August 2016
Master's Degree Thesis

A cryptographic evaluation of double random phase encoding in the gyrator domain

Graduate School of Chosun University

Department of Computer Engineering

Nishat Sultana

A cryptographic evaluation of double random phase encoding in the gyrator domain

자이레이터 도메인상에서의 이중 랜덤 위상 인코딩 암호성능 평가에 관한 연구

August 25, 2016

Graduate School of Chosun University

Department of Computer Engineering

Nishat Sultana

A cryptographic evaluation of double random phase encoding in the gyrator domain

Advisor: Prof. Moon Inkyu, PhD

A thesis submitted in partial fulfillment of
the requirements for a Master's degree

April 2016

Graduate School of Chosun University

Department of Computer Engineering

Nishat Sultana

니샷 술타나의 석사학위논문을 인준함

위원장	조선대학교	교수	이상웅	(인)
위 원	조선대학교	교수	문인규	(인)
위 원	조선대학교	교수	권구락	(인)

2016년 5월

조선대학교 대학원

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

A cryptographic evaluation of double random phase encoding in the Gyrator domain

Nishat Sultana
Advisor: Prof.Inkyu Moon, Ph.D.
Department of Computer Engineering
Graduate School of Chosun University

In this study, cryptographic properties of double random phase encoding (DRPE) scheme in the discrete Gyrator domain with avalanche and bit independence criteria are evaluated. Experimental results demonstrate that the DRPE in the discrete Gyrator domain possesses excellent avalanche and bit independence properties and hence can significantly aid to preserve data confidentiality and integrity. The rotation angle of the Gyrator transform can be regarded as an additional key which increases the security of the encryption system. We compare our results with the avalanche and bit independence criterion (BIC) performances of the conventional DRPE scheme. Although Gyrator transform based image cryptosystem has been widely studied, to the best of my knowledge, it is the first report on a cryptographic evaluation of discrete Gyrator transform with avalanche and bit independence criterions.

한 글 요 약

니샷 술타나
지도 교수: 문인규
컴퓨터공학과
대학원, 조선대학교

자이레이터 도메인상에서의 이중 랜덤 위상 인코딩 암호성능 평가에 관한 연구

본 논문에서는 아발란치 및 비트독립 판정기준을 이용하여 이산 자이레이터 도메인상에서의 이중 랜덤 위상 인코딩 방법의 암호성능 평가에 관한 연구를 수행한다.

본 연구에서의 실험결과들로부터 이산 자이레이터 도메인상에서의 이중 랜덤 위상 인코딩 기법은 우수한 아발란치 및 비트독립 특성을 가지고 있음을 증명하였으며, 이러한 우수한 암호성능을 가지는 이산 자이레이터 도메인상의 이중 랜덤 위상 인코딩 기법은 영상데이터의 비밀성 및 무결성 보증에 특별히 효과적으로 활용될 수 있을 것이다. 자이레이터 변환의 회적각은 DRPE 기반 암호알고리즘의 암호성능 향상을 위한 추가적인 암호파라미터로서 사용될 수 있음을 기존의 DRPE 기반 암호알고리즘과의 암호성능 비교 분석을 통하여 증명하였으며, 또한 이산 자이레이터 도메인상의 이중 랜덤 위상 인코딩 기법이 우수한 아발란치 및 비트독립 값을 가짐을 처음으로 증명하였다.

Chapter 1

I. Introduction

Exchange of sensitive information has become an integral part of our day to day life. Information that once was used to be transmitted in the form of a manuscript or voice, now travel thousands of kilometers within a blink of eyes. The evolution of these ongoing technological advancements has opened a new door of endless possibilities for us. With the rapid development of new security measures for the transmission and storage of our valuable information, new security flaws are also exposed. Therefore, the security of information passed over an open channel has become a fundamental issue. Considering the shortcomings of transmission media and weaknesses of the algorithms, assurance of the confidentiality and data integrity to protect our information against unauthorized access and use have become more important than ever. This has resulted in the development of highly secure information hiding techniques. Among many of those techniques, Cryptography and Steganography are the two most popular methods available to assure information security. Cryptography distorts the message by transforming the data into some other gibberish form so that the information cannot be understood. In contrast, Steganography hides the existence of the message by embedding the message into some other messages (i.e. messages, graphics or sounds) so that it cannot be seen.

At present, numerous cryptographic techniques exist for image encryption and decryption. However, it has become an important issue to evaluate how robust these methods are in terms of protecting confidentiality, integrity and authenticity of the images. Avalanche and bit independence properties are two very important

security measures of cryptographic algorithms which have great impact on preserving confidentiality, integrity and authenticity of the safely transmitted data. In this study, we evaluated avalanche and bit independence properties of discrete Gyrator domain based double random phase encoded scheme.

This thesis is organized as follows. In this chapter, first, the motivation of this work is discussed. Then a review of the related works is introduced. In chapter 2, the theoretical background of information hiding and cryptography is introduced. In chapter 3, an introduction to optical domain based image encryption systems is provided. Then the mathematical modeling of Fast algorithm of discrete Gyrator transform with double random phase masks is shown. Then we shed light on the concept of photon counting imaging. We then describe what avalanche and bit independence criterion is, in the last part of section 3. In section 4, we show and discuss our experimental results. Finally, we conclude our discussion in section 5.

1.1 Motivation

We are undeniably living in a technology dominant age. As a result, we are exposed to a notable array of visual imagery. The digital technology available today has begun to diminish the trust on the integrity of the visual imagery [1]. The availability of powerful image processing tools can easily modify the digital images in such a deceptive way that the doctored image seems indistinguishable from the authentic one [2]. These tampered images appear regularly with a burgeoning frequency and sophistication in the fashion industry, prevailing media outlets, tabloid magazines, scientific journals, political campaigns, courts and so on. Therefore, development of reliable encryption techniques or cryptosystem is of

great interest among scientists to help restore some trust to digital images by converting plaintext into ciphertext before transmitting the data through an insecure communication channel [1-2]. It is critical to ensure that the information being exchanged does not compromise the security.

Digital encryption algorithms have been predominant in preserving the confidentiality, integrity and authenticity of the digitally transmitted data. Among many of these techniques, Data encryption standard (DES), Advanced encryption standard (AES), Rivest-Shamir-Adelman (RSA) and Elliptic curve cryptosystems (ECC) are the most commonly used platforms. Concurrently, to analyze the encryption algorithms, several cryptographic attack methods have been contrived. For example, brute force attacks, meet-in-the-middle attacks, linear cryptanalysis and differential cryptanalysis. The former two focuses on the length of the key. In contrast, the linear cryptanalysis and differential cryptanalysis depends on the statistical analysis of the plaintext and the encryption key. To make the cipher algorithm robust against the statistical attacks, avalanche effect and bit independence criterion are the two most important properties to take into account first. Although digital forgeries may leave no visual traces of having been tampered, however, such modifications usually perturb the underlying statistics of an image [1]. Therefore, we can analyze the avalanche and bit independence properties to construct robust image cryptography algorithms because a slight modification in the image would introduce a huge difference in the new message digest. The above mentioned digital encryption algorithms have acceptable avalanche and bit independence properties [3].

Encryption techniques based on optical techniques have attracted significant attention of the researchers in the past two decades. As compared to their digital counterparts, the cryptographic properties of these systems have not been analyzed

thoroughly till now. To get wider acceptance, optical cryptosystems must prove the same security measures as their digital competitors. We believe that the investigation of these properties in encryption algorithms would be a very significant addition for evaluation of further cryptographic performance. This encouraged to evaluate avalanche and bit independence properties of discrete Gyrator domain based DRPE.

1.2 Related works and thesis contribution

The optical encryption techniques have a significant role in the image cryptography field as they offer the high-speed parallel processing ability, multiple keys and multiple degrees of freedom. The double random phase encoding (DRPE) scheme is such a widely used optical encryption technique, which has been used for image encryption, authentication, information hiding and watermarking. It has been implemented in different domains like Fourier, Fresnel and Gyrator domains, etc. Among all these domains, avalanche and bit independence properties were tested for Fourier and Fresnel domains in [3]. In this work, we evaluated avalanche and bit independence properties of the DRPE in the discrete Gyrator domain. Gyrator transform based image encryption has been widely implemented for single image [4-8], double image [9-14], multi-image [15] and color [16-22] image encryption. In this domain, a secret image is encrypted applying random operations in image Gyrator transform domains. Therefore, it is possible to encrypt the image using random phase encoding. Since, the rotation angle in Gyrator transform is an additional key, therefore it can be more secure than that of traditional DRPE technique in the Fourier domain [23]. Recently, the expression of Gyrator transform (GT) has been rewritten based on convolution operation and known as discrete Gyrator transform (DGT). In this expression, conventional GT can be

expressed using phase-only filtering, Fourier transform and inverse Fourier transform. This expression is regarded as the fast algorithm of discrete Gyrator transform and simple to implement [7, 24]. It has been claimed in [23] that, based on the periodicity of the Gyrator transform, the rotation angle in a single Gyrator transform can possibly be obtained approximately by applying exhaustive search with a known-plaintext attack. However, since Gyrator transform is continuous, it is very time consuming to apply thus exhaustive search techniques. More importantly, if we integrate the photon counting imaging (PCI) with discrete Gyrator transform, the cryptosystem becomes more secure than the DRPE in Gyrator domain [25]. Therefore, we also evaluate the avalanche and bit independence properties of the photon counting DRPE algorithm in the discrete Gyrator domain.

Chapter 2

II. Background

Cryptography is the heart of secret communication. Nevertheless, we also need to know the concurrent information hiding techniques. The communication media we use to transmit data, is not secure. Therefore, we need to construct robust and secure algorithms to assure data security. Information hiding techniques play a very important role in designing these algorithms. In this chapter, the background of the basic information hiding techniques is reviewed briefly. Since, this work broadly relates to image cryptography, therefore, we emphasized more on the study of cryptography than other concurrent information hiding techniques.

2.1 Information Hiding

Data or information has prime importance to any organization or any individual person. Like the way we do not want our conversation being overheard as it contains the potential of being misused, in the same way, the data of any organization or of any person also requires the guarantee of integrity and confidentiality. To avoid any kind of forgery, the interchange of information among the transmitter and the receiver must be done in the utmost secure way. During any information exchange, fundamentally, two types of threats exist. The eavesdropper might try to overhear the conversation in order to tamper the information and change the original meaning or it may try to listen in order to decode it and use it to his or her advantage. These attacks violates the

confidentiality and integrity of the transmitted information. Providing access to the intended user and avoiding access of the unintended user is a very difficult task. The main significance of data hiding techniques comes from the unreliability of the transmission mediums. Therefore, the construction of reliable and secure data hiding techniques is of great interest to the researchers. The most popular data hiding techniques are:

i. Cryptography.
ii. Steganography.
iii. Watermarking.

2.2 Cryptography

The term ‘Cryptography’ originated from the Greek language where Crypt means ‘hidden or secret” and graphein means ‘writing’. It is an art of converting data into an undecipherable format called cipher text. After receiving the ciphertext, the receiver deciphers or decrypt the message into the original plain text.

