JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 262 - 274
https://publishoa.com
ISSN: 1309-3452

A Comprehensive Study on Design and Development of Optical Image Encryption Techniques

Anshika Malsaria,
Manipal University Jaipur

Pankaj Vyas,
Associate Professor, Manipal University Jaipur

Manjit Kaur,
Gwangju Institute of Science and Technology

ABSTRACT
Since image processing algorithms can work with a vast volume of data easily, optical cryptographic techniques are commonly used in image security. Since the proposed DRPE, image encryption in particular has gotten a lot of coverage. DRPE employs various approaches for example-4f and Fourier Transform (FT) to encrypt local as well as spectral data; image encryption is done on the basis of input along with the Fourier planes using random phase coding. The complete process of encryption transforms the input image to awhite sound in this manner. Confidentiality is obtained by the method of translation. Only when the information of location and the secret key are perfectly matched would the secret picture be revealed. Random category masks may be thought of as hidden keys in general, and since the key space is too big, blind deconvolution alone is insufficient to reconstruct the original picture. The standard DRPE methodology was discussed in this paper, as well as its numerical emulation, sampling considerations in the spatial as well as frequency domains, and the benefits and drawbacks of different transforms. Additionally, certain optical coding and scrambling methods are investigated. The paper ends with a discussion of recent advances in the area of optical image encryption, as well as a look forward to the future challenges.

Keywords*:* DRPE, AES, Ptychography, Cryptography, Re-Encryption

Introduction
The popularity of the internet is growing day by day. Information like text, images, videos are widely transferred over the Internet. All the Information are prevented with some mean of security parameters that provide legitimate user authentication. A variety of encryption algorithms are present to secure communication channels. The majority of internet users do not aware of the security implemented on channels. As the digital market is growing, the security issues are also growing. In many online transactions, the user's identity is very important. Securing the authentication details based on various security mechanisms requires. Without protection personal and companies' information may be at high risk. A lot of money spent on research and development of security algorithm and technologies. Military services also require a highly secure platform to transfer secret information over secure lines. Most of the information is image-based. So, the requirement of a good security mechanism otherwise the important information will be open for security threats like modification, duplication, eavesdropping [1-10]. Optical encryption technology comes into light after the proposal of Réfrégier and Javidi (1995) Double random phase encryption. Optical encryption has the capability of high speed and parallel processing. Double random phase encryption works in various domains like fraction Fourier transform, Fresnel transform, Linear canonical transform, Gyrator transform, Hartley transform. These transforms help the DRPE to improve flexibility, security, and implementation. The main advantages of optical encryption are -(i)Optical instruments having capabilities of parallel processing (modulator and lenses). ii)Optical encryption method having capabilities to work in multidimensional and multiple parameters. iii)optical encryption requires the knowledge of optics, computer

applications, image processing, signal processing so attackers need to understand all the things before attacking the optics cryptosystem [81-85].

Most image encryption researches in past years based on the DRPE encryption technique. It's built on the 4f optical system idea. In image processing, random-phase encoding is used to encode the input and Fourier planes. Since, DRPE(acronym for double random phase encryption) performs various image multiplication with the help of random phase mask (RPM) in both the spatial and temporal domains (DRPE). The input picture is transformed to white noise during the encryption process. The encrypted image is captured using digital holographic technologies. In the encryption method, the second RPM serves as a

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 262 - 274
https://publishoa.com
ISSN: 1309-3452

hidden key. The method of decryption is the opposite of encryption. The original picture will reform if the hidden key and its spatial details are perfectly balanced. Two concerns with DRPE were found. The hidden keys, for instance, are the same resolution as the original pic, whichis way too high. Second, since DFT-DRPE needs a lot of room, the computational cost is very high.

The architecture of the (DRPE) method is used to study the optical encryption technique in this article [11-30].The optical surveillance system's benefits and drawbacks are discussed. This analysis would provide useful information about existing optical protection system technologies which will aid in future innovations. There are three purposesof this article.:

(i) The project was based on a detailed review of current optical image encryption techniques.
(ii) Considering all possible cryptanalysis methods.
(iii) There are benefits and disadvantages to of optical image encryption technique. Some methods are resistant to a number of threats, but they have problems with computational speed and latency. As a result, the difference between computational speed and efficiency against different security threats must be explored.

This paper's major contributions are as follows::

A thorough investigation of various optical image encryption methods was carried out. The various transforms, as well as traditional DRPE and efficiency tests, have been explored in relation to optical image encryption techniques.
Differential and key tests have been conducted on current encryption methods. Future research directions in the development of effective optical image encryption techniques have been investigated.

1. Structural analysis of DRPE technique

The implementation of DRPE is done by making the optical setup called 4f is shown in Figure 1. [4]

