Optical Encryption Techniques: An Overview

M.A. Mohamed[1], A.S. Samarah[1], M.I. Fath Allah[2]

[1] Faculty of Engineering-Mansoura University-Egypt

[2] Delta Academy of Science for Engineering and Technology-Egypt

ABSTRACT

Over the years extensive studies have been carried out to apply coherent optical methods in real time communications and multimedia transmission. This is especially true when a large amount of information needs to be processed. The transmitted data can be intercepted by non-authorized people; this explains why considerable effort is being devoted at the current time to data encryption and secure transmission. In this paper, a literature survey of the performance and methodology of some recent optical encryption techniques will be presented. These techniques have been applied on different applications.

Keywords: *Independent Component Analysis (ICA), Fractional Fourier Transform (frFT).*

1. Introduction

Any commercial, military, and/or civil communication system should have at least a minimum security level, which depends on the nature of the application, and acceptable transmission rates [1]. Over the years intensive research has been directed toward coherent optics, especially the issues of compression and encoding, because of the potential for new technological applications in telecommunications [2]. Since optical techniques appear as practical tools in securing and validating information, researchers done significant efforts to investigate these techniques under the insight of cryptoanalysis [3]. Optical encryption has reached a level of maturity recently with the publication of realistic attacks that exploit its inherent weakness of linearity [4-6]. This serious security problem associated with repeated use of the same key can be defended against through the use of modes of encryption [7], which promise to make optical encryption a viable symmetric cryptosystem [4]. To encourage widespread use, the field of optical encryption should offer a cohesive and fully featured suite of practical and unique applications [4]. A single frame work for the different applications will allow a single optical hardware arrangement to support this wide range of applications without modification [4]. Optics system can provide many degrees of freedom to handle parameters such as amplitude, phase, wavelength, and polarization [8]. The next of this paper is organized as follows; section-2 provides the related work, section-3 introduces optical encryption methodologies, and section-4 presents conclusions.

2. Related Work

Image processing tools as well as spectral algorithms, based on spectral filtering, have been used to encrypt images. In [9, 10], they proposed a method using a random phase. A multiplication of the image spectrum by a pseudo-random phase is applied. Fractional Fourier transform (frFT) was the key element in other optical encryption algorithms [11, 12]. In such circumstances, hacking is easily performed by finding out this parameter. The multiplexing basic principle consists on encrypting several images into a single package in order to not only to bring the change for multiple users, but also to increase data security. In case of using a single encoding mask, the problem for the end user will be the cross talk among the overlapping of decoded images. To avoid this cross-talk, a classical solution involves setting the encrypting optical parameters in a way to define separately the encoded images or to modify the encrypting machine. So far, multiplexing methods were performed such that the encrypted images are completely uncorrelated. In this case, the main issue is the superposition of the decrypted information over the non-decrypted data, this last acting as noise. Several multiplexing encryption methods were proposed, for instance, wavelength multiplexing [13], multiplexing by random-phase mask shifting [14], modifying the polarization state [15], or using multiple apertures that changes between exposures [16, 17].

For 3D objects, optical encryption has been demonstrated [18], and also a hologram watermarking technique can be regarded as a restricted example of multiplexing two such objects [19]. Although a hierarchical optical security system has been reported [20], in this case the decryption key consists only of a small sequence of scalars. A multi-level image encryption method has also been proposed based on cascaded multiple-phase retrieval by an iterative Fresnel transform algorithm [21].

In another communication [22], in order to increase the data security transmission, a multichannel puzzle-like encryption method was proposed. In that method, the input information is decomposed and each decomposed part is encrypted separately. To retrieve the whole information, the properly decrypted channels are composed. Using the full capacity of both amplitude and phase of an object as separate channels, an encryption scheme was proposed [23]. In this scheme, different information can be coded in amplitude and phase, in such a way that an amplitude-authorized user can receive the phase encoding but without the appropriate key is unable to read it.

In a recent communication [24], a method of image encryption has been proposed that can encrypt a set of plaintexts into many similar cipher texts. In optoelectronic systems [25-27], attempts to conceal the delay time by choosing it close to a characteristic time of the system, such as the fast time-scale of the filter, will not be successful since in this parameter region the system is not chaotic. In a first attempt to conceal the delay time in electro-optical systems, a cascaded system consisting of a combination of an all-optical system [28] and opto-electronic phase-chaos system [25] has been proposed [29]. Optical image encryption with the ability of multi-dimension and parallel processing becomes a focus since the pioneer work [30] about optical encryption based on double random phase encoding was proposed by Refregier and Javidi. Unnikrishnan [31] extended this technique to the fractional Fourier domain, and then the frFT is widely used in image encryption due to its good properties and feasibility with optical implementation [32, 33, 34, 35, 36].

