August 2015
Master's Degree Thesis

A New Hash Function Based on Image Cipher

Graduate School of Chosun University

Department of Computer Engineering

Tabassum Nasrin Haque

A New Hash Function Based on Image Cipher

영상암호기반 새로운 해쉬함수에 광한 연구

August 25, 2015

Graduate School of Chosun University

Department of Computer Engineering

Tabassum Nasrin Haque

A New Hash Function Based on Image Cipher

Advisor: Prof. Moon Inkyu, PhD

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

April 2015

Graduate School of Chosun University

Department of Computer Engineering

Tabassum Nasrin Haque

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

A New Hash Function Based on Image Cipher

Tabassum Nasrin Haque

Advisor: Prof. Moon Inkyu, Ph.D.

Department of Computer Engineering

Graduate School of Chosun University

A new hash function for image cipher has been proposed. Hash functions are widely used for data encryption and authentication. It is an important cryptographic primitive. It is best known as its important role in digital signature. This is better than other signature schemes such as RSA and discrete algorithm. However it is mostly used for block data. This has some certain properties for safety and resistance towards attacks. The newly proposed image hash function fulfills all the properties of a hash function and proves to be more robust towards collision resistance and preimage resistance.

In this new method the input image is first encrypts by double random phase encoding (DRPE) method. Thus the image gets encrypted. After that to compress and authenticate the image for better security; the image is further processed by photon counting imaging. In the receiving end the image can be decrypt but the original data cannot be visible to the receiver. If the receiver has true set of image then it can check the authenticity of the image. While using the photon counting

imaging, the image gets compressed and gives a fixed output length. Thus fulfills one of the properties of hash function. In this thesis the other properties of Hash function are also proved. The performance evaluation has been shown using nonlinear correlation with the true and false image set.

한 글 요 약

영상암호기반 새로운 해쉬함수에 광한 연구

하크 타바쑴 나스린

지도 교수: 문인규

컴퓨터공학과

대학원, 조선대학교

본 논문에서는 대용량 멀티미디어 데이터의 비밀성 및 무결성 보장을 위한 핵심 기술로서 새로운 영상단위 해시함수 알고리즘을 제안한다. DRPE 및 포톤카운팅 이미징 기술을 효과적으로 결합하여 영상데이터를 효과적으로 해시 처리할 수 있는 알고리즘을 설계하였으며, 제안한 알고리즘이 해시함수의 특성을 가짐을 실험결과를 통하여 입증하였다. 또한 기존 SHA 및 MD4 해시함수 기술과의 비교설명 등으로 제안한 해시함수 알고리즘의 우수성을 입증하였다. 제안된 해시알고리즘은 대용량 멀티미디어 데이터를

빠른 시간 내에 효율적으로 강인하게 해시처리 할 수 있는 기술로 활용될 수 있을 것이다.

CHAPTER 1

Introduction

1.1 MOTIVATION

In this 21st century when life has become smoother because of digitization of media and frequent use of platforms like internet; it's also an important question that how secure are they? Recently the use of digital images has been increased in a tremendous way. However, while transmitting through non-secure channels (i.e. internet) the image can be corrupted or changed by a third party of interest. Therefore copyright and integrity of images has become a great concern.

Image authentication is a term used for securing image data in various ways. It is used to compress and encrypt image data and verify the genuineness of the data at the receiving end [5]. Image compression means reducing the size of an image without or with a certain loss of data. This is needed because for an image which need to be transmitted over a channel will consume a large bandwidth according to its size. So if the size can be reduced the bandwidth needed for the transmission of the compressed image will be less. Encryption on the other hand is needed to provide security to the information. This is a method or a process for protecting information from undesirable attacks by converting it into a form non recognizable by its attackers. Data encryption mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or incomprehensible during transmission. The goal is to protect the content of the

data against the attackers. The reverse of data encryption is data decryption, which recovers the original data. Image authentication has got importance because of its use in a large number of application sectors such as medical, military and judicature. If an image is not authenticated, it can get intercepted and can be reproduced to exploit an evidence of medical diagnostic, military targets or false proofs of events. To protect the authenticity of multimedia images, several approaches have been proposed. These approaches include conventional cryptography, fragile and semi-fragile watermarking and digital signatures that are based on the image content.