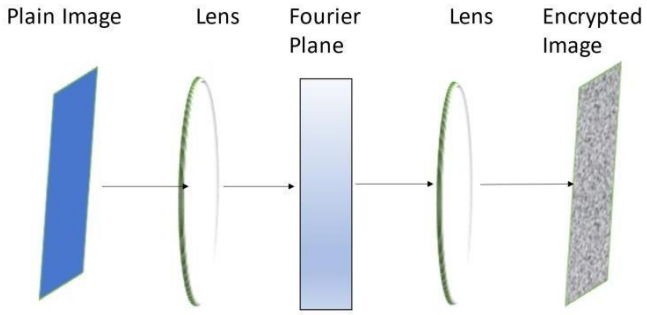

Figure 1: DRPE 4f setup

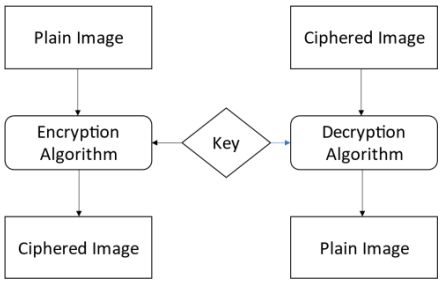

*Figure 2***:** General approach for image encryption

Here a filter performs the masking and then the second activity will done by lens that is the inverse Fourier transform^{-1} in the output plane to get the encrypted image. There are only two-phase plates in DRPE which are used as a secret key. To improve performance and key, fractional Fourier transform (FRT) was used with the DRPE scheme [8]. There are three planes in DRPE: input plane, second is encrypted plane, and third is output plane. The keyspace is larger than traditional DRPE as the FRT is having three parameters that connect any two outof three planes; so, the secret key is two-phase plates. FRT based DRPE also having six parameters which used asthe secret keys.

Working of DRPE (Double Random Phase Encryption)
In this part, DPRE is discussed along with its encryption and decryption techniques.

Encryption-
Always encryption of image based on hiding the image which is then generated by the cipher image using some algorithm with keys. In Figure 2 DRPE encryption method is shown. Here in the DRPE technique first the image monochromatic waves pass from propagator1(P1) having plane (x, y) then the OFT (optical Fourier transform) takes place on P1, then Propagator 2 P2 having plane (x, y),then again OFT2 of the plain image and finally the cipher image is obtained. All the terms come in Fourier optics image processing techniques. Alike quantum optics, optical sources information needs to be extracted by the mean of some informative tool [8]. The spatial frequency domain (kx, ky) as the conjugate of the spatial (x, y) domain is

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 262 - 274
https://publishoa.com
ISSN: 1309-3452

used in Fourier optics. The two propagators in DRPE encoding $P1(x, y)$ and $P2(x, y)$ are independent phase function and worked in spatial and frequency domain.

Refrégiér and Javidi [5] proposed the DRPE technique. This technique is based on the 4f setup (Fig. 1) that, along with the spectrum, transforms the image as input into white noise. Since images have RGB density, converting RGB to white density is needed to encrypt input images. To encrypt an image, a switch in both amplification and position knowledge is available. because at the decryption process with amplitude or phase spectral information the plain image can be reformed. Cipher image is complex value so to obtain amplitude and phase information is necessary.

$$\boldsymbol{E(x,y) = DRPE(I(x,y), P1(x,y), P2(x,y)) = OFT(I(x,y) \times P1(x,y) \times P2(x,y)}$$

(1)

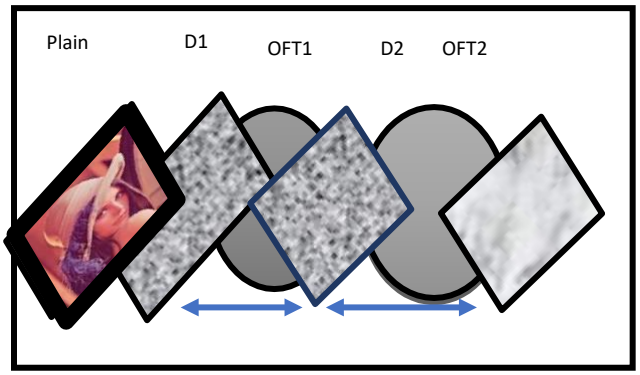

Figure 3. Encryption in DRPE

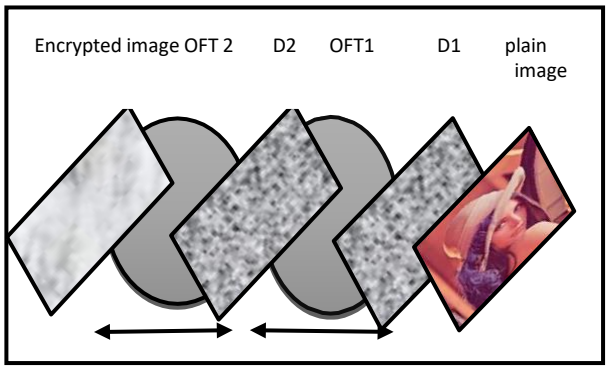

Figure 4. Decryption in DRPE

Decryption-

For decryption (ref Figure 4) the inverse process of DRPE is performed using two diffusers just like encryption and calculate their inverse optical Fourier transform.

$$\boldsymbol{(x,y) = DRPE^{-1}(E(x,y), P1(x,y), P2(x,y))}$$

$$\boldsymbol{= DRPE(E(x,y), P1 \times (-x,-y), P2 \times (-x,-y)} \qquad \textbf{(2)}$$

2. Literature Survey

A literature survey contains a review of various existing optical image encryption techniques transforms. This section discusses various DRPE transformations that are used in optical encryption algorithms to convert images in the spatial and frequency domain. They all contribute to the security of an algorithm for optical image encryption.

