding author :
e-mail: nkn@iitp.ac.in; Tel.: + 91-612-2552027; Fax: + 91-612-2277383; (Naveen K Nishchal)

[6-8]. An intensity sensing device, such as a charge-coupled device (CCD) camera cannot record any phase information. It is possible to tuck away an optical message in only one small section of 2-D array, trick that forces unauthorized users to find the message's position before they can begin to decode it.

Optical information system consists of light source, lenses, mirrors, beam splitters, detectors, and display devices, such as, liquid crystal spatial light modulator (SLM). These components can be arranged in various configurations to suit the type of desired optical information processing set-up [6]. The following scenario describes some of the basic processes in an optical system. Information in the form of light wave passes through a converging lens that introduces delay or phase-shift to the incident wavefront by an amount proportional to; the thickness of lens, refractive index of the lens, and the wavelength of light. The light is distributed at the back focal plane of the lens, according to the spatial frequencies that were present in the original information. This spatial distribution in back focal plane can be described mathematically as the Fourier transform (FT) of the input information. The Fourier transforming capability of a converging lens is a crucial property of the optical processors because it allows further manipulation of the information in the spatial frequency domain [6].

Optical security techniques have generated considerable amount of interest amongst the researchers' in the last few decades. Several optical security techniques have been realized to broaden the research area of information security like authentication verification [9-11], watermarking [12-14], hiding [15-18], and encryption [19-95]. In this paper, we review various image encryption schemes reported in literature with special emphasis on optical asymmetric cryptosystems.

1.1 Optical symmetric image encryption schemes

Amongst the various optical security techniques reported in literature, encryption is an effective approach to ensure the security of information. To protect the stored information, it is required to encrypt the data/image. An optical encryption scheme turns the original information into a stationary white noise by using random phase codes (key). An unauthorized user cannot reveal the original data without knowledge of the exact key codes. The original information can be encoded optically by using various encryption techniques. Double random phase encoding (DRPE) based encryption [19-25], digital holography-based encryption [26-28], polarization encryption [29-33], interference-based encryption [34-38], and interference of polarized light based encryption [39, 40], are some of the major symmetric optical encryption techniques, which have been reported in the literature. Out of these, DRPE based encryption scheme has been studied extensively.

A. *DRPE based encryption scheme*

In the conventional DRPE technique [19], the primary image is encrypted using two random phase masks (RPMs), one bonded with the primary image and another placed in the Fourier domain, respectively. Unnikrishnan *et al* [20] proposed an optical encryption method using random phase encoding in the fractional Fourier transform (FRT) domain. Fourier transform operators in DRPE scheme were replaced with FRT operators. The remarkable feature of optical encryption based on the FRT is the fractional order, which enlarges the key space and further enhances the security of encryption schemes [21, 22].

In Fresnel transform (FrT) based image encryption techniques; optical wavelength, propagation distance, and sampling parameters are considered as additional keys for image encryption. Mathematically, FrT is computed through Fresnel-Kirchhoff formula. Matoba and Javidi [23] proposed an encrypted optical memory system using RPMs as keys in the FrT domain, which added a third dimension to the RPMs by shifting the RPM away from the Fourier plane. Situ and Zhang [24] proposed flexible and compact way of optical DRPE in FrT domain. In this scheme, a primary image is encrypted into random noise using two statistically independent RPMs, in the input and FrT planes, respectively. This scheme is lensless, which requires less hardware component and is easier to implement as compared to conventional DRPE scheme.

B. *Holography based encryption scheme*

Optical holography is a technique in which both the amplitude and phase of an object of interest can be recorded as a hologram in the form of interference fringes [7]. Usually, a hologram is recorded on a flat surface that contains information about the whole three-dimensional (3D) object. When optical wave field from a diffuse object is recorded as a hologram, the hologram becomes noisy pattern because the interference fringes of randomly phase modulated waves are recorded in the hologram. Nevertheless, the image of an object can be reconstructed from hologram in perfect form. This diffuse type holography can be used for image encryption and watermarking [12]. On the other hand, digital recording of holograms has potential advantages over optical techniques in that no physical or chemical developing is required after exposure. Hence, processing of holograms is possible in real-time [8].

Several image encryption schemes have also been proposed using digital holography [26-28]. Among them, DRPE scheme based on digital holography has been widely investigated because of its high security level and digital transmission characters [26,27]. But these encryption schemes usually require recording of several interferograms with three or four step phase-shifting. This results into low efficiency and are poor in real-time. However, the recording of less number of holograms is required in two-step phase-shifting holography and also have better real-time applicability [28].

C. *Polarization based encryption scheme*

Optical encryption using the concept of polarization has attracted much attention because polarization encryption provides additional flexibility in the design of encryption keys [26-30]. Unnikrishnan *et al* [29] demonstrated an optical encryption scheme based on polarization of light for binary images. Polarization encoding has also been proposed to secure holographic memory [30]. Biener *et al* [31] presented an approach for geometrical phase encryption using spatial polarization state manipulation. Polarization of light using Stokes-Mueller formalism has main advantage over Jones vector formalism that it manipulates only intensity information, which is a measurable quantity. Alfalou and Brosseau [32] proposed dual encryption scheme of images using polarized light. In this scheme, Stokes-Mueller formalism is used to parameterize the intensity images. The image is encrypted using the concept of polarized light encoding in which two independent optical plane waves are used. The first plane wave illuminates input image and is encoded into given states of polarization. Second plane wave illuminates intensity key image and is encoded into another state of polarization. Then these two waves are mixed to obtain first level of encryption. The resulting waves are then passed through a matrix of linear polarizer, to obtain the second level of encryption. For decryption, encrypted image is passed through another pixilated polarizer with appropriate angles which gives the original image. Recently, Dubreuil *et al* [33] analyzed the security proposed by Alfalou and Brosseau [32], to chosen ciphertext-attack, chosen-plaintext attack, known-plaintext attack, and some other attacks like brute force attack and video sequence attack. This method is found to be resistant against brute force and video sequence attacks because of the high number of combinations of the keys. However, the method is vulnerable to known- and chosen-plaintext attacks when more than one plaintext-ciphertext pair is known.

D. *Interference based encryption scheme*

Several image encryption methods have been proposed in literature in which an image is encoded into phase-only masks (POM) using iterative algorithm. These methods are not cost effective rather they are time consuming. To overcome the drawbacks, a simple method of image encryption based on interference principle has been proposed [34], in which image to be encrypted is encoded into two pure POMs analytically. For decryption, analytically generated POMs optically interfere and give the original image. This encoding process is simple and does not require the iterative algorithm. Extending this pioneering work, several image encryption methods have been reported [35-38]. Interference based encryption scheme has also been used for information hiding [35]. Weng *et al* [36] reported experimental verification of optical image encryption based on interference. The phase-only SLM is used to generate the desired phase retardations and holographic plate

is used to record the modulated wavefronts in two step holographic exposure process. It has been reported that this method has a drawback when only one of the two masks is used in the verification process [37]. Although the encrypted image cannot be decrypted exactly, one can still find the silhouette of the encrypted image [37]. Silhouette may be obtained due to the equipollent nature of the POMs generated by analytical method. Recently, a silhouette free multiple image encryption method using position multiplexing based on interference has been proposed by Qin and Gong [38]. The information of multiple images is hidden into three POMs without using iterative algorithm.