Qing Guo [32] proposed a novel adaptive watermarking algorithm based on random fractional Fourier transform. Sanjay Rawat and Balasubramanian Raman [33] applied fractional Fourier transform and visual cryptography to a copyright protection scheme. Linfei Chen [34] introduced frFT into multiple image encryptions and watermarking technique. However, many transforms, including frFT, are linear and relatively weak against some common attacks, for example, chosen- and known-plaintext attacks. The vulnerability of the double random phase encoding method against chosen-cipher text attacks has been demonstrated in [37]. Recently, chaos-based encryption methods have been popular [38] and hybrid in optical communication [39, 40].

3. Optical Encryption Methodologies

In this section, several optical encryption techniques will be introduced. The problem statement, the main objectives, and the main idea of each methodology will be studied.

3.1 All Optical Video Image Encryption

In the last two decades, wireless communications have been introduced in various applications. However, the transmitted data can be, at any moment, intercepted by non-authorized people [1]. In order to secure data transmission, one should pay attention to two aspects: transmission rate and encryption security level. In this manuscript, these two aspects have been addressed by proposing a new video-image transmission scheme. The new system consists in using the advantage of optical high transmission rate and some powerful signal processing tools to secure the transmitted data [1]. The main idea of this approach is to secure transmitted information at two levels: (i) the classical level by using an adaptation of standard optical technique, and (ii) the spatial diversity, by using independent transmitters; in this level, a hacker should intercept not only one channel but all of them in order to retrieve information. At the receiver, independent component analysis (ICA) algorithms can be easily applied to decrypt the received signals and retrieve information [1]. The transmission encryption/decryption scheme of this technique is depicted in Fig. (1).

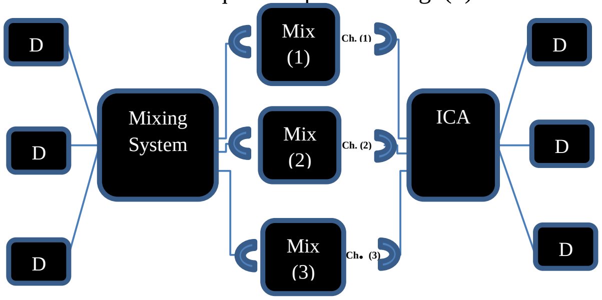

Fig. (1) Encryption/Decryption Scheme

The summary of how the video sequence can be encrypted and decrypted using ICA techniques is illustrated in Fig. (2) [1].

3.2 Grating Modulation & Multiplexing

The concept of an all-optical encrypted movie has been introduced for the first time. This movie joints several encrypted frames corresponding to a time evolving situation employing the same encoding mask. Thanks to a multiplexing operation the encrypted movie information could be compacted into a single package. But the decryption of this single package implies the existence of cross-talk if the encoded information doesn't be adequately pre-processed before multiplexing [3].

This approach has been used to introduce an external tool that allows one to spatially separate the different frames Fi. For this reason in step 2 of Fig. (3), a physical grating G_i has been introduced in contact with each encrypted frame E_i, and the grating has been rotated for the different frames. In this way, different spatial “labels” for each frame have been assigned. Once this procedure is accomplished, all frames will be multiplexed. The multiplexing operation results from the addition of the modulated encrypted information obtained by the grating attaching procedure for each encrypted input frame. In general, this procedure will be extended to not only the grating rotation but also to a simultaneous pitch variation in a way to expand the possibilities to increase the number of “labeled” frames [3].

In this regard, a grating modulation has been introduced to each encoded image, and then all of these encoded images have been multiplexed. After appropriate filtering and synchronizing procedures applied to the multiplexing, the movie could be decrypted and reproduced. This movie is only properly decoded when in possession of the right decoding key. The new concept thus involves the idea of encoding a dynamic situation. Besides, to retrieve the complete dynamic input information, it is necessary not only to properly decrypt the images but also to compose them [3]. The encryption process (step 1) as well as theta speckle modulation and multiplexing (step 2) is demonstrated in Fig. (3) [3].

where R: is the random phase mask, Fi: is the ith frame, R': is the key mask, Ei: is the ith encrypted frame, and Gi: is the ith amplitude grating [3]. The filtering process is illustrated in Fig. (4). A Fourier transform of the input reveals the existence of paired spots belonging to each "labeled" frames located a different spatial positions. These positions depend on the pitch and orientation of the "labeling" grating [3].

of modes of encryption [42]. In this methodology, a basic optical encryption that admits several cryptography applications based on multiplexing has been presented [4]. Users can decrypt different private images from the same encrypted image, a super-user can have a key that decrypts all encrypted images, and multiplexed images can be encrypted with different levels of security. This system is presented in the context of a general framework of optical encryption application development.