The joint transform correlator (JTC) [2] is used to propose optical image encryption. The initial picture and one of the stage plates are inserted into the JCT input plane in this work as encryption keys. After that, the Fourier Transform is used. The Fourier combined spectrum of combined energy is available as an enclosed image after conversion. A step pad, which serves as a reduction key, is placed in the appropriate location on the space shuttle during the deceleration period. By filtering the background frequency and converting the Fourier variables, the encrypted image is programmed on the Fourier spectrum plane. JTC encryption thus overcomes the limitations of standard DRPE. The encrypted image is accessible and does not require the use of a complex stage plate as a hidden key since it is based on Fourier's power output. The consistency of the dissipation is unchanged by improving the secret key in the input plane because it just improves the form of the hidden image.

In 2004, a new approach for embedding images on the Fresnel domain [6] was suggested. It has three planes: one for input, one for encryption, and one for output. Unlike other encryption techniques, this one does not need lenses; instead, it encrypts images using the Fresnel look. The first picture is pre-edited using a phase plate on the input plane during the encryption process. The picture is then continued in the encryption plane and modeled a second time using the Fresnel axis. Finally, the Fresnel distribution is used at the same time. Not only are the two type plates used as hidden keys in the encryption process, but the two levels of use are also used as keys.

The most commonly used encryption algorithm today is chaos-based encryption. The conflict method [9] is a strong non-linear system capable of generating a random sequence of good and suitable data encryption. To encrypt the records, a

turbulent scheme was proposed [10]. Since then, chaotic cryptography has gotten a lot of coverage as a branch of cryptography. Digital images are then encrypted with the help of a chaotic mapping approach for example- the CKBA encryption method, Kolmogorov-based encryption schemes, picture transformations and encryption, and random map-based encryption, which is generated by a complex system.

In paper [11] proposes another approach based on encryption which is the sensation of compression and double- phase randomization, which can complete image compression while still providing simultaneous encryption. To construct a measuring matrix with two random phase covers, we use a hyperchaotic method. The first image is then calculated using a matrix scale to achieve simultaneous encryption and compression, in which the compressed image is rewritten by encoding a random process with two random phase masks, and eventually the resulting image is confused and separated using a hyperchaotic method.

The Differential Evolution (DE) approach is used in this paper [12] to implement a new effective techniques for the encryption of image encryption based on the magnitude and deception of a section. The delivery of the keyed discrete Fourier transform (DFT) it operate on the principle of DE for the encryption purposes is the work's breakthrough. The hidden key has been exchanged between encryption and decryption until now. On the first image to be nailed, a four-dimensional (2-D) transformation is performed first. Second, using the Linear Feedback Shift Register (LFSR) generator, a crossover was performed between two sections of the encrypted picture. Similarly, based on the LFSR reference generator, main changes are made to the individual components of such chosen objects. To ensure the protection of emerging indices, the LFSR index creator starts the seed with a shared secret key. The picture pixels' locations are altered as a result of the operation. A new image encryption scheme based on the DE system and constructed with a simple delivery method is being created. The descriptive technique is a structured procedure that employs the same key. This embedded picture is found to be entirely skewed, allowing the planned work to become more rigid. The suggested image encryption scheme is verified by imitation results.
With the exponential growth of electronic data sharing, data protection for data collection and dissemination has become increasingly necessary. Since photographs are widely used in manufacturing processes, it is critical to safeguard sensitive image data against unauthorized entry. We evaluated existing image encryption methods and compression added two of them in this paper [13]. (Screen encryption such as Mirror and Visual Cryptography). The proposed approaches have been implemented for the sake of research. The study' findings are presented in this article.
Digital Signatures and Graphics Encryption Technology: A new approach for encrypting safe image transfer has been suggested by Aloka Sinha and Kehar Singh [19]. The original edition of the original photograph has an optical digital signature attached to it. The required debugging code, such as Bose Chaudhuri Hochquenghem (BCH)code, is used to encode the images. Since the image has been removed from the recipient, a digital signature may be used to check the image's validity.

Lost Image Encoding and Encryption Using Scanner: SS Maniccam and N.G. Bourbakis [20] have developed a modern approach for compressing and encrypting binary and gray pictures that is unmistakable. The SCAN approach produces SCAN patterns, which are used in focus and encryption schemes. SCAN is a two-dimensional, two-pronged method for locating a good location.

Fractional Fourier Transform (FFT)
The Fourier transform (FT) is further subdivided into Fractional Fourier Transform (FRT), which has one fractional-order. Under the linear transform, the Fourier transform (FT) captures the signal in the space domain androtates it by 2 radians. It is orthogonally projected in the spatial frequency domain, while FRT is similar in that it rotates orthogonally in such a way that it gets mixed in the frequency space domain to perform operations. Hence, rotation angle is directly proportional to the FRT order. As a result, the FT is the ultimate fractional Fourier transform for its Ist order [15]. In optical encryption, FRT is used to encrypt two-dimensional data. As fractional orders are applied to the x- and y-axes, the system's performance, security, and robustness improve. It defends against blind decryption attacks. FRT should be unitary in nature, conserve power, and be completely reversible.

The Fresnel transform (FST)
It's a propagation of free space. Any FST is related to a FRT using quadratic step multiplication [16]. A particular category of LCT is the FST. This is a lensless technique that requires less hardware and is simpler to implement. Planes have three parts: input, transformation, and output. The encryption and decryption processes used the locations for RPM (random step masks) as keys. The cipher image was filmed in a photorefractive medium using holographic techniques. The “Random Phase Method” and the “Jigsaw Method” are always with the two optical encryption schemes focuses on the FST also given in the

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 262 - 274
https://publishoa.com
ISSN: 1309-3452

approach. 3-phase keys in various Fresnel domains are used in the "Random Phase System." The input plane is attached to the first RPM (random phase mask), while the transform plane is attached to the second RPM. The cipher picture is generated when the device is illuminated perpendicularly with wavelength. The "Jigsaw Process," like the FRT, uses the Jigsaw transform (JT) in many Fresnel domains. Digital holographic methods necessitate encryption and decryption procedures of all frameworks.