Interference based encryption scheme suffers from alignment problem because it is difficult to collimate two beams into a collinear path. To solve this problem, optical image encryption based on interference between two polarized wavefronts has been proposed [39]. In this technique, a polarization selective diffractive optical element (PSDOE) is used to generate the desired polarized wavefronts. The PSDOE is a phase-only optical element fabricated on a birefringent substrate where ordinary and extra-ordinary polarized light will have different refractive indices. An encryption and verification method based on interference principle has also been reported [40], in which two different images are encoded into three diffractive phase elements by using two different incident wavelengths. The two wavelength parameters and the distances serve as keys for decryption. These schemes alleviate the alignment problem of interference and do not need iterative encoding and offer multiple levels of security. The PSDOE consists of a 2-D array of pixels, which is employed to generate two desired polarized wavefronts by modulating the incident polarized beam. Each pixel of the PSDOE offers a phase delay corresponding to the etched surface-relief depth of the birefringent substrate [39,40].

E. *Multiple image encryption*

In communication system, there is a requirement for several users to share the common information simultaneously and in a controlled way. Generally, in multiple image encryption methods, two or more images are encoded into a single image using optical or digital techniques. To secure multiple images, various encryption schemes have been suggested [41-47]. Situ and Zhang [41] proposed a technique of wavelength-multiplexing and position-multiplexing into the DRPE system. Shortt *et al* [42] proposed a technique for compression of optically encrypted digital holograms using neural network. Further, multiple image encryption method has been reported claiming the solution to the problems of cross-talk and increasing the multiplexing capability and also security to the cryptosystems [43-47].

In multiple image encryption methods, an important issue is to reduce cross-talks and accordingly increase number of images that can be encrypted simultaneously. Hwang *et al* [44] proposed multiple image encryption and multiplexing using modified Gerchberg-Saxton (G-S) phase retrieval algorithm in FrT domain. Owing to the need of image compression to reduce the size of the data, which ultimately affects the digital processing time, researchers have combined the schemes of compression to encryption/decryption. Alfalou and Brosseau [45] proposed a scheme to compress and encrypt simultaneously multiple images using spectral multiplexing. Alfalou and Mansour [46] proposed multiplexing and encoding of multiple images, which enables to obtain better compression and transmission information rates. Deng and Zhao [47] proposed a method for multiple-image encryption using phase retrieval algorithm and intermodulation in FT domain. In this method, all plaintexts are extracted from the ciphertext without any cross-talk.

F. *Color image encryption*

Most of the proposals on image encryption in literature deal with binary/gray-scale images. The images are encrypted and decrypted by a monochromatic light therefore; the decrypted images do not preserve their color information. The color information of an image is useful in many practical applications, such as security verification of human facial images. In general, a color image provides more information as compared to a monochromatic one. Also, it is believed that additional color information could contribute

to a higher level of security than binary and gray images. Color is an effective descriptor. A color image plays a significant role in our society. Now-a-days color image encryption has become an important field of research for data security [48-56].

Most of the color image encryption schemes belong to the three-channel processor, in which each channel is encrypted or decrypted independently. Processing three primary color components independently increases the complexity and computational cost [49-54]. Some optical color image encryption schemes based on wavelength multiplexing [49], FRT [50], phase encoding in hue, saturation, and value color space [51], Arnold transform [52], and fractional –wavelet transform [53] have been reported. A multiplexing and encryption technique for four color images in FRT domain has also been reported [54].

In color image encryption schemes, the image is decomposed into three primary color components; red, green, and blue, and hence three channels are created for processing. Some single channel color image encryption methods have been proposed [55,56]. Deng and Zhao [55] proposed a single-channel method for color image encryption using modified G-S algorithm (MGSA) and mutual encoding in the FrT domain. A technique of color image encryption using wavelength multiplexing has been proposed by Hwang [56].

Most of the image encryption systems based on mathematical transform are linear systems, which are relatively weak in comparison to the nonlinear encryption systems. The reason is that the functional relationship among plaintext, ciphertext, and key is comparatively simple in a linear encryption system, which makes the encryption system potentially insecure against some common attacks. Any optical security system cannot be claimed secure unless it is able to endure various attacks such as brute force attack, chosen-ciphertext attack, chosen-plaintext attack, known-plaintext attack etc [57-61]. In the analysis of an encryption scheme, it is assumed that attackers already know the encryption algorithm as well as encryption domain and other resources.

The brute force attack against any cryptosystem consists of trying every possible key until finding the correct one. For two phase keys, each of size $N \times N$ pixels and that each pixel has L possible phase values, the number of trials required to retrieve both phase keys will be $L^{2N \times N}$. Suppose $L = 64$ phase levels and $N = 200$ pixels. Then the number of trials would be 64^{80000}, which is a large number. However, these numbers can be reduced by considering appropriate phase key combinations. For binary phase keys, the number would reduce to 2^{80000}. This attack may be possible because of availability of high speed computers [59].

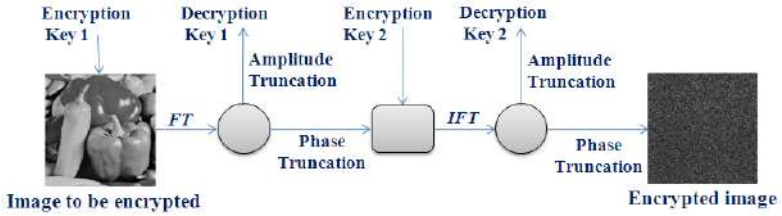
2 Asymmetric cryptosystems

2.1. Phase-truncation based approach

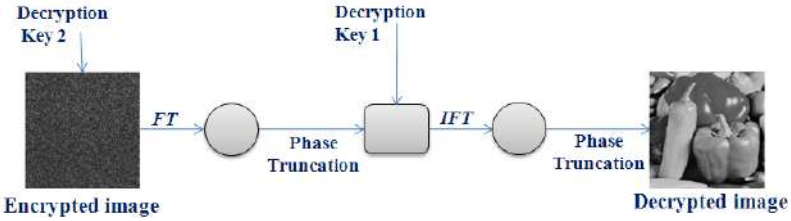
A. *Fourier transform domain*

Most of the optical image encryption schemes which have been discussed in previous sections are considered as symmetric cryptosystem, in which encryption keys are identical to decryption keys. These cryptosystems would suffer from problems, such as, key distribution and management under an environment of network security. To solve this problem, asymmetric cryptosystems have been proposed [62-95]. Peng *et al* [62] proposed asymmetric cryptography based on wavefront sensing technology. In this scheme, the encryption key is derived from optical parameters, such as wavelength, focal length, or their combination and the decryption key is obtained from a regular point array formed by microlenslet array. Qin and Peng [63] proposed an asymmetric cryptosystem based on phase-truncated Fourier transforms (PTFTs), in which the encryption keys differ from the decryption keys. Also, only the amplitude of the Fourier spectrum is retained while phase part of the spectrum is truncated.

The block diagrams of asymmetric cryptosystem based on PTFT for encryption and decryption procedures have been shown in Figs 1(a) and (b), respectively. In phase truncation based asymmetric cryptosystem in FT domain, similar to DRPE two statistically independent



(a)



(b)

Fig 1. (a) Block diagram of asymmetric cryptosystem for encryption (b) block diagram of asymmetric cryptosystem for decryption.

