INVESTIGATIONS ON ENCRYPTION TECHNIQUES FOR COLORED AND GRAY SCALE IMAGES IN FOURIER- AND FRACTIONAL FOURIER DOMAINS

by

MADHUSUDAN

Instrument Design and Development Centre

Thesis submitted

in fulfillment of the requirements for the degree of Doctor of Philosophy

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI
NEW DELHI-110 016 (INDIA)

January 2009

Dedicated to

Mummy & Papa

CERTIFICATE

This is to certify that the thesis entitled, " **Investigations on Encryption Techniques for Colored and Gray Scale Images in Fourier- and Fractional Fourier Domains ",** being submitted by **Mr. Madhusudan**, to the Indian Institute of Technology, Delhi, for the award of Degree of *Doctor of Philosophy* in Physics is a record of bonafide research work carried out by him under our supervision and guidance. He has fulfilled the requirements for submission of the thesis, which to the best of our knowledge has reached the requisite standard.

The material contained in the thesis has not been submitted in part or full to any other University or Institute for the award of any degree or diploma.

(Prof. CHANDRA SHAKHER)
Instrument Design Development Centre
I. I. T. Delhi
New Delhi-110 016

(Prof. KEHAR SINGH)
Emeritus Fellow
Department of Physics
I.I.T. Delhi
New Delhi-110 016

January, 2009

ACKNOWLEDGEMENT

I am very grateful to my thesis advisors Professor Chandra Shakher and Professor Kehar Singh for introducing me to this fascinating area of research. Their devotion to research has been a constant source of inspiration to me during the course of my research work. I would like to imbibe this quality from them in my future career. I express my profound sense of gratitude towards them for their valuable guidance and encouragement.

I acknowledge Dr. Hem Chandra Kandpal for always encouraging me in my academic endeavors. I am very grateful to Dr. Joby Joseph, Dr. K.N. Chopra, and Dr. Arvind Kumar for their encouragement and moral support during the course of my research work. They have always been more than willing to help me, whenever I approached them. I also acknowledge all my mentors and teachers including Dr. Tabish Qureshi, Dr. Mohammad Sami, Dr. Jagdish Chandra Khulbe, Prof. Subhash Chopra, Prof. Anurag Sharma, Mr. S.P.S. Yadav, Prof. G. N. Tiwari, and Dr. Umesh Chandra Pandey.

I am also thankful to my seniors Dr. Dinesh Ganotra, Dr. Naveen Kumar Nishchal, and Dr. G. Unnikrishnan with whom I had numerous discussions on various aspects of my research. I also thank Renu, Pramod, Rakesh, Bhargab, Anith, Shaily, Rakesh, Gyanendra and Madan Singh for all their valuable help. I would also like to thank all my friends Madan, Jagat, Arvind and Rajesh for all their help and moral support.

I thankfully acknowledge the support of Mr. Saurabh Dalela, Director-iCAT and Mr. Rajesh Singh, CEO & PD-NATRiP. Special thanks to Mr. B. Bhanot, Mr. Sunil Chaturvedi, Mr. T. M. Balaraman, Mr. M. J. Singh, Mr. U. D. Bhangale, Mr. S.M. Haragapurkar, Mr. S.K. Kalia and Mr. S.R. Marathe for inspiring me from time to time. I would also like to thank all my colleagues at ARAI and iCAT for their help and support.

I deeply acknowledge my loving wife Rashmi for extending great cooperation as well as the emotional support. I would also like to express great affection towards my son Diptanshu whose birth has taught me the real meaning of the word 'responsibility'. Words fail to express the profound sense of gratitude I feel for my beloved sisters Mamta and Minakshi, brother-in-law Vipul, Tarun, Bua and Phuphaji, in-laws, Nanaji, Naniji, and late grandparents for all the love and affection they have showered on me. Without their affection and encouragement all this would not have been possible.

I dedicate this thesis to my loving Mummy and Papa.

(MADHUSUDAN)

ABSTRACT

The popularization of networking, internet, and multimedia has lead to remarkable research efforts in the area of data security. There has been a phenomenal increase in the rate at which the information is being disseminated. However, information frauds are progressively becoming a serious concern for many banks, businesses, and consumers etc. Every year, billions of dollars are spent on curtailing the information frauds and many of these losses are passed on, to have to be borne by the consumers. It is therefore very important to develop novel methods for security applications. A relatively new field, denoted as "Multimedia Security", is aimed towards these emerging technologies and applications as described below:

Cryptography is one of the reliable tools to ensure security, integrity, and authentication of electronic data. Traditional methods are based on the principles of cryptography [Naor and Shamir 1994; Schneier 1995] to develop systems providing the diverse security services. Majority of such systems are digital in nature. Security of these cryptosystems is attributed to powerful algorithms and larger key lengths, which in turn are computationally intensive in terms of time as well as power. As a result of this, a major bottleneck is posed particularly when a large amount of data has to be encoded. Therefore, in addition to these, optoelectronic cryptosystems are the possible alternatives on account of massive parallelism and inherent speed, despite being less programmable. It is also believed that optical encryption technologies sometimes provide a complex environment and are more resistant to attacks than digital/electronic systems.