Linear canonical transform (LCT)

The LCT transform is a multi-transform integral transform. It's a three-dimensional transform with four parameters and one restriction that's visualized in the time-frequency domain as the special linear group SL(R). The FT, FRT, as well as FST are also all variants of both the linear canonical transform (LCT), and yet they all employ quadratic phase systems (QPS) to perform their calculations [17]. The image is encrypted using DRPE [29], and LCT is used. In this encryption scheme, the randomly generated propagators, the frequency, and all of the LCT specifications have been used as keys. Another word for it is Extended FRT. In the 2D LCT, the conditional integral transform includes three elements. It is possible to use the OFT, optical FRT, FST, even general LCT.

The Gyrator transform (GT)

It falls under the category of linear canonical transforms (LCT). The GT is commonly used in optical as well as digital image recognition, holography, and model development [18]. The optical design for the GT has been recommended as three dimensions having circuit connecting across them. Every lens is made up of two identically driven convergent thin cylindrical lenses. The rotation of two thin cylindrical lenses regulates the transition angle. For a wide variety of angle parameters, this configuration will perform the GT. It belongs to the linear canonical transforms category (LCT). Using chaotic random phase masks, GT was used to encrypt the 2D file. The chaos feature manipulates the random process masks. The GT has been used as an optical image encryption scheme that employed a specific phase promising techniques. For color picture encryption, the DRPE scheme with the GT has been suggested. The affine transform and also the Arnold transform are two optical image processing approaches that are associated with GT (ART). In the sense of GT as a whole, The first random propagator D1(x;y) multiplies the input image I(x;y) before passing it into the first GT method of angle 1. The resulting image is then multiplied by the second random propagator P2(x,y) and passed through the angle 2 GT method [29].

Ref	Year	Technique	Planes/class/phase	key	Security	Research Gaps from existing work	Proposed work improvements
[16]	2019	Symmetric cryptosystem	Symmetric cryptosystem	The intensity ofthe input image	High	Security achieved in this is high but the keys functionality is not good both the sides.	Use ECC for security.
[11]	2020	In the Fresnel transform domain, key image phase as well as chaotic random phaseencoding	2 phase (image and chaotic)	Key phase mask	High	Authentication systems encode only one bit of encrypted form at a time, whereas cryptographic algorithms encrypt several bits at once (typically 64 bits in current ciphers). H	More than one bit willencrypt at a time.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 262 - 274
https://publishoa.com
ISSN: 1309-3452

[29]	2017	Gyrator transform	Every lens is made up of two identically driven convergent thin cylindrical lenses.	Using chaotic random phase masks, GT was used to encrypt the 2D file.	Much higher	Various companies use a variety of encryption schemes in the information systems field.	Proposed work can work on image as well as text.
[82]	2018	CKBA encryption method	Can produce a random sequence of good and suitable data encryption.	Image transitions and encryption and random map-based encryption	Good	Random sequence does not work sometimes.	The sender and receiver use separate keys and encryption/decryption data, implying that the key is shared. Asymmetric encryption is a term used to describe digital signature.
[12]	2011	Differential Evolution (DE) method	Keyed discrete Fourier transform (DFT) concept followed by DE operations for encryption purposes.	The secret key has been shared between both encryption	High	Secret key is same for both the sides.	Advanced version of the previous one.

Table 1: Comparison of DRPE based encryption techniques.

Factors	DRPE with AES		DRPE with 3DES		DRPE with ECC
Key Length	128,192	or	112,168		56 bits
	256 bits		bits		

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 262 - 274
https://publishoa.com
ISSN: 1309-3452

Cipher Type	Symmetric		Symmetric		Symmetric
	block cipher		block cipher		block cipher
Block Size	128,192	or	64 bits		64 bits
	256 bits				
Developed	2000		1978		1977
Security	Considered		One	only	Proven
	secure		weak which		inadequate
			exit in DES		

Table 2: Comparative analysis over security algorithms.

S.no	Types of attacks	Parameter name	Description
1	Brute force attack	Key space	The brute force attack is described asguessing the correct key by evaluating the key value, which can be thwarted by using an algorithm with a sufficiently large key space.
2	Statistical attack	(i) Histogram analysis, (ii) Correlation coefficient analysis	(i) Details will be leaked if the values of pixels in the histogram are not standardized. As a result, uniform distribution is useful for fending off statistical attacks. (ii) The encrypted image must have a low overlap with neighboring pixels (horizontal, vertical, and diagonally).
3	Differential attack	(i) NPCR (ii) UACI	(i) Number of pixels change rate – $\frac{\sum s,t D(s,t)}{M \times N} \times 100\%$ Where, M&N are width and height of image respectively, $D(s,t) = \{ 1, c1(u,v) \neq c2(u,v) \; 0, otherwise$ Where C1 and C2 represent the ciphered image before and after pixel modification. (ii) Overall changing severity on a unifiedscale – $\frac{\sum_{u,v} \lvert C_1(u,v) - C_2(u,v) \rvert}{M \times N \times 255} \times 100\%$
4	Noise attack	(i) PSNR (ii) MSE	(i) PSNR(Peak signal to noise ratio) – It computes the quality of the recovered image $10 \times log_{10} \frac{255 \times 255}{MSE} (db)$ (ii) Mean square error – It determines the MSE between the recovered and plain image.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 262 - 274
https://publishoa.com
ISSN: 1309-3452