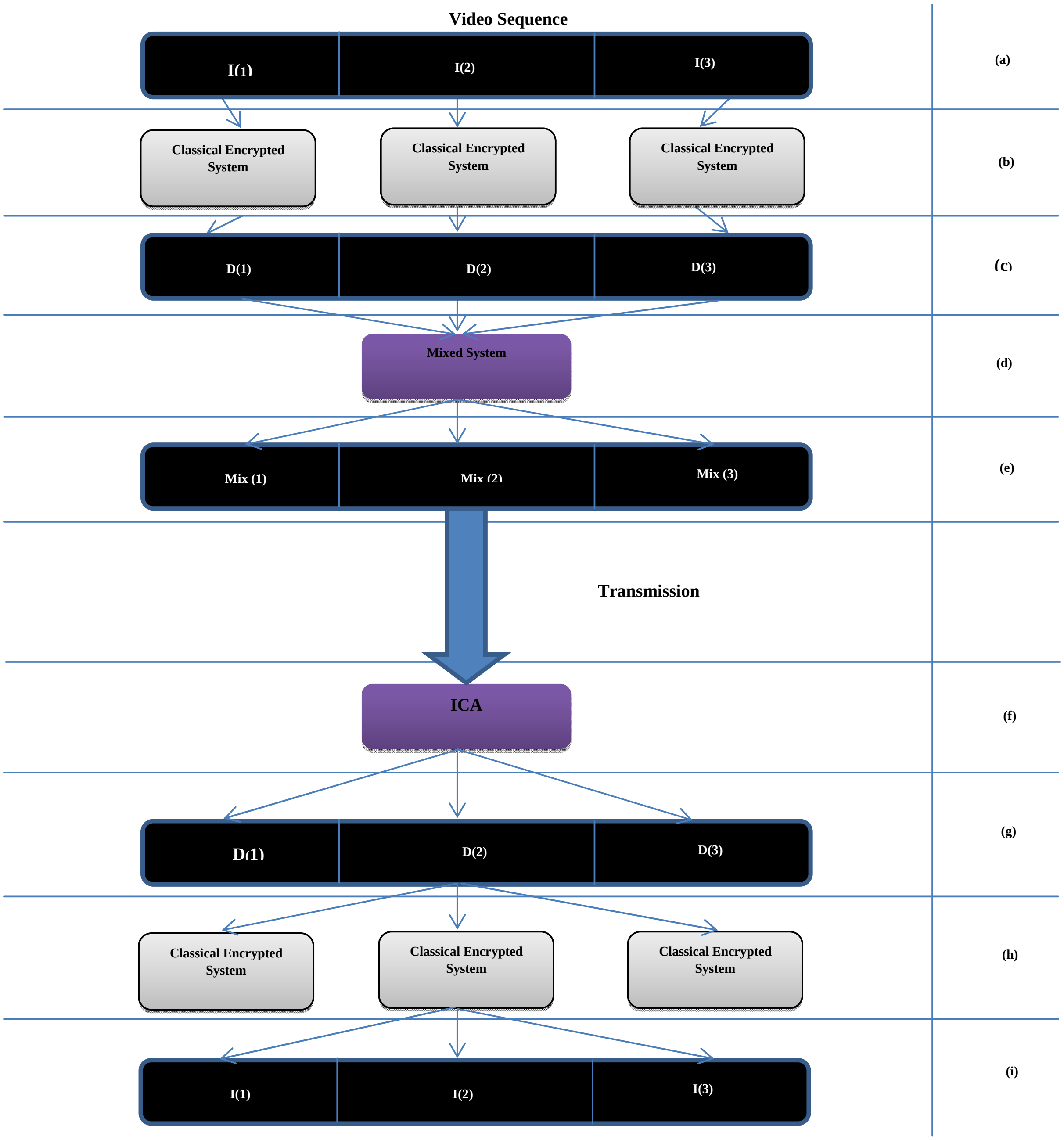
Video Sequence
I(1)
I(2)
I(3)
(a)
Classical Encrypted System
Classical Encrypted System
Classical Encrypted System
(b)
D(1)
D(2)
D(3)
(c)
Mixed System
(d)
Mix (1)
Mix (2)
Mix (3)
(e)
Transmission
ICA
(f)
D(1)
D(2)
D(3)
(g)
Classical Encrypted System
Classical Encrypted System
Classical Encrypted System
(h)
I(1)
I(2)
I(3)
(i)