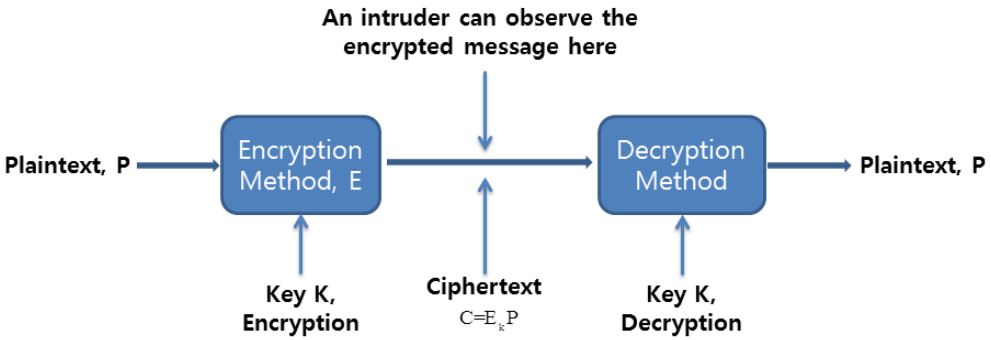

Figure 1. Block diagram of an encryption system.

Safeguarding information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction has cardinal significance in Cryptography. Therefore, it incorporates encryption/decryption, hashing, digital signatures, timestamps, etc. to ensure security aspects of the information systems.

Cryptography in the modern age is synonymous with encryption. The original information originated from the source is known as plaintext and the encrypted data is regarded as the ciphertext. Cryptography has 3 basic steps:

A. **Encryption:** It is the method of encrypting the original plain text to some unintelligible form. The output of this step is known as the cipher text.
B. **Message transfer:** This step involves the transmission of the cipher text to the recipient.
C. **Decryption:** In this step, the receiver on the other side, decrypts the cipher text to obtain the original plain text back.

Cryptography is broadly categorized into two types:

i. Symmetric key cryptography

Symmetric key cryptography refers to the encryption techniques in which the sender and the receiver share the same key. Many encryption algorithms like AES, DES, RC5 etc. use symmetric key encryption. This technique consists of five components: plain text, encryption algorithm, secret key, cipher text and decryption algorithm. Encryption algorithm encrypts by various operations on the plain text using the secret key.

The secret key is not dependent on the plain text and is selected by one of the communicating parties. The output produced by this step is called the cipher text.

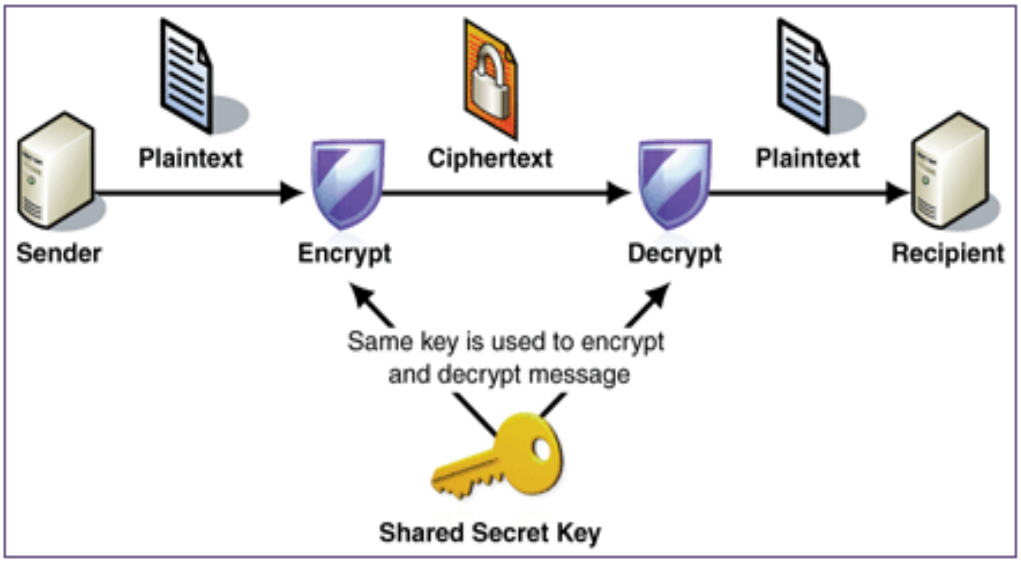

Figure 2. Schematic diagram of a Symmetric key encryption system.

The cipher text and the secret key are the inputs of the decryption algorithm and it produces plaintext as output. A significant drawback of symmetric key cipher is that it requires the secret key to be shared by each pair of the communicating parties, and also the key itself to be shared in a secured medium. Any unintended user having the secret key possesses a threat of ciphering the text.

ii. Asymmetric key cryptography

The asymmetric key cryptography is also known as public key cryptography. It uses a public key and private key pair. Public keys can be freely distributed while its pairing private key must be kept secret. The public key is used for the encryption purpose. The cipher text is then sent to the receiver. At the receiving end, it uses the secret key in the decryption algorithm to obtain the plain text back.

Public key cryptography can also be used in digital signatures. Digital signatures

can be permanently tied to the content of the message being signed. The secret key is used for signing the contents and the corresponding public key is used to validate the authenticity of the signature.

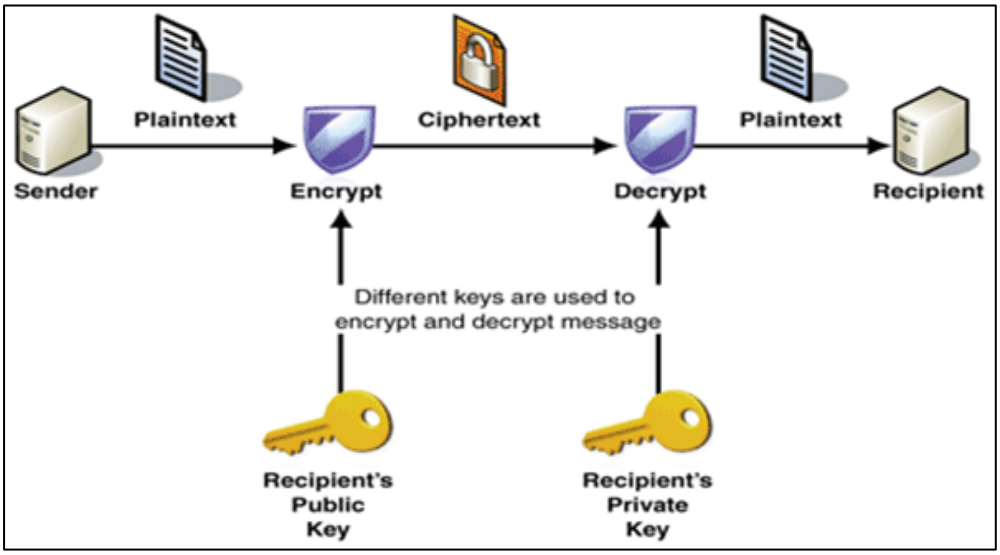

Figure 3. Schematic diagram of an Asymmetric key encryption system.

2.1.1 Goals of Cryptographic algorithms

Confidentiality, Integrity, Authentication and Non-repudiation are the key tenets of the cryptographic algorithms. Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Below is a description of the goals of the cryptosystems.

A. Confidentiality

Confidentiality is plausibly the most common aspect of information security. Any organization needs to shield against malicious attacks that jeopardize the

confidentiality of its information. For example, in military, concealment of sensitive information is a major consideration. In cryptography, Confidentiality is stated as the service which guarantees the protection against the disclosure of the information to unauthorized entities. Which means information is accessible only to the intended recipient and inaccessible to others. The term secrecy is synonymous with confidentiality and privacy. Cryptographic systems achieve confidentiality by means of several approaches ranging from physical protection to mathematical algorithms which render data unintelligible.

B. Integrity

In information security, Data integrity is the service by which accuracy and completeness of data over its entire life-cycle is desired to be maintained and assured. It addresses the unauthorized modification of data from the source entity to the destination entity. To assure data integrity, a cryptographic encryption algorithm must be able to verify data alteration by unauthorized parties and an intruder should be unable to replace a false image for a legitimate one. The hash function is one of the fundamental cryptographic primitives to assure data integrity.

C. Authenticity

Authentication assures the identity of the actual source and the receiver of the information. Authentication ascertains that the communicating entity is the one that it claims to be. In general, the authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the

two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

D. Non-Repudiation

Non-repudiation guarantees that the sender and the receiver cannot deny the authenticity of their signature on the transmitted information which they originated. Thus, when a message is sent, the receiver can assure and prove that the received message was sent by the alleged sender in real. Similarly, when a message is received, the sender can claim and prove that the alleged receiver in fact received the message.

2.1.2 Cryptanalysis and Cryptographic Attacks

Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. Cryptographic attacks are designed to subvert the security of cryptographic algorithms, and they are used to attempt to decrypt data without prior access to a key. They are part of Cryptanalysis, which is the art of deciphering encrypted data. Cryptanalysis and Cryptography (the art of creating hidden writing, or ciphers) form the science of Cryptology. Below is a brief review of different cryptographic attack methods:

(a) Known Plaintext Attack

A known plaintext attack is an attack where a cryptanalyst has access to a plaintext and the corresponding ciphertext and seeks to discover a correlation between the

two. Often the cryptanalyst knows a chunk of plaintext, maybe only a single probable word, and then tries to determine some further chunks of plaintext—or the key and thereby the complete plaintext. Ex. Stereotypical phrases (Yours sincerely), frequent words etc.

(b) Ciphertext-Only Attack

A ciphertext-only attack is an attack where a cryptanalyst has access to a ciphertext, but does not have access to corresponding plaintext. With simple ciphers, such as the Caesar Cipher, frequency analysis can be used to break the cipher.

(c) Chosen Plaintext Attack

A chosen plaintext attack is an attack where a cryptanalyst can encrypt an arbitrary plaintext of his choice and study the resulting ciphertext. The goal of the attack is to gain information which reduces the security of the encryption scheme. This is most common against asymmetric cryptography, where a cryptanalyst has access to a public key.

(d) Chosen Ciphertext Attack

A chosen ciphertext attack is an attack where a cryptanalyst chooses a ciphertext and attempts to find a matching plaintext. The cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key. In the attack, an adversary has a chance to enter one or more known ciphertexts into the system and obtain the resulting plaintexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.

(e) Side Channel Attacks

Side channel attacks leverage additional information based on the physical implementation of a cryptographic algorithm, including the hardware used to encrypt or decrypt data. The cryptographic attack methods previously described assume that a cryptanalyst has access to the plaintext or ciphertext (sometimes both) and possibly the cryptographic algorithm. A side channel attack leverages additional information, such as time taken (or CPU cycles used), to perform a calculation, voltage used, and so on.

(f) Brute Force Attacks

A brute force attack systematically attempts every possible key. It is most often used in a known plaintext or ciphertext-only attack.