RPMs; $exp\{i2\pi r_1(x,y)\}$ and $exp\{i2\pi r_2(x,y)\}$, respectively are employed to encode an image $f(x,y)$ into an asymmetric ciphertext, $E(x,y)$ as real-valued and stationary white noise [63].

$$E_1(u,v) = PT\{FT[f(x,y)\times \exp\{i2\pi r_1(x,y)\}]\} \tag{1}$$

$$E(x,y) = PT\{IFT[E_1(u,v)\times \exp\{i2\pi r_2(u,v)\}]\} \tag{2}$$

Here, IFT represents inverse Fourier transform operation. For complete retrieval of an image, the decryption keys (DKs) are generated as

$$P_1(u,v) = AT\{FT[f(x,y)\times \exp\{i2\pi r_1(x,y)\}]\} \tag{3}$$

$$P_2(x,y) = AT\{IFT[E_1(u,v)\times \exp\{i2\pi r_2(x,y)\}]\} \tag{4}$$

For decryption, the encrypted image, $E(x,y)$ multiplied with second decryption key, $P_2(x,y)$ is inverse Fourier transformed.

$$e_1(u,v) = PT\{IFT[E(x,y)\times P_2(x,y)]\} \tag{5}$$

The decrypted image, $d(x,y)$ is obtained by multiplying phase-truncated value obtained from Eq (5) with first decryption key, $P_1(u,v)$ and by performing FT operation,

$$d(x,y) = PT\{FT[e_1(u,v)\times P_1(u,v)]\} \tag{6}$$

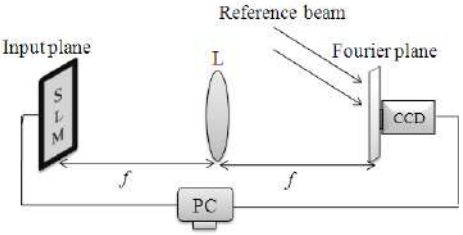
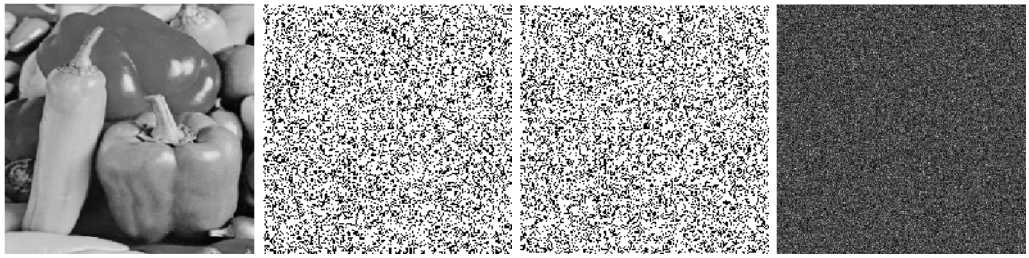


Fig 2. schematic diagram for optical encryption and decryption

The schematic diagram for decryption is shown in Fig 2. From Eqs (3) and (4), it can be seen that the decryption keys are related to the original image and encryption keys. Therefore, using arbitrarily

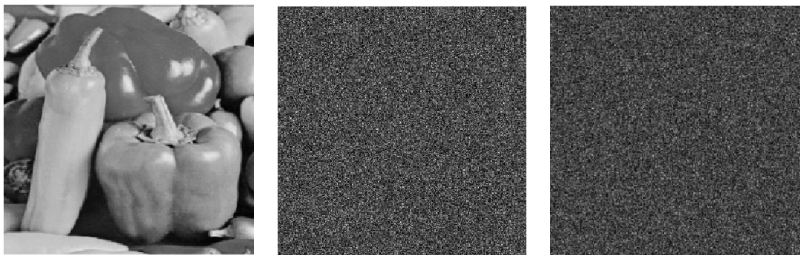
selected encryption keys or decryption keys may result incorrect decryption. Main problem for an opponent is to reproduce decryption keys because phase truncation leads to one way function. It is also claimed that this scheme offers immunity against existing attacks [63]. The decrypted image can be obtained only if correct decryption keys are used.

For validation of optical asymmetric cryptosystem based on phase-truncation approach, computer simulations have been carried out on MATLAB 7.10 platform. The simulation results for optical asymmetric cryptosystem based on amplitude-truncation and phase-truncation in FT domain are shown in Figs 3(a-e). An image of a capsicum of size 256 × 256 pixels to be encrypted is shown in Fig 3(a). Figures 3(b) and (c) show the first and second decryption keys respectively. Figure 3(d) shows the encrypted image. Figure 4(a) shows the decrypted image obtained after using all correct keys. Figure 4(b) shows the decrypted image obtained after using wrong decryption keys. Figure 4(c) shows the decrypted image obtained after using encryption keys.



(a) (b) (c) (d)

Fig 3(a). An image of capsicum to be encrypted, (b) first decryption key, (c) second decryption key, and (d) encrypted image.



(a) (b) (c)

Fig 4(a). Decrypted image obtained after using all correct keys, (b) decrypted image obtained after using wrong decryption keys, and (c) decrypted image obtained after using encryption keys.

Based on the principle of amplitude- and phase-truncation, two decryption keys; universal key and special key are generated. In this asymmetric encryption method, each of them can be used for decryption independently in absence of the other [64]. Wang and Zhao [65] proposed multiple image encryption method based on FT domain nonlinear operations. The RPMs for encryption and additional keys, which are determined by the original images and generated by the nonlinear operations during encryption processes is necessary for image decoding. This concept of asymmetric cryptosystem has also been combined with phase retrieval algorithm for encrypting two gray-scale images [66]. In this scheme, two covert images are encoded into an overt image using phase retrieval algorithm. Deng and Zhao [67] proposed a color image encryption using the concept of an asymmetric cryptosystem in FT domain. Later, it has been found that the asymmetric cryptosystems based on phase-truncation in FT domain is vulnerable to special attack in which encrypted information can be obtained if encryption keys are known to the attackers [68]. This attack is based on a two step iterative amplitude retrieval approach, which can reveal encrypted information by using encryption keys and ciphertext.

The phase truncation approach has been further modified [69-74]. Wang and Zhao [69] enhanced security of phase-truncation based image encryption scheme by amplitude modulation. Wang and Zhao [70] proposed double image encryption in which images are encoded into amplitude ciphertext and two pure POMs. Ding *et al* [71] proposed security enhanced phase- and amplitude-truncation based image encryption scheme. For security enhancement, spherical wave illumination has been employed. An asymmetric encryption scheme has been combined with joint transform correlator (JTC) based encryption [72]. The attack analysis has also been carried out, which infers that this scheme is resistant to hybrid attack. The hybrid attack is the combination of specific attack on asymmetric cryptosystem and chosen-plaintext attack on image encryption based on JTC.

Recently, Wang and Zhao [73] proposed an amplitude-phase retrieval attack free cryptosystem based on direct attack to PTFT-based encryption using a random amplitude mask. Liu *et al* [74] proposed an asymmetric cryptosystem based on mixture retrieval type of Yang-Gu algorithm.

B. *Fractional Fourier transform domain*

In this section, we discuss asymmetric image encryption schemes in FRT domain. An image to be encrypted, $f(x,y)$, is multiplied with an *RPM*, $exp[j2\pi r_1(x, y)]$, and then its fractional spectrum is obtained, which may be given as [75,76],

$$F(u,v) = K\iint \{f(x,y)\times \exp[i2\pi r_1(x,y)]\}\times \exp\left[j\pi \frac{x^2+y^2+u^2+v^2}{\tan\alpha} - 2j\pi \frac{xyuv}{\sin\alpha}\right] dxdy \tag{7}$$

The symbol K represents a complex constant, which is defined as

$$K = \frac{\exp\left[-j\left(\frac{1}{4}\pi \operatorname{sgn}(\sin\alpha)\right) - \frac{1}{2}\alpha\right]}{|\sin\alpha|^{1/2}} \tag{8}$$

$\alpha = a\pi/2$ and $\alpha \neq n\pi$, where n is an integer. Here (x, y) and (u, v) are coordinates of the input and fractional planes, respectively. Here $r_1(x, y)$ is a random white sequence uniformly distributed in the interval [0, 1]. Similarly, Eqs. (1) to (6) can be used for encryption and decryption processes by replacing FT with FRT. The encryption and decryption process of optical asymmetric cryptosystem in FRT domain are illustrated with the help of Figures 5(a) and (b), respectively.