Fig. (2) Encryption/Decryption System using ICA

3.3 Optical Encryption with Multiple Security Levels

The serious security problem associated with repeated use of the same key can be defended against through the use

A real-world three-dimensional scene has been illustrated. It has been captured with digital holography, and encrypted using the fractional Fourier transform, where different users have access to different three dimensional objects in the scene [4]. The schematic diagram of this technique is obtained in Fig. (5) [4].

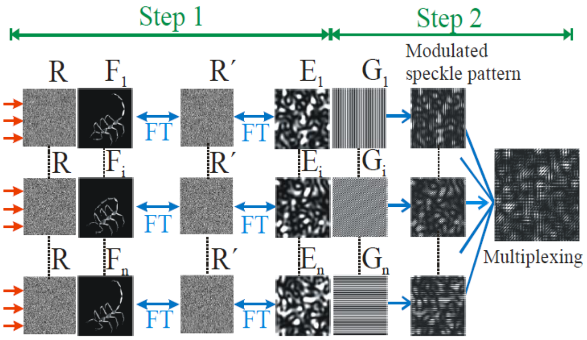

Fig. (3) The main procedure steps

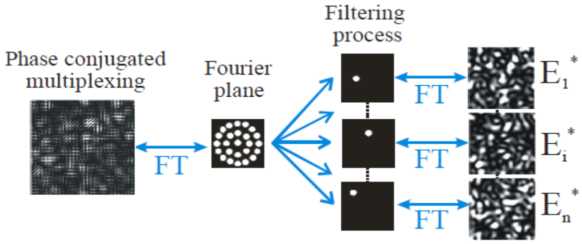

Fig. (4) Filtering Process

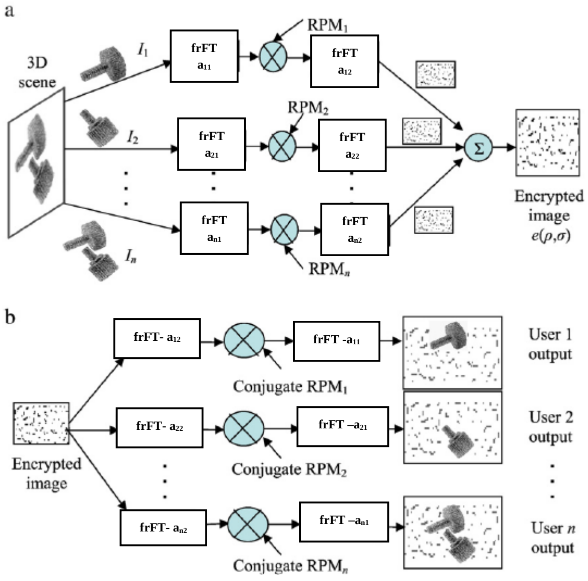

Fig. (5) Schematic of (a) the encryption system, and (b) the decryption system

3.4 Electro-Optic Phase Chaos System

An electro-optic phase chaos system with two feedback loops organized in parallel configuration such that the dynamics of one of the loops remains internal has been considered [41]. This configuration intrinsically conceals in the transmitted variable the internal delay times, which are critical for decoding. The scheme also allows for the inclusion, in a very efficient way, of a digital key generated as a long pseudorandom binary sequence. A single digital key can operate both in the internal and transmitted variables leading to a large sensitivity of the synchronization to a key-mismatch. The combination of intrinsic delay time concealment and digital key selectivity provides the basis for a large enhancement of the confidentiality in chaos-based communications [41]. Flexibility and parameter concealment are necessary to achieve a good degree of security. In particular, the systems usually considered for chaos-based communications leverage on delay to generate high dimensional chaotic carriers on which the message is encoded [41]. The proposed setup is illustrated in Fig. (6) where; SL: is the Semiconductor Laser, PM: is the Phase Modulator, MZI: is the imbalanced Mach-Zehnder Interferometer, PD: is the Photodiode, x1(t) and x2(t) are the dimensionless output voltages of the RF drivers for the external and the internal loops while R(t) and m(t) are the pseudo-random bit sequence and message, respectively. Sub-index 1 refers to the loop whose output is transmitted while 2 refers to the internal loop [41].