(g) Linear Cryptanalysis and Differential Cryptanalysis

Differential cryptanalysis and linear cryptanalysis are related attacks used primarily against iterative symmetric key block ciphers. An iterative cipher (also called a product cipher) conducts multiple rounds of encryption using a subkey for each round. Examples include the Feistel Network used in DES and the State rounds used in AES. In both attacks, a cryptanalyst studies changes to the intermediate ciphertext between rounds of encryption. The attacks can be combined, which is called differential linear cryptanalysis.

A goal of strong encryption is to produce ciphertexts that appear random where a small change in a plaintext results in a random change in the resulting ciphertext. This quality is called diffusion, and any changed ciphertext bit should have a 50% chance of being a 1 or a 0. Both attacks seek to discover non-randomness (cases where the 50% rule is broken) in an effort to discover potential subkeys.

I. Linear Cryptanalysis

Linear cryptanalysis is a known plaintext attack that requires access to large amounts of plaintext and ciphertext pairs encrypted with an unknown key. It focuses on statistical analysis against one round of decryption on large amounts of ciphertext. The cryptanalyst decrypts each ciphertext using all possible subkeys for one round of encryption and studies the resulting intermediate ciphertext to seek the least random result. A subkey that produces the least random intermediate cipher for all ciphertexts becomes a candidate key (the most likely subkey).

II. Differential Cryptanalysis

Differential cryptanalysis is a chosen plaintext attack that seeks to discover a relationship between ciphertexts produced by two related plaintexts. It focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm. A plaintext pair is created by applying a Boolean exclusive or (XOR) operation to a plaintext. For example, XOR the repeating binary string 10000000 to the plaintext. This creates a small difference (hence the term differential cryptanalysis) between the two. The cryptanalyst then encrypts the plaintext and its XORed pair using all possible subkeys, and it seeks signs of non-randomness in each intermediate ciphertext pair. The subkey that creates the least random pattern becomes the candidate key.

2.3 Steganography

Steganography is a practice of hiding/concealing the message, file, image within another message, file or image. The word steganography is of Greek origin and means "covered writing" or "concealed writing". In other words, it is the art and

science of communicating in a way which hides the existence of the communication. The goal is to hide messages inside other harmless messages in a way that does not allow an enemy to even detect that there is a second message present. Steganography focuses more on high security and capacity. Even small changes to stego medium can change its meaning. Steganography masks the sensitive data in any cover media like images, audio, video over the internet. Steganography involves four steps: 1. Selection of the cover media in which the data will be hidden. 2. The secret message or information that is to be masked in the cover media. 3. A function that will be used to hide data in the cover media and its inverse to retrieve the hidden data. 4. An optional key or the password to authenticate or to hide and unhide the data. The cover chosen should be done very carefully. The cover chosen should contain sufficient redundant information which can be used to hide the data, because Steganography works by replacing the redundant data with the secret message.

2.4 Watermarking

A watermark is a recognizable image or pattern that is impressed onto paper, which provides evidence of its authenticity. Watermark appears as various shades of lightness/darkness when viewed in transmitted light. Watermarks are often seen as security features to banknotes, passports, postage stamps and other security papers. Digital watermarking is an extension of this concept in the digital world. Today there have been so much of data over internet that it has forced us to use mechanisms that can protect ownership of digital media. Piracy of digital information is very common, be it images, text, audio or video. These can be produced and distributed very easily. So, it becomes very important to find out who is the owner of the document. Digital watermarking provides a solution for

longstanding problems faced with copyright of digital data. Digital watermark is a kind of marker covertly embedded to any digital data, such as audio or image data. It can later be extracted or detected to make assertion about data. This information can be information about the author, copyright or an image itself. The digital watermark remains intact under transmission/transformation, allowing us to protect our ownership rights in digital form. Digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. A watermarking system's primary goal is to ensure robustness, i.e., it should be impossible to remove the watermark without tampering the original data. Digital watermarking is a passive protection tool. It just marks the data, but does not degrade it, nor controls access to data. One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies. Another application is in broadcast monitoring, the television news often contains watermarked video from international agencies.

Chapter 3

III. Optical domain based Image Security

Images are different from text in many aspects. Although the traditional cryptosystems can be directly utilized to encrypt images, however, it is not a good idea for two causes. The first reason is that the image size is almost always likely to be much greater than that of the text. Therefore, the traditional cryptosystems require much computational time to directly encrypt the image data, which is a big issue for designing efficient encryption algorithms. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable. Another issue of using digital cryptographic systems is that some of those algorithms, which were originally thought to be secure have finally been broken i.e. DES and Wireless Equivalent Privacy protocol. Taking all of these issues into consideration, development of optical domain based image encryption techniques are becoming popular among the researchers. One major advantage of optical domain based image encryption process over the conventional digital encryption techniques is the speed of processing large amounts of information. In addition, optical security can employ numerous parameters for encryption, including wavelength, phase information, spatial frequency or polarization of light. However, for any cryptosystem to be trusted, its ability to endure an attack from a third party under certain conditions must be proved. Although it is true that optical technology may initially represent a technological barrier for an attacker, one should not trust a system based only on this feature in the long run. Therefore, we believe that optical cryptosystems must pass the same security tests of their digital competitors.

3.1 Double Random Phase Encoding (DRPE)

Double random phase encoding (DRPE) proposed in 1995, has been studied and implemented vastly in the information security aspect [26]. It was found robust to different types of noise and distortion [27]. The encoded image using two random phase masks is a complex function consists of phase and amplitude. The real and imaginary parts of this complex function are independent stationary white noise data [28]. The phases of the statistically independent random masks (keys) in the spatial and frequency domains are uniformly distributed in the interval [0, 1] and expressed as exp[i2πn(x, y)] and exp[i2πb(μ, ν)], with n(x, y) and b(μ, ν). The encryption process can be shown with the following equation:

$$f_c(x,y) = \Im^{-1}\Big[\Im\big[f(x,y)\exp[i2\pi n(x,y)]\big]\exp[i2\pi b(\mu,\nu)]\Big], \qquad (1)$$

Where $\Im$ and $\Im^{-1}$ are 2D Fourier and inverse Fourier transforms. The procedure is reversed for the decryption. Figure 4 shows the DRPE schematic in the Fourier domain.

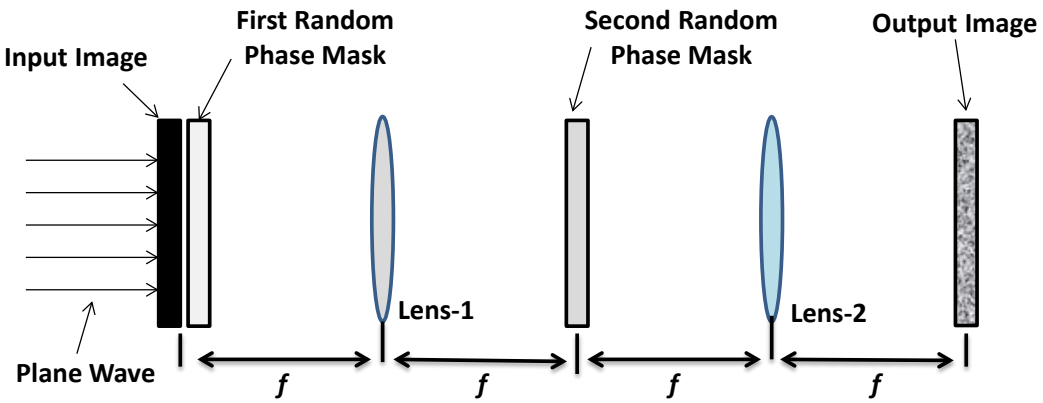

Figure 4. Schematic diagram of the DRPE in Fourier domain (f is the focal length of the lens).

Since DRPE has been reported as vulnerable to chosen cipher text attacks, many improvements in the conventional DRPE system have been taken place afterwards. Recently, the DRPE system integrated with photon counting imaging (PCI) technique was proposed by Pérez-Cabré to improve the cryptographic performance of DRPE system. The photon counting DRPE scheme introduces an additional layer of protection and thus makes the cryptosystem more secured.

3.2 Mathematical Modeling of DRPE in Gyrator Domain

Gyrator transforms (GT) belongs to the orthosymplectic class of linear canonical transforms as well as the fractional Fourier transforms and produces the rotation in twisted position-spatial frequency planes of phase space [29-30]. For the large range of rotation angles α, GT domain can be constructed with only three generalized lenses with a fixed distance between them [30]. GT expression of a two dimensional function $f_i(\vec{g}_i)$ having rotation angle α, can be defined as:

$$f_o(\vec{g}_o) = G^{\alpha}[f_i(\vec{g}_i)](\vec{g}_o) = \iint f_i(x_i, y_i) K_{\alpha}(x_i, y_i; x_o, y_o) dx_i dy_i$$
$$= \frac{1}{|\sin\alpha|} \iint f_i(x_i, y_i) \left\{ \exp\left[i2\pi \frac{(x_o y_o + x_i y_i)\cos\alpha - (x_i y_o + x_o y_i)}{\sin\alpha} \right] \right\} dx_i dy_i, \quad (2)$$

$$K_{\alpha}(x_i, y_i; x_o, y_o) = \frac{1}{|\sin\alpha|} \times \exp\left[i2\pi \frac{(x_o y_o + x_i y_i)\cos\alpha - (x_i y_o + x_o y_i)}{\sin\alpha} \right], \quad (3)$$

where α= pπ/2, 0 ≤ α < 2π, 0 ≤ p < 4 and GT is expressed as G^{α}. $\vec{g}_i$ and $\vec{g}_o$ represents the input and output plane coordinates and $K_{\alpha}(x_i, y_i; x_o, y_o)$ is the Kernel function of the GT. Gyrator transform is periodic with 2π [16]. For p=0 (α=0), the transform is an identity transform. At p=1 (α=π/2), the direct Fourier transform with rotation of the coordinate at π/2 is obtained. When p=2 (α=π), it corresponds

to reverse transform. For p=3 (α=3π/2), the system resembles to the inverse Fourier transform with rotation of the coordinate at π/2. Inverse Gyrator transform corresponds to Gyrator transform at rotation angle - α [23, 25].

Fresnel diffraction integral in the free space under paraxial approximation can be used to obtain the calculation of discrete GT. However, if we think about the computational scheme, it would require a larger computational load. A fast algorithm of discrete GT obtained by simulating the convolution expression of fractional Fourier transform accelerates the application and the validity of the aforementioned algorithm has been proved by numerical simulation in [24]. If we want to construct an image cipher, a fast algorithm is more preferred. Therefore, we follow fast algorithm of discrete Gyrator transform to design our algorithm.