1.2 IMAGE AUTHENTICATOIN

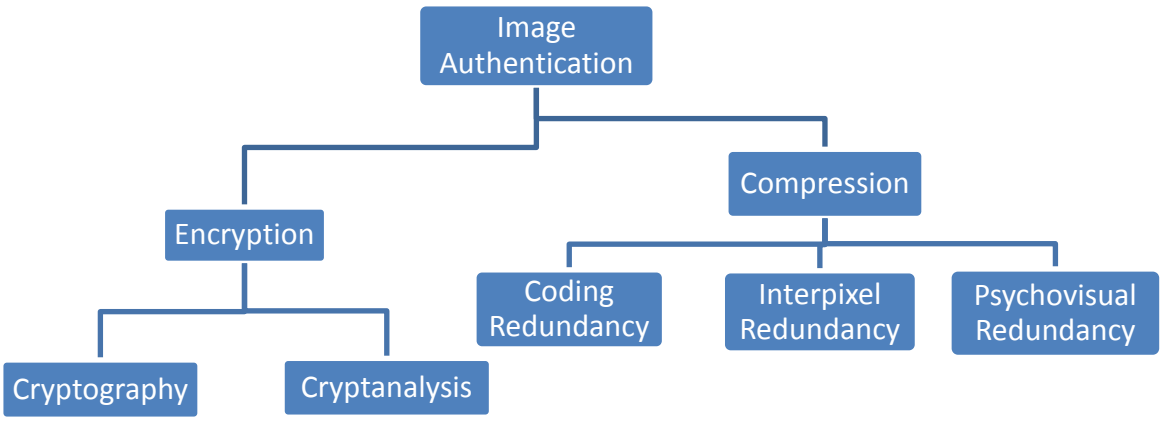


Fig 1.1: Image authentication classification

A process of authentication should achieve a compact illustration of associate degree image by reducing the image storage as well as transmission requirements. Compression is done by reducing one or a lot of the 3 basic data redundancies:

- Coding Redundancy
- Interpixel Redundancy
- Psychovisual Redundancy

Coding redundancy is present once when optimum code words are used. Interpixel redundancy is obtained from correlations between the pixels of a picture. Psychovisual redundancy refers to those information that's unrecognizable by the human visual system (i.e. visually non-essential information). Image compression techniques decreases the amount of bits required to represent an image by taking advantage of those redundancies. An inverse method known as decompression (decoding) is applied to the compressed image to obtain the reconstructed image. The target of compression is to reduce the amount of bits as much as possible, whereas keeping the resolution intact and therefore the visual quality of the reconstructed image as near the initial image as attainable. Image compression systems area unit composed of 2 distinct structural blocks : An encoder and a decoder.

2.1.1 Image Encryption

Encryption and decryption are two phases of a process called cryptography[10],[6]. Cryptography is a process of storing and transmitting data in a form that only intended person can read and process it. It is a science of protecting information by encoding it into an unreadable format. Data that can be read or understood without any special measurement is called *plaintext*. The method of rearranging the data into some unreadable form is called *encryption.* Encrypted plaintext is called *ciphertext*. The algorithm used to encrypt a plaintext is called *cypher*. An algorithm works in a combination with a *key* – a word, number, or phrase – to encrypt the data.

Based on the keys used in a cypher, there are two type of algorithm namely *Symmetric Key algorithm* and *Asymmetric Key algorithm*. In symmetric key there is a single key that is used in both ends to encrypt and decrypt a data. But in case of asymmetric key there are two keys that are used in the algorithm namely *public key* and *private key*. An encryption/decryption system is also called a cipher, or a cryptosystem. Accordingly, the encryption machine is called an encipher, and the decryption machine is called a decipher. The message for encryption is called the plaintext, and the encrypted message is called the ciphertext.

2.1.2 Image Compression

Image compression is used to minimize the size of an image without degrading its quality [1]. The reduction in file size allows more images to be stored in a given

amount of disk or memory space. It also reduces the time required for images to be sent over the Internet or downloaded from Web pages. Image compression may be lossy or lossless. Lossless compression is preferred for archival purposes and often for medical imaging, technical drawings, clip art, or comics. Lossy compression methods, especially when used at low bit rates, introduce compression artifacts.