Digital watermarking and information hiding [Javidi 2005, Lacy *et. al.*1998, Kishk and Javidi 2002] can be considered as methods for protecting data from unauthorized distribution. Digital watermarking has many applications; for example, it can be used in ownership affirmation by adding a watermark to the image to be protected using a code

that is known only to the author. If someone claims the ownership of the image, he or she should be able to recover the hidden image. In this application, the watermark should be robust to intended destruction and removal trials. Another application of digital watermarking is in copy-prevention systems by developing a copying machine that detects the watermark and rejects any copying process if the document is not authentic. There are also many other applications for digital watermarking, such as identity card verification and fraud detection. Several information-hiding and watermarking techniques have been proposed. In digital image watermarking, an image is embedded within another image, referred to as the host, such that the host image does not suffer from severe degradation.

An information-hiding system should satisfy a number of conditions. For example, the embedded data should be robust against modification trials, signal-processing operations, and removal attacks and the embedded data should be hidden from the human eye. Information-hiding systems can be categorized as either spatial-domain systems or Fourier-domain systems, according to the domain in which the image is embedded. Spatial-domain systems are easy to implement but suffer from the degradation in the host-image quality, and these are not robust against signal-processing operations such as compression and filtering. Fourier-domain filtering is more robust to signal-processing operations, but the hidden image may be easier to remove from the watermarked image.

In an encryption system [Javidi 2005], we desire to encode information in such a way that, even if it is viewed or recorded, only the use of the correct key would fetch the correct information. Various digital and optical techniques [Javidi 2005] have been proposed for image encryption, based on various concepts such as chaotic maps, double random phase encoding (DRPE) [Refregier and Javidi 1995], fractional Fourier transform (FRT) [Ozaktas *et. al.*2001], Fresnel transform, wavelet transform, digital holography, and Hilbert transform (HT) etc. But major bottleneck is that all these techniques use gray

scale images. However, lot of research is going on for the encryption of color images. Zhang and Karim [1999] have used a single channel encryption of a color image in the Fourier domain. A visual secret sharing scheme based on color information of images has been proposed by Yang and Laih [2000]. Hou [2003] has proposed a digital technique for visual cryptography of RGB images. A wavelet-based coding method for digital encryption of colored images has been presented by Martin *et. al.*[2005]. Lukac and Plataniotis [2005] have proposed a cost-effective encryption scheme for color image using secret sharing technique.A shared key encryption scheme of JPEG color images has also been proposed by Sudharsanan [2005].

Encryption technique for RGB images using wavelength multiplexing and lens-less Fresnel transform hologram, and later using digital holography and FRT has also been proposed by Chen and Zhao [2006, 2007]. Nien *et. al.*[2007] have demonstrated a digital image encoding and decoding using a novel chaotic random generator. Shyu [2007] has proposed a novel encryption scheme for colored images using random grids. A digital security scheme for colored images using spatio-temporal chaos and singular value decomposition has been proposed by Peng and Liu [2008]. Ge et. al [2008] have presented a half blind color image hiding and encryption scheme in the factional Fourier domain. Amaya *et. al.*[2008] have presented a multi-channel digital encryption technique based on joint transform correlator.

The **present thesis** reports the results of investigations on some new digital architectures for encryption of colored and gray scale images in the Fourier as well as the fractional Fourier domain. These architectures make use of various color spaces, elementary mathematical steps, and some specialized filters for multiplexing, information hiding, and encryption. Some of the proposed systems are by and large unconventional on account of being nonlinear, multi-channel or three-dimensional in nature. Multi-channel encryption scheme for colored images in the RGB color space is analyzed in the Fourier

as well as the fractional Fourier domain. Simulation studies on encryption algorithms to encode data using the radial Hilbert transform (RHT), the Fourier transform and the FRT has been presented. Multiplexing and encryption techniques for colored images using the complex algebra have also been discussed as a part of the work. Nonlinear multi-channel image encryption system based on natural logarithms has been demonstrated and a full phase digital encryption technique using the HSV color space [Gonzalez 2006 *et. al.*] has also been presented. Suggestions have been made for the optical implementation in some cases.