Using the triangle equation, $\cot\alpha = -\tan[\alpha/2] + 1/\sin\alpha$, Eq. (3) can be expressed as follows:

$$K_\alpha(x_i, y_i; x_o, y_o) = \frac{\exp\left[-i2\pi(x_i y_i + x_o y_o)\tan\frac{\alpha}{2}\right]}{|\sin\alpha|} \times \exp\left[i2\pi\frac{(x_i - x_o)(y_i - y_o)}{\sin\alpha}\right]. \quad (4)$$

Combining Eqs. (2) and (4), the convolution equation of GT can be constructed as follows:

$$f_o(x_o, y_o) = f_g = p_1(x_o, y_o)\left\{\left[f_i(x_i, y_i)\, p_1(x_i, y_i)\right] * p_2(x_i, y_i)\right\}, \quad (5)$$

where the symbol '*' represents the convolution operation. P_1 and P_2 are two phase only masks, which are equal to

$$p_1(x, y) = e^{-i2\pi xy\tan\frac{\alpha}{2}}, \quad (6)$$

$$p_2(x,y)=\frac{e^{i2\pi xy\csc\alpha}}{|\sin\alpha|}. \tag{7}$$

Since we are using two random phase masks RP1 and RP2 and two different angles α_1 and α_2 as additional phase keys, our new phase masks in the discrete Gyrator domain are as follows:

$$p_1'(x,y)=e^{-i2\pi RP1(x,y)\tan\frac{\alpha_1}{2}}, \tag{8}$$

$$p_2'(x,y)=\frac{e^{i2\pi RP2(x,y)\csc\alpha_2}}{|\sin\alpha_2|}. \tag{9}$$

According to the convolution property of Fourier transform, Eq. (5) can be written as:

$$f_g=p_1'\Im^{-1}\left[\Im\left[p_1'f_i\right]\Im\left[p_2'\right]\right]. \tag{10}$$

The Fourier transform of the phase function $p_2'(x,y)$ can be calculated as:

$$P(\mu,\nu)=\Im\left[p_2'(x,y)\right]=e^{-i2\pi\mu\nu\sin\frac{\alpha_2}{2}}. \tag{11}$$

We substitute $\Im\left[p_2'\right]$ with P in Eq. (10) and get our final equation of discrete Gyrator transform as follows:

$$f_g=p_1'\Im^{-1}\left[\Im\left[p_1'f_i\right]P\right]. \tag{12}$$

Two times of FFT algorithm can be implemented for the calculation of discrete Gyrator transform. Thus the computational speed is increased [7, 24].

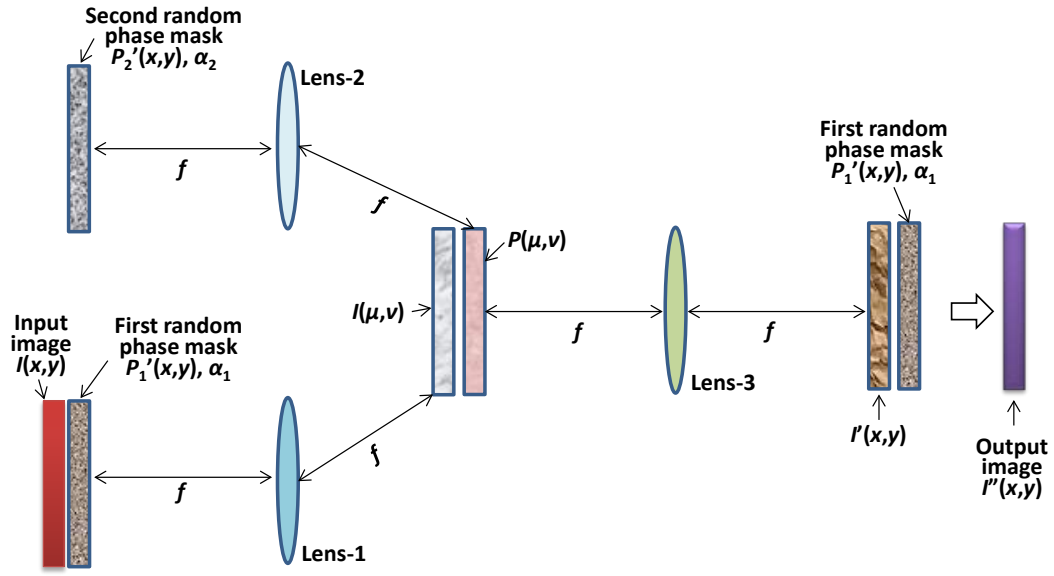

Figure 5. Schematic diagram of DRPE in discrete Gyrator domain (f is the focal length of the lens).

3.3 Photon Counting Imaging

Photon counting imaging (PCI) has the advantage that in the entire scene, the number of photons can be limited by having a controlled expected number of incident photons. A photon limited image carries less information than that of the original counterpart and hardly reveal the original appearance of the primary image. Thus, such system improves information authentication robustness against intruder attacks. By generating a sparse encrypted data, it generates distributions with fewer photons than conventional imaging techniques and also provides substantial bandwidth reduction [31-34].

The Poisson distribution of the probability of counting l_j photons at pixel j can be shown by the following equation:

$$Poisson(l_j;\lambda_j)=\frac{[\lambda_j]^{l_j}e^{-\lambda_j}}{l_j!}, l_j=0,1,2..., \quad (13)$$

where λ_j is the Poisson parameter defined by:

$$\lambda_j = N_p x_j, \quad (14)$$

where N_p is the expected number of incident photons, x_j is the normalized irradiance at pixel j, such that $\sum_{j=1}^{N} x_j = 1$ and N is the total number of pixels in the scene [31].

It has been proved that photon limited encrypted distributions have sufficient information for successful authentication and retrieval of the signal [31-34]. Although the signal can be retrieved after decryption, it remains visually unrecognizable noise like signal to the receiver because of the sparse representation of the encrypted image. Even though intruder attacks and tries to get some information from the decrypted image, it cannot recognize the image by visual inspection [31-33].

We can make an assumption from the previous discussion that integration of PCI can make the system one-way as the decrypted image will always be visually unrecognizable and will be useful only for image verifications. Therefore, usually the sparse distributed photon limited image obtained by applying PCI is not intended for visualization of the original primary image. Rather, it is intended for the verification of the authenticity of the original image by means of optical correlation.

3.4 Avalanche and bit independence criterions

When the security of the cryptographic systems is analyzed, it is needed to measure whether the systems fall under a certain optimum level of security or not. To verify the security, cryptographic test methods such as avalanche, strict avalanche and bit independence criteria are of great interest to measure the degree of security of the designed cryptographic networks [35]. If an optical domain based encryption algorithm is designed, it is fundamental to observe these properties to analyze the robustness of the designed algorithm against statistical attacks. If the designed algorithms achieve a satisfactory bit independence and avalanche effect, it can be claimed that the resulting algorithm is robust against statistical attacks [3].

i. Avalanche and strict avalanche criterions

In cryptographic function design, avalanche effect is a very well-known heuristic. Although the name of this criterion was first coined by Feistel, the original idea links back to Shannon's notion of diffusion [36]. From the view of an encryption algorithm, an avalanche effect is evident if a small change in the plaintext or key brings a large change in the cipher-text drastically. For encryption, it is a characteristic in which a small change in the message produces a large change in the message digest [37].

Avalanche effect intuitively reflects the idea of high-nonlinearity [38]. If a substantial degree of avalanche effect is not exhibited during the avalanche test, then the designed algorithm has poor randomization, which helps a cryptanalyst to make predictions about the input, being given only the output. This weakness of the algorithm may be partially or completely be ample enough to break the algorithm [39].

Webster and Tavares proposed the combination of completeness and the avalanche effect as a new criterion namely strict avalanche criterion (SAC). It is a generalization of the avalanche effect. When i and j (1, 2, 3…, n) are input and output bits respectively, mathematically, the function $f:\{0,1\}^n \to f\{0,1\}^n$ satisfies SAC, when on average 50% of the output bits exhibits change with the change in one input bit [39].

Suppose an encryption process E is represented as $Y = E(X, K)$, where X is the plaintext, K is the encryption key and Y is the ciphertext. If we change the plaintext into X', then after encryption, we obtain the new ciphertext $Y' = E(X', K)$. If we change the key into K', then the ciphertext becomes $Y'' = E(X, K')$. If we consider the Hamming distance between the original ciphertext Y and the ciphertext Y' (which we obtain by encrypting after changing some bits of the original plaintext) is $H(Y, Y')$, then the avalanche effect can be calculated from the following equation:

$$Avalanche = \frac{H(Y, Y')}{Num(Y)}, \tag{15}$$

where $Num(Y)$ denotes the total number of binary bits of the ciphertext. Similarly, the avalanche equation for some big change in the key (K') can be represented by the following equation:

$$Avalanche = \frac{H(Y, Y'')}{Num(Y)}, \tag{16}$$

where $H(Y, Y'')$ is the Hamming distance between the original ciphertext Y and the ciphertext Y'' (with some bits changed in the key).

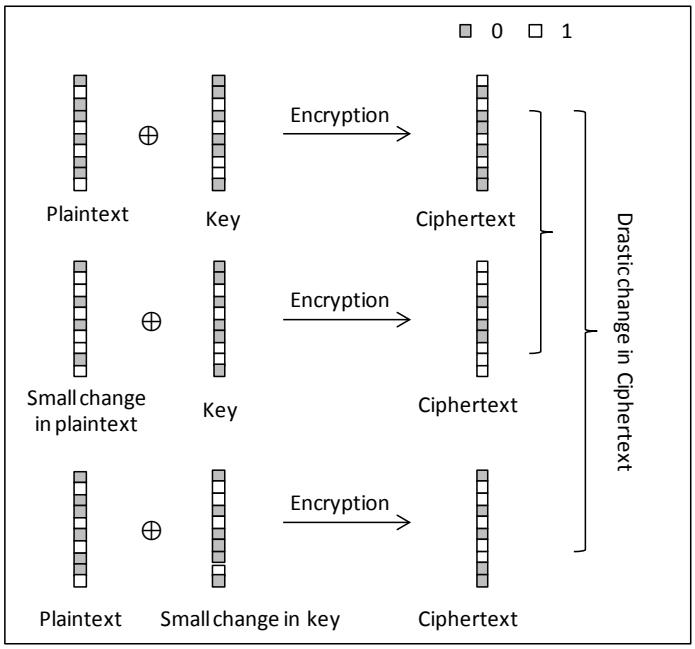

Figure 6. Illustration of avalanche effect in data encryption (when an plaintext or a key is changed slightly the ciphertext changes significantly).

ii. Bit independence criterion

Bit independence criterion (BIC) was introduced by Webster and Tavares as another property for S-box security. It is a test of randomness of a cryptographic encryption algorithm [38]. If the bit independence criterion is satisfied, then it is not possible to infer one value in the sequence from the others [37]. We measure the degree of independence between a pair of avalanche variables by calculating the correlation coefficient. BIC is satisfied if any change in the single input bit i in the plaintext or in the encryption key results in a change in a way that any two output bits j and k in the ciphertext are changed independently of each other. Suppose there are total N bits in the plaintext and according to BIC, the plaintext can be changed N times when only one bit is flipped at a time. The bit

independence (BI) between bit j and k in the ciphertext can be defined using the absolute correlation coefficient as follows:

$$BI\left(C\left(b_j\right),C\left(b_k\right)\right)=\left|corr\left(\left(b_j^1\ldots,b_j^i\ldots,b_j^N\right),\left(b_k^1\ldots,b_k^i\ldots,b_k^N\right)\right)\right|, \quad (17)$$

where C(bj) and C(b_k) connotes the j^{th} and k^{th} bit in the ciphertext, and b_j^i and b_k^i denotes the values of the j^{th} and k^{th} bit in the ciphertext with change in the i^{th} bit in the plaintext. If the resulting value of Eq. (17) leans to 1, then it reveals strong correlation between two bits. The bit independence criterion implies that each pair of bits in the ciphertext for a given crypto algorithm should be bit independent. Accordingly, the bit independence criterion (BIC) for an encryption algorithm can be demonstrated with the following equation:

$$BIC(E(X,Y))=\max_{\substack{1\le j,k\le N\\ j\ne k}} BI\left(C\left(b_j\right),C\left(b_k\right)\right), \quad (18)$$

where E(X, K) connotes the encryption algorithm. If BIC(E(X, K)) is far from 1, it demonstrates that the algorithm satisfies bit independence criterion in a very well manner. Conversely, the BIC(E(X, K)) value close to 1 means some bit pairs are dependent on each other in the encrypted image [38].