2.1.3 Various Methods of Image Encryption

There are several methods of image authentication. However before talking about the various methods we need to keep in mind some essential requirements for image authentication [10]. Those can be enlisted as:

- Sensitivity
- Robustness
- Localization
- Recovery
- Security
- Portability
- Complexity

There are basically two types of image authentication. One is strict authentication and the second one is content based image authentication or selective authentication. The techniques under these two criteria are discussed below:

A. Strict Authentication

Strict image authentication methods do not tolerate any changes in the image data. These methods can be further separated in two groups according to the techniques that are used: methods based on conventional cryptography and methods that use fragile watermarking.

i. Methods Based on Conventional Cryptography

Image authentication methods based on cryptography compute a message authentication code (MAC) from images using a hash function. The resulting hash (h) is further encrypted with a secret private key S of the sender and then appended to the image. For a more secure exchange of data between subjects, the hash can be encrypted using public key K1 of the recipient (Fig 1.2a). The verification process is depicted in Fig. 1.2 (b). The receiver computes the hash from the received image. The hash that was appended to the received image is extracted and decrypted using private key K1. The extracted hash and the calculated one are then compared. Techniques that are based on the hash computing of image lines and columns are known as line–column hash functions. [11].

i. Fragile Watermarking

Watermarking consists of a watermark, hiding it in the image, and then extracting it when it is necessary. Fragile watermarking belongs to the strict authentication class, while semifragile watermarking to the selective authentication class. Some authors define reversible watermarking, also called erasable or invertible, as a subgroup of

fragile watermarking. The idea behind reversible watermarks is to reconstruct the exact original image when the image is declared as authentic. Thus, it reconstructs the information that was lost during watermarking.

