February 2017
Master's Degree Thesis

Double Random Phase Encoding Method with a Poisson-Multinomial Distribution

Graduate School of Chosun University

Department of Computer Engineering

Lata Ayesha Akter

Double Random Phase Encoding Method with a Poisson-Multinomial Distribution

포아송-다중분포 기반 이중 랜덤 위상 인코딩 방법

February 25, 2017

Graduate School of Chosun University

Department of Computer Engineering

Lata Ayesha Akter

Double Random Phase Encoding Method with a Poisson-Multinomial Distribution

Advisor: Prof. Moon In Kyu, PhD

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

February 2017

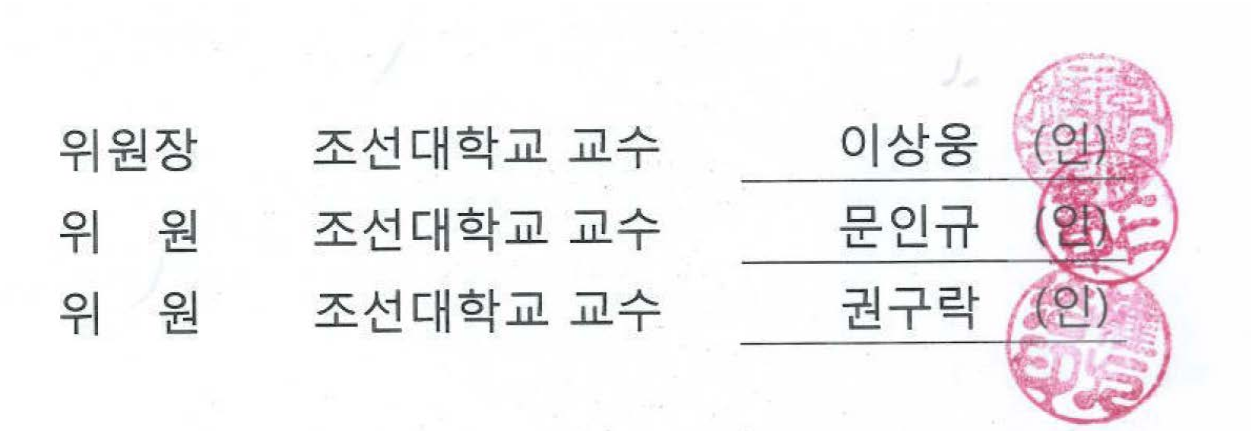
Graduate School of Chosun University

Department of Computer Engineering

Lata Ayesha Akter

February **2017**	**Master's Degree Thesis**	**Double Random Phase Encoding Method with a Poisson-Multinomial Distribution**	**Lata Ayesha Akter**

라타 아이샤 액터의 석사학위논문을 인준함



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

2017 년 02 월

조선대학교 대학원

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Double Random Phase Encoding Method with a Poisson-Multinomial Distribution

Lata Ayesha Akter
Advisor: Prof. In kyu Moon, Ph.D.
Department of Computer Engineering
Graduate School of Chosun University

In this research, a new approach is proposed for authenticating digital color image where a new approach, Poisson-Multinomial Distribution (PMD) is introduced to integrate with Double Random Encryption method. The main goal of this study is to reduce the complexity of the application and propose a simplified way for applying the PCI scheme on three channels simultaneously. Getting the stationary white noise after applying DRPE on the three channels separately and then applying PMD based PCI on the encrypted 3D image, the final output will be hard to break for an attacker. Unlike the previous system, the new scheme works precisely with the original digital RGB image. At first, the system encrypts those three channels of the image individually with DRPE method and the amplitude part of the encrypted image is photon counted using PMD. At last to obtain the compressed optimal result, a probability density function is used. On the authentication part, the reference digital image is encrypted by the same method and then both of the encrypted images are compared with a statistical nonlinear correlation method. The experiments say that, this proposed Poisson-multinomial distribution based method is proven to be a good and simplified one that can be used to encrypt digital color images and in addition even if the number of photons is really low, this new system can perfectly differentiate between true class and false class image.

한 글 요 약

포아송-다중분포 기반 이중 랜덤 위상 인코딩 방법

라타 아이샤 액터

지도 교수: 문인규

컴퓨터공학과

대학원, 조선대학교

본 연구에서는 포아송-다항 분포 (PMD) 기반 광자 계수 이미징 (PCI) 및 이중 랜덤 위상 부호화 (DRPE) 방식을 이용하는 새로운 컬러영상 인증 방법을 제안한다. 제안한 방법에서는 컬러영상의 효과적 인증을 위하여 우선 참조컬러영상에 기존의 DRPE 을 적용하여 암호화된 영상 값을 생성한다. 이렇게 암호화된 영상에 새로운 방식의 PMD 기반 PCI 기법을 적용하여 공격자가 해독하기 어려운 패턴의 암호화된 영상 값을 출력한다. 기존 DRPE 시스템과 달리, 본 논문에서 제안한 인증방식은 RGB 의 컬러영상을 단 한번의 DRPE 계산을 통하여 효율적으로 암호화할 수 있다는 것을 특징으로 한다. 마지막으로 제안한 새로운 암호기법으로부터 획득한 참조결과영상과 입력결과영상사이의 비선형 상관계수 값을 계산하여 효과적으로 컬러영상을 인증할 수 있음을 컴퓨터 실험결과를 통하여 입증한다.

CHAPTER 1

INTRODUCTION

Now, it is the modern era of automation where everyone and everything is depending on computerization, digitalization and no matter how far the distance is, to communicate with each other they are totally depending on internet. And since we are talking about information communication then we must mention about digital image which is playing a very important role in this field. An image can carry various information of an object and on top of that if it is a color image then it can represent various information of an object such that-object recognition, visualization and characteristics. Now-a-days the utilization of digital images has been boosted up incredibly. On the other hand, when we try to transport them through unprotected carrier such as internet, the image can be twisted or changed by an attacker. Hence, it is a high time to become more cautious about the authentication and legitimacy of images.

In this chapter, at first we will give a brief introduction about the necessity of image security and the motivation where we will explain why it is important to authenticate the image. After that we will show a review of background works where we will know about the previous achievements in this image authentication filed. And on the last part of this chapter we are going to explain the current work and our research contribution.

1.1 Motivation

By the term “Image authentication”, we mean to check the validity of the image whether it is still unchanged or already corrupted by any third party attacker in the midway of transmission. In order to smooth the transmission process the image data is needed to be compressed so that it can be easily sent to the other side. Otherwise it usually takes a huge amount of bandwidth to go to the receiver’s side. Hence, to scale down the size of an image, the compression algorithm is used.

Moreover, to keep the image safe from the outside attacker, it is necessary to encrypt the image data which means to give extra security layer for protecting the image. This is a technique that totally changes the actual data and transforms it into a different form that no one can recognize what was it before. By this way it will be protected and even though it has been changed for transmission, on the receiving end by authentication method it can be retrieved easily. This whole information securing process is known as Cryptography. There have many methods those are well-known in this information security field; Stenography is also one of them. However, there is an important difference between Stenography and Cryptography. As for Stenography, it try to conceal the actual message by implanting it into another data so that no third party can know that there is a message hiding behind that data. On the other hand, in Cryptography, the system convolve the main message with the help of another data and alter the message into a stationary noise that even though the attacker knows that this is the message still he cannot understand the actual message.

Now-a-days, in this digital century when everyone is depending on wireless communication via internet, the demand of data encryption technology or cryptography is showing a high pick in order to keep the genuineness, privacy and incorruptibility of the information. To secure the transmittable data, many encryption algorithms are being used in this cryptographic field. Among them – Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir-Adelman (RSA) and Elliptic Curve Cryptosystems (ECC) are the most frequently used encryption techniques. On the other hand, as expected, attackers are also being active to break those encryption systems so that they can get the confidential information. For instance, Brute force attack, Meet-in-the-Middle attack, Chosen-Cipher text attack, Chosen-Plaintext attack, Linear Cryptanalysis and Differential Cryptanalysis are some well-known attacks. The Brute-Force attack and Meet-in-the-Middle attack, these two attacks usually target the key-length of the cryptosystem and Chosen-Cipher text and Chosen-Plaintext attacks analyze the chosen plaintexts and cipher-texts. On the other hand, Linear and Differential Cryptanalysis focuses on the statistical studies of the plaintext and the encryption key. In most cases, the encryption system encipher the data in a way that it is really hard for an intruder to break the code, instead it will tampered the cipher data and try to make it difficult for the receiver to get the original data. Moreover, sometimes the attackers alter the encrypted data so that

when receivers get the transmitted data they cannot authenticate the information even though the data is a valid one. In order to make the encryption system more strong it is necessary to make it analytically and statistically protected.

The use of images in information communication over wireless channels is became popular now-a-days since images can easily carry variety of information at once. Hence, to secure the image during trespassing open channels many methods have been created in this time being. Cryptographic researchers have been working on how to protect the information carrier images as well as authenticate them after transmission. Considering the digital encryption with optical encryption it is obvious that encryption methods in image cryptography have not been investigated efficiently. In order to grab more attention on image cryptosystem it is necessary to demonstrate that the security level of optical cryptosystem is as strong as the established digital cryptosystem. It is obvious that development on this filed will enhance the robustness of the cryptographic platform. Motivating by that concept, in this research work we have studied about an efficient cryptographic method for color image and using that method how we can verify the genuineness of the image.