Chapter 4

IV. Experimental Results and Analysis

In this work, all experiments were performed under the following environment:

1) Computer: Intel® Core™ i5-2500,

2) CPU: 3.30GHz,

3) RAM: 4GB,

4) OS: Windows 7,

5) Matlab: R2014a.

Also, all resulting data were digitally recorded and stored in computer without optical configuration. In the simulation part of our experiment, a grayscale image of size 50×50 is used to test the avalanche criterion. An illustration of the used image is shown in Figure 7.

Figure 7. Illustration of the gray scale image used for testing avalanche criterion.

We converted the amplitude value of the encrypted image by the DRPE in discrete Gyrator domain into binary representation whenever we analyzed our proposed method for bit units. We used IEEE 754 double precision floating point format for binary representation and only considered the fractional portion consisting of 52 bits of significant digits. The values of this portion were only altered when even one bit was flipped otherwise the value in the sign and exponent portions were similar for the majority of the amplitude values with double formats. Therefore, we only concentrated on the 52 bits of the significant digits to carry the experiment without loss of generality.

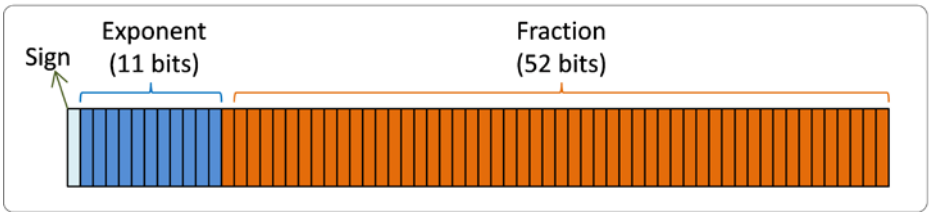

Figure 8. IEEE 754 double-precision binary floating-point format.

We averaged 100 experimental results to calculate the avalanche values. To calculate the avalanche effect, we conducted the experiment changing plaintext, first phase key, second phase key and rotation angle independently. The rotation angles were randomly chosen and kept fixed at α_1=0.32 and α_2=0.75 to calculate these values. Figure 9 and Table 1 presents the avalanche values obtained by varying the number of bits in the plaintext, Figure 10 and Table 2 presents the avalanche values obtained by varying number of bits in the first phase key, and Figure 11 and Table 3 presents the avalanche values obtained by varying number of bits in the second phase key.

Table 1. Avalanche effect changing some bits of the plaintext in Discrete Gyrator and Fourier Domain.

Number of changed bits in plaintext	Avalanche Effect			
	Discrete Gyrator Domain (Bit Unit)	Discrete Gyrator Domain (Pixel Unit)	Fourier Domain (Bit Unit)	Fourier Domain (Pixel Unit)
1	0.4999	1	0.2798	0.8350
5	0.4993	1	0.4233	1
10	0.4999	1	0.4580	1
15	0.4994	1	0.4628	1
20	0.4993	1	0.4727	1
25	0.4986	1	0.4737	1
30	0.4998	1	0.4723	1
35	0.4985	1	0.4740	1
40	0.4992	1	0.4730	1
45	0.4994	1	0.4691	1
50	0.4996	1	0.4751	1

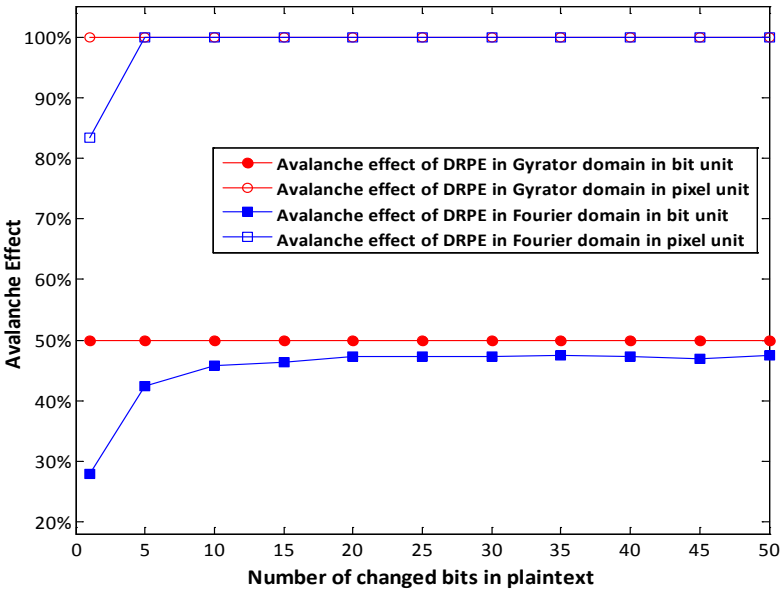

Figure 9. Avalanche effect with some bits in the plaintext inverted.

Table 2. Avalanche effect with some bits of the first key inverted in Discrete Gyrator and Fourier Domain.

Number of changed bits in first random key	Avalanche Effect			
	Discrete Gyrator Domain (Bit Unit)	Discrete Gyrator Domain (Pixel Unit)	Fourier Domain (Bit Unit)	Fourier Domain (Pixel Unit)
1	0.4987	1	0.2618	0.6952
5	0.4993	1	0.4014	1
10	0.4990	1	0.4321	1
15	0.4992	1	0.4731	1
20	0.5003	1	0.4629	1
25	0.5004	1	0.4813	1
30	0.5005	1	0.4797	1
35	0.4993	1	0.4742	1
40	0.4994	1	0.4848	1
45	0.4989	1	0.4722	1
50	0.4997	1	0.4842	1

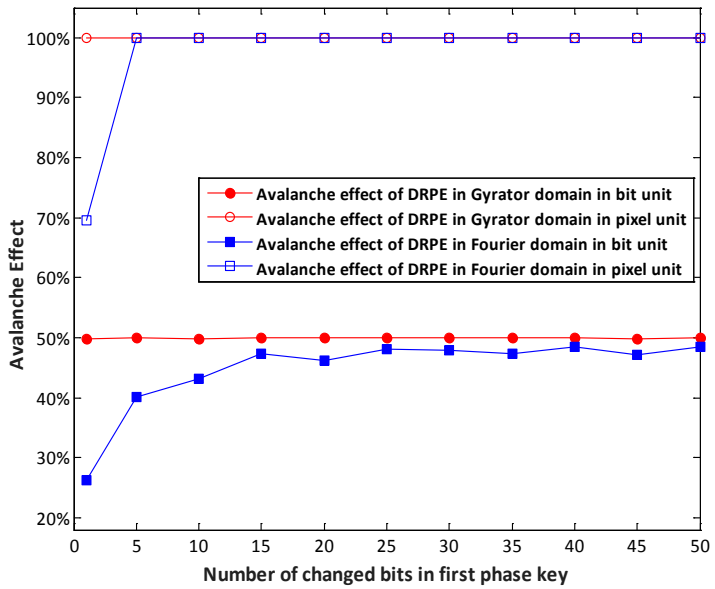

Figure 10. Avalanche effect with some bits in the first phase key inverted.

Table 3. Avalanche Effect changing some bits in second random key for DRPE in Discrete Gyrator and Fourier Domain.

Number of changed bits in second random key	Avalanche Effect			
	Discrete Gyrator Domain (Bit Unit)	Discrete Gyrator Domain (Bit Unit)	Fourier Domain (Bit Unit)	Fourier Domain (Pixel Unit)
1	0.4986	1	0.2332	0.7641
5	0.4993	1	0.3622	1
10	0.4987	1	0.4348	1
15	0.5000	1	0.4488	1
20	0.4998	1	0.4693	1
25	0.4994	1	0.4761	1
30	0.4991	1	0.4655	1
35	0.4996	1	0.4700	1
40	0.4988	1	0.4794	1
45	0.4990	1	0.4682	1
50	0.5000	1	0.4770	1

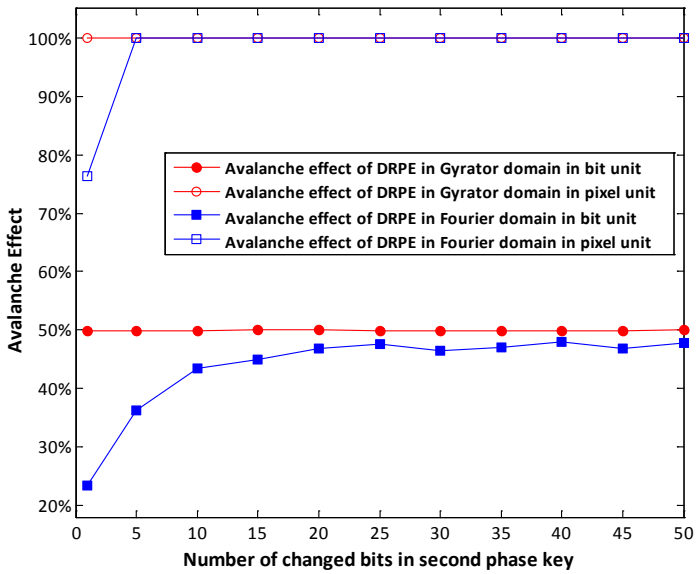

Figure 11. Avalanche effect with some bits in the second phase key inverted.

In all of the figures, resulting avalanche values are indicated as the avalanche effect of DRPE in bit unit. Furthermore, avalanche effects in pixel unit is also calculated and shown in all of the figures labeled as DRPE in pixel unit.

Table 4. Avalanche Effect for different Rotation angles of DRPE in Discrete Gyrator.

Rotation angle, α (Degrees)	Avalanche Effect with 1 bit change in		
	Plaintext (bit unit)	First Random Key (bit unit)	Second Random Key (bit unit)
45	0.4994	0.5009	0.4994
60	0.4992	0.4996	0.4987
90	0.4991	0.4980	0.4997
120	0.4990	0.4984	0.4989
135	0.4990	0.4998	0.4996
150	0.4986	0.4998	0.4996
210	0.4995	0.4984	0.4991
225	0.4990	0.4995	0.4989
240	0.4998	0.5000	0.4988
270	0.4993	0.4994	0.4990
300	0.4996	0.4995	0.5007
315	0.4991	0.4973	0.4988
330	0.4999	0.4998	0.4980

It is evident from the Figs. 9, 10 and 11 that the DRPE in discrete Gyrator domain shows better avalanche effect as compared to that of Fourier domain. All avalanche values obtained by varying the number of bits in the plaintext, first phase key and second phase key of the DPRE in discrete Gyrator domain are very close to 50%. In contrast, avalanche effects for less than 10 bits change in the plaintext, less than 15 bits in the first phase key and less than 20 bits in the second phase key of the DRPE in Fourier domain was not satisfactory as it was not close to 50%.