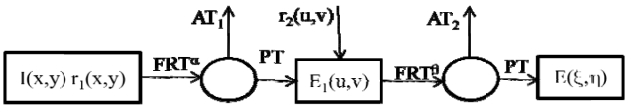


Fig 5(a). Schematic diagram for optical encryption and decryption

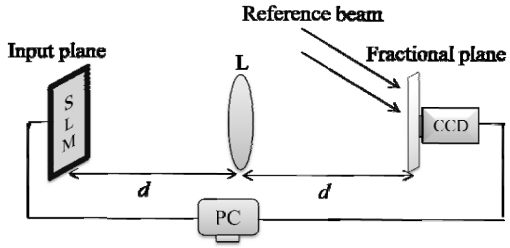


Fig 5(b). Block diagram for optical encryption and decryption

For simulation study an image of capsicum as shown in Fig 3(a) has been used. Figure 6(a) shows the encrypted image and Fig 6(b) shows the decrypted image obtained after using correct fractional orders along with other keys. Figures 6(c-h) show the decrypted images obtained after using fractional orders with difference of 0.02, 0.04, 0.06, 0.08, 0.1, and 0.12, respectively.

Now we discuss fractional domain asymmetric encryption schemes which have been combined with other encryption schemes. An image encryption scheme for securing multiple images which combines the concept of interference principle and phase-truncation approach has been proposed in Ref. 75. In this encryption scheme, multiple images are encoded into phase-truncated function and individual and common keys generated for multiple images. Then, phase-truncated function is encoded into two phase-only functions using optical interference.

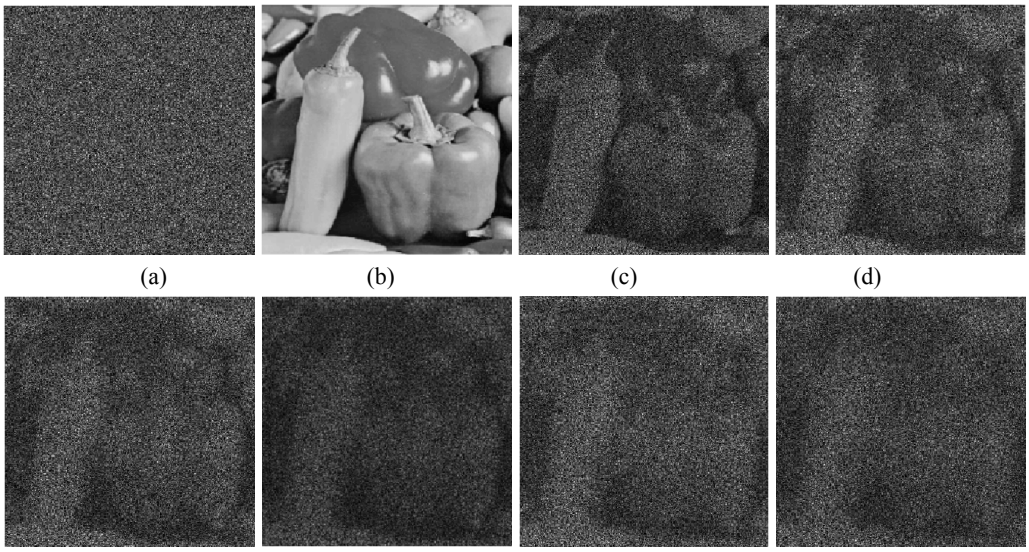


Fig 6 (a). Encrypted image in FRT domain, (b) decrypted image obtained after using correct fractional orders along with other keys, (c-h) decrypted images obtained after using different fractional orders with differences 0 .02, 0.04, 0.06, 0.08, 0.1, and 0.12, respectively.

For decryption, the two POMs which were generated analytically interfere with each other and the phase-truncated function is obtained. Finally, original images are obtained by reverse concept of phase truncation based encoding. Usually, the collimation of two beams into co-axis is not a simple task. The collimation which is always needed for optical decryption of interference based encryption scheme has been sort out by using a PSDOE. In this scheme, the collimation is easier since all optical elements are in the same optical axis. This concept has been used for single channel color image encryption in FRT domain [76]. Wang *et al* [77] proposed color image hiding based on phase-truncation and phase retrieval technique. They also proposed an asymmetric multiple-image hiding using phase retrieval technique based on amplitude- and phase-truncation [78]. Further, FRT domain asymmetric cryptosystems and its cryptanalysis have also been reported [79]. An asymmetric cryptosystem for securing multiple images using two beam interference principles has also been proposed [80].

C. *Fresnel transform domain*

An optical image encryption based on asymmetric cryptosystem in the FrT domain has been proposed by Chen and Chen [81], for securing color images. Recently, FrT domain asymmetric cryptosystems using different schemes have been reported [82,83]. In this section, first we discuss FrT domain optical asymmetric cryptosystem based on amplitude- and phase-truncation approach. These cryptosystems have been combined with other schemes for security enhancement [82-85]. Also, such cryptosystems have shown immunity against various types of attacks like known-plaintext and chosen plaintext attacks [82].

The encryption and decryption processes of FrT domain optical asymmetric cryptosystem based on amplitude- and phase-truncation can be illustrated by using Figs 1(a) and (b) by replacing FT with FrT operation. For encryption, an image to be encrypted, $f(x,y)$, is multiplied with RPM, $\exp[i2\pi r_1(x,y)]$, and then its FrT is obtained [82-84],

$$E_1(u,v) = \frac{\exp\left\{\dfrac{i2\pi z}{\lambda}\right\}}{i\lambda z}\iint \left\{e(x,y)\times \exp[i2\pi r_1(x,y)]\right\}\times \exp\left[\frac{i\pi}{\lambda z}\left((x-u)^2+(y-v)^2\right)\right]dxdy \tag{9}$$

Here λ denotes the wavelength, z denotes free space propagation distance, and (x, y) and (u, v) are the coordinates of input and Fresnel planes, respectively. Here $r_1(x,y)$ is a random phase function uniformly distributed in the interval $[0, 2\pi]$. Similarly, Eqs (1) to (6) can be used for encryption and decryption processes by replacing FT with FrT function.

The encryption process should be realized digitally using a computer and decryption can be realized optically using an optical set-up as shown in Fig. 2 by replacing lens with free space propagation. The phase-truncated image bonded with the second decryption key, can be displayed over an electrically addressed SLM and its FrT can be obtained, which should be recorded with a CCD camera and stored in a personal computer for further numerical processing.

The FrT domain asymmetric cryptosystem has been combined with the polarized light encoding in Ref. 85. The phase-truncated value obtained by asymmetric cryptosystem is encoded and decoded by using the concept of Stokes-Mueller (S-M) formalism. Image encryption based on polarization using S-M formalism has main advantage over Jones vector formalism that it manipulates only intensity information, which is a measurable quantity. Thus any intensity image can be encrypted and decrypted using this scheme. The proposed encryption scheme offers several advantages such as lens free setup, flexibility in the encryption key design, uses asymmetric keys, and have immunity against special attack [85].