1.2 Previous Achievements in Image Authentication Field

As we mentioned before, Image encryption and authentication techniques have a great impact on the area of optical cryptography for having rapid parallel transmitting capability, numerous keys and different degrees of freedom. The Double Random Phase Encoding (DRPE) method is one of the most popular and extensively used schemes in the optical cryptographic operations such as-image encryptions, verifications, information hiding and water marking [5]. This scheme has been applied on various domains as well, for example: Fourier domain, Fresnel domain and also Gyrator domain where it showed different level of performance respectively. DRPE has several properties those are counted as the advanced added values for securing information. It has that capability of altering the image data into a total stationary white noise and as a result the output DRPE encrypted image is entirely different from the original input image and visually unrecognizable. And only using the exact encryption keys it is possible to revive the primary image. Although this scheme has

good performance in the area of image security [7-8], it is also a proven fact that DRPE algorithm is defenseless to chosen-cipher text attacks [9,10]. Hence, the invader who frequently accesses the DRPE system can retrieve the encryption keys. To solve this problem Pérez-Cabré et al. [11,12] has established a method where he integrated a photon counting imaging method with the original DRPE system. PCI can yields an image data where the distribution is scarce. The processed data from this combined system is totally different from the input image and hence, can secure DRPE from illegitimate strikes to promote its shield in a certain degree. The main point of this method is to verify the image rather than retrieving the original image. For verification, a statistical method, non-linear correlation can be used [11,12,17,18]. Nonetheless, this propitious algorithm proclaimed in [11,12] was experimented only on binary and monochrome images. Now-a-days, the use of color image has gone really viral universally for item resolution, perception and encryption [19-24]. It can present a collection of bulk information to the outer world. Therefore, it is really demanding to establish a verification method for multispectral color images. Current researches proved that, in the case of multispectral visualization of photon-starved 3D scenes, it is feasible to apply multispectral photon counting integral imaging system adopting Bayer images [25].

As an extension of that work, in 2014, Faliu Yi et al. [1] created a new method where Multispectral Photon-Counting Imaging (MPCI) is integrated with DRPE which can be used to authenticate multispectral images. On that process, the original RGB image is down-sampled into three channels (red, green and blue) [25] which are then encrypted individually and the amplitude part of the encrypted image is then photon counted [1]. After applying photon counting imaging technique, the relative phase information of nonzero amplitude is possessed for decryption. In order to authenticate the encrypted image, the system used a statistical nonlinear correlation method [11,12]. To transform the decrypted Bayer image into a RGB image, an efficient interpolation approach is used. However, in every step of that process, the system had to do the computation individually for each of the channels.

1.3 Current Research Contribution

Since the present established method works with down-sampled Bayer image and because of that each channel needs to go through the whole integrated process individually, thence it required more computational time. On this regard, it would be more efficient if we could find a way to apply the encryption process simultaneously on these three channels. By focusing that point, our research shows that, it is possible to apply the integrated process without down-sampling the 3D image. The main purpose of our proposed system is to apply the whole encryption process and photon-counting scheme without breaking the bonding of 3 channels. In this current process, at first we applied the DRPE technique on the color image where the system encrypts three color channels individually. After encrypting the original image by double random phase encoding method, a photon-counting imaging method is applied on the amplitude part of the output image. This time, the photon-counting imaging technique follows a Poisson-Multinomial distribution [41]. This photon-counted image is then optimized for achieving a lower bandwidth to ensure a smoother transmission over risky open channels. On the optimization part the system used a method called probability density function that works with the photon counted image and the probabilities of finding specific colors of the image pixels. The function will give a two dimensional output and that will be the final message digest for transmitting to the receiver end. For authentication part, we encrypted the reference image with the same process and compared both encrypted images by using statistical nonlinear correlation algorithm. Comparing to other methods [19-24], our recommended integrated system of Poisson-Multinomial Distribution (**PMD**) based Photon-Counting Imaging (**PCI**) and Double Random Phase Encoding (**DRPE**) scheme using in this study, can authenticate the image under low-light level whereas the image will be masked visually.

The main purpose of proposing this new method is to find a simplified way to encrypt a digital color image which can optimize the computational time and complexity. Most of the digital cameras use CCD (Charge Coupled Device) image sensor. Physically, when those CCD sensored cameras take picture, the images are captured as a Bayer image format. Hence, on the previous work [1], the author down-sampled the previously stored digital color image and converted it to a

Bayer image to operate the integration process to make it as similar as the practical one. However, this proposed system will only work for digital color images not for instrumental use. Since in a 3D color image each pixel has three colored photons and physically it is almost impossible to classify them accurately, so this new method can be applied only on digital color images. Using Matlab simulation, mathematically, we can identify and classify each and every element of a digital color image; therefore, it is possible to apply multivariate method on them.

On the later chapters, the results of using that technique are discussed in detail. There, the simulation results evidently clarify that the proposed method can be a simplified and efficient one for authenticating a digital color image.

CHAPTER 2

CONCEPTUAL HISTORY

For a secured intercommunication, cryptography is playing an irreplaceable and important role. However, it is also required for us to get the proper knowledge of basic cryptographic methods. For transferring the information we need to use some transmission channels, which are not protected. On this regard, for the protection of transmitting information it is really important to formulate powerful and unassailable techniques. Data concealing algorithms are the core elements for establishing these methods. The conceptual history of the fundamental data hiding algorithms is examined concisely in this chapter. Here, we highlighted precisely the discussion of cryptography rather than explaining other related techniques of information concealing, as our research roughly depicts to image cryptography.

2.1 Data Concealing

For any system or any particular personage, information or data always holds a great significance. As people want their privacy when they are talking about their personal matters so that nobody can take advantage of that, it is also demanding to keep the confidential information of a system or organization protected from outer intruder and assures the incorruptibility and confidentiality. In order to exchange data from sender to recipient it is important to do it in a very unassailable approach, so that nobody can break the protection shield. Basically, between any kind of data transmissions there are two kinds of risks, those possibly can be occurred. In order to alter the message and switch the real context, the wiretapper can endeavor to listen in or else it can try to decrypt the message so that the decoded information can be used for its own benefit. The genuineness and secrecy of the interchanging data is breached by these invasions. In addition, it is a very tough job to grant admittance to destined consumer and bypass access of the remote user. The core idea of information hiding tactic originated from this erroneousness of the communication systems. As a consequence, the importance as well as the necessity of developing more stable and

riskless information hiding methodologies has grabbed the attention of the scientists. There are many prominent information concealing methods frequently used in this field. We can classify them by three types:

i. Watermarking;

ii. Steganography and

iii. Cryptography.

2.2 Watermarking

Watermarking is a technique to facilitate the proof of the genuineness where a transparent image or text is imposed into papers or images. If we try to find watermarking in remitted light, it can be identified as a discrete combination of light and dark shadows. Generally this method is used on security purposes such as in post-stamps, liquid money, confidential papers and passports. As a continuation of watermarking method, this new era of digitalization introduced us with a new technique, Digital Watermarking. Now-a-days where people are too much dependent on virtual world and hence there is huge number of information those are transporting via internet that bind us to keep the genuineness of the data. On the other hand, plagiarism is a very frequent phenomenon in this digital age whether it is an audio, video, text or image. Moreover, it is really not that much difficult to generate or spread. In these circumstances, it is especially necessary to identify the actual heir of the information. The long-established complications regarding the ownership of the digital information are being solved now by using this digital method. This is one special type of flag that is secretly planted to the transmittable digital information, for example, images, audio or video data. For the affirmation of the information this marking can be identified or removed later. The marker can be the clue of author, ownership information or can be an image too. This digital marker can stay unchanged even after any kinds of alteration of data which secures the proof of legitimacy of the digital data. Only after applying some algorithms this marking can be distinguished, otherwise it cannot be identified. A marker that is recognizable even after altering the transmitting data is useless. To make it futile to get rid of the marker without touching the original information is the main objective of this digital algorithm. This method is an uninvolved securing

mechanism. This method only signs the data instead of altering it or taking the authority of the data. Find out the origin of the data is one of the applications of this method. At the speck of transportation a water-marker is planted into the transmitted digital data. By chance, if someone makes an imitation of the actual water-marked data then the identified watermark can disclose the origin of that information. One of the widely used applications of this method is to identify the root of unjustly plagiarized movies and videos. It is also used by television broadcasting companies. When they broadcast any program or news usually they use a logo of their own identity, so that even if someone makes a copy of that program the logo will be copied along with that video identifying their ownership.

2.3 Steganography

The process of securing information by covering the data with another data is known as Steganography. The name itself bears the definition according to the Greek origin. By way of explanation, this is a scientific method of exchanging information that makes the transmission invisible to the outer world. The core idea is concealing the message within another simple-looking message that no one will doubt that there actually exists a message. The main target of this method is to make the protection level and scope more strong. The context of the actual message can be altered even if there is a tiny bit of modification in the hiding medium. Any kind of hypersensitive data on the open channel i.e., video, image or audio can be concealed by this technique. Steganography has 4 basic parts mentioned bellow:

1. A data hiding median to conceal the information.
2. A private data or message which is needed to be hidden.
3. An algorithm which is required to mask the message within hiding median and that method must be reversible.
4. An additional key-word or sign for authentication that means the striking item only which can make the message invisible or visible.

It is required to select the hiding median cautiously. Since the methodology of Steganography is to

alter the unnecessary data by private data, hence, the hiding medium has to hold enough inessential data.

2.4 Cryptography

According to the Greek origin, the word 'Cryptography' means 'secret writing'. In other words, it is a process where the secret message is altered into an unrecognizable state known as cipher-text that cannot be retrieved without the help of proper key. By the help of proper decrypting key finally the receiver can decode the cipher-text and get the original message.

Protecting personal data from illegal users and keeping them untouched from being used or being opened to the third party are the main focus of Cryptography. Hence, timestamps, encoding, hashing and digital signature are used in Cryptography for assuring the safety issue of the confidential data. In this digital era this is equivalent to encoding. Plaintext is the actual message which is needed to be encrypted and after encryption the resultant data which will be opened to the communication channel is called Cipher-text. Cryptography has 3 major parts:

A. Encryption: It is the process of altering the elementary message into some unrecognizable state. The resultant message digest from this step is called Cipher-text.

B. Cipher-text transmission: In this step, the encrypted cipher-text is sent to the receiver-end.

C. Decryption: This step decodes the cipher-text into its actual plaintext format for the recipient.

Cryptography can be classified by 2 categories:

i. Symmetric Key Cryptography

In Symmetric key cryptography, it uses only one key, that means here source and recipient uses same key to encrypt and decrypt. Some popular Symmetric key cryptographic techniques are- DES, AES, RC5 etc. Symmetric key cryptography contains 5 elements-plaintext, encoding algorithm, secret shared key, cipher-text and decoding algorithm. Using the secret shared key sender encrypts the plaintext with several processes. The secret shared key which is chosen by either sender or receiver is independent and not related to the plaintext. Cipher-text is made by this encryption process with the help of the shared key.