We assume that the integration of the rotation angle and random phase shiftings assisted discrete Gyrator domain to outperform the Fourier domain in this regard. In the discrete Gyrator domain, the 100% change in pixel values with respect to one bit change in the plaintext, first phase key and second phase key shows very satisfactory avalanche effect which means one bit change affects all of the surrounding values and proves Shannon's diffusion property strongly.

In the next step, we varied the values of a single rotation angle, α to observe the resulting avalanche effects. The rotation angles are selected according to the condition of α as stated in chapter 3. The resulting avalanche values are shown in Table 4. From this table, we can observe that the resulting avalanche effects of these values of α are all nearly 50%. We can notice that any change in the rotation angle results in a drastic change in all of the bits which proves the good strength of the rotation angle as a key.

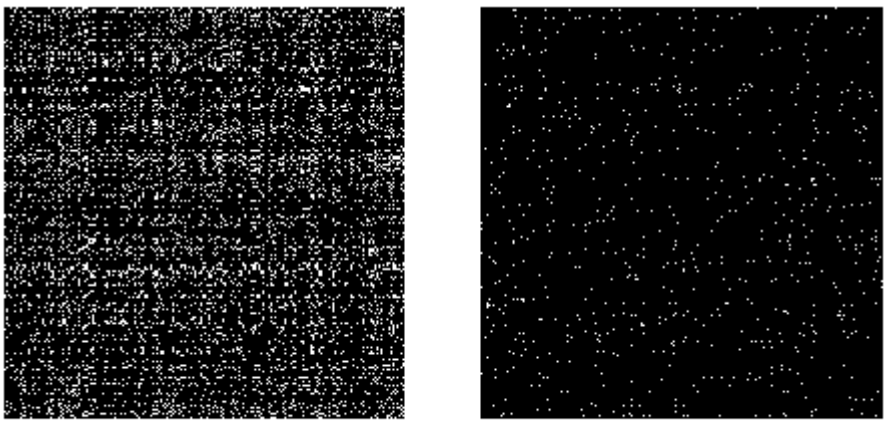

Figure 12. Illustration of the photon counted Gyrator domain DRPE images with (a) $Np=10^5$, (b) $Np=10^4$.

After experiments on the significance of rotation angle, we tested the avalanche effect of the DRPE systems integrated with photon counting imaging (PCI). An illustration of the photon counted ($N_p=10^5$) lena.jpg image of size 512x512 is shown in figure 12(a). This experiment is divided into two parts. First, we checked avalanche effects varying the number of bits of the plaintext, first phase key and second phase key of the photon counting DRPE in the discrete Gyrator domain keeping the number of incident photons fixed at 10^5. At this time, the randomly selected rotation angles were kept fixed to $\alpha_1=0.32$ and $\alpha_2=0.75$. We compared these values with avalanche effects of the photon counting DRPE in Fourier domain.

Figure 13. Illustration of the image used for bit independence criterion test.

Figure 14 and Table 5; Figure 15 and Table 6; and Figure 16 and Table 7 demonstrates the results of the first part. From Figs. 14, 15, and 16 we can see that for both Fourier and Gyrator domain, the avalanche effect results are almost similar if we keep the number of photons fixed at 10^5.

Table 5. Avalanche Effect of PCI (10^5) integrated DRPE changing n bits of the plaintext.

Number of changed bits in plaintext	Avalanche Effect			
	Discrete Gyrator Domain PCI (Bit Unit)	Discrete Gyrator Domain PCI (Pixel Unit)	Fourier Domain PCI (Bit Unit)	Fourier Domain PCI (Pixel Unit)
1	0.4989	1	0.4892	1
5	0.5004	1	0.4984	1
10	0.4994	1	0.4985	1
15	0.4979	1	0.4991	1
20	0.4986	1	0.4986	1
25	0.4986	1	0.4988	1
30	0.4989	1	0.4985	1
35	0.4990	1	0.4986	1
40	0.4986	1	0.4989	1
45	0.4978	1	0.4990	1
50	0.4979	1	0.4989	1

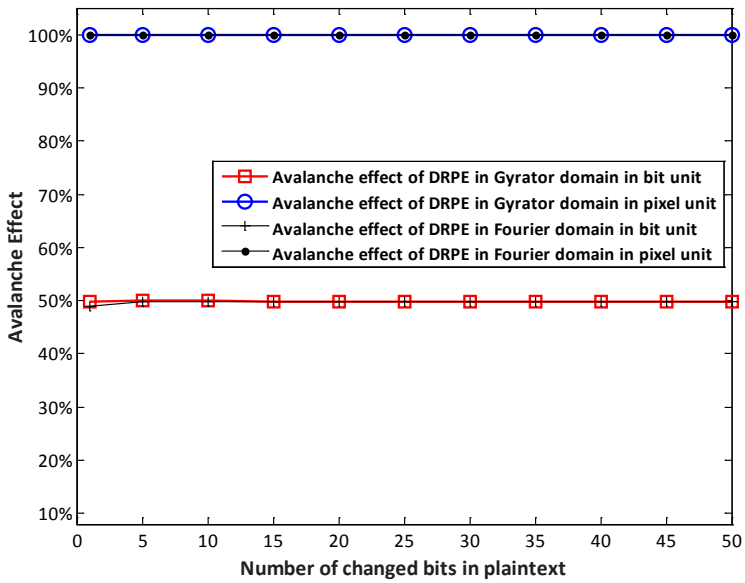

Figure 14. Avalanche effect with some bits in the plaintext inverted after integrating photon counting imaging in DRPE ($Np=10^5$).

Table 6. Avalanche Effect of PCI (10^5) integrated DRPE changing n bits of the first phase key.

Number of changed bits in first random key	Avalanche Effect			
	Discrete Gyrator Domain PCI (Bit Unit)	Discrete Gyrator Domain PCI (Pixel Unit)	Fourier Domain PCI (Bit Unit)	Fourier Domain PCI (Pixel Unit)
1	0.4991	1	0.4889	1
5	0.4983	1	0.4987	1
10	0.4989	1	0.4983	1
15	0.4976	1	0.4989	1
20	0.4982	1	0.4986	1
25	0.4990	1	0.4989	1
30	0.4991	1	0.4986	1
35	0.4978	1	0.4985	1
40	0.4979	1	0.4988	1
45	0.4980	1	0.4997	1
50	0.4986	1	0.4990	1

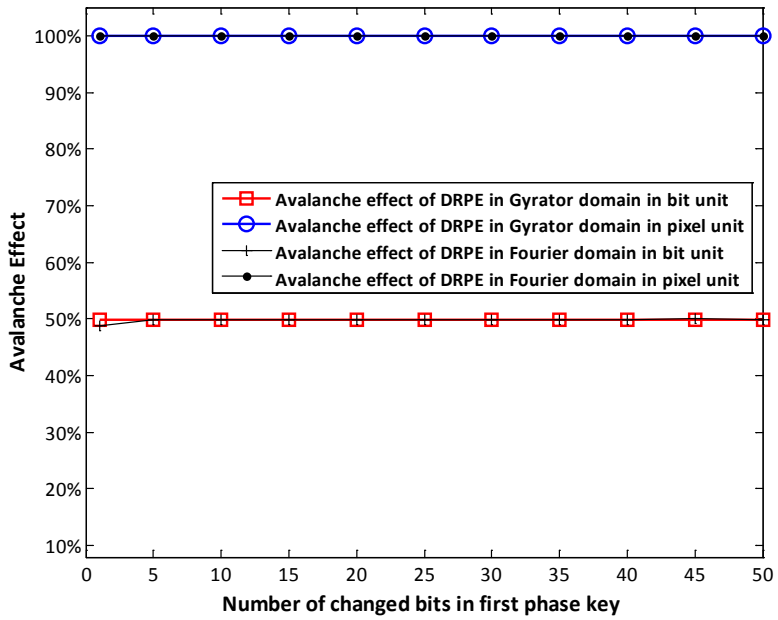

Figure 15. Avalanche effect with some bits in the first phase key inverted after integrating photon counting imaging in DRPE ($Np=10^5$).

Table 7. Avalanche Effect of PCI (10^5) integrated DRPE changing n bits of the second phase key.

Number of changed bits in second random key	Avalanche Effect			
	Discrete Gyrator Domain PCI (Bit Unit)	Discrete Gyrator Domain PCI (Pixel Unit)	Fourier Domain PCI (Bit Unit)	Fourier Domain PCI (Pixel Unit)
1	0.5000	1	0.4858	0.9999
5	0.4987	1	0.4983	1
10	0.4991	1	0.4976	1
15	0.4982	1	0.4985	1
20	0.4988	1	0.4989	1
25	0.4991	1	0.4984	1
30	0.4990	1	0.4984	1
35	0.4986	1	0.4992	1
40	0.4980	1	0.4987	1
45	0.4977	1	0.4993	1
50	0.4987	1	0.4987	1

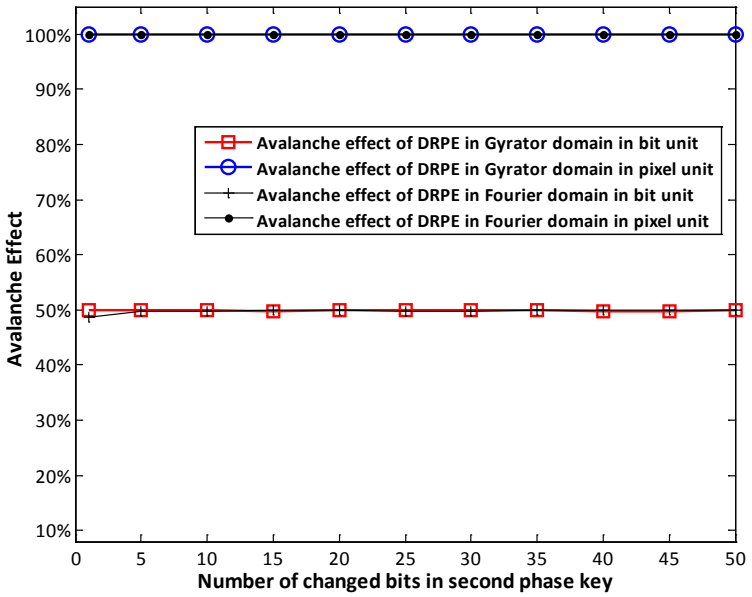

Figure 16. Avalanche effect with some bits in the second phase key inverted after integrating photon counting imaging in DRPE ($Np=10^5$).

In general, photon counting imaging systems are designed for low light levels (photon starved conditions) or night vision. Logically, the less photon it contains, the less information it has to interpret visually since the scene becomes more sparse due to less photon arriving at each pixel. Therefore, in the second part, we tested the avalanche effect keeping the number of incident photons fixed at 10^4 and varied the number of bits in the plaintext, first phase key and second phase key respectively. The resulting avalanche effect values changing the number of bits in plaintext are shown in Figure 17 and Table 8. Avalanche effect values changing the number of bits in the first phase key are shown in Figure 18 and Table 9. Avalanche values changing the number of bits in the second phase key are shown in Figure 19 and Table 10.