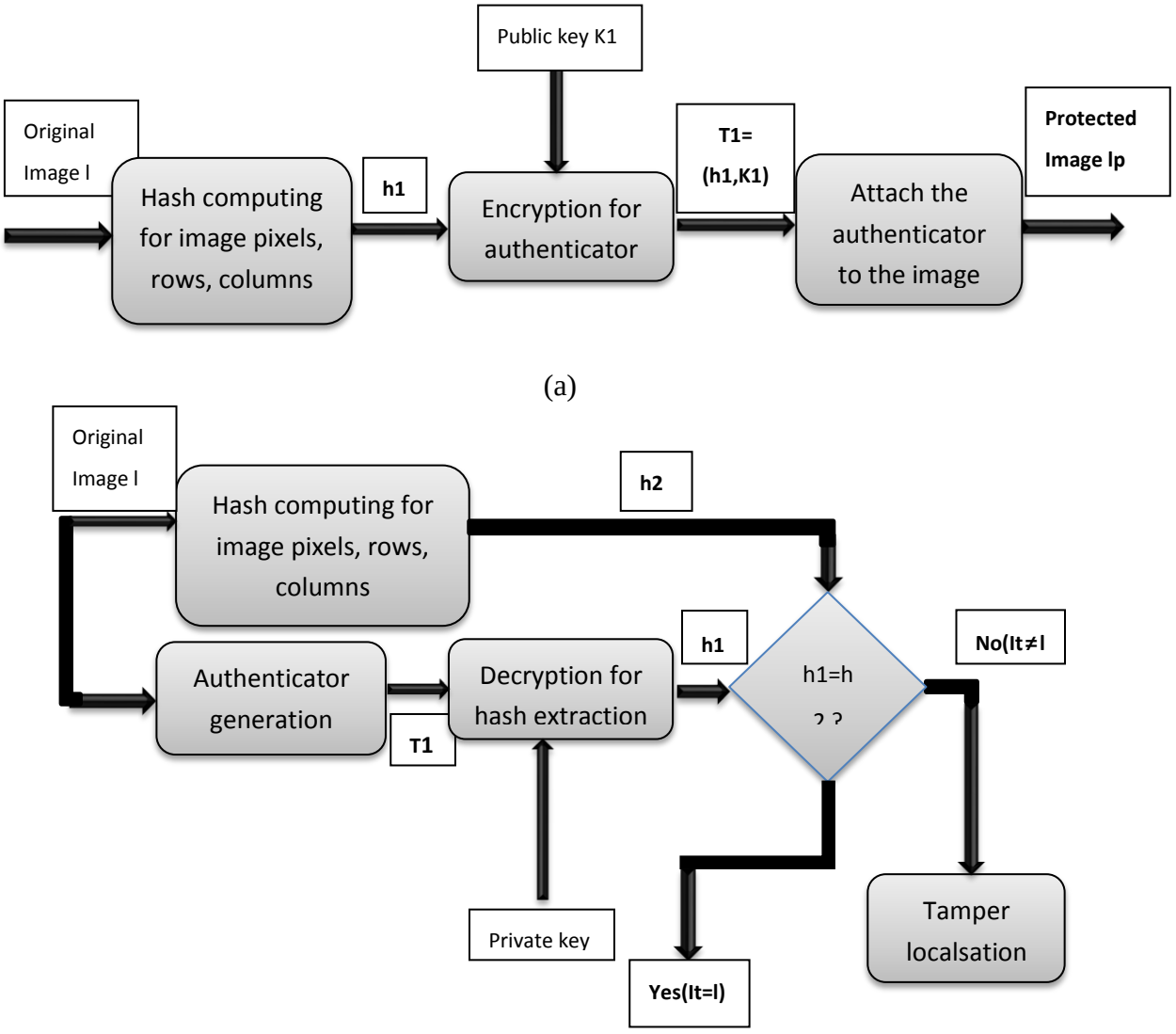


Fig 1.2: Strict authentication system by conventional cryptography (a)generation of authenticator; (b)verification of authenticity

B. Content Based Image Authentication or Selective Authentication

A lot of applications that base their decisions on images need authentication methods that can tolerate content preserving manipulations while at the same time detect any manipulation that change the image content. This leads to new watermarking methods known as semifragile watermarking, and to new approaches known as content-based signatures.

i. Semi-fragile Watermarking

Robust watermarking is designed to resist all attempts to destroy the watermark. Its main application includes the intellectual property protection and owner identification. The robustness of the embedded watermark is crucial to resist any intentional and even unintentional manipulation. The goal of these techniques is not the verification of the image authenticity, but rather the verification of their origins. Semi-fragile watermarking combines characteristics of fragile and robust watermarking techniques. Basically, the idea of semi-fragile watermarking is to insert a watermark in the original image in such a way that the protected image can undergo some specific image processing operations while it is still possible to detect malevolent alterations and to locate and restore image regions that have been altered. For image authentication purposes watermarking algorithms should be invisible. Visible watermarking algorithms are applied for on-line content distribution, transaction tracking or owner identification. The procedures of generating a watermark and embedding it into the image can be dependent on a

private or public, symmetric or asymmetric, key system in order to increase the overall system security. This is a trade-off between security and computational time. [11].

ii. Image Authentication by Digital Signature Based on the Image Content

Most recent investigations in the domain of image authentication were concentrated on digital signatures applied to the image content; these approaches offer high performance and promise additional breakthroughs in the near future. An image authentication system by digital Signature based image content consist in (1) extracting specific high level characteristics from the original image; (2) applying a hash function to these characteristics in order to reduce their size; (3) digitally signing the hash value using an existing digital signature algorithm such as a private or public key system to increase the overall security; (4) attaching the signature to the original image or inserting it in the image using techniques for data dissimulation. Likewise, the verifying procedure of an image authenticity consists in (1) generating the image signature using the same algorithm; (2) extracting the attached or dissimulated signature; (3) comparing these two signatures using a comparison algorithm to decide whether the image was altered or not; (4) determining the image regions that were manipulated. When the image is declared as not authentic, information from the original signature could be used to partially or even completely restore the regions that were corrupted. The algorithm used to compare the signatures directly depends on the selected characteristics and the dissimulation method.

CHAPTER 2

THEORETICAL BACKGROUND

2.1 Double Random Phase Encoding

The technique which produces a two dimensional complex valued stationary white noise from a two dimensional input image is called double random phase encoding (DRPE) technique. DRPE is done by modulating a primary image $f(x,y)$, which represents the spatial domain; with two random phase mask which are also called random noises.

2.1.1 Fundamental Concept

Let $n(x,y)$ and $b(u,v)$ be two random noises which are uniformly distributed over the range [0,1]. The corresponding two random phase masks in the spatial and frequency domains can be expressed as $\exp[j2\pi n(x,y)]$ and $\exp[j2\pi b(u,v)]$. This two phase masks are randomly distributed from 0 to 2π in the input image plane and Fourier domain. At first, the primary image is multiplied with the phase mask of spatial domain which is $\exp[j2\pi n(x,y)]$. Then the resultant product is transformed to the Fourier domain using Fourier transform and then multiplied with the Fourier mask which is $\exp[j2\pi b(u,v)]$ [2]. The final encrypted double random phase encryption can be expressed as,

$$\psi(x,y) = \Im^{-1}[\Im[f(x,y)\exp[j2\pi n(x,y)]]\exp[j2\pi b(u,v)]] \ldots\ldots (1)$$

Where, $\Im$ denotes two dimensional Fourier transform and $\Im^{-1}$ stands for inverse Fourier transform.