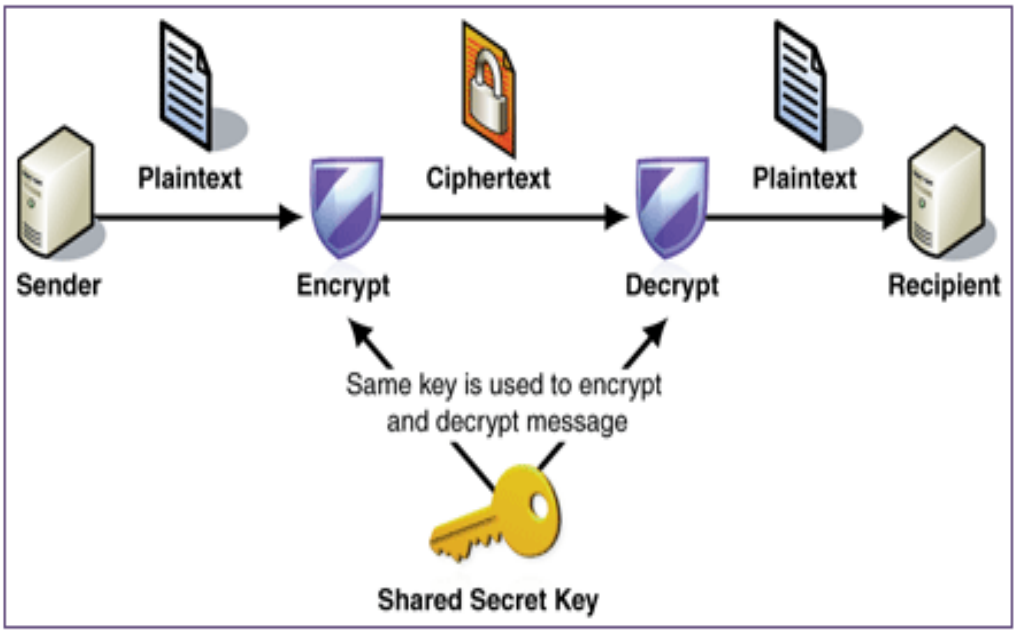


Figure 1. Schematic diagram of a Symmetric key encryption system.

The decryption process works with the received cipher-text and the secret shared key and returns the plaintext as resultant product. One major disadvantage of the symmetric key cryptography is to make the secret key shared for both connecting parties and in addition they need to share the key in a protected channel. A third party user carrying secret key's information can become a dangerous risk for the system.

ii. Asymmetric Key Cryptography

'Public key Cryptography' is another name of 'Asymmetric key Cryptography'. A couple of public key and secret key is used in this system. The private key is secret when on the other hand the coupled public key is opened to the communicating medium. To encrypt the plaintext this public key is required and after encryption the resultant cipher-text is sent to the recipient. The receiver then with the help of secret key decodes the cipher-text through decryption algorithm and finally can retrieve the original message. Digital signature algorithms also use this Asymmetric key cryptography. In digital signature, the system makes a signature and attaches that with the message permanently. For making this signature the secret key is used while on the other end public key is used to verify that signature.

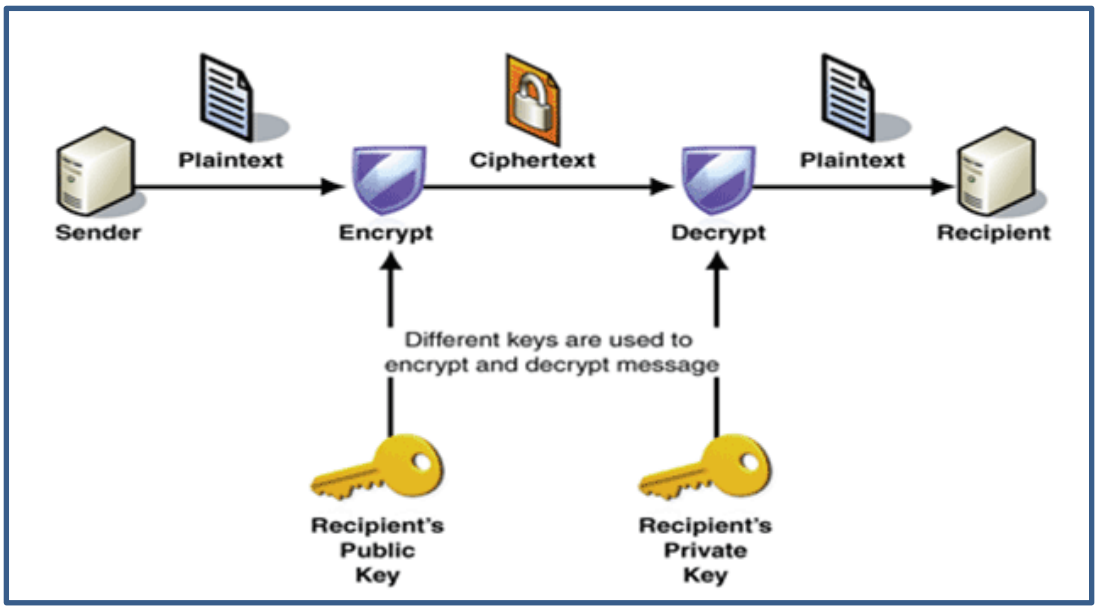


Figure 2. Schematic diagram of an Asymmetric key encryption system.

2.4.1 Objectives of Cryptographic Algorithms

The principle concepts of Cryptographic systems are - Secrecy, Integrity, Legitimacy and Non-Denial. Basically, Cryptosystems are the combination of these principles. A brief description of these principles is given below:

i. Secrecy or Confidentiality

One of the major features of data security is Secrecy or Confidentiality. It is required for every system to be well protected in case there is any kind of unexpected wicked attacks that may be threatening for the secrecy of the data. For instance, confidentiality of hypersensitive data is very important in military. According to cryptography, A service is known as Confidentiality when it ensures the security against the exposure of private data to an unauthorized user. It does mean that the data is only available to destined users instead of unauthorized one. The word 'privacy' is synonymous with secrecy and confidentiality. After using various algorithms whether it is physical or mathematical, the cryptographic system can finally attain Secrecy or confidentiality while making the data totally unrecognizable to the third party attackers.

ii. Integrity

The protocol which protects and ensures the efficiency and fullness of the information over its whole life-time is defined as Data Integrity in the field of data security. If transmitting data is being altered by an attacker during its way of transmission then this service can detect that change. A cryptographic encoding method should be capable of identifying changed data which is done by an attacker and the original data should not be replaced with the false data by a third party user, for ensuring information integrity. One of the basic and original cryptographic features for ensuring data integrity is Hash function.

iii. Legitimacy

The identification of valid sender or receiver of the data is ensured by ‘Legitimacy’. Legitimacy or Authentication verifies the transmitting users who demand themselves to be a valid user. Basically, this protocol focused on ensuring the authenticity of a transmission. Whether it’s an alarm or warning signal if that is a single piece of message then the authentication protocol ensures the receiver about the legitimacy of the demanding source. On the assumption of a progressing transmission, i.e. the interaction between a user-end and a host, it provides two features. On the beginning, when the system initializes the network, Authenticity service ensures about the authentic users by verifying their identity as sender and receiver. After that, to keep the transmission channel protected from unauthorized attackers so that they cannot hamper the transmission by impersonating as an owner, this protocol ensures the stability of the connection.

iv. Non-Denial

Non-Denial or Non-repudiation service gives assurance that it is impossible for the communicating authorized users to refuse the legitimacy of their sign on the communicating data which is created by them. Therefore, a recipient can be ensured and get the evidence of the legitimacy of message sender when it get the message. By the same way, when a sender sends a message and it is received by the receiver, the sender can get the information of the legitimate recipient and can be assured that the authorized receiver got the message.

2.4.2 Cryptanalysis and Cryptographic Risks

Investigating the data systems in pursuance of getting the concealed properties of the method is known as ‘Cryptanalysis’. Cryptographic attacks are designed in a way that they can destroy the protection shield of cryptographic methods and they can also try for decoding the cipher-data without even having a proper decryption key. These attacks are treated as a part of Cryptanalysis while having the mechanism of decrypting the encoded information. Cryptology is an art of science that combines Cryptography and Cryptanalysis. Different cryptographic risks are briefly discussed below:

i. Known Plaintext Attack

When a cryptanalyst get to know a plaintext and its respective cipher-text then he/she will try to find similarities between them, this attack is known as ‘Known Plaintext Attack’. Usually, they known a small portion of the plaintext using which they try to figure out other parts of the original message or encryption key and by this way they can retrieve the whole message. i.e. Stereotypical phrases: ‘Yours Sincerely’ or commonly used words like this etc.

ii. Cipher-text-Only Attack

Cipher-text-only attack is occurred when the attacker only knows the cipher-text but not the corresponding plaintext. For uncomplicated ciphers like Caesar Cipher, it is not that difficult for a cryptanalyst to break the cipher by using a frequency analysis method.

iii. Chosen Plaintext Attack

A Chosen Plaintext attack is happened when it is possible for an attacker to encode a randomly chosen plaintext and then analyze the resultant cipher-text. The main reason for attacking is to attain data that weakens the protection shield of the encoding algorithm. This attack is frequently used against Public key Cryptography as the attacker can access the public key.

iv. Chosen Cipher-text Attack

A Chosen Cipher-text attack is possible when a cryptanalyst selects a random cipher-text and try to find out an appropriate plaintext for that. By selecting a cipher-text and getting that's decrypted value using an unknown key, little by little the attacker collects the data. While attacking, an attacker can insert several selected cipher-texts inside the scheme and can achieve the derived plaintext. Masked decryption key can be attained by analyzing these decrypted plaintexts from the chosen cipher-texts.

v. Side Channel Attacks

The main goal of this attack is to get other partial data on the basis of physical involvements of cryptographic method along with the hardware which is used to encode or decode information. According to all the attacking protocols which are explained earlier, they are assumed to be worked with either plaintext or cipher-text and some can also have access over the cryptographic system. Like its name, a side channel attack influences supplementary data i.e. estimated time for calculations or CPU usage during calculations, used voltage etc.

vi. Brute Force Attacks

In a Brute Force attack an attacker literally try to use each and every possible key for decryption. Usually this attack is applied on a known plaintext or cipher-text-only attack. Hence, it requires sufficient memory capacity.

vii. Linear Cryptanalysis and Differential Cryptanalysis

Linear and Differential Cryptanalysis are two connected attacks where the combination is mainly utilized against repetitive symmetric key block ciphers. A repetitious cipher which is also known as a product cipher manages various rounds of encoding by using a sub-key for individual round. For instance, the Feistel Network is used in DES and AES used the state rounds. In this pair of attacks, the attacker observes any kinds of changes in the intermediate cipher-text between the rounds of

encoding. When the attacks are united then it is called Differential Linear cryptanalysis. One of the main goals of a robust encryption algorithm is to make the cipher-texts looks like arbitrary while a single alteration in the plaintext results in an arbitrary change in the resulting cipher-text. This type of quality is known as diffusion. Any kinds of altered cipher-text bit must contains 50% possibilities of become '1' or '0'. These two attacks want to find non-randomness in an attempt of disclosing hidden sub-keys.