Chapter 1 contains an introduction and overview of the research in the area of optical and digital security. It includes a discussion on various digital as well as the optical techniques used for encryption, image hiding, cryptography, and watermarking in multimedia security. The chapter also contains a brief introduction to the FRT, the Hilbert transform (HT), theory of color images, concept of- various color spaces, and description of some techniques for image encryption in the Fourier as well as the fractional Fourier domain. This chapter also includes a detailed comparison of various optical/digital methods for image encryption and the motivation behind the various studies done as a part of the proposed thesis. A brief discussion about different types of noise commonly encountered in the digital and optical information processing / communication systems, is also included.

Chapter 2 reports the simulation studies on the multi-channel image encryption and decryption technique for the RGB images [Plataniotis and Venetsanopoulos 2000; Gonzalez 2006 *et. al.*]. Majority of the work done in the field of encryption has been carried out using monochrome images and very little work has been carried out in the field of color image encryption. Inclusion of the color information adds another dimension to this subject as color is a vital feature of an image. This chapter is divided into two sections. Section I discusses the encryption in the Fourier- as well as the fractional Fourier

domain DRPE. In this technique, each of the color channels (i.e. R, G, and B) are encrypted independently using the DRPE technique in the Fourier and the fractional Fourier domain. The random phase keys and the fractional orders of the FRT have been used as keys for encryption and decryption. The proposed technique is shown to be quite suitable for the encryption and decryption of multi-colored text as the use of incorrect keys in one or more than one channels leads to a meaning less information. The performance of the proposed scheme has also been analyzed with respect to the variation in the encryption keys. A detailed analysis of the performance of the proposed technique has been done in presence of different types of noise. Robustness of the scheme has also been verified against the occlusion attack on the encrypted data and the random phase keys. Simulation results to demonstrate the performance of the system have also been presented against the attacks using the partial windows of the correct random phase masks.

The multi-channel approach for encryption of the RGB images described in previous paragraph is quite promising. Nevertheless, it is quite vulnerable to attacks on account of being linear. Therefore to overcome this problem a multi-channel encryption technique for RGB images has also been discussed in the FRT domain, with an application of natural algorithms [Section II]. The proposed scheme is not based on the conventional DRPE algorithm and uses the base changing rule of logarithms to encode the input image inside the input plane random phase mask. Algorithms for the single-channel digital implementation of the scheme have been discussed and its extension to 3-channels has also been carried out. The proposed technique has been evaluated against the variation in the encryption key parameters like random amplitude mask, random phase mask, and factional orders of the FRT. The technique is shown to be extremely secure against occlusion and noise attacks [Frauel *et. al.*2007, Ge *et. al.*2008] because of the nonlinearity

introduced by the logarithms. It is also shown that the technique is quite secure against attacks using partial windows of the correct random phase masks.

Chapter 3 reports introduction of the RHT [Davis *et. al.*2000] to enhance the quality of the DRPE based image encryption schemes in both Fourier as well as fractional Fourier domain. This chapter is divided into two sections. Section I discusses image encryption technique using the RHT filter for spatial frequency segregation. The ability of the RHT mask to extract the high frequency spectrum of an image has been utilized. This method is based on the DRPE in the FRT domain. Here the RHT filter is multiplied with the image obtained after the first FRT and the high frequency and the remaining frequencies are separated out into two different channels. These channels are encoded independently using different random phase masks as well as fractional orders of the FRT. Thus the proposed scheme uses more keys as compared to the conventional DRPE and is therefore more robust against unauthorized access. The performance of the proposed scheme has also been analyzed with respect to the variation in the encryption parameters like fractional orders of the FRT as well as the fractional orders of the RHT. The robustness of the technique has also been verified in the presence of the different types of noise added to the encrypted data as well as to the random phase masks. The effect of occlusion of the encrypted data and the random phase masks has also been studied and the evaluation of the system performance has been carried out against the attacks using partial windows of the random phase masks. Simulation results have been presented to demonstrate the robustness of the proposed technique.

Section II, discusses a simple but effective technique for optical image encryption using the integral order RHT in the Fourier domain. The integral orders of the RHT serves as an additional key for the encryption apart from the random phase masks required in conventional DRPE. The Fourier spectrum of the input image is encoded using an RHT mask of an arbitrary integral order. During decryption another RHT mask of exact

negative order to the previous one is required to unwrap the additional phase introduced by the RHT mask during encryption. Digital simulations have been presented and schematic for its optoelectronic implementation has been shown.