			$\frac{1}{m,n}\sum_{p=1}^{m}\sum_{q=1}^{n} \| A_1(p,q) - A_2(p,q) \|^2$ Where A1 (p, q) is the original image and A2 (p, q) is the restored image, and m and nare the image width and height.
5	Occlusion attack	PSNR(peak signal to noise ratio)	Any data may be lost during transmission, making decrypting the picture more difficult. It's used to see how the ability to retrieve plain images from ciphered images can be tested. PSNR is a metric that is used to assess occlusion efficiency.

Table 3. Parameters and description

No	Ref No.	Year	Technique	Key Space	Compressive Sensing	Speed
[1]	[31]	2016	Bitplane decomposition and chaotic maps	0.25×10^{64}	No	Low
[2]	[73]	2016	substitution cipher as well synonymous.	10^{108}	No	Low
[3]	[74]	2016	Technique of dynamic random growth	$>10^{96}$	No	Moderate
[4]	[17]	2017	Hartley and Graytor transformation	$>2^{100}$	No	Low
[5]	[29]	2017	action on DNA sequence	8.39 × 1054	No	Good
[6]	[49]	2017	disorderly structure with a cyclic change	$8^{256\times256}$	No	Low
[7]	[69]	2017	Map lattice with mixed linear-nonlinear coupling	$>10^{120}$ No	No	Moderate
				Moderate		
[8]	[71]	2017	Sensing that is compressed	3.4×10^{38}	Yes	Good
[9]	[72]	2017	Binary bitplane	4.916×10^{322}	No	Moderate
[10]	[75]	2017	Confusion-based swapping strategy	0.18×10^{60}	No	Good
[11]	[77]	2017	The map of Arnold	$>2^{100}$	No	Moderate
[12]	[81]	2017	Self-adaptive and spatiotemporal disorderly mechanism	10^{56}	No	Moderate
[13]	[85]	2018	Mapping logically	10^{112}	Yes	Moderate
[14]	[11]	2018	High-dimensional chaotic mechanism and spatial bit level permutation	1.03×10^{114}	No	Low
[15]	[22]	2018	Bit level permutation	10^{42}	No	Low
[16]	[23]	2019	Nonlinear optical multi-image encryption scheme canonical transform	2.5×1057,which is large	No	Low
[17]	[24]	2019	Nonlinear chaotic system and linear canonical transformation	Pixel scrambling	Yes	Low

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 262 - 274
https://publishoa.com
ISSN: 1309-3452

[18]	[25]	2021	Optical image encryption based on quantum walks	10^{128}	No	Good
[19]	[26]	2021	Exploiting optical chaos	10^{114}	Yes	Moderate
[20]	[27]	2021	Hadamard single-pixel imaging and Arnold transformation	coefficient matrix key increases	No	Low
[21]	[28]	2021	Secure Optocrypto system for 2D logistic based fractional fourier	2D-FrFT angles and fractional orders	No	Moderate
[22]	[29]	2021	A fast and secure public-key image encryption scheme based on Mordell elliptic curves	public-key image encryption	No	Good

Table 4: Comparison of techniques based upon parameters

Techniques	Advantages	Disadvantages
Runlength Encoding	Simple and not require CPU power,	Useful for files with such a lot of effective combination.
Fractal Encoding	Good Encoding frame	sluggish encoding.
LZW Encoding	A complex codeword table is created	It takes up more data storage,
Arithmetic encoding	fractional values	complicated tasks
Vector Quantization	simple converter with no parameter approximation.	correct code at a very slow pace.
Huffman Encoding	data compression is both easy and effective	Good estimation is necessary for good results.
Double Random Phase Encoding (DRPE)	two random process masks. Loading time is short.	Speckle noise due to the random phase mask
Off-axis holography system	Support 3D object watermarking	Reference wave required
Phase shifting holography system	Support 3D object watermarking;	Reference wave required; Multiple host images required
Cascaded phase only mask architecture	Non-destructive to host image	Hard to implement in real optical experiment
Joint Transform Correlator (JTC)	Easy to implement optically	Not applicable for watermarking 3D object
Ghost imaging system	Simplest image detector	Long image acquisition time; Noise in reconstructed image

Ptychography	Support 3D object watermarking; Noise resistant; Easy to implement optically	Recording of multiple diffraction patterns required

Table 5: Image compression and crambling algorithms.

3. Problems Discussion

(1) Some sensor networks, along with DRPE and interleaved stage only mask systems, are complex to realize in optical applications probably a combination of processes needed underneath coherent light illumination. This problem can be fixed by combining these optical devices with indecipherable operations like authentication scheme [44,45], in which a true deciphered result is generated by an approximate combining (as well as a very precise integration) of integrated circuits.
(2) By analyzing main reference brightness patterns [46] and iterative reconstruction algorithms [47], different imaging speed in a ghost imaging system can be accelerated for watermarking. Information security and imaging speed must both be guaranteed at the same time.
(3) For a ptychography device, the amount of waste it collects is immense (multiple diffraction patterns). A compressed method must be developed to reduce data size while enhancing the stability of the retrieved wavelet domain [48]. .