It is noted that the photon counting DRPE in Fourier domain did not show satisfactory avalanche effect when the number of photons were 10^4 and the number of flipped bits were less than 10 in the plaintext and first phase key.

Also, from Figure 19 we can observe that the avalanche effects were relatively poor for the photon counting DRPE in the Fourier domain when the number of flipped bits were less than 15 in the second phase key. In contrast, the photon counting DRPE in the discrete Gyrator domain with potentially low photon level ($Np=10^4$) showed very good avalanche effects of nearly 50% for all of the changes in the number of bits in the plaintext, first phase key and second phase key. Therefore, the DRPE in the discrete Gyrator domain integrated with PCI performs better than the photon counting DRPE in the Fourier domain even if we slightly decrease the number of photons and it is more acceptable as an image authentication system as compared to the photon counting DRPE in the Fourier domain.

Table 8. Avalanche Effect of PCI (10^4) integrated DRPE changing n bits of the plaintext.

Number of changed bits in plaintext	Avalanche Effect			
	Discrete Gyrator Domain PCI (Bit Unit)	Discrete Gyrator Domain PCI (Pixel Unit)	Fourier Domain PCI (Bit Unit)	Fourier Domain PCI (Pixel Unit)
1	0.5006	1	0.4222	1
5	0.4997	1	0.4766	1
10	0.4986	1	0.4861	1
15	0.4977	1	0.4880	1
20	0.4982	1	0.4915	1
25	0.4989	1	0.4892	1
30	0.4988	1	0.4900	1
35	0.4991	1	0.4927	1
40	0.4985	1	0.4913	1
45	0.4980	1	0.4920	1
50	0.4991	1	0.4930	1

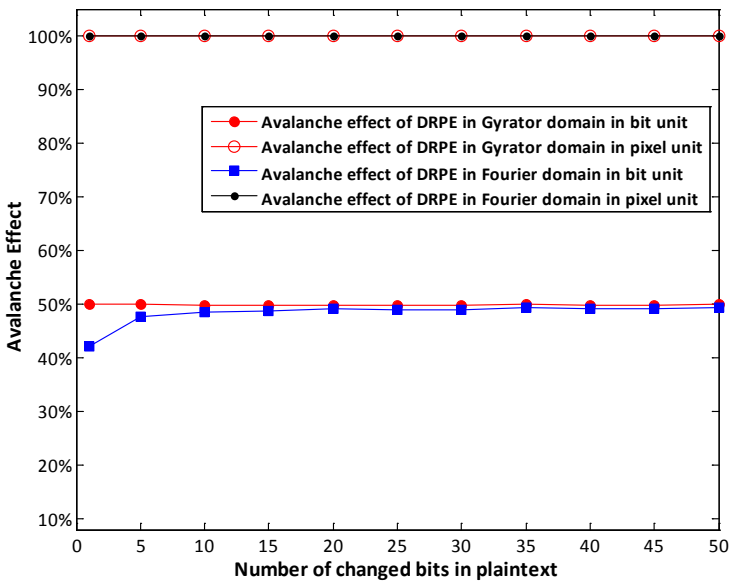

Figure 17. Avalanche effect with some bits in the plaintext inverted after integrating photon counting imaging in DRPE ($Np=10^4$).

Table 9. Avalanche Effect of PCI (10^4) integrated DRPE changing n bits of the first phase key.

Number of changed bits in first random key	Avalanche Effect			
	Discrete Gyrator Domain PCI (Bit Unit)	Discrete Gyrator Domain PCI (Pixel Unit)	Fourier Domain PCI (Bit Unit)	Fourier Domain PCI (Pixel Unit)
1	0.4982	1	0.4188	0.9999
5	0.4989	1	0.4700	1
10	0.4980	1	0.4874	1
15	0.4988	1	0.4904	1
20	0.4984	1	0.4908	1
25	0.4987	1	0.4923	1
30	0.4987	1	0.4917	1
35	0.4987	1	0.4948	1
40	0.4988	1	0.4932	1
45	0.4990	1	0.4934	1
50	0.4985	1	0.4941	1

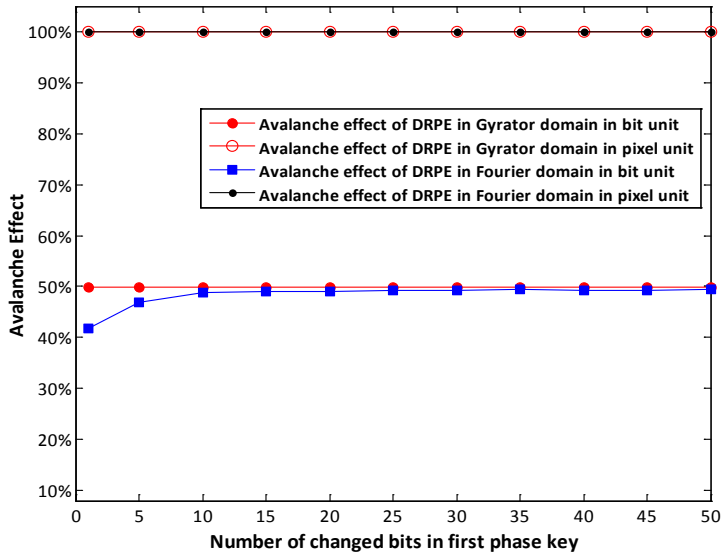

Figure 18. Avalanche effect with some bits in the first phase key inverted after integrating photon counting imaging in DRPE ($Np=10^4$).

Table 10. Avalanche Effect of PCI (10^4) integrated DRPE changing n bits of the second phase key.

Number of changed bits in second random key	Avalanche Effect			
	Discrete Gyrator Domain PCI (Bit Unit)	Discrete Gyrator Domain PCI (Pixel Unit)	Fourier Domain PCI (Bit Unit)	Fourier Domain PCI (Pixel Unit)
1	0.4979	1	0.3674	0.9865
5	0.4991	1	0.4580	1
10	0.4985	1	0.4793	1
15	0.4989	1	0.4854	1
20	0.4987	1	0.4887	1
25	0.4991	1	0.4882	1
30	0.4992	1	0.4879	1
35	0.4984	1	0.4928	1
40	0.4986	1	0.4906	1
45	0.4976	1	0.4929	1
50	0.4989	1	0.4922	1

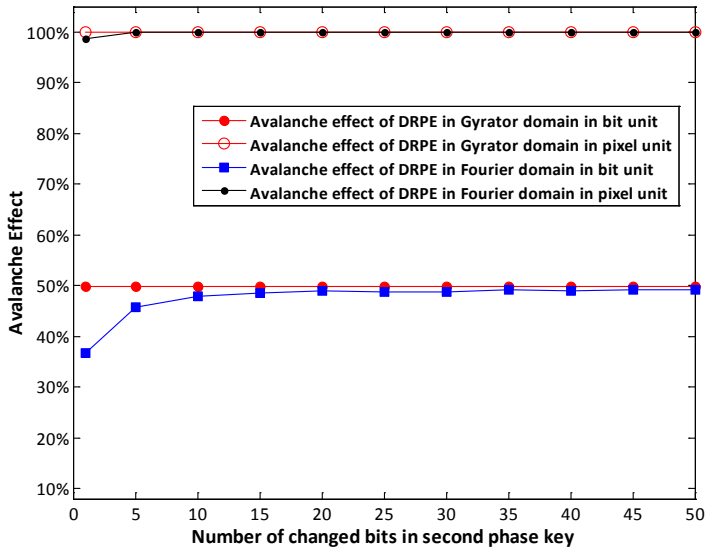

Figure 19. Avalanche effect with some bits in the second phase key inverted after integrating photon counting imaging in DRPE ($Np=10^4$).

After evaluating avalanche effect criterion, we tested bit independence criterion (BIC) of the DRPE systems in both domains. To test the BIC, a binary cameraman image was utilized. The binary image used for this purpose is shown in Figure 13. All of the bit independence values were measured taking an average of 100 numerical simulations. A correlation value obtained from Eq. (17) shows satisfactory bit independence criterion if it is not close to 1. A comparison table showing bit independence values for the DPRE in the discrete Gyrator domain and the DRPE in the Fourier domain is shown in Table 11.

Table 11. Bit independence criterion for DRPE in the Fourier and discrete Gyrator domains.

Repeatedly changing bits in	Bit independence criterion	
	Discrete Gyrator domain	Fourier domain
Plaintext	0.2606	0.2820
First random key	0.4381	0.4809
Second random key	0.3936	0.5638

Table 12 shows bit independence values for the photon counting DPRE in the discrete Gyrator domain and the photon counting DRPE in the Fourier domain. The rotation angles were randomly chosen as α_1=0.35 and α_2=0.75 to calculate these values. From the Table 11 and Table 12 we can observe that the DRPE in the discrete Gyrator domain shows better bit independence performance than that of DRPE in the Fourier domain. Also, encryption systems with PCI integration and encryption systems without PCI integration both shows good bit independence values since all of the values are far less than 1.

Table 12. Bit independence criterion for DRPE in the Fourier and discrete Gyrator domains after integrating photon counting imaging.

Repeatedly changing bits in	Bit independence criterion	
	Photon counting discrete Gyrator domain	Photon counting Fourier domain
Plaintext	0.2393	0.3126
First random key	0.2049	0.2884
Second random key	0.1867	0.3675

Avalanche and bit independence properties signify the robustness against statistical analysis. Verification of these properties has paramount importance in designing of the cryptographic algorithms, especially for block cipher designing. Gyrator domain is being widely implemented in image encryption recently. Therefore, analysis of avalanche and bit independence properties of encryption systems in the Gyrator domain is important to investigate its feasibility of being used in the secure image authentication systems based on DRPE. Image encryption algorithms in the Fourier domain have weaknesses which might lead to the easy statistical analysis of it. Our study shows that the encryption system in the discrete Gyrator domain can be used as a more efficient alternative to encryption schemes in the Fourier domain as it is found to be more secure and robust against statistical attacks.

Chapter 5

V. CONCLUSIONS

In this study, the avalanche and bit independence characteristics of double random phase encoding (DRPE) scheme in the discrete Gyrator domain are evaluated. In addition, the avalanche and bit independence characteristics of double random phase encoding (DRPE) scheme in the PCI integrated discrete Gyrator domain are investigated. By comparing avalanche and bit independence properties of Fourier and discrete Gyrator domains of both systems, it has been discovered that the DRPE in the discrete Gyrator domain apparently performs better than that of conventional DRPE in the Fourier domain. The rotation angle in the discrete Gyrator domain provides an additional layer of security and thus assist to ensure image confidentiality. The integration of the PCI makes the system visually unintelligible and improves security while conserving the avalanche and bit independence criterions successfully. The analysis of avalanche and bit independence properties of the cryptosystems in virtual optical domain can be regarded as an effective tool for the future design of the robust cryptosystems in optical domain instead of conventional digital block ciphers.