An extension of the above mentioned technique has also been presented using the integral order RHT filter bank in the Fourier as well the FRT domain. The filter bank is made by using multiple RHT masks of different integral orders. By doing this we could increase the number of keys for encryption and decryption and thus enhance the security to a larger extent as compared to the scheme proposed in the previous paragraph. It is also demonstrated that the FRT based technique is more reliable and secure as compared to its Fourier counterpart as well as the conventional DRPE technique. It happens on account of larger number of keys due to the application of fractional orders of the FRT in addition to the integral order of the RHT masks of the filter bank. Simulation results in support of the idea have been presented. The performance of the proposed scheme has also been analyzed against occlusion, noise, reshuffling of the Hilbert masks, rotation of the RHT filter bank and attacks using partial windows of the correct random phase keys [Frauel *et. al.*2007, Ge *et. al.*2008]. The schematic for the optoelectronic implementation of the technique has also been presented and discussed.

Chapter 4 discusses digital- multiplexing and encryption techniques for colored images using elementary complex algebra and the FRT. This chapter is divided into two sections. Section I discusses new method to encrypt and decrypt colored twin images using single-channel in FRT domain through quadrature multiplexing. The twin RGB images to be encrypted are converted into an indexed format [Gonzalez 2006 *et. al.*] by extracting their color maps and multiplied with the sine and cosine of a random mask. Subsequently, the encoded images are multiplexed together as real and imaginary parts of a complex number. The main advantage of this technique is the simultaneous encryption of two colored images using only two random phase masks and the FRT through a non-

DRPE based approach. Detailed study has been done to evaluate the performance of the proposed technique under various situations like variation of fractional orders of the FRT, use of incorrect random phase keys for decryption, addition of different types of noise to the encrypted data as well as the random phase keys, effect of occlusion of the encrypted data [Frauel *et. al.*2007, Ge *et. al.*2008], and reshuffling of the orthogonal keys.

Section II discusses a multiplexing and encryption technique for four RGB images in the FRT domain. The proposed algorithm also uses elementary complex algebra to multiplex the four input images and to encrypt these in the FRT domain using well-known DRPE lay-out. It is important to mention that the input images have been embedded inside the two random phase masks used for encryption and decryption. The performance of the technique has been verified against the variation in the fractional orders of the FRT and the random phase keys. It is important to note that both the phase keys are required to recover the input images, as the partial information for de-multiplexing is embedded inside these keys in the form of input images. This is in contrast to the conventional DRPE in which the input plane random phase key stands redundant during decryption. The robustness of the proposed techniques has been analyzed against occlusion, noise, and attacks using partial windows of the correct random phase keys [Frauel *et. al.*2007, Ge *et. al.*2008].

Chapter 5 describes, two different encryption schemes for colored phase images using a Fourier domain double random phase encoding technique. In the first technique the encryption and decryption of RGB images using HSV color space has been demonstrated. The technique is supposedly three-dimensional in nature. Simulation results are presented to demonstrate the performance of the proposed technique against variation of the encryption keys. It is shown that the proposed system is extremely sensitive to occlusion and attacks using partial random phase keys. It is also shown that the system performs well in the presence of noise contamination.

In the second technique, a multi-channel technique for encryption and decryption of RGB phase images in the Fourier domain has been presented. Since the numbers of encryption keys used in the proposed scheme are quite large as compared to the conventional single channel DRPE system, it is secure more secure as compared to the later. In addition to this, the technique carries all the advantages of phase encryption. The performance of the system has been analyzed against the variation in encryption keys, and digital simulations are presented to support the idea. The robustness of the technique has also been analyzed against occlusion, noise, and attacks using partial window of correct RPMs.

Chapter 6 contains a summary of important conclusions and scope for future work in the area of data security. The methods presented in chapter 2 may be extended to other color spaces like HSV, HIS, NTSC, etc. Some alternate multiplexing techniques can also be used to achieve better security and higher robustness against attacks. Extension of the encryption techniques described in chapter 2 to 4 is also possible in phase domain. It is also possible to extend the work reported in chapter 3 to the domain of colored images. Some future work may consider the use of chaotic maps, fractals, and random grids etc. It is also possible to device methodologies to introduce nonlinearity in the proposed encryption schemes in order to have more secure systems. Prospects of security enhancement can also be explored by combining the proposed methods with the help of watermarking and image hiding techniques. A detailed cryptanalysis of the proposed techniques is also desirable.

TABLE OF CONTENTS