The subsequentsectioncontainsvariousobjectivesrequiredtoaccomplishtheproposed technique: To study and analyzethe performance of optical image encryption algorithms.

- To design and implement novel lensless phase-based image encryption techniques.
- To utilize efficient transform domain approaches to enhance the proposed techniques further.
- To compare and validate the proposed technique with the existing optical image encryption techniquesusing some well-known quality metrics.

4. Conclusion

This paper discusses the latest optical picture encryption methods in depth. This paper based on the DRPE methodology and the different transforms that can be used in DRPE to enhance image protection. The procedure is an addition of a well-known DRPE framework that includes an additional random phase key. The efficiency of the proposed scheme is assessed, and it is observed that it is comparable to DRPE in terms of PSNR and MSE metrics, but it provides better security.
The benefits and drawbacks of fractional transformations, Fresnel transforms, Hartley transforms, and Gyrator transforms were explored. Optical picture encryption methods have been addressed in terms of their challenges and potential study directions. Optical image encryption is still an underdeveloped area, according to a study of emerging optical image encryption techniques. For upcoming projects, an alternative to building a robust and reliable technique by combining the optical encryption method with different encryption techniques.

References

[1]. Xing Yuan Wang, Yu Taohou, Shibing Wang, Ruili“ A new image encryption algorithm based on CML and DNA sequence” DOI 10.1109/ACCESS.2018.2875676, IEEE
[2]. Nomura, T., and Javidi, B. (2000). Optical encryption using a joint transform correlator architecture. Optical Engineering, 39(8), 2031–2035.
[3]. P. Réfrégier and B. Javidi, “Optical image encryption based on input plane and Fourier planerandom encoding,” Opt. Lett. 20, 767–769 (1995).
[4]. J.W. Goodman, “Introduction to Fourier optics” (McGraw-Hill)
[5]. Chen w.chen. “space-based optical image encryption”. optics express 2010:18(26)

[6]. Y Situ, G., and Zhang, J. (2004). Double random-phase encoding in the Fresnel domain. Optics Letters, 29(14), 1584–1586.
[7]. Nomura, T., and Javidi, B. "Optical encryption using a joint transform correlator architecture. Optical Engineering", 39(8), 2031–2035. (2000).
[8]. Unnikrishnan, G., Joseph, J., and Singh, K. "Optical encryption by double-random phase encoding in the fractional Fourier domain". Optics Letters, 25(12), 887–889(2000).
[9]. Li, T. Y., and Yorke, J. A. (1975). Period three implies chaos. The American MathematicalMonthly, 82(10), 985–992.
[10] Matthews, R. (1989). On the derivation of a "chaotic" encryption algorithm. Cryptologia, 13(1), 29–42.
[11]. Huiqing Huang, Shouzhi Yang, Image Encryption Technique Combining Compressive Sensingwith Double Random-Phase Encoding, Published 2018.
'[12]. Ibrahim S I Abuhaiba1 and Maaly A S Hassan2, IMAGE ENCRYPTION USING DIFFERENTIAL EVOLUTION APPROACH IN FREQUENCY DOMAIN, An International
Journal(SIPIJ) Vol.2, No.1, March 2011.
[13]. øsmet Öztürk1 and øbrahimSo÷ukpınar 2, Analysis and Comparison of Image Encryption Algorithms, World Academy of Science, Engineering and Technology International Journal of Computerand Information Engineering Vol:1, No:3, 2007.
[14]. Hennelly BM, Sheridan JT. "Optical encryption and the space bandwidth product". Optics Communications 2005;247(4-6):291–305.
[15]. Sahin A, Ozaktas HM, Mendlovic D. "Optical implementations of two dimensional fractional Fourier transforms and linear canonical transforms with arbitrary parameters". Applied Optics 1998;37(11):2130–41.
[16]. Priyanka Maana, Hukum Singh, Charan Kumaric "Symmetric cryptosystem to secure images utilizing chaotic deterministic phase mask in Fresnel transform domain employing singular value decomposition". International Conference on Computational Intelligence and Data Science (ICCIDS 2019).
[17]. Priyanka Maana, Hukum Singh, A Charan Kumari "Image encryption using the Gyrator transform and random phase masks generated by using chaos"2020 Juan M. Vilardy et al 2017 J. Phys.: Conf. Ser. 850 012012
[18]. Tajahuerce E, Lancis J, Javidi B, Andrés P. "Optical security and encryption with totally incoherent light". Optics Letters 2001;26(10):678
[19] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, 2003, 1-6
[20] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN",
Pattern Recognition 34 (2001), 1229-1245
[21] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), 83-91
[22]. Xing-Quan Fu Bo-Cheng Liu Yi-Yuan Xie Wei Li Yong Liu "Image Encryption-Then- Transmission Using DNA Encryption Algorithm and The Double Chaos" Volume 10, Number 3, June 2018
[23]. Sheng Yuan, Yangrui Yanga, Xuemei Liu, Xin Zhou, ZhenzhuoWeia "Optical image transformation and encryption by phase-retrieval-based double random-phase encoding and compressive ghost imaging"
[24]. Guanghui Ren1 •Jianan Han1 • Jiahui Fu1 • Mingguang Shan2 "Asymmetric multiple image interference cryptosystem using discrete cosine transform and conditional decomposition"
[25]. Zhengjun Liu, Hang Chen, Walter Blondel, Zhenmin Shen, Shutian "Image Security Based On Iterative Random Phase Encoding In Expanded Fractional Fourier Transform Domains" Optics and Lasers in Engineering 2018
[26]. Rekha Agarwal, Vinod Patidar, Gurpreet Kaur "Chaos-based multiple order optical transforms for 2D image encryption", Engineering Science and Technology, an International Journal Feb 2020
[27]. Pankaj Rakheja, Rekha Vig, Phool Singh "Double image encryption using 3D Lorenz chaotic system, 2D non-separable linear canonical transform and QR decomposition" 2020
[28]. Zhi-Jing Huang, Shan Cheng, Li-Hua Gonga, Nan-Run Zhou "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform" Optics and Lasers in Engineering 2020
[29]. Liansheng Suai, MinjieXua, Ailing Tian "Optical noise-free image encryption based on quick response code and high dimension chaotic system in gyrator transform domain" Optics and Lasers in Engineering in 2017
[30]. Mehak Khurana, Hukum "Data Computation and Secure Encryption Based on Gyrator Transform using Singular Value Decomposition and Randomization" International Conference on Computational Intelligence and Data Science (ICCIDS 2018).
[31] Xu, Lu, et al. "A novel bit-level image encryption algorithm based on chaotic maps." *Optics and Lasers in Engineering* 78 (2016): 17-25.
[32] Wang XY, Zhang HL. A color image encryption with heterogeneous bit-permutation and correlated chaos. Opt Commun2015; 342:51–60.