(a). Linear Cryptanalysis

This is one kind of known plaintext attack where it is necessary for having access to huge number of plaintext and cipher-text couples which are encrypted by an unknown key. This attack concentrates on statistical analysis against one round of decoding on huge number of cipher-texts. For one round of encoding the attacker decodes each and every cipher-text by using all existing sub-keys and analyzes the output of intermediate cipher-text to find the minimum arbitrary result. A sub-key will become a candidate key where these sub-keys earlier produced the optimal arbitrary mid-level cipher for all cipher-texts.

(b). Differential Cryptanalysis

Differential cryptanalysis is one kind of Chosen Plaintext attack which works for disclosing the connection between the resultant cipher-texts created by two related plaintext. It works by analyzing the statistical data of two inputs and outputs which are used in a cryptographic system. One couple of plaintext is yielded from the application of a Boolean Exclusive OR (XOR) operation on a plaintext. For instance, XOR the iterative binary string 10000000 to the plaintext. Because of this a small difference is created between them which indicates the term Differential Cryptanalysis. After that the plaintext and its corresponding XORed couple are encrypted with the help of all the possible sub-keys by the cryptanalyst and a sign of non-arbitrariness in each intermediate cipher-text couple is searched by it. The sub-key finally becomes candidate key when it creates the minimum arbitrary pattern.

CHAPTER 3

OPTICAL CRYPTOGRAPHY

3.1 Double Random Phase Encoding (DRPE)

Double random phase encoding (DRPE) [29-36] is performing a very significant role in information security while acting as a core element of optical and digital data security system [26-33]. According to the concept of DRPE, the elementary image *I(x,y,z)*, which symbolizes the spatial coordinates with 3 channels-red, green and blue, is encrypted into static white noise data employing two arbitrary phase masks. Those two random phase masks used in DRPE are presented as $\exp(2\pi n(x,y,z))$ and $\exp(2\pi b(\mu,\nu,\omega))$ where $n(x,y,z)$ and $b(\mu,\nu,\omega)$ systematically dispersed over (0,1). However, these fields are analytically autonomous. Following formula shows the encrypting process of DRPE scheme [2] for 3D image:

$$I_c(x,y,z) = \Im^{-1}[\Im[I(x,y,z)\exp(j2\pi n(x,y,z))]\exp[j2\pi b(\mu,\nu,\omega)]] \quad (1)$$

In this equation, $\Im$ and $\Im^{-1}$ represent a two-dimensional Fourier Transform and an inverse Fourier Transform, correspondingly, where they encrypt three color channels individually. This following figure is representing the DRPE process in Fourier domain.

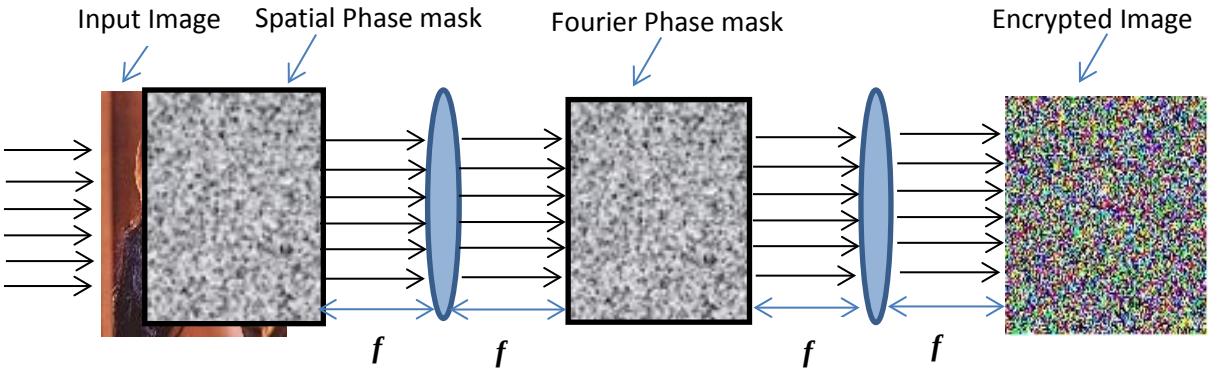


Figure 3: Schematic outline of the DRPE algorithm in Fourier domain (*f* is the focal length of the)

3.2 Poisson-Multinomial Distribution (PMD)

Poisson Multinomial Distributions (PMDs) are one of the most basic nonparametric multidimensional families of distributions. For example- they express the distribution of how many out of *n* thrown balls will fall into *k* bins, when the balls (perhaps because of weight or other characteristics) have different biases towards falling into the different bins. The distribution of counts emitted from single voxel is multinomial and therefore the distribution of counts from all voxels is the sum of multinomial distributions from individual voxels. The sum of such distributions is governed by the Poisson-multinomial distribution which from definition described the sum of non-identically distributed multinomial distributions. The Poisson-multinomial distribution is complex from the computational point of view and evaluation of likelihood based on this model is unpractical. The likelihood using PMD cannot be easily evaluated because it involves the sums of probabilities over the intersections of high-dimensional subsets and is not feasible from the computational point of view. Instead, for computational purposes we will use a simplified version where we find a relationship between Poisson distribution and Multinomial distribution. We follow with the formal specification of the Poisson-multinomial model in nuclear imaging.

3.3 Photon-Counting Imaging (PCI)

To identify the attribute of light, researchers are struggling with their heart and soul for decades. The Photon electric effect was detected for the first time when Heinrich Hertz did some examinations. The presence of photons was reported by Einstein, what indicates that for a given range, it is possible to present a physical limitation on the minimal light force for any kind of detected incident. If an indicator can identify every single photon then that can be known as Perfect Detector. A detector that can catch each and every photon can also calculate the highest probable Signal-to-Noise ratio. And being able to provide maximum SNR is the main characteristics of photon counting. In photon counting method at first it normalizes the image amplitude and then filters the normalized image by a high pass filter. At the end, the resultant filtered image will be multiplied by the number of expected photons. Finally, a photon-limited encoded image digest will

be produced by Poisson-random distribution. Image can be encrypted and also compressed through this method. On the other hand, if images are encrypted using PCI, then it will be impossible to retrieve the original image as this is a compression process.

3.4 Poisson-Multinomial Distribution (PMD) based Photon-Counting Imaging (PCI)

As a significant factor of optical imaging approaches, Photon-counting imaging technique has been prosperously adapted in areas for instance – 3-dimentional imaging and 2-dimentional or 3-dimentional object sensibility in photon-starved environment [37-40] or night view, conditions in which image sensors can catch only a restricted number of photons [37-40]. Simply, photon-counting imaging is a system that controls the number of photons landing at a pixel in an image. If we pass alone a short amount of event photons to the seized picture area then we can obtain photon counting imaging which is multispectral. As a consequence, this monochromatic imaging scheme accommodates the hypothesis that the liability of estimating photons at each random pixel in a taken image pursues a Poisson distribution [11,37-40]. Moreover, depending on the coherent state of light, the photons may follow a binomial, negative binomial, multinomial distribution, or negative multinomial distribution. Nevertheless, since the Poisson distribution acts like a bounding case of Binomial distribution while the number of trials gets very large and the probability of success is very low, hence all alone the previous researches [1], they broke the 3D images (RGB color images) into 2D images (Bayer images with separated 3 channels) to make it monochromatic so that it is possible to apply binomially distributed Poisson distribution based photon counting imaging technique. Because of that they had to use demosaicing algorithm to combine those 3 channels after applying photon counting imaging technique on each channel separately. In this paper we focused on the 3D image characteristics. As a color image has three types of colors per pixel, thus we are using multinomial distributional statistics for Poisson distribution which is known as Poisson-Multinomial distribution. Here, this PMD distribution works on 3 color channels simultaneously. Henceforth, this Poisson-multinomial distribution following photon-counting imaging technique is not monochromatic but polychromatic. As a result, we don’t need to apply any

demosaicing algorithm to combine the channels since the PMD based Photon-Counting technique is doing all the calculations synchronously.

Practically it's very hard to evaluate Poisson-Multinomial Distribution, thus for computing we used a simplified multinomial distribution for Poisson, while finding a relationship between Multinomial distribution and Poisson distribution. At first we calculated the Poisson-multinomial mean, λ of three colors on each pixel and then using those mean values we calculated the multinomial distribution of that pixel. In this way we evaluated the Poisson-multinomial distributed photon-counted 3D image. The probability of counting $n_c(x,y,z)$ number of photons in a random pixel (x,y,z) for a specific color on the 3D color image can be calculated by this following Poisson-Multinomial distribution equation :

$$\begin{aligned} &Poisson-Multinomial\left(\lambda_c(x,y,z)\middle|N_p=n_r+n_g+n_b\right) \\ &=\left[\frac{N_p!}{n_r(x,y,z)!\times n_g(x,y,z)!\times n_b(x,y,z)!}\right]\times\left({\lambda_r}^{n_r}(x,y,z)\times{\lambda_g}^{n_g}(x,y,z)\times{\lambda_b}^{n_b}(x,y,z)\right) \end{aligned} \tag{2}$$

here, N_p represents the total number of photons in a pixel on the color image and for c=3 categories (red, green, and blue) and N_p number of photons per pixel we can calculate the Poisson-multinomial mean, $\lambda_c(x,y,z)$ for each color of a random pixel by using following formula [41]:

$$\lambda_c(x,y,z)=\sum_{i=1}^{Np}p_{ci}(x,y,z) \tag{3}$$

where, $P_{ci}(x,y,z)$ represents the probability of the ith photon which is captured under 'c' color category. After calculating the mean, we can evaluate the resultant photon-counted image by following function:

$$C_{PCI}(x,y,z)=mnrnd\left(N_P,\lambda_c(x,y,z)\right) \tag{4}$$

here, *mnrnd(.)* is a function to generate random numbers from the multinomial distribution with the parameter $\lambda_c(x,y,z)$ and N_P. Finally we can get the photon-counted 3D image with this method. By using this formula we can control the number of photon and it is possible to authenticate the image under a very low light level.