A collision attack has been carried out on an asymmetric cryptosystem based on phase- truncated FrT [86]. In this attack, two distinct inputs can generate identical output. An attacker finds the encryption keys in such a way that when it is applied to encrypted image it produces an arbitrary image instead of original one. It has been proved that asymmetric cryptosystem based on phase- truncation approach is vulnerable to collision attack.

A known-plaintext attack has been carried out on phase-truncation-based cryptosystem, in which two asymmetric decryption keys are generated for decrypting original image independent of the encryption domain [87]. Recently, a nonlinear cryptosystem based on G-S phase-retrieval algorithm in FrT domain has been proposed [88]. In this scheme, two asymmetric keys are generated from G-S phase retrieval algorithm.

2.2 Phase-retrieval based approach

A. *Encryption*

Phase-retrieval algorithm is another approach which has been used for implementing the asymmetric cryptosystem [74]. In this scheme, phase retrieval algorithm such as Yang-Gu algorithm is used for obtaining encrypted image in FT domain with the help of amplitude modulation. G-S algorithm is also used for obtaining two levels of encryption in FrT domain with the help of amplitude modulation [88]. For obtaining the first level of encryption, image to be encrypted and RPM are used as input to the phase-retrieval algorithm. For obtaining the second level of encryption, intermediate amplitude value of first step of phase-retrieval algorithm and a second RPM are used as input to the phase-retrieval algorithm.

Suppose $g(x, y)$ is input plaintext to be encrypted and $exp\{i2\pi r_1(x, y)\}$ is the RPM. The product of the amplitude of input plaintext to be encrypted and the RPM after n^{th} iteration is written as a complex function, $g_n'(x, y)$

$$g_n'(x,y) = \left|g(x,y)\right| \times \exp\{i2\pi r_n(x,y)\} \tag{10}$$

The FT of above complex function (Eq (10)) is calculated a

$$\begin{aligned} G_{n+1}(u,v) &= FT\left[g'_n(x,y)\right] \\ &= FT\left[\left|g(x,y)\right| \times \exp\left\{i2\pi r_n(x,y)\right\}\right] \\ &= \left|G_{n+1}(u,v)\right| \times \exp\left\{i\varphi_n(u,v)\right\} \end{aligned} \tag{11}$$

The obtained amplitude, G_{n+1} (u,v) in Eq.(11) is called the first level of encryption. The first decryption key is obtained with the help of phase, $\exp(i\varphi_n(u, v)$. Replace amplitude with random amplitude mask, $R_1(u,v)$ as

$$G'_{n+1}(u,v) = R_1(u,v) \times \exp\{i\varphi_n(u,v)\} \tag{12}$$

Here, RPM, $exp\{i2\pi r_1(x, y)\}$ and random amplitude mask, $R_1(u, v)$ serve as a encryption keys for the first level of encryption. Now inverse FT perform as

$$\begin{aligned} G''_{n+1}(x,y) &= IFT[G'_{n+1}(u,v)] \\ &= \left|G''_{n+1}(x,y)\right| \times \exp\{i\varphi_n(x,y)\} \end{aligned} \tag{13}$$

Amplitude of Eq. (13) is replaced with amplitude of plaintext to be encrypted

$$\begin{aligned} g'_{n+1}(x,y) &= \left|g(x,y)\right| \times \exp(i\varphi_n(u,v) \\ &= \left|g(x,y)\right| \times \exp\{ir_{n+1}(u,v)\} \end{aligned} \tag{14}$$

Convergence of the iteration process is completed by calculating mean square error (MSE) between $abs[G_{n+1}''(x, y)]$ and $abs[g(x, y)]$, which is defined as

$$MSE = \frac{\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}[\left|g(x,y)\right| - \left|G''_{n+1}(x,y)\right|]^2}{N \times N} \tag{15}$$

For obtaining the second level of encryption, G-S algorithm is again used. Now the first level of encrypted image, $G_{n+1}(u,v)$ and another RPM, $exp\{i2\pi r_2(x,y)\}$ are used as input to G-S algorithm.

The encryption of second level is also obtained by similar steps as used during first level of encryption. Any complex function $D_m'(u,v)$ after m^{th} iteration can be written with the help of first level of encrypted image, $G_{n+1}(u,v)$ and another *RPM*, $exp\{i2\pi r_2(u,v)\}$ as

$$D'_m(u,v) = \left|G_{n+1}(u,v)\right| \times \exp\{i2\pi r_{2m}(u,v)\} \tag{16}$$

The FT of Eq. (16) is calculated as

$$\begin{aligned} D_{m+1}(x,y) &= FT\left[D'_m(u,v)\right] \\ &= \left|D_{m+1}(x,y)\right| \times \exp\{i\varphi'_m(x,y)\} \end{aligned} \tag{17}$$

Replace amplitude with another random amplitude mask, $R_2(x,y)$

$$D'_{m+1}(x,y) = R_2(x,y) \times \exp\{i\varphi'_m(x,y)\} \tag{18}$$

Then inverse FT of Eq. (18) is calculates as

$$\begin{aligned} D''_{m+1}(u,v) &= IFT\left[D'_{m+1}(u,v)\right] \\ &= \left|D''_{m+1}(u,v)\right| \times \exp\{i\varphi''_m(u,v)\} \end{aligned} \tag{19}$$

Now the amplitude is replaced with intensity of first level of encrypted image

$$D'_{m+1}(u,v) = \left|G_{n+1}(u,v)\right| \times \exp(i\varphi''_m(u,v) = \left|G_{n+1}(u,v)\right| \times \exp\{ir_{2(m+1)}(u,v)\} \tag{20}$$

In this case, the convergence of the iteration process is completed by computing MSE between $abs[D''_{m+1}(u, v)]$ and $abs[G_{n+1}(u, v)]$. The second RPM, $exp\{i2\pi r_2(x, y)\}$ and second random amplitude mask, $R_2(u, v)$ are the encryption keys for second level of encryption. Here amplitude of $D_{m+1}(x, y)$ [Eq (14)] is the encrypted image.

The block diagram of asymmetric cryptosystem based on phase-retrieval algorithm in FT domain is shown in Fig 7. The use of phase-retrieval algorithm randomizes the input plaintext during encryption and due to the use of random amplitude mask; it offers better security [84].

For decryption of original images, the asymmetric decryption keys are calculated with the help of Eqs (11), (17), and (20), as follows

$$p_1(u,v) = \exp\{i\varphi_n(u,v)\} \times \exp\{-ir_{2(m+1)}(u,v)\} \tag{21}$$

$$p_2(x,y) = \exp\{i\varphi'_m(x,y)\} \tag{22}$$

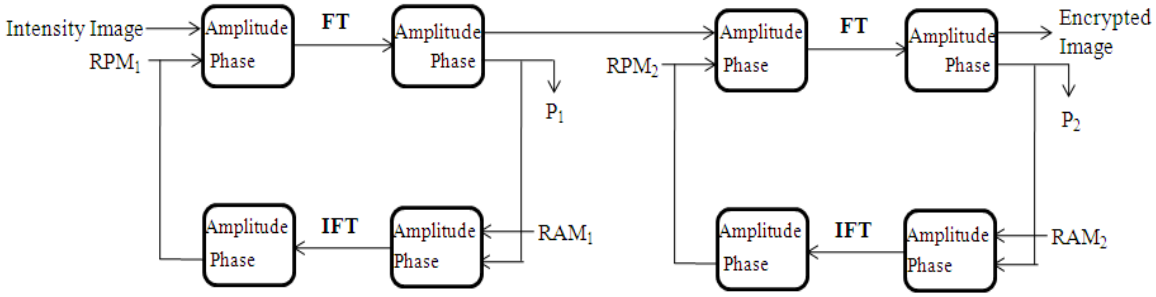


Fig 7. Block diagram for optical encryption and decryption

It can be found that the inverse FT of Eq (17) is equivalent to Eq (20) and if it is multiplied with $exp\{-ir_{2(m+1)}(u, v)\}$, then it returns to the first level of encrypted image, $G_{n+1}(u, v)$. In this scheme, both the decryption keys are not same as intermediate phases obtained through the G-S phase-retrieval algorithm. They are derived from intermediate phases. Therefore, the decryption keys can retrieve the original image using basic DRPE architecture.