[33] Wang XY, Liu LT, Zhang YQ. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 2015; 66:10–8.
[34] Abuturab MR. an asymmetric single-channel color image encryption based on Hartley transform and gyrator transform. OptLasersEng 2015; 69:49–57.
[35] Wang XY, Zhang YQ, Bao XM. A novel chaotic image encryption scheme using DNA sequence operations.OptLasersEng2015; 73:53–61.
[36] Wang, Xing-Yuan, Sheng-Xian Gu, and Ying-Qian Zhang. "Novel image encryption algorithm based on cycle shift and chaotic system." Optics and Lasers in Engineering 68 (2015): 126-134.
[37] Zhang YQ, Wang XY. Asymmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice.InfSci2014; 273(20):329–51.
[38] Huang R, Rhee KH, U chida S. A parallel image encryption method based on compressive sensing.MultimedToolsAppl2014; 72(1):71–93.
[39] Zhou YC, Cao WJ, Chen CLP. Image encryption using binary bitplane. Signal Process 2014;100:197–207.
[40] Chen, Jun-xin, et al. "A fast image encryption scheme with a novel pixel swapping-based confusion approach." Nonlinear Dynamics 77.4 (2014): 1191-1207.
[41] Ye GD, Wong KW. An efficient chaotic image encryption algorithm based on a generalized Arnold map. Nonlinear Dyn2012; 69(4):2079–87.
[42] Teng, Lin, and Xingyuan Wang. "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive." Optics Communications 285.20 (2012): 4048-4054.
[43] Sethi, Nidhi, and Deepika Sharma. "A novel method of image encryption using logistic mapping." Int. J. Comput. Sci. Eng 1.2 (2012): 115-119.
[44] Liu HJ, Wang XY. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun2011; 284(16):3895–903.
[45] Zhu ZL, Zhang W, Wong KW, Yu H. A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci2011; 181(6):1171–86.
[46] Somasundaram K. and Domnic S. "MODIFIED VECTOR QUANTIZATION METHOD FOR IMAGE COMPRESSION" Proceeding of World Academy Of Science , Engineering and TechnologyVOLUME 13 MAY 2006
[47] Fränti P. NevalainenO. and Timo Kaukoranta" COMPRESSION OF DIGITAL IMAGES BY BLOCK TRUNCATIN CODING: A SURVEY " The Computer Journal, 37 (4), 308-332, 1994 .
[48] M. Naor, A. Shamir. Visual cryptography. Workshop on the Theory and Application of Cryptographic Techniques 1994; 1-12.
[49] Y. Shi, X. Yang. Optical hiding with visual cryptography. J Opt 2017; 19:115703.
[50] Z. Zhang, X. Ma, J. Zhong. Single-pixel imaging by means of Fourier spectrum acquisition. Nat Commun 2015, 6.
[51] M. F. Duarte, M. A. Davenport, D. Takbar, J. N. Laska, T. Sun, K. F. Kelly, et al. Single-pixelimaging via compressive sampling. IEEE Signal Proc Mag. 2008; 25(2):83-91.
[52] H. Kim, Y. H. Lee. Optimal watermarking of digital hologram of 3-D object. Opt Express 2005;13(8):2881-6
[53] RLE compression available at "http://www.prepressure.com/library/compressionalgorithm/rle"
[54] Jindal V. , Verma A. K and Bawa S. "IMPACT OF COMPRESSION ALGORITHMS ON DATA TRANSMISSION ".
[55] Huffman Coding available at "http://cs.gettysburg.edu/~skim/cs216/lectures/huffman.pdf"
[56] Chapter 7 Lossless Compression Algorithms available at "http://www.course.sdu.edu.cn/download/12c34ecb-6cbf-46d7-af99- 982aaf6bf620.pdf"
[57] Iombo C." PREDICTIVE DATA COMPRESSION USING ADAPTIVE ARITHMETIC CODING"A Thesis.(http://etd.lsu.edu/docs/available/etd-07032007-100117/unrestricted/Iombo_thesis.pdf
[58] Kashyap N. and Singh S.N "REVIEW OF IMAGES COMPRESSION AND COMPRESSION OF ITS ALGORITHMS" International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 12, December 2013.
[59] Singh A. and Gahlawa M. "IMAGE COMPRESSION AND ITS VARIOUS" International Journal of Advanced Research in Computer Science and Software Engineering. Volume 3, Issue 6, June 2013
[60] Kumar D."A STUDY OF VARIOUS IMAGE COMPRESSION TECHNIQUES " available at "http://rimtengg.com/coit2007/proceedings/pdfs/43.pdf"
[61] Constant Area Coding available at "http://cis.cs.technion.ac.il/Done_Projects/Projects_done/VisionCla sses/DIP_1998/Lossless_Compression/node26.html "