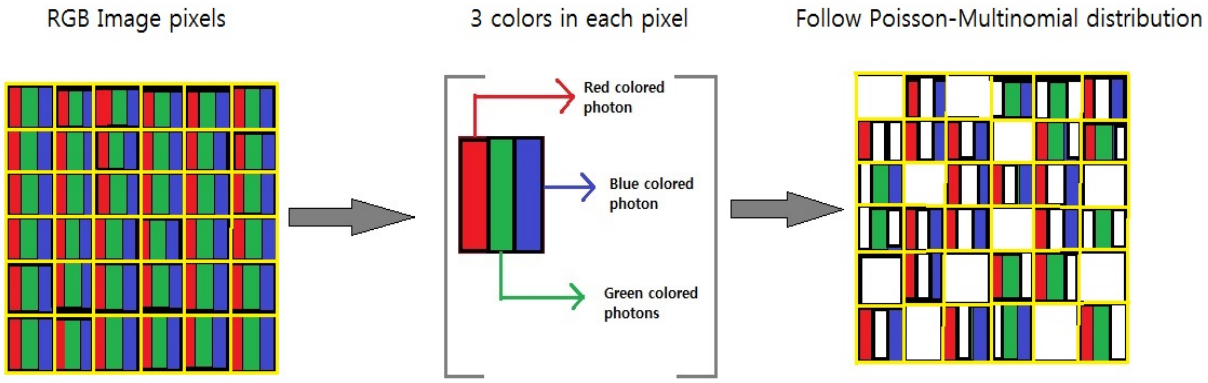


Figure 4: Schematic diagram of Poisson-Multinomial distribution based Photon-Counting method.

3.5 Optimization

After applying the photon counted imaging technique followed by a double random phase encoding scheme, the resultant image digest will be optimized by a multinomial probability density function. This function works with the number of different colored photons and the probabilities of them existing on the image pixels. This function calculates and gives a probability of finding a value in a specific interval that means in a given range what is the probability of an event to happen. Probability density function, in other words, the density of the distribution that indicates the relative likelihood for a random distribution to take on a given value.

The probability density function equation for multinomial distribution is defined as follows:

$$PDF\left(n_1, n_2, \ldots, n_k \middle| \lambda_1, \lambda_2, \ldots, \lambda_k\right) = \left(\sum_{i=1}^{k} n_i\right)! \times \prod_{i=1}^{k} \frac{\lambda_i^{n_i}}{n_i!}$$

$$= \left(n_r + n_g + n_b\right)! \times \left(\frac{\lambda_r^{n_r}}{n_r!} \times \frac{\lambda_g^{n_g}}{n_g!} \times \frac{\lambda_b^{n_b}}{n_b!}\right) \quad (5)$$

where, 'n_i' denote the multinomial distributed photon numbers for specific colored photons on a pixel that will sum to the total number of photons per pixel and 'λ_i' indicate the probabilities to find respective colored photons on the image pixel which will be sum to 1. The probabilities for one pixel should all be in the interval (0,1).

Finally an optimized output will be generated by using following function:

$$C_{pdf}(x,y) = mnpdf\left(C_{PCI}(x,y,z), \lambda_c(x,y,z)\right) \quad (6)$$

here, *mnpdf(.)* is a function that generates the probability density function for multinomial distribution of the photon-counted image. It works with $C_{pdf}(x,y,z)$ which is the photon counted image and the mean 'λ_c' to evaluate the density. The resultant output will be two-dimensional digest. The Poisson-multinomial distribution based PCI method itself is a compression method and using that algorithm the encrypted image can be compressed up to 66.67% but the resultant image size will be same. However, by adding the explained Probability density function after PCI, the size of the resultant final image cipher can be minimized till 66.67% (according to 'lena.jpg' image experiment results).

3.6 Proposed Methodology

Since DRPE itself is unsafe to chosen-cipher text and chosen-plaintext attacks [9,10], hence in the previous works [11,12] they combined the DRPE scheme with Poisson distribution based PCI method and made it stronger against any kind of outside attack. Later the method was upgraded for color images by separating three channels of that down-sampled Bayer image and applying the integrated method on each channel consequently [1]. In this study, that recent work [1] has been extended by finding a technique for applying the whole integration process on the 3D image unlike separating the channels. On the following part the proposed combined process is being explained.

At first the original 3D color image, $I(x,y,z)$ is encrypted with two random phase masks, where one is in spatial domain and another is in Fourier domain. These phase masks encrypt the color channels individually. After encryption a 3D cipher image, $I_c(x,y,z)$ will be found which is a distribution of stationary white noise that exactly looks like Figure-4(DRPE encrypted image part), visually unrecognizable. The encrypted image contains phase value and amplitude value on each pixel. In the previous work they kept the phase information untouched because they wanted to decrypt the image [1]. However, in this work we are not going to decrypt the photon-counted encrypted image. We will apply Poisson-Multinomial distribution based photon-counting imaging technique on the

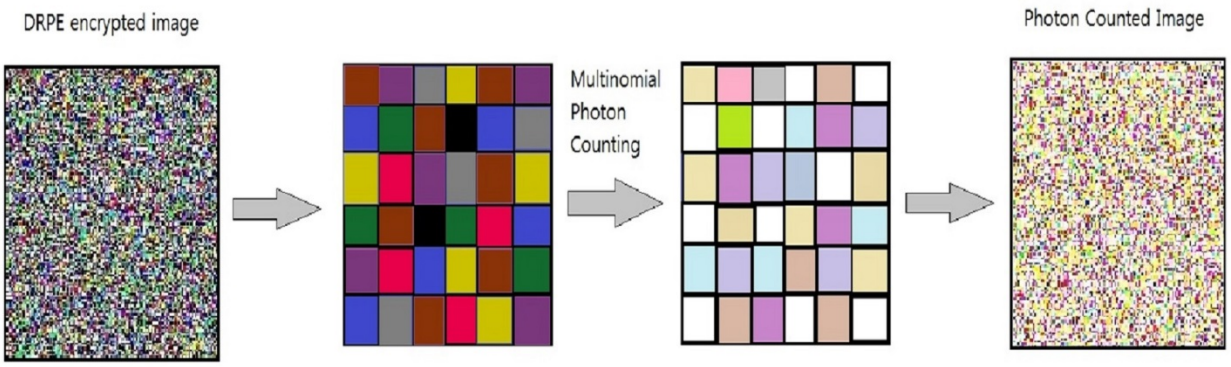


Figure 5: Illustration of DRPE to Multinomial-PCI

amplitude part of the DRPE encrypted output image. After applying PCI method we will get an image, $C_{PCI}(x,y,z)$ which size is as same as the input image (Figure -5, After applying PMD based PCI part), even though this image is already compressed. Hence, to optimize the encrypted image so that we can get a smaller output, we used a probability density function, *mnpdf(.)*, which is a Matlab built-in function that works with the Poisson-multinomial distributed photon numbers and their corresponding mean (λ) of the output image. The final output is a 2D image which will be transmitted.

On the receiver end, for authentication, at first the reference image is gone through in the same process like original image. Afterwards, the original image output and reference image output are compared by a statistical method, non-linear cross correlation for checking legitimacy. A schematic presentation of the proposed method is shown in Figure-6.

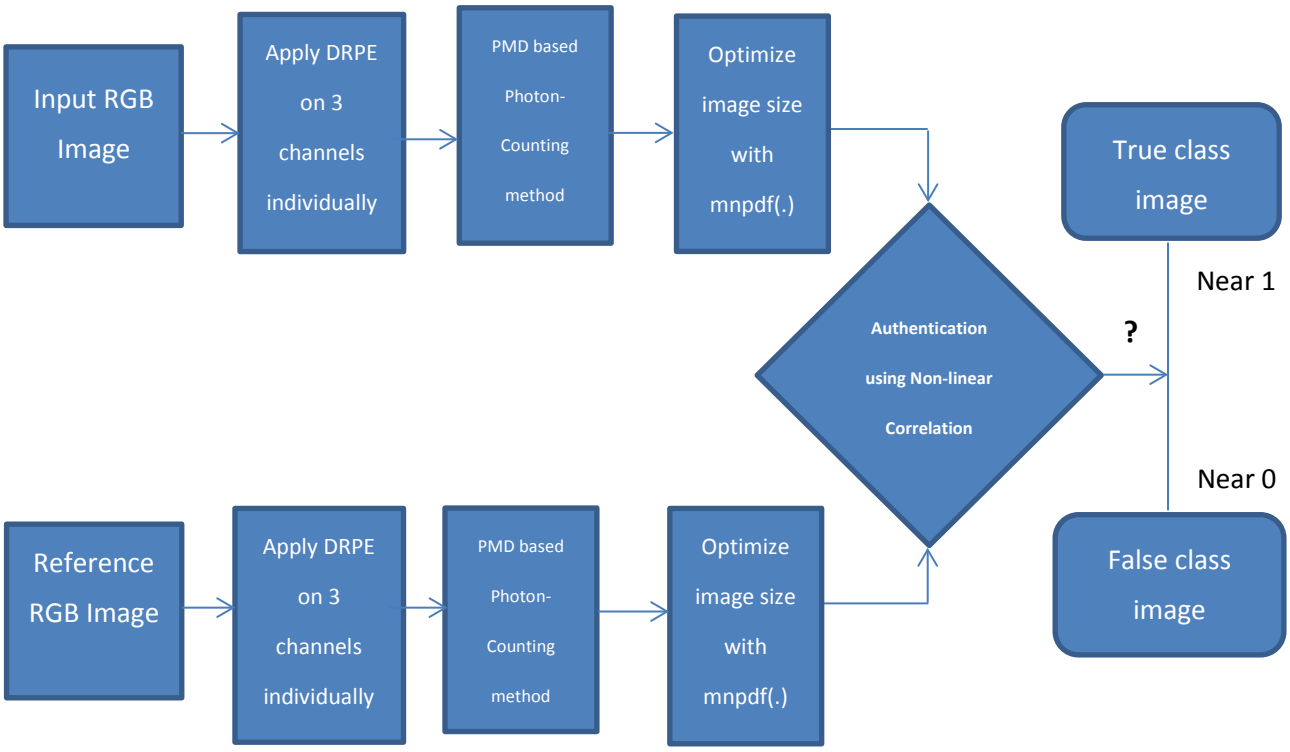


Figure 6: Work-flow diagram of the proposed method.