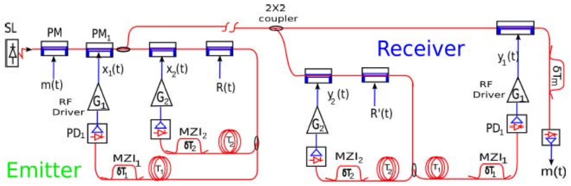

Fig. (6) Transmitter & receiver setup in the parallel configuration

3.5 Encryption Based on Cat Map & frFT

With the development of the multimedia technology, more and more important information comes from video and images [8]. The security of video and image information over internet becomes a serious issue. In this technique, an image encryption method based on chaos and fractional Fourier transform (frFT) has been proposed. The original image is first multiplied by random phase generated by logistic map and sequentially transformed by the fractional Fourier transform. Then the pixels of the transformed image are scrambled using two-dimensional cat map. The parameters of chaos function play an important role as keys in this proposed encryption method [8]. The block diagram of encryption process is shown in Fig. (7) [8].

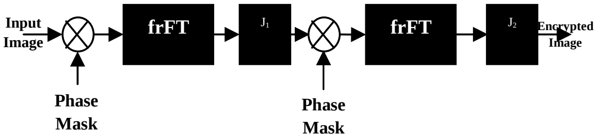

Fig. (7) Encryption Process

4. Conclusions

Due to the importance of information security issue, this paper has concentrated on study of different optical encryption techniques. The main ideas of some optical encryption techniques have been introduced. In the future, the fusion or mixing between some of these techniques can be applied to get better performance.

References

[1]A. Alfalou, A. Mansour, "All-Optical Video-Image Encryption with Enforced Security Level using ICA," Journal of Optics Pure and Applied Optics, hal-00579211, version 1, PP: 1-21, march 2011.

[2] A. Alfalou, C. Brosseau, " Optical Image Compression and Encryption Methods," Adv. Opt. Photon 1, hal-00516980, PP: 589-636, Sep 2010.

[3]F. Mosso, M. Tebaldi, "All-Optical Encrypted Movie," Optical Society of America, Vol. 19, No. 6, PP: 5706-5712, March 2011.

[4]N. K. Neshchal, T. J. Naughton, "Flexible Optical Encryption with Multiple Users and Multiple Security Levels," ELSEVIER, Optics Communication 284, PP:735-739, 2011.

[5] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Opt. Lett. 30 (2005) 1644.

[6] G. Situ, G. Pedrini, W. Osten, Appl. Opt. 49 (2010) 457.

[7] T.J. Naughton, B.M. Hennelly, T. Dowling, J. Opt. Soc. Am. A 25 (2008) 2608.

[8]Y. Liu, J. Lin, J. Fan, N. Zhou, "Image Encryption Based on Cat Map and Fractional Fourier Transform," Journal of Computational Information Systems 8:18, PP: 7485:7492, 2012.

[9] P. R´efr´egier and B. Javidi. Optical image encryption based on input plane and Fourier plane random encoding. Optics. Letters., Vol. 20, pp: 767-769, 1995.

[10]F. Goudail, F. Bollaro, B. Javidi, and P. R´efr´egier, Influence of a perturbation in a double phase-encoding system. J. Opt. Soc. Am. A,Vol. 15, pp: 2629-2638, 1998.

[11]Guohai Situ and Jingjuan Zhang. Position multiplexing for multiple-image encryption. Journal of Optics A: Pure and Applied Optics, Vol. 8, No 5, pp: 391-397, May 2006.

[12]Zhou Xin, Yuan Sheng, Wang Sheng-wei and Xie Jian. Affine cryptosystem of doublerandom- phase encryption based on the fractional Fourier transform, Applied Optics, Vol. 45, Issue 33, pp: 8434-8439, 2006.

[13]G. Situ and J. Zhang, “Multiple-image encryption by wavelength multiplexing,” Opt. Lett. 30(11), PP:1306–1308, 2005.

[14]J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, “Multiplexing encryption-decryption via lateral shifting of a random phase mask,” Opt. Commun. 259(2), PP:532–536, 2006.

[15]J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, “Multiplexing encrypted data by using polarized light,” Opt. Commun. 260(1), PP:109–112, 2006.

[16]J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, “Multiple image encryption using an aperture modulated optical system,” Opt. Commun. 261(1), PP: 29–33, 2006.