[62] Run Length Encoding (RLE)Discussion and Implementation by Michael Dipperstein available at "http://michael.dipperstein.com/rle"
[63] Chapter 7 Huffmen Coding Tree available at http://algoviz.org/OpenDSA/Books/Everything/html/Huffman.html
[64] Grewal R. K. and Randhawa N."IMAGE COMPRESSION USING DISCRETE COSINE TRANSFORM & DISCRETE WAVELET TRANSFORM" International Journal of Computing & Business Research ISSN (Online): 2229-6166
[65] Kaur H. G. and Sharma S."FRACTAL IMAGE COMPRESSION –A REVIEW" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 2, February 2012
[66] Fractal Image Compression available at "http://wwwinst.eecs.berkeley.edu/~ ee225b/sp10/lectures/fractalcompression.pdf"
[67] Lecture notes on Data Compression Arithmetic coding available at "http://www.cs.ucf.edu/courses/cap5015/Arithmetic_coding_modifi ed_2005.pd
[68] Arithmetic Coding by Campos A.S.E available at "http://www.arturocampos.com/ac_arithmetic.html"

[69] J. Li, L. Zhong, Q. Zhang, Y. Zhou, J. Xiong, J. Tian, X. Lu. Optical image hiding based on dual- channel simultaneous phase-shifting interferometry and compressive sensing. Appl Phys B 2017; 123(1):4.
[70] T. Shimobaba, Y. Endo, R. Hirayama, D. Hiyama, Y. Nagahama, S. Hasegawa, M. Sano, T. Takahashi, T. Kakue, M. Oikawa, T. Ito. Holographic microinformation hiding. Appl Opt 2017; 56(4):833-7.
[71] J. Li, T. Zhong, X. Dai, C. Yang, R. Li, Z. Tang. Compressive optical image watermarking using joint Fresnel transform correlator architecture. Opt Laser Eng 2017; 89:29-33.
[72] W. Chen. Ghost identification based on single-pixel imaging in big data environment. Opt Express 2017; 25(14): 16509-16.
[73] J. Zhang, Z. Wang, T. Li, A. Pan, Y. Wang, Y. Shi. 3D object hiding using three-dimensional ptychography. J Opt 2016; 18(9):095701.
[74] W. H. Xu, H. F. Xu, Y. Luo, T. Li, Y. S. Shi. Optical watermarking based on single-shot-ptychography encoding. Opt Express 2016; 24(24):27922-36.
[75] W. Xu, Y. Luo, T. Li, H. Wang, Y. Shi. Multiple-Image Hiding by Using Single-Shot Ptychographyin Transform Domain. IEEE Photon J 2017; 9(3):1-10.
[76] M. Naor, A. Shamir. Visual cryptography. Workshop on the Theory and Application of Cryptographic Techniques 1994; 1-12.
[77] Y. Shi, X. Yang. Optical hiding with visual cryptography. J Opt 2017; 19:115703.
[78] Z. Zhang, X. Ma, J. Zhong. Single-pixel imaging by means of Fourier spectrum acquisition. Nat Commun 2015, 6.
[79] M. F. Duarte, M. A. Davenport, D. Takbar, J. N. Laska, T. Sun, K. F. Kelly, et al. Single-pixelimaging via compressive sampling. IEEE Signal Proc Mag. 2008; 25(2):83-91.
[80] H. Kim, Y. H. Lee. Optimal watermarking of digital hologram of 3-D object. Opt Express 2005;13(8):2881-6.
[81] H. T. Chang, C. L. Tsan. Image watermarking by use of digital holography embedded in the discrete-cosine-transform domain. Appl Opt 2005; 44(29):6211-9.
[82] Huiqing Huang 1,2 and Shouzhi Yang 1, Image Encryption Technique Combining Compressive Sensing with Double Random-Phase Encoding, Published 3 April 2018.
[83] Eman Tarek, Osama Ouda, and Ahmed Atwan, Image-based Multimodal Biometric Authentication Using Double Random Phase Encoding, International Journal of Network Security, Vol.20, No.6, PP.1163-1174, Nov. 2018.
[84] R. Kumar and B. Bhaduri, "Double image encryption in fresnel domain using wavelet transform, gyrator transform and spiral phase masks," in Fifth International Conference on Optical and Photonics Engineering, pp. 104490O, June 2017.
[85] M. Takeda, K. Nakano and H. Suzuki, "Key-length analysis of double random phase encoding," Applied Optics, vol. 56, no. 15, pp. 4474–4479, 2017.