If the non-linear cross correlation result shows an output which is near to 1 then that does mean that the comparing images are same, hence, the reference image is a true class image. On the other hand, if the comparing results give a value which is tense to 0(zero), then that means the comparing image is a non-authorized false class image. By using the proposed method a suitable value is obtained, that is almost 1 when an authorized image is used as a reference image. On the contrary, when a non-authorized false class image is used as a reference image to authenticate the received image, then the proposed method gave an output which is very small, near to 0.

On the next chapter the results and simulation outcomes will be discussed in details.

CHAPTER 4

SIMULATION OUTCOMES & RESOLUTIONS

This chapter is consisted of two main sections. One is the familiarization of the fundamental simulation parameters for image authentication and the second section is for numerical result analysis of digital color image authentication based on a new method where the image is encrypted by double random phase encoding scheme and then photon counted by a multinomial method based on Poisson-multinomial distribution technique.

4.1 Image Authentication Using Non-Linear Cross-Correlation

All the outcomes presented in this study are achieved from numerical analysis using virtual optics on Matlab R2013a. The simulations are executed on a computer which is operated by a 64-bits Windows 7 operating system where it has an Intel Core i5 processor of 3.07GHz with a RAM of 4 GB. The images which are used on this process are having the size of 128. For the experiments, stored images are used here instead of optical settings, since this method is proposed for digital image specially. However, as this system is not decrypting the image cipher and also because of the PCI in photon-limited situation, the image won't be visually recognizable, hence it is required to use a statistical method to authenticate the image. As showed in this work, a Non-linear Cross-Correlation [11,12,17,18] technique is used to compare the encrypted original image and the encrypted reference image. The equation given bellow is presenting the calculation of non-linear cross-correlation between two encrypted images those are being compared:

$$nlcc(a,b) = \Im^{-1}\left\{O(x,y)R(x,y)\right|^{k} \exp\left[i\left(\phi_O(x,y) - \phi_R(x,y)\right)\right]\Big\} \qquad (7)$$

here, $O(x,y)$ and $R(x,y)$ are 2D Fourier transform of the encrypted original image and encrypted reference images respectively. On the other hand, $\phi_O(x,y)$ and $\phi_R(x,y)$ are the phase value of the previously mentioned images. The '*k*' mentioned in the equation defines the power of non-linearity.

The cross-correlation value will be changed if we change this *k* value. For example, if value of *k* is 0 then this equation will act like a phase extractor which will give a high frequency value and if k is 1 then the equation will act like a linear filter [11,12]. In order to find a perfect value of '*k*' it is necessary to evaluate the highest Peak-to-Correlation Energy (PCE) by using the equation [11,12] given bellow :

$$PCE = \frac{\max\left[\left|nlcc(a,b)\right|^2\right]}{\sum_{i=1}^{X}\sum_{j=1}^{Y}\left|nlcc\left(a_i,b_j\right)^2\right|} \tag{8}$$

The non-linear cross-correlation between the encrypted outputs of original image and reference image are presented in this equation as $nlcc\left(a_i,b_j\right)$ and *X* and *Y* are indicating the rows and columns of the *2D* outputs in *x* and *y* axes, correspondingly. According to the above equation, 'Pick-to-Correlation Energy' means the proportion between maximum intensity value for non-linear cross-correlation result of the comparing images and the summation of the intensity energy of all the correlation values. Hence, for a good non-linear cross-correlation result we will find a higher PCE value [1].

4.2 Numerical Result Analysis

As we can see in Figure-7, for various values of *k*, PCE value changes in different number of photons. Here, different colors indicates the changed values of *k* and *x* axis shows the change of photon number. On the other hand, *Y* axis is showing the final results in changing PCE values. It is noted that, the PCE value increased when we increased the number of photons. By analyzing this above graph we can easily pick the appropriate value for *k*. According to the graph, it's clear that when *k=0* we can get highest PCE value which is almost 1(for Lena image). Therefore, in this paper, in order to do all the calculations we used 0 (zero) as the value of *k*. Moreover, it is also noticed that, when the number of photon is 10^5 then we can get the highest PCE value which is 1. On this basis, we can say that, when *k=0* and number of photon is 10^5 then we can perfectly authenticate the original image.

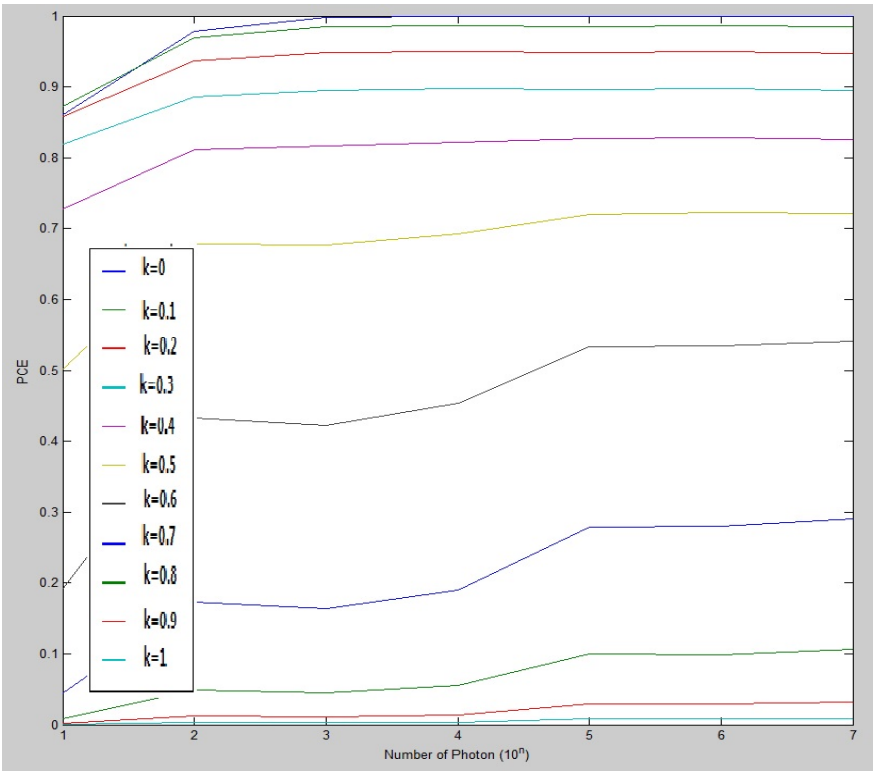


Figure-7: PCE values for different values of 'k' using true class image. (Lena 3D-image)

For those experiments we did in this project, we used one standard 3D RGB color image (Lena image) taken from Kodak true color image data sets (Figure-8). The dimension of the image is $128 \times 128 \times 3$. We used this image as original image and reference true class image for authentication process of the proposed system.

Figure-8: true class 3D RGB color image. (Lena image)

The original image is encrypted with double random phase encoding technique and then the amplitude part of the encrypted image is photon counted by a process where by using a Poisson-multinomial distribution method we can control the number of photon on three channels equally without separating them like previous work. The photon counting encrypted 3D output image is then compressed to 2D image by using a probability density function while calculating there number of photons per pixel. To authenticate the legitimacy of the true image at first we will encrypt the reference image with the same process and then since the images are visually unrecognizable thus we used a statistical comparing method named non-linear cross-correlation.

Table 1: Maximum Correlation results for different number of photons per pixel for a true class image (Lena image)

Number of Photons per pixel	Maximum Correlation Value
10	0.9351
10^2	0.9923
10^3	0.9991
10^4	0.9999
10^5	1

For Photon-counting imaging we used 10^5 numbers of photons to get standard result. However, we can still authenticate the image even if we take only 10 photons per pixel (according to Table-1). Figure-5 shows the visually unrecognizable encrypted Image, which is encrypted by the proposed method. After encrypting the reference true class image with the same technique and comparing these two encrypted images with non-linear cross correlation for authentication, proposed system gives the above results showing in Table-1. Following graph is a visual representation of the outputs:

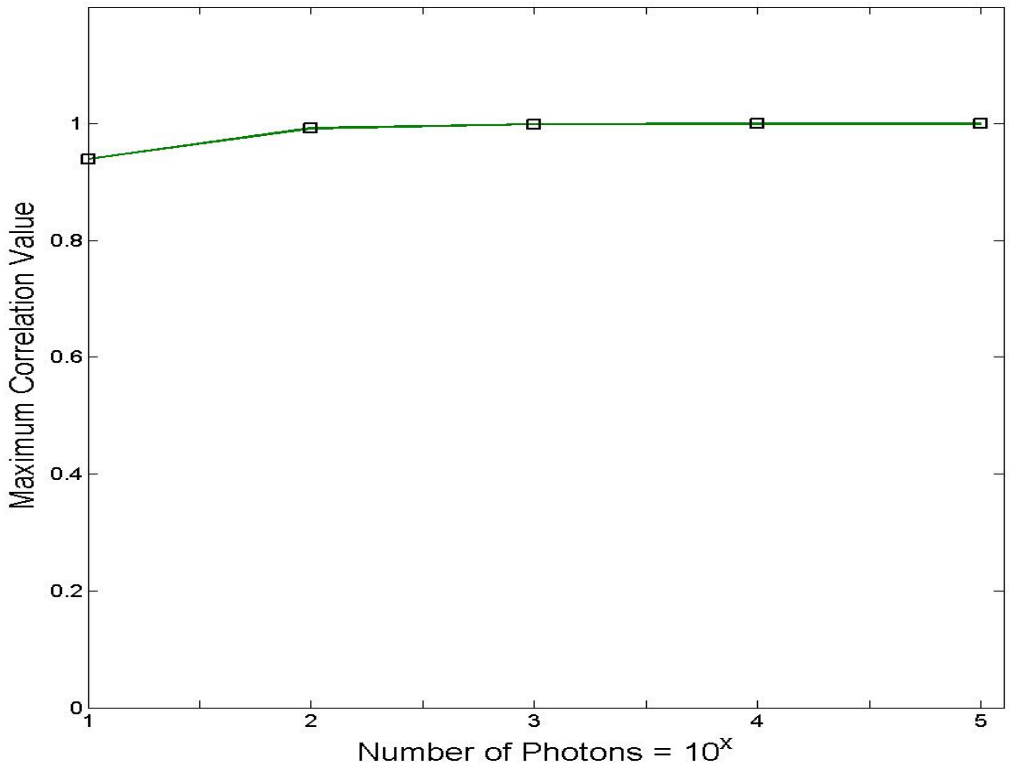


Figure-9: Maximum cross-correlation between original and true class encrypted images (Lena image) for different number of photons.(k=0)

If we notice Figure-9 we can see that for true class reference image, this system is giving a high value which is nearly 1. The graph is showing different values for changed number of photons per pixel. The raising values of cross-correlation between two comparing encrypted images are showed in *y* direction in response to the increasing number of photons per pixel showed in *x* direction.