[17]J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, “Code retrieval via undercover multiplexing,” Optik (Jena) 119, PP:139–142, 2008.

[18]E. Tajahuerce, B. Javidi, Appl. Opt. 39 (2000) 6594.

[19] S. Kishk, B. Javidi, Opt. Express 11 (2003) 874.

[20] C.H. Yeh, H.T. Chang, H.C. Chien, C.J. Kuo, Appl. Opt. 41 (2002) 6128.

[21]X.F. Meng, L.Z. Cai, Y.R. Wang, X.L. Yang, X.F. Xu, G.Y. Dong, X.X. Shen, H. Zhang, X. C. Cheng, J. Opt. A Pure Appl. Opt. 9 (2007) 1070.

[22]D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, Opt. Commun. 281 (2008) 3434.

[23] J.F. Barrera, R. Torroba, Appl. Opt. 48 (2009) 3120.

[24]X. Yong-Liang, Z. Xin, Y. Sheng, C. Yao-Yao, Opt. Commun. 283 (2010) 2789.

[25] R. Lavrov, M. Peil, M. Jacquot, L. Larger, V. Udaltsov, and J. Dudley, ”Electro-optic delay oscillator with nonlocal nonlinearity: Optical phase dynamics, chaos, and synchronization,” Phys. Rev. E 80, 026207/1-9, 2009.

[26]L. Larger, J. Goedgebuer, and V. Udaltsov, ”Ikeda-based nonlinear delayed dynamics for application to secure optical transmission systems using chaos,” Comptes Rendus Physique 5, PP:669-681, 2004.

[27]R. M. Nguimdo, P. Colet, and C. R. Mirasso, ”Electro-optic delay devices with double feedback,” IEEE J. Quantum Electron. 46, PP:1436-1443, 2010.

[28]R. Lang and K. Kobayashi, ”External Optical Feedback Effects on Semiconductor Injection Laser Properties”, IEEE J. Quantum Electron. 16, 347, 1980.

[29]J. Hizanidis, S. Deligiannidis, A. Bogris, and D. Syvridis, “Enhancement of Chaos Encryption Potential by Combining All-Optical and Electrooptical Chaos Generators”, IEEE J. Quantum Electron. 46, 1642-1649 (2010).

[30] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett., pp. 767 – 769, 1995.

[31]G. Unnikrishnan, J. Joseph, K. Singh. Optical encryption by double-random phase encoding in the fractional Fourier domain, Opt. Lett, 887 – 889, 2000.

[32]Qing Guo, Jun Guo, Zhengjun Liu, Shutian Liu. An adaptive watermarking using fractal dimension based on random fractional Fourier transform, Opt. Laser Technol, pp. 124 – 129, 2012.

[33]Sanjay Rawat, Balasubramanian Raman. A blind watermarking algorithm based on fractional Fourier transform and visual cryptography, Signal Process, pp. 1480 – 1491, 2012

[34]Linfei Chen, Daomu Zhao, Fan Ge. Gray images embedded in a color image and encrypted with FRFT and Region Shift Encoding methods, Opt. Commun, pp. 2043 – 2049, 2010.

[35]Zhengjun Liu, Qiuming Li, Jingmin Dai, Xiaogang Sun, Shutian Liu, Muhammad Ashfaq Ahmad. A new kind of double image encryption by using a cutting spectrum in the 1-D fractional Fourier transform domains, Opt. Commun, pp. 1536 – 1540, 2009

[36]Xiang Peng, Lingfeng Yu, Lilong Cai. Digital watermarking in three-dimensional space with a virtual-optics imaging modality, Opt. Commun, pp. 155 – 165, 2003.

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

[38]Lizhen CHEN. A Novel Image Encryption Scheme Based on Hyperchaotic Sequences, Journal of Computational Information Systems, pp. 4159 – 4167, 2012.

[39]Narendra Singh, Aloka Sinha. Gyrator transform-based optical image encryption, using chaos, Opt. Lasers Eng. 47, 539, 2009.

[40]Nanrun Zhou, Yixian Wang, Lihua Gong, Hong He, Jianhua Wu. Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform, Opt. Commun, pp. 2789 – 2796, 2011.

[41]R. M. Nguimdo, P. Colet, " Electro-optic phase chaos systems with an internal variable and a digital key," Optical Society of America, OCIS codes: (250.0250,060.0060,140.0140,190.0190), 2012.

[42]T.J. Naughton, B.M. Hennelly, T. Dowling, J. Opt. Soc. Am. A 25 (2008) 2608.