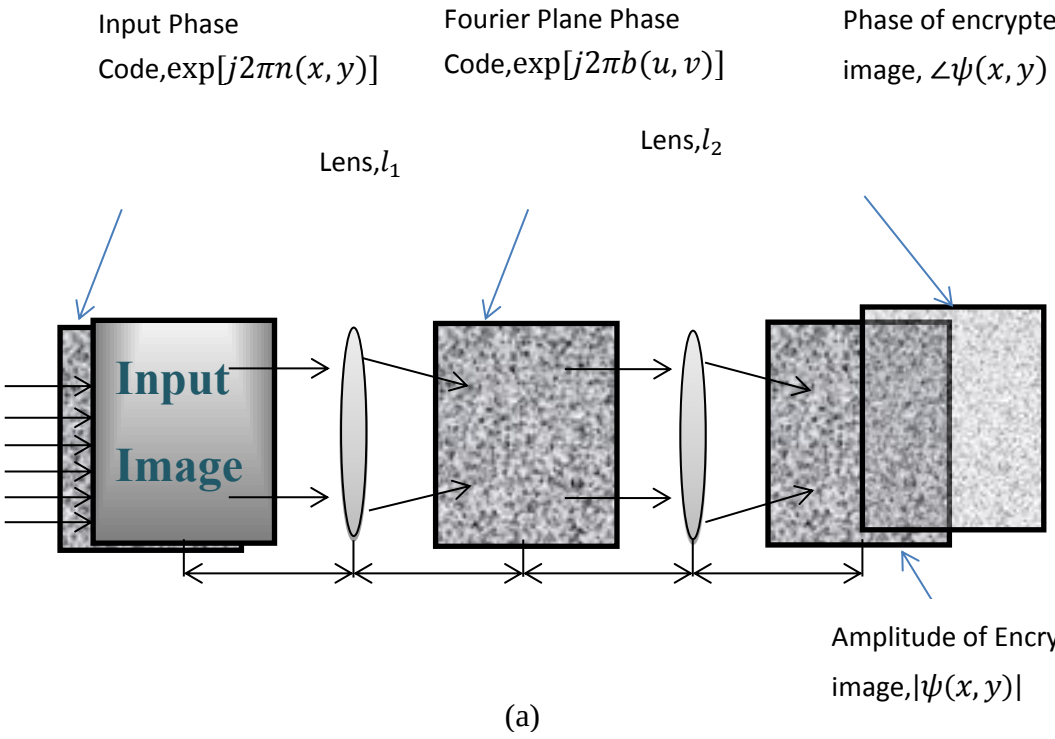
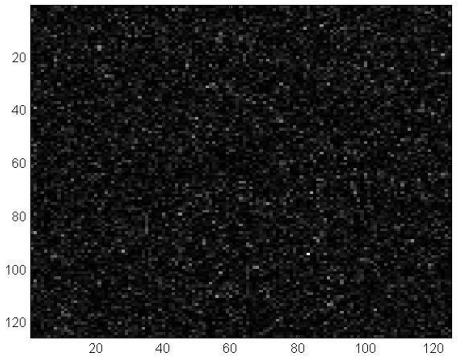
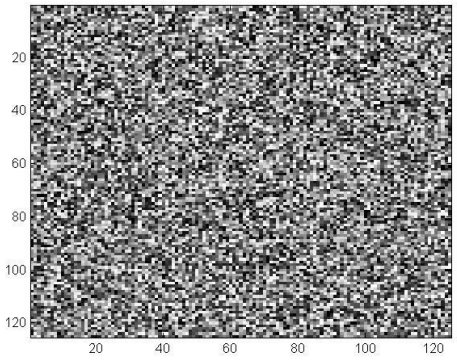


Fig 2.1: Schematic diagram of (a) DRPE encryption process and (b) decryption process

The resultant image is white stationary noise. It has both the amplitude and phase information. The image can be partially recovered by either of the information.