After observing the above graph in Figure-9, we can clearly understand that even in a very low-light level we can still authenticate the image easily and when the number of photon is 10^5 then it gives the highest value 1. We did this calculation by using the '*k*' value as 0.

Figure-10: Unauthorized false class 3D RGB color image. (Mona_Lisa.jpg)

Moreover, in order to prove the efficiency the proposed authentication system we did another experiment on a false class image. There we encrypted an unauthorized false class image (which is different from the original image) with our presented method and applied the non-linear cross-correlation statistical method to compare both encrypted images. Figure-10 is showing the unauthorized image which we used in this experiment as a false class image. This has the same dimension and properties like original image but the image is different as we can see here. We used different image in order to see whether the system can differentiate the dissimilarity between them or not.

Table 2: Maximum Correlation results for different number of photons per pixel for a false class image (Mona_Lisa image)	
Number of Photons per pixel	**Maximum Correlation Value**
10	0.0783
10^2	0.0822
10^3	0.0818
10^4	0.0654
10^5	0.0556

According to the above Table, maximum values of non-linear cross correlation between original image and the false class unauthorized image are showing. For a better visual view these results are plotted on the following graph:

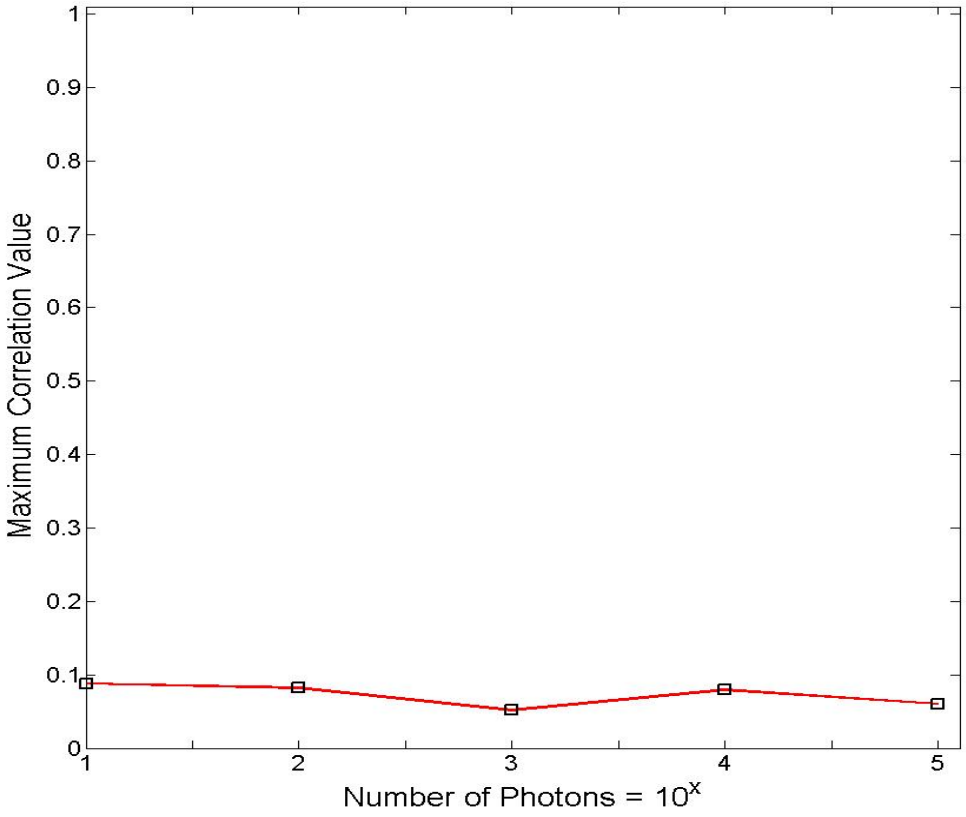
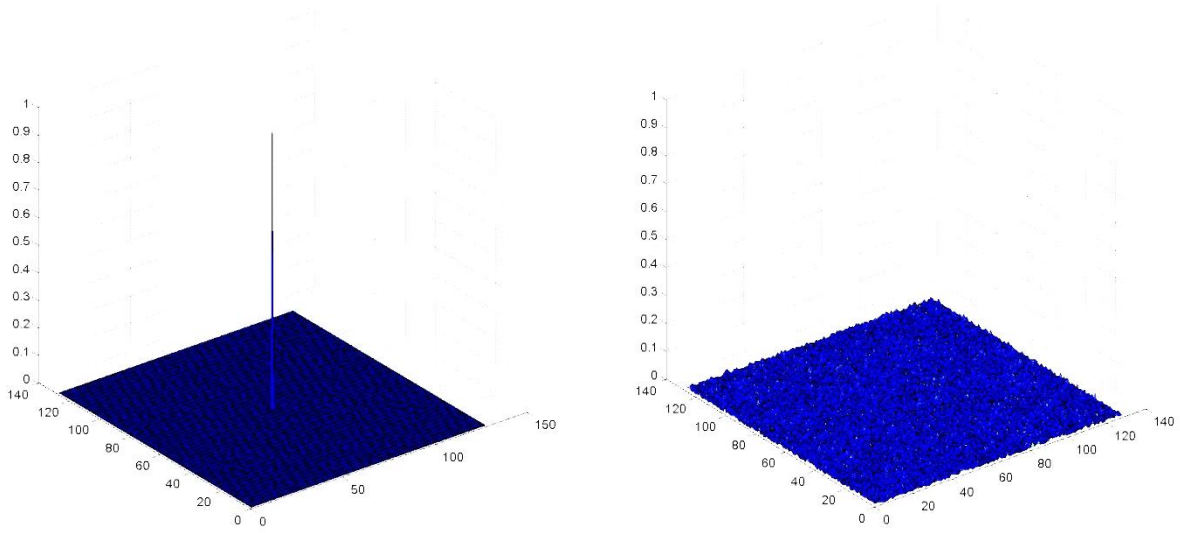


Figure-11: Maximum cross-correlation between original and false class encrypted images (Mona_Lisa.jpg) for different number of photons.(k=0)

According to this graph, the values are very small even though we increased the number of photons per pixel. The values are too small that they can be considered as zero. It is noted that, even if the number of photons are too small still we can appropriately identify that the comparing images are not same. The huge difference between figure-9 and figure-11 declares that our proposed method can successfully authenticate a color image with minimum number of photons in a photon-limited environment. For a better visual view, in Figure-12 we have shown the plane graph of the simulation results for authorized and unauthorized images. Here, it is clear that for true class image the plan gives a high pick (in figure-12(a)), while on the other hand for false class image the plan is not showing any pick (in figure-12(b)).



(a) (b)

Figure-12: (a) Non-linear correlation plan between encrypted reference and true class images; (b) Non-linear correlation plan between encrypted reference and false class images.

After inspecting all these simulations, it is evidently clear that this system can efficiently authenticate digital color image in a very simple and direct way, without being separated or combined their color channels as it adopts a multinomial distribution. Moreover, we did all the experiments while encrypting the images with same keys since contrarily it cannot show the expected result and on the consequence we cannot authenticate the image. Hence, it proves that this proposed system cannot authenticate successfully if we do not use the same keys for encryption.

These experiments demonstrate that the protection offered by this new method can make DRPE stronger while confronting brute-force attacks.

CHAPTER 5

CONCLUSION

From the past researches, scientists have created many methods to ensure the security of the information which are transmitted through insecure open channels. Since three dimensional color images has three color channels and it was necessary to calculate each channels, therefore the system had to encrypt each of the channels individually. However, it made the system taking more time and using additional algorithm along with the process for calculation. The main purpose of this research was to reduce the complexity and find a simplified way to do all the calculation for those three channels at the same time rather than separating them. Here, in this study, we have introduced a new distribution scheme for photon-counting imaging technique. As we all know that photons only follow Poisson distribution and since here we need to work with multi-dimensional imaging system that is why this method is really useful for this integration of DRPE and Photon-counting Imaging. The Poisson-Multinomial Distribution (PMD) based Photon-Counting Imaging (PCI) scheme which has been introduced in this paper, is applied for the first time on digital color images and in addition it is showing a good simulation results. Moreover, it is giving an extra security to DRPE for increasing robustness against third party attacks. The experiments results also indicates that this proposed system can authenticate a color image in a very low-light level, even if the number of photon is very small. In addition, we can attain a very high reduction of bandwidth of the output image where the compression percentage is really high. However, this method is mathematically proven to be a good one for digital images by using Matlab simulations, but for practical application it is not feasible. Since every pixel of a color image contains three types of photon hence, it is hard to detect the specific color for the detector.

BIBLIOGRAPHY

[1] Yi. Faliu, I. Moon and L. Yeon, “A Multispectral Photon-Counting Double Random Phase Encoding Scheme for Image Authentication,” Sensors, Vol. 14(5), PP. 8877-8894, 2014.

[2] P. Réfrégier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett., Vol. 20, PP. 767–769, 1995.

[3] Z. Liu, S. Li, W. Liu, Y. Wang and S. Liu, “Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding,” Opt. Laser Eng., Vol. 51, PP. 8–14, 2013.