B. *Decryption*

For decryption, the encrypted image multiplied with second asymmetric key is inverse Fourier transformed. The obtained Fourier transformed function is further multiplied with first asymmetric key and inverse Fourier transformed. Theoretically, the decrypted image is obtained by using both asymmetric keys as

$$d_1(u,v) = FT[\left|D_{m+1}(x,y)\right| \times p_2(x,y)] \tag{23}$$

$$d(x,y) = IFT[d_1(u,v) \times p_1(u,v)] \tag{24}$$

The decryption procedure of proposed scheme can be realized optically with the help of DRPE architecture, as shown in Fig 8. In this DRPE based decryption scheme, an encrypted image bonded with second decryption key is placed in the input plane and illuminated with a coherent light source. Its Fourier spectrum is multiplied with second decryption key, which can be placed at Fourier plane. Intensity of decrypted image can be recorded at output plane through a CCD camera.

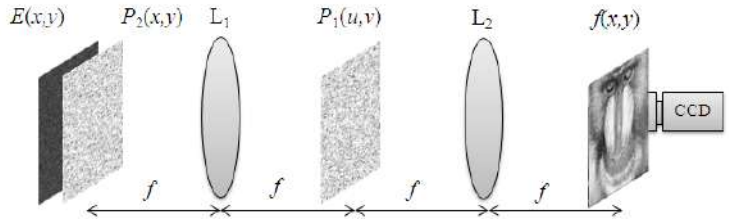
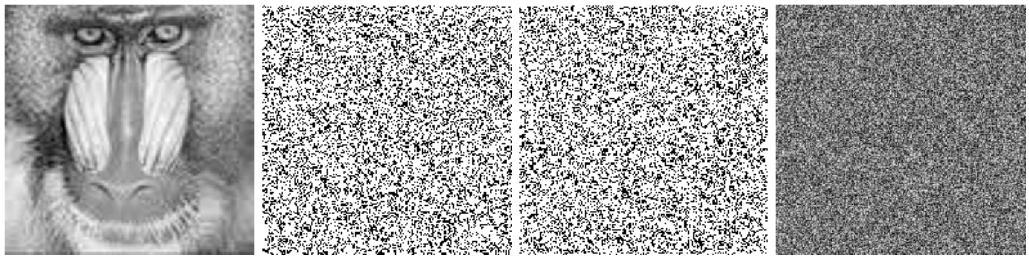


Fig 8. Schematic diagram for optical decryption

For numerical simulation, an image of baboon, as shown in Fig 9(a) has been used. Figures 9(b) and (c) show the first and second asymmetric decryption keys, respectively. Figure 9(d) shows the encrypted image. Figure 10(a) shows the relation between values of MSE and number of iterations during generation of first asymmetric decryption key. Figure 10(b) shows the relation between values of MSE and number of iterations during generation of second asymmetric decryption key.

Figure 11(a) shows the decrypted image of baboon obtained after using all correct keys. Figure 11(b) and (c) show the decrypted images of baboon obtained after using wrong decryption keys and encryption keys, respectively. Figure 11(c) shows the decrypted image of baboon obtained after using keys generated according to phase truncation approach.

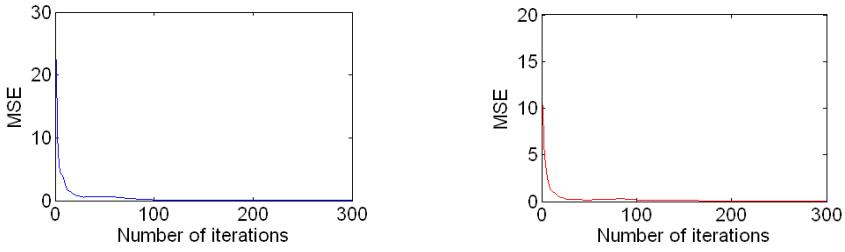


(a) (b) (c) (d)

Fig 9(a). An image of baboon to be encrypted, (b) first decryption key, (c) second decryption key, and (d) encrypted image.

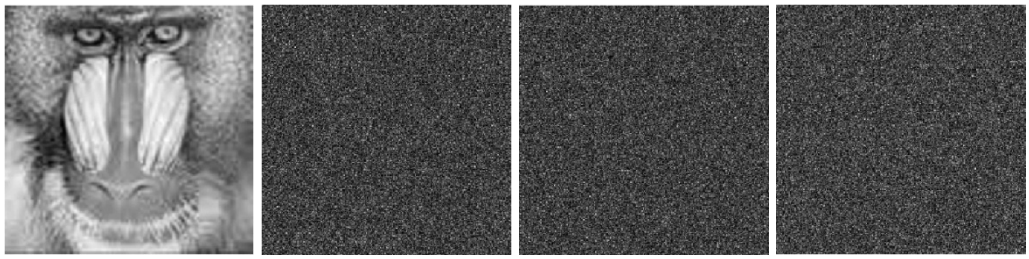
Recently, it has been a subject of discussion that the asymmetric cryptosystems based on PTFT [63] and asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm [74] and their derivatives are not asymmetric cryptosystems in true sense [89]. It has been claimed that the authors have ignored a fundamental rule in designing an asymmetric cryptosystem. According to fundamental rule of asymmetric cryptosystem, public and private keys should be independent of the image to be encrypted. But, in a recent communication it has been agreed that these cryptosystems can be called as an 'optical asymmetric cryptosystem' rather than 'asymmetric cryptosystem' [90, 91]. It is not necessary that an optical cryptosystems should follow exactly the same terminology, structures, and algorithms of general digital cryptography [90]. Wang *et al* [91] reported a detailed discussion on asymmetric cryptosystem and proposed a new attack on optical asymmetric cryptosystem based on PTFT. They argued that optical cryptosystems and digital cryptosystems are two different kinds of cryptosystems.

Deng [92] proposed a hybrid attack on double images encryption method with resistance against the specific attack based on an asymmetric algorithm. An optical asymmetric cryptography using 3D space based model has also been proposed [93]. In this scheme, RPM and plaintext are combined as a series of particles. Liu *et al* [94] also proposed asymmetric cryptosystem by using modular arithmetic operation based on DRPE. Most recently, Fan *et al* [95] proposed asymmetric cryptosystem based on two step phase-shifting interferometry and elliptic curve algorithm.



(a) (b)

Fig 10. (a) plot between MSE and number of iterations during generation of first decryption key and (b) plot between MSE and number of iterations during generation of second decryption key.



(a) (b) (c) (d)

Fig 11 (a). Decrypted image obtained after using all correct keys, (b) decrypted image obtained after using all wrong decryption keys, (c) decrypted image obtained after using encryption keys, and (d) decrypted image obtained after using keys generated according to phase truncation approach.