BIBLIOGRAPHY

[1] H. Farid, “Image Forgery Detection,” IEEE Signal Processing Magazine 26, 16-25 (2009).

[2] P. Kr. Naskar, S. Majumdar, P. Das, and A. Bose, “An Analytical Survey on Different Secured Image Encryption Techniques,” IJCAT 1, 396-403 (2014).

[3] I. Moon, F. Yi, Yeon H. Lee, and B. Javidi, “Avalanche and Bit Independence Characteristics of Double Random Phase Encoding in the Fourier and Fresnel Domains,” J. Opt. Soc. Am. A 31, 1104-1111 (2014).

[4] N. Singh and A. Sinha, “Gyrator Transform-Based Optical Image Encryption, Using Chaos,” Opt. and Lasers in Eng. 47, 539-546 (2009).

[5] Z. Liu, X. Lie, C. Lin, J. Dai, and S. Liu, “Image Encryption Scheme by Using Iterative Random Phase Encoding in Gyrator Transform Domains,” Opt. and Lasers in Eng. 49, 542-546 (2011).

[6] Z. Liu, M. Yang, W. Liu, S. Li, M. Gong, W. Liu, and S. Liu, “Image encryption algorithm based on the random local phase encoding in gyrator transform domains,” Opt. Commun. 285, 3921-3925 (2012).

[7] S. Daza, F. Vega, L. Matos, C. Moreno, M. Diaz, and Y. Daza, “Image encryption based on convolution operation in the gyrator transform domain,” Proceedings of the IECON, 1527-1529 (2012).

[8] Z. Liu, H. Chen, T. Liu, P. Li, L. Xu, J. Dai, and S. Liu, “Image encryption by using gyrator transform and Arnold transform,” Journal of Electronic Imaging 20, 013020 (2011).

[9] H. Li and Y. Wang, “Double-image encryption based on iterative gyrator transform,” Opt. Commun. 281, 5745-5749 (2008).

[10] Z. Liu, Q. Guo, L. Xu, M. Ahmad, and S. Liu, “Double image encryption by using iterative random binary encoding in gyrator domains,” Opt. Express 18, 12033-12043 (2010).

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

[12] H. Li, Y. Wang, H. Yan, L. Li, Q. Li and X. Zhao, “Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform,” Opt. Lasers Eng. 51, 1327-1331 (2013).

[13] Q. Wang, Q. Guo, and L. Lei, “Double image encryption based on phase-amplitude mixed encoding and multistage phase encoding in gyrator transform domains,” Opt. Lasers Technol. 48, 267-279 (2013).

[14] Z. Shao, H. Shu, J. Wu, Z. Dong, G. Coatrieux, and J. Coatrieux, “Double color image encryption using iterative phase retrieval algorithm in quaternion gyrator domain,” Opt. Express 22, 4932-4942 (2014).

[15] Q. Wang, Q. Guo, and L. Lei, “Multiple-image encryption system using cascaded phase mask encoding and a modified Gerchberg-Saxton algorithm in gyrator domain,” Opt. Commun. 320, 12-21 (2012).

[16] M. Abuturab, “Color image security system using double random-structured phase encoding in gyrator transform domain,” Appl. Opt. 51, 3006-3016 (2012).

[17] M. Abuturab, “Color information security system using discrete cosine transform in gyrator transform domain radial-Hilbert phase encoding,” Opt. Lasers Eng. 50, 1209-1216 (2012).

[18] M. Abuturab, “Color information cryptosystem based on optical superposition principle and phase-truncated gyrator transform,” Appl. Opt. 51, 7994-8002 (2012)

[19] L. Sui and B. Gao, “Color image encryption based on gyrator transform and Arnold transform,” Opt. Lasers Technol. 48, 530-538 (2013).

[20] H. Chen, X. Du, Z. Liu, and C. Yang, “Color image encryption based on the affine transform and gyrator transform,” Opt. Lasers. Eng. 51, 768-775 (2013).

[21] M. Abuturab, “Single-channel color information security system using LU decomposition in gyrator transform domains,” Opt. Commun. 323, 100-109 (2014)

[22] M. Abuturab, “An asymmetric color image cryptosystem based on Schur decomposition in gyrator transform domain,” Opt. Lasers Eng. 58, 39-47 (2014)

[23] J. Sang, J. Zhao, Z. Xiang, B. Cai, and H. Xiang, “Security Analysis of Image Encryption Based on Gyrator Transform by Searching the Rotation Angle with Improved PSO Algorithm,” Sensors 15, 19199-19211 (2015).

[24] Z. Liu, D. Chen, J. Ma, S. Wei, Y. Zhang, J. Dai, and S. Liu, “Fast Algorithm of Discrete Gyrator Transform Based on Convolution Operation,” Optik-International Journal for Light and Electron Optics 122, 864-867 (2011).

[25] M. Juan O. Vilardy, S. Maria, and E. Pérez-Cabré, “Secure Image Encryption and Authentication Using the Photon Counting Technique in the Gyrator Domain,” presented at IEEE 20th Symposium on Signal Processing, Images and Computer Vision 1-6 (2015).

[26] Z. Xin, D. Lai, S. Yuan, D. Li, and J. Hu, “A Method for Hiding Information Utilizing Double-Random Phase-Encoding Technique,” Opt. & Lasers Technol. 39, 1360-1363 (2007).

[27] S. Kishk and B. Javidi, “Information Hiding Technique with Double Phase Encoding,”Appl. Opt. 41, 5462-5470 (2002).

[28] G. Unnikrishnan, J. Joseph, and K. Singh, “Optical Encryption by Double-Random Phase Encoding in the Fractional Fourier Domain,” Opt. Letters 25, 887-889 (2000).

[29] H. Li, “Image Encryption Based on Gyrator Transform and Two-Step Phase-Shifting Interferometry,” Opt. and Las. in Eng. 47, 45-50 (2009).

[30] J. Rodrigo, A. Tatiana, and L. María, “Gyrator Transform: Properties and Applications,” Opt. Express 15, 2190-2203 (2007).

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

[32] E. Pérez-Cabré, C. Héctor, S María, and B. Javidi, “Photon-Counting Double-Random-Phase Encoding for Secure Image Verification and Retrieval,” Jour. of Opt. 14, 094001 (2012).

[33] E. Pérez-Cabré, M. Cho, and B. Javidi, “Information Authentication Using Photon-Counting Double-Random-Phase Encrypted Images,” Opt. Letters 36, 22-24 (2010).

[34] S. Rajput, D. Kumar, and N. Nishchal, “Photon Counting Imaging and Phase Mask Multiplexing for Multiple Images Authentication and Digital Hologram Security,”Appl. Opt. 54, 1657-1666 (2015).

[35] S. Gupta and S. Yadav, “Performance Analysis of Cryptographic Hash Functions,” Int’l Jour. of Sci. and Res. 4, 2319-7064 (2015).

[36] V. Goyal, A. O’Neill, and V. Rao, Correlated-input secure hash functions (Springer, 2011).

[37] W. Stallings, Cryptography and Network Security Principles and Practice (Prentice Hall, 2011).

[38] J. Castro, J. Sierra, A. Seznec, A. Izquierdo, and A. Ribagorda, “The Strict Avalanche Criterion Randomness Test,” Math. and Com. in Simulation 68, 1-7 (2005).

[39] A. ALabaichi, R. Mahmod, and F. Ahmad, “Analysis of Some Security Criteria for S-boxes in Blowfish Algorithm,” Int’l Jour. of Dig. Content Tech. and its Applications 7, 8 (2013).

ACKNOWLEDGEMENTS

Though only my name is printed on the cover of this thesis, a great many people have contributed to its entire journey. I owe my gratitude to all those people who have made this thesis possible and because of whom my graduate experience has been one that I will cherish forever.

First and foremost, I am deeply indebted to my thesis advisor, Professor Inkyu Moon, who opened the door for me to pursue higher studies in abroad. I have been amazingly fortunate to have an advisor who gave me the freedom to explore on my own, and at the same time the guidance to recover when my steps stumbled. I would have been completely lost without his guidance. I am greatly thankful to him for reading my reports, commenting on my views and helping me understand and enrich my ideas. His patience, encouragement, support and insightful suggestions throughout this journey helped me immensely to come this far. His confidence in my abilities makes me dream higher to pursue a PhD. I vow that I will try my very best to commit to my students and strive to be as good of an advisor as Professor Moon has been to me.

It is a great pleasure for me to thank all of the faculty and staff members of my school for their precious support and advices. I express my sincere gratitude to Prof. Inkyu Moon, Prof. Lee Sangwoong, Prof. Kwon Gu Rak, Prof. Cho Beomjoon, Prof. Chung Il Yong and Prof. Young-Sik Kim for offering valuable courses which helped me significantly in being a researcher. Besides, I deeply thank the teachers of my language School, Inha University for teaching me Korean Language with passion. I believe that my language learning experience has an immense impact on my personal and academic skill development, and for that I offer my heartfelt thanks to them.

To my lab-mates, thanks for the cooperation and support. I would like to convey my sincere gratitude to each of my colleagues, Keyvan Jaferjadeh, Tabassum Nasrin Haque, Dr. Faliu Li, Ayesha Akter Lata, Ghomali Samaneh, Han Minggu, Dr. Jeong Yu Seon and Kim Hwan for their consistent support. I greatly look forward to continue a lifelong friendship with all of you.

I would like to especially thank my big brother from the lab, Keyvan Jaferjadeh. The experimental part of my thesis would not have been possible without his help. I am indebted to him for his valuable opinions and time. Also, when my advisor was in USA, Keyvan Jaferjadeh encouraged and guided me like a true mentor. I cannot adequately express how thankful I am for this. I am greatly thankful to Tabassum for referring me as a potential KGSP student to our advisor and also for helping me greatly in the first semester. Of all the people I have worked with in the lab, I will miss hanging out with Ayesha the most. She has been a sister and a source of great emotional support.

My greatest gratitude goes to my friend Iqbal Hossain, who patiently advised and guided me to balance my personal and academic life. The simple phrase, ‘thank you’, cannot present how much his friendship and care means to me.

I have been blessed with a friendly and cheerful group of fellow students and fellow country mates in the graduate school. All of them became my family in this foreign land. Thank you all for the emotional support, entertainment and encouragements. Special thanks to Ahlam Mallak, Sanjay Basukala, Shajeel Iqbal, Adnan Hashmi, Sadeque Reza Khan, Anie Farahida Binti Omar, Saruar Alam for always being there for me whenever I needed.

I thank the Almighty for giving me the strength and patience to work through all these years so that today I can stand proud with my head held high.

I acknowledge the great contribution of the National Institute for International Education (NIIED), Government of South Korea for providing me with the necessary funding and fellowship to pursue a Master's degree at Chosun University as a Korean Government Scholarship student.

Finally, I would like to acknowledge the people who mean the world to me, my parents, my sisters and my nephew-nieces. I don't imagine a life without their love and blessings. Thank you mom and dad for showing faith in me and giving me liberty to choose what I desired. I consider myself the luckiest in the world to have such a supportive family, standing behind me with their love and support.