[4] Y. Zhang, B. Wang and Z. Dong, “Enhancement of image hiding by exchanging two phase masks,” J. Opt. A Pure Appl. Opt., Vol. 11, PP. 125406, 2009.

[5] C. Yao-yao, Z. Xin, X. Yong-liang, Y. Sheng and W. Xiu-ling, “An improved watermarking method based on double random phase encoding technique,” Opt. Laser Technol., Vol. 42, PP. 617–623, 2010.

[6] Y. Sheng, Z. Xin, M. Alam, L. Xi and X. Li, “Information hiding based on double random-phase encoding and public-key cryptography,” Opt. Express, Vol. 17, PP. 3270–3284, 2009.

[7] B. Javidi, A. Sergent, G. Zhang and L. Guibert, “Fault tolerance properties of a double phase encoding encryption technique,” Opt. Eng., Vol. 36, PP. 992–998, 1997.

[8] D. Monaghan, U. Gopinathan, G. Situ, T. Naughton and J. Sheridan, “Statistical investigation of the double random phase encoding technique,” JOSA A, Vol. 26, PP. 2033–2042, 2009.

[9] Y. Frauel, A. Castro, T.J. Naughton and B. Javidi, “Resistance of the double random phase encryption against various attacks,” Opt. Express, Vol. 15, PP. 10253–10265, 2007.

[10] A. Carnicer, M. Montes-Usategui, S. Arcos and I. Juvells, “Vulnerability to chosen-cypher text attacks of optical encryption schemes based on double random phase keys,” Opt. Lett., Vol. 30, PP. 1644–1646, 2005.

[11] E. Pérez-Cabré, H. Abril, M. Millán and B. Javidi, “Photon-counting double-random-phase encoding for secure image verification and retrieval,” J. Opt., Vol. 14, PP. 094001, 2012.

[12] E. Pérez-Cabré, M. Cho and B. Javidi, “Information authentication using photon-counting double-random-phase encrypted images,” Opt. Lett., Vol. 36, PP. 22–24, 2011.

[13] S. Liu, C. Guo and J.T. Sheridan, “A review of optical image encryption techniques,” Opt. Laser Technol., Vol. 57, PP. 327–342, 2014.

[14] M.S. Millán García-varela and E. Pérez-Cabré, “Optical data encryption. In Optical and Digital Image Processing: Fundamentals and Applications,” John Wiley & Sons: New York, NY, USA, PP. 739–767, 2011. Sensors, Vol. 14, PP. 8893, 2014.

[15] A. Alfalou and C. Brosseau, “Optical image compression and encryption methods,”Adv. Opt. Photon, Vol. 1, PP. 589–636, 2009.

[16] G. Situ and J. Zhang, “Double random-phase encoding in the Fresnel domain,” Opt. Lett., Vol. 29, PP. 1584–1586, 2004.

[17] B. Javidi, “Nonlinear joint power spectrum based optical correlation,”Appl. Opt., Vol. 28, PP. 2358–2367, 1989.

[18] M. Cho and B. Javidi, “Three-dimensional photon counting double-random-phase encryption,”Opt. Lett., Vol. 38, PP. 3198–3201, 2013.

[19] D. Mendlovic, P. Garcia-Martinez, J. Garcia and C. Ferreira, “Color encoding for polychromatic single-channel optical pattern recognition,” Appl. Opt., Vol. 34, PP. 7538–7543, 1995.

[20] Y. Hou, “Visual cryptography for color images,” Pattern Recognit., Vol. 36, PP. 1619–1629, 2003.

[21] M. Joshi, Chandrashakher and K. Singh, “Color image encryption and decryption using fractional Fourier transform,” Opt. Commun., Vol. 279, PP. 35–42, 2007.

[22] N. Zhou, Y. Wang, L. Gong, H. He and J. Wu, “Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform,” Opt. Commun., Vol. 284, PP. 2789–2796, 2011.

[23] M.R. Abuturab, “Color information cryptosystem based on optical superposition principle and phase-truncated gyrator transform,” Appl. Opt., Vol. 51, PP. 7994–8002, 2012.

[24] M.R. Abuturab, “Color image security system using double random-structured phase encoding in gyrator transform domain,” Appl. Opt., Vol. 51, PP. 3006–3016, 2012.

[25] I. Moon, I. Muniraj and B. Javidi, “3D Visualization at Low Light Levels Using Multispectral Photon Counting Integral Imaging,” J. Disp. Technol., Vol. 9, PP. 51–55, 2013.

[26] H. Malvar, L. He and R. Cutler, “High-quality linear interpolation for demosaicing of Bayer-patterned color images,” IEEE Int. Conf. Acoust. Speech Signal Proc., Vol. 3, PP. 485–488, 2004.

[27] R. Ramanath, W. Snyder, G. Bilbro and W. Sander, “Demosaicing methods for Bayer color arrays,” J. Electron. Imaging, Vol. 11, PP. 306–315, 2002.

[28] B. Gunturk, J. Glotzbach, Y. Altunbasak, R. Schafer and R. Mersereau, “Demosaicing: Color filter array interpolation,” IEEE Signal Proc. Mag., Vol. 22, PP. 44–54, 2005.

[29] P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce and J. Lancis, “Optical encryption based on computational ghost imaging,” Opt. Lett., Vol. 35, PP. 2391–2393, 2010.

[30] X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura and K. Kuroda, “Secure Optical Memory System with Polarization Encryption,” Appl. Opt., Vol. 40, PP. 2310–2315, 2001.

[31] J. Sang, S. Ling and M. Alam, “Efficient Text Encryption and Hiding with Double-Random Phase-Encoding,” Sensors, Vol. 12, PP. 13441–13457, 2012.

[32] W. Chen and X. Chen, “Space-based optical image encryption,” Opt. Express, Vol. 18, PP. 27095–27104, 2010.

[33] O. Matoba and B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” Opt. Lett., Vol. 24, PP. 762–764, 1999.

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

[35] H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi and N. Ohyama, “Known plaintext attack on double-random-phase encoding using fingerprint as key and a method for avoiding the attack,” Opt. Express, 18, 13772–13781, 2010. Sensors, Vol. 14, PP. 8894, 2014.

[36] H. Suzuki, M. Yamaguchi, M. Yachida, N. Ohyama, H. Tashima and T. Obi, “Experimental evaluation of fingerprint verification system based on double-random-phase encoding,” Opt. Express, Vol. 14, PP. 1755–1766, 2006.

[37] I. Moon and B. Javidi, “Three-dimensional recognition of photon-starved events using computational integral imaging and statistical sampling,” Opt. Lett., Vol. 34, PP. 731–733, 2009.

[38] B. Tavakoli, B. Javidi and E. Watson, “Three dimensional visualization by photon counting computational integral imaging,” Opt. Express, Vol. 16, PP. 4426–4436, 2008.

[39] Y. Hayasaki, Y. Matsuba, A. Nagaoka, H. Yamamoto and N. Nishida, “Hiding an Image with a Light-Scattering Medium and Use of a Contrast-Discrimination Method for Readout,” Appl. Opt., Vol. 43, PP. 1552–1558, 2004.

[40] I. Moon and B. Javidi, “Three dimensional imaging and recognition using truncated photon counting model and parametric maximum likelihood estimator,” Opt. Express, Vol. 17, PP. 15709–15715, 2009.

[41] John G Webster, E Russell Ritenour, Slavik Tabakov and Kwan-Hoong Ng, “Statistical Computing in Nuclear Imaging; Series in Medical Physics and Biomedical Engineering,” Cap.-3 :Counting statistics.

ACKNOWLEDGEMENTS

The time between my Master's degree studies, it was the valuable support of everyone that helped me to go through all the difficulties and I am greatly thankful to them. Because of them I have got countless moments those are deserved to be held in my heart as a precious one for the rest of my life.

I sincerely want to express my gratitude to my honorable advisor Professor Inkyu Moon. As a mentor he is an outstanding person who guides his scholars with persistence and dedication. I could finally complete my thesis work only because of his persistent and advisory guidance. First and foremost, it is his believe over me that build up my confidence and lead me to work more passionately. As my well-wisher, he also thinks about my prospective and instructs me to do accordingly for my betterment.

I am also immensely thankful to my parents, Md. Abdul Hye Khan and Laila Arjuman, and My siblings, Md. Tofayel Ahmed, Latifa Yeasmin Happy and Md. Liaqat Hossain, who are the greatest persons in my heart. It is their unconditional love and support that always inspire my life. I also want to give thanks to my best friend Nadera Sultana Tany, who has shared countless hours of laughter and joy with me even though she was not together with me here in Korea. I am greatly indebted to all the professors of Chosun University who once offered me worthy courses and gave their valuable advice during my study period. They are , Prof. Moon Inkyu, Prof. Lee Sang Woong, Prof. Kwon Gu Rak, Prof. Kim Young Sik, Prof. Cho Beom joon and Prof. Jhong Il Young. I also want to give thanks to my colleagues who made my experience a significant and memorable one. My colleagues are- 정유선 언니 , Yi Faliu 오빠, Keyvan 오빠, Samaneh 언니, 김환, Ijaz Ahmad, Ezat, Nishat Sultana and Tabassum Nasrin Haque. Senior colleague Keyvan 오빠 is like my brother and helped me every time I face a problem. Their support really helped me during this time being.

I also want to thank my friends, who are a great support for me in Korea, Sanjay Basukala, Shajeel Ikbal, Adnan Hashmi, Thien Than, Lynn, Sarwar, Md. Saifur Rahman, Hur Madina Mina, Lavanya,

Ahlam Mallak, Maron, Sadiq Reza and Farahida Omar who comforted me in every single step of my thesis writing by giving me mental support. They inspired me to win over any kind of complications and hardships. Because of my friends I got to know more about Korea. Thanks to my friends that in this two years I have gathered numerous joyful memories to preserve for the lifetime. My delighted time with them in Korea is unforgettable.

Besides, I really want to express my gratitude to one person, my undergraduate mentor, Professor Md. Zafar Ikbal. He is the one who showed me the way to explore the world of knowledge and it is because of his inspiration that I am here today.

Finally, I must say that, everything happens for a good reason and Allah always has better plan for us. I have my belief on him and I am following his guidance accordingly. In a word, wholeheartedly I am grateful to all of my professors, colleagues, family and friends who have supported me a lot. I wish for their prosperity from the bottom of my heart.