4 Conclusion

Various asymmetric image encryption schemes in Fourier, Fresnel, and FRT domains based on amplitude- and phase-truncation and phase-retrieval algorithm have been reviewed. It has been found that these cryptosystems have immunity against most of the attacks because of non-linearity in such asymmetric cryptosystems. It has also been found that some of the asymmetric schemes are vulnerable to special kind of attacks in which two encryption keys are considered as public keys. The asymmetric cryptosystems in variants scheme like FrT and FRT domains offer better security as compared to FT domain schemes.

References

1. Rhee M Y, Cryptography and Secure Communication, McGraw-Hill, (1994).
2. Beckett B, Introduction to Cryptography, Blackwell scientific publication, Oxford, Chap. 14, (1988).
3. Javidi B (Ed), Optical and Digital Techniques for Information Security, Springer, (2005).
4. Kaufmann G H (Ed), Advances in Speckle Metrology and Related Techniques, Wiley, (2011).
5. Gonzalez R C, Woods R E, Digital Image Processing, 2nd edn, Prentice Hall, (2002).
6. Goodman J W, Introduction to Fourier Optics, 3rd edn, Viva Books, (2007).
7. Hariharan P, Basics of Holography, Cambridge Univ Press, 2002.
8. Schnars U, Jueptner W, Digital Holography: Digital Hologram Recording, Numerical Recording, and Related Techniques, Springer-Verlag, (2005).
9. Javidi B, Horner J L, Optical pattern recognition for validation and security verification, *Opt Eng*, 33(1994)1752-1756.
10. Javidi B, Zhang G, Li J, Experimental demonstration of random phase encoding technique for image encryption and image verification, *Opt Eng*, 35(1996)2506-2512.
11. Doh Y H, Yoon J S, Choi K H, Alam M S, Optical security system for the protection of personal identification information, *Appl Opt*, 44(2005)742-750.

12. Takai N, Mifune Y, Digital watermarking by holographic technique, *Appl Opt,* 41(2002)865-873.
13. Nishchal N K, Optical image watermarking using fractional Fourier transform, *J Opt,* (Springer-India), 38(2009)22-28.
14. Nishchal N K, Hierarchical encrypted image watermarking using fractional Fourier domain random phase encoding, *Opt Eng*, 50(2011)097003.
15. Kishk S, Javidi B, Information hiding technique with double phase encoding, *Appl Opt*, 41(2002)5462-5470.
16. Chen Y Y, Wang J H, Lin C C, Hwang H E, Lensless optical data hiding system based on phase encoding algorithm in the Fresnel domain, *Appl Opt,* 52(2013)5247-5255.
17. Mehra I, Nishchal N K, Image hiding using joint transform correlator and modified Gerchberg-Saxton phase retrieval algorithm, *Asian J Phys,* 22(2013)167-174.
18. Mehra I, Nishchal N K, Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding, *Opt Express,* 22(2014)5474-5482.
19. Refregier P, Javidi B, Optical image encryption based on input plane encoding and Fourier plane random encoding, *Opt Lett*, 20(1995)767-769.
20. Unnikrishnan G, Joseph J, Singh K, Optical encryption by double-random phase encoding in the fractional Fourier domain, *Opt Lett*, 25(2000)887-889.
21. Hennelly B, Sheridan J T, Optical image encryption by random shifting in fractional Fourier domains, *Opt Lett*, 28(2003)269-271.
22. Nishchal N K, Naughton T J, Flexible optical encryption with multiple users and multiple security levels, *Opt Commun,* 284(2011)735-739.
23. Matoba O, Javidi B, Encrypted optical memory system using three-dimensional keys in the Fresnel domain, *Opt Lett*, 24(1999)762-764.
24. Situ G, Zhang J, Double random phase encoding in the Fresnel domain, *Opt Lett*, 29(2004)1584-1586.
25. Liu S, Guo C, Sheridan J T, A review of optical image encryption techniques, *Opt Laser Technol*, 57(2014)327-342.
26. Javidi B, Nomura T, Securing information by use of digital holography, *Opt Lett*, 25(2000)28-30.
27. Nishchal N K, Joseph J, Singh K, Securing information using fractional Fourier transform in digital holography, *Opt Commun,* 235(2004)253-259.
28. Meng X F, Cai L Z, Xu X F, Yang X L, Shen X X, Dong G Y, Wang Y R, Two-step phase-shifting interferometry and its application in image encryption, *Opt Lett*, 31(2006)1414-1416.
29. Unnikrishnan G, Pohit M, Singh K, A polarization encoded optical system using ferroelectric spatial light modulator, *Opt Commun,* 185(2000)25-31.
30. Matoba O, Javidi B, Secure holographic memory by double-random polarization encryption, *Appl Opt,* 43(2004)2915-2919.
31. Biener G, Niv A, Kleiner V, Hasman E, Space-variant polarization scrambling for image encryption obtained with subwavelength gratings, *Opt Commun*, 261(2006)5-12.
32. Alfalou A, Brosseau C, Dual encryption scheme of images using polarized light, *Opt Lett*, 35(2010)2185-2187.
33. Dubreuil M, Aflalou A, Brosseau C, Robustness against attacks of dual polarization encryption using Stokes-Mueller formalism, *J Opt*, 14(2012)094004.
34. Zhang Y, Wang B, Optical image encryption based on interference, *Opt Lett*, 33(2008)2443-2445.
35. Zhang Y, Wang B, Dong Z, Enhancement of image hiding by exchanging two phase masks, *J Opt A: Pure Appl Opt*, 11(2009)125406.
36. Weng D, Zhu N, Wang Y, Xie J, Liu J. Experimental verification of optical image encryption based on interference, *Opt Commun,* 284(2011)2485-2487.
37. Kumar P, Joseph J, Singh K, Optical image encryption using jigsaw transform for silhouette removal in interference-based methods and decryption with single spatial light modulator, *Appl Opt,* 50(2011)1805-1811.
38. Qin Y, Gong Q, Interference based multiple-image encryption with silhouette removal by position multiplexing, *Appl Opt,* 52(2013)3987-3992.

39. Zhu N, Wang Y, Liu J, Xie J, Zhang H, Optical image encryption based on interference of polarized light, *Opt Express,* 17(2009)13418-13424.
40. Niu C H, Wang X L, Lv N. G, Zhou Z H, Li X Y, An encryption method with multiple encrypted keys based on interference principle, *Opt Express,* 18(2010)7827-7834.
41. Situ G, Zhang J, Multiple image encryption by wavelength multiplexing, *Opt Lett*, 30(2005)1306-1308.
42. Shortt A E, Naughton T J, Javidi B, Compression of optically encrypted digital holograms using artificial neural networks, *IEEE J Display Technol*, 2(2006)401-410.
43. Barrera J F, Henao R, Torroba R, Tebaldi M, Bolognini N, Multiplexing encryption-decryption via lateral shifting of a random phase mask, *Opt Commun,* 259(2006)532-536.
44. Hwang H E, Chang H T, Lie W N, Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain, *Opt Lett,* 34(2009)3917-3919.
45. Alfalou A, Brosseau C, Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption, *Opt Lett*, 35(2010)1914-1916.
46. Alfalou A, Mansour A, Double random phase encryption scheme to multiplex and simultaneous encode multiple image, *Appl Opt,* 48(2009)5933-5947.
47. Deng X, Zhao D, Multiple-image encryption using phase retrieval algorithm and intermodulation in Fourier domain, *Opt Laser Technol*, 44(2012)374-377.
48. Zhang S, Karim M A, Color image encryption using double random phase encoding, *Microwave Opt Tech Lett*, 21(1999)3118-3123.
49. Chen L, Zhao D, Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms, *Opt Exp,* 14(2006)8552-8560.
50. Joshi M, Shakher C, Singh K, Color image encryption and decryption using fractional Fourier transform, *Opt Commun*, 279(2007)35-42.
51. Joshi M, Shakher C, Singh K, Phase image encryption of colored images using double random phase encoding techniques in HSV color space, *Opt Rev*, 16(2009)511-516.
52. Shi X, Zhao D, Color image hiding based on the phase retrieval technique and Arnold transform, *Appl Opt*, 50(2011)2134-2139.
53. Chen L, Zhao D, Color image encoding in dual fractional Fourier-wavelet domain with random phases, *Opt Commun,* 282(2009)3433-3438.
54. Joshi M, Shakher C, Singh K, Fractional Fourier transform based image multiplexing and encryption technique for four-color images using input images as keys, *Opt Commun*, 283(2010)2496-2505.
55. Deng X, Zhao D, Single channel color image encryption using a modified Gerchberg-Saxton algorithm and mutual encoding in the Fresnel domain, *Appl Opt,* 50(2011)6019-6025.
56. Hwang H E, Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain, *Opt Commun,* 285(2012)567-573.
57. Carnicer A, Usategui M M, Arcos S, Juvells I, Vulnerability to chosen-cyphertext attacks of the optical encryption schemes based on double random phase keys, *Opt Lett*, 30(2005)1644-1646.
58. Peng X, Chang P, Wei H, B Yu, Known plaintext attack on optical encryption based on double random phase keys, *Opt Lett*, 31(2006)1044-1046.
59. Frauel Y, Castro A, Naughton T J, Javidi B, Resistance of the double random phase encryption against various attacks, *Opt Express,* 15(2007)10253-10265.
60. Peng X, Wei H, Zhang P, Chosen-plaintext attack on lensless double random phase encoding in Fresnel domain, *Opt Lett*, 31(2006)3261-3263.
61. Qin W, Peng X, Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys, *J Opt* 11(2009)075402.
62. Peng X, Wie H, Zhang P, "Asymmetric cryptography based on wavefront sensing, *Opt Lett*, 31(2006)3579-3581.

63. Qin W, Peng X, Asymmetric cryptosystem based on phase-truncated Fourier transforms, *Opt Lett*, 35(2010)118-120.
64. Qin W, Peng X, Meng X, Gao B, Universal and special keys based on phase-truncated Fourier transform, *Opt Eng,* 50(2011)080501.
65. Wang X, Zhao D, Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain, *Opt Commun,* 284(2011)148-152.
66. Wang X, Zhao D, Double-image self-encoding and hiding based on phase-truncated Fourier transforms and phase retrieval, *Opt Commun,* 284(2011)4441-4445.
67. Deng X, Zhao D, Single channel color image encryption based on asymmetric cryptosystem, *Opt Laser Tech*, 44(2012)136-140.
68. Wang X, Zhao D, A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms, *Opt Commun,* 285(2012)1078-1081.
69. Wang X, Zhao D, Security enhancement of a phase-truncation based image encryption algorithm, *Appl Opt*, 50(2011)6645-6651.
70. Wang X, Zhao D, Double images encryption method with resistance against the specific attack based on an asymmetric algorithm, *Opt Express,* 20(2012)11994-12003.
71. Ding X, Deng X, Song K, Chen G, Security improvement for asymmetric cryptosystem based on spherical wave illumination, *Appl Opt,* 52(2013)467-473.
72. Mehra I, Rajput S K, Nishchal N K, Cryptanalysis of an image encryption scheme based on joint transform correlator with amplitude and phase-truncation approach, *Opt Lasers Eng*, 52(2014)167-173.
73. Wang X, Zhao D, Amplitude-phase retrieval attack free cryptosystem based on direct attack to phase-truncated Fourier transform-based encryption using a random amplitude mask, *Opt Lett,* 38(2013)3684-3686.
74. Liu W, Liu Z, Liu S, Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm, *Opt Lett,* 38(2013)1651-1653.
75. Rajput S K, Nishchal N K, Image encryption based on interference that uses fractional Fourier domains asymmetric keys, *Appl Opt*, 51(2012)1446-1452.
76. Rajput S K, Nishchal N K, Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask, *Appl Opt*, 51(2012)5377-5386.
77. Wang Q, Guo Q, Zhou J, Color image hiding based on phase-truncation and phase retrieval technique in fractional Fourier domain, *Optik,* 124(2013)1224-1229.
78. Wang Q, Guo Q, Lei L, Asymmetric multiple-image hiding using phase retrieval technique based on amplitude and phase-truncation in fractional Fourier domain, *Optik,* 124(2013)3898-3902.
79. Rajput S K, Nishchal N K, Fractional domain asymmetric cryptosystem and cryptanalysis, *Proc SPIE,* 8769(2013)87691Y.
80. Mehra I, Nishchal N K, Asymmetric cryptosystem for securing multiple images using two beam interference phenomenon, *Opt Laser Technol*, 60(2014)1-7.
81. Chen W, Chen X, Optical color image encryption based on asymmetric cryptosystem in the Fresnel domain, *Opt Commun,* 284(2011)3913-3917.
82. Rajput S K, Nishchal N K, Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform, *Appl Opt*, 52(2013)871-878.
83. Rajput S K, Nishchal N K, Security enhanced asymmetric cryptosystem in Fresnel domain, *Asian J Phys,* 22(2013)117-126.
84. Rajput S K, Nishchal N K, Multiple image encryption based on known-plaintext attack and modified G-S phase retrieval algorithm, *Proc SPIE,* 8769(2013)87690X.
85. Rajput S K, Nishchal N K, Image encryption using polarized light encoding and amplitude- and phase-truncated Fresnel transform, *Appl Opt,* 52(2013)4343-4352.
86. Mehra I, Rajput S K, Nishchal N K, Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification, *Opt Eng*, 52(2013)028202.

87. Rajput S K, Nishchal N K, Known-plaintext attack on encryption domain independent optical asymmetric cryptosystem, *Opt Commun,* 309(2013)231-235.
88. Rajput S K, Nishchal N K, Fresnel domain nonlinear image encryption scheme based on Gerchberg-Saxton phase-retrieval algorithm, *Appl Opt,* 53(2014)418-425.
89. He W, Meng X, Peng X, Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang–Gu algorithm: comment, *Opt Lett*, 38(2013)4044-4044.
90. Liu W, Liu Z, Liu S, Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang–Gu algorithm: reply, *Opt Lett*, 38(2013)4045-4045.
91. Wang X, Chen Y, Dai C, Zhao D, Discussion and a new attack o f the optical asymmetric cryptosystem based on phase-truncated Fourier transform, *Appl Opt*, 53(2014)208-213.
92. Deng X, A hybrid attack on double images encryption method with resistance against the specific attack based on an asymmetric algorithm, *Opt Commun,* 317(2014)7-12.
93. Chen W, Chen X, Optical asymmetric cryptography using a three-dimensional space-based model, *J Opt*, 13(2011)075404.
94. Liu W, Liu Z, Wu J, Liu S, Asymmetric cryptosystem by using modular arithmetic operation based on double random phase encoding, *Opt Commun,* 301-302(2013)56-60.
95. Fan D, Meng X, Wang Y, Yang X, Peng X, He W, Asymmetric cryptosystem and software design based on two-step phase-shifting interferometry and elliptic curve algorithm, *Opt Commun,* 309(2013)50-56.

-

[*Received*: 1.3.2014; *accepted*: 22.4.2014]