(a)





(b) (c)

Fig 2.2: :(a) Original Image , (b) Amplitude of DRPE image, (c) Phase value of DRPE image

To retrieve the original image the process needs to be reversed. At first the Fourier transform of $\psi(x, y)$ takes place and then multiplied by the first decryption key

which is a complex conjugate of the Fourier domain phase mask. It can be expressed as $\exp[-j2\pi b(u,v)]$ and by doing that function $\Im[f(x,y)\exp[j2\pi n(x,y)]$ is obtained. The inverse Fourier transform is used to get the original image back. If $f(x,y)$ is a real and positive function then the primary image can be retrieved by an intensity sensitive device such as a CCD camera.

2.1.2 Advantages and Limitations

DRPE has very good security and has robustness to many attacks such as brute force attack. One of the main reasons of its wide range of use is the system is very easy to implement. Also it's easily applicable in several image formats such as black and white, gray level and color images. By changing or updating phase keys, a lot of attacks can be prevented. However, even after having so many advantages the system can be compromised in an attack where the attacker tricks a user to encrypt a known image. This type of attack is called chosen-plain text attack. As a result the phase key of Fourier domain can be recovered by the attacker.

2.2 Photon Counting Imaging

For a long time scientists has been working on detection of the nature of light. In early 17th century Ren´e Descartes suggested that light might consist of moving particle which was agreed by Sir Isaac Newton afterwards. However, the theory was then rejected by Christian Huygens during that period of time and later on by Augustin Fresnel at the beginning of 19th century. In 1901 Max Planck suggested

that radiative transfers can occur through packets of energy called quanta. In 1905 Albert Einstein explained how photo electron works. Heinrich Hertz first experimented and observed the photo electric effect in187. Einstein described the existence of photos which means a physical limit on the minimum light intensity for any observed phenomenon exists for a given area. The detector which can detect each individual photon can be called as perfect detector. If the detector can detect each photon then it can provide the maximum possible signal-to-noise ratio. This ability can be expressed as photon counting.

Conventionally photon-counting imaging is used for detecting two dimensional imaging of an ultra-weak light of an encrypted distribution. In typical PCI method a photo multiplier tube is used for detection. However with the course of time and advancement of technology; new photon counting imaging techniques and devices has been introduces. Now-a-days PCI is incorporated with other techniques for better image authentication. A sparse representation of the encryption process is used while retrieving the original image. However, the decrypted image is not a clear visualization of the original image. It is used for image authentication and verification using non-linear processor.

As previously discussed, there are security flaws in the traditional double-random-phase encryption processes. Pérez-Cabré et al. proposed a modification to the DRPE: Instead of using this algorithm as a linear encryption/decryption scheme, modify the process as an authentication method [7]. To do this, photon-counting is performed on the amplitude of the encrypted image. Photon-counting is a process

that limits the number of photons arriving at a pixel in an image. Note that this is a nonlinear transformation of the data. Since photon-counting is performed on the amplitude of the encrypted image, information is lost. Thus, rather than recover the primary input image in the decryption process, a noise-like decrypted image is obtained. Since only the amplitude information was modified, and not the phase information, it is possible to authenticate the photon-limited encrypted image using nonlinear processors. This can have many applications in security including correctly verifying an identification card.

2.2.1 Fundamental Concept

Photon-counting, itself is modeled as a Poisson distribution [7]. That is not to say that a Poisson distribution is the only model. Depending on the coherent state of light, the photons may follow a binomial, negative binomial, multinomial distribution, or negative multinomial distribution [36]. For experiments, we assume that the coherent state can be modeled as a Poisson distribution. Moreover, the fewer the number of photons arriving at a pixel, the sparser the scene becomes. The probability density function for counting the number of photons at an observation area or arriving at pixel j can be modeled as,

$$P(l_j;\lambda_j) = \frac{[\lambda_j]^{l_j} e^{-\lambda_j}}{l_j!} \text{ For } \lambda_j > 0 \;\; l_j \epsilon \{.,1,2,\ldots.\} \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Here. l_j is the number of photons detected at pixel j and λ_j is the Poisson parameter defined as,

$$\lambda_j = N_p x_j$$

Where, N_p is total number of photons and x_j is normalized irradiance at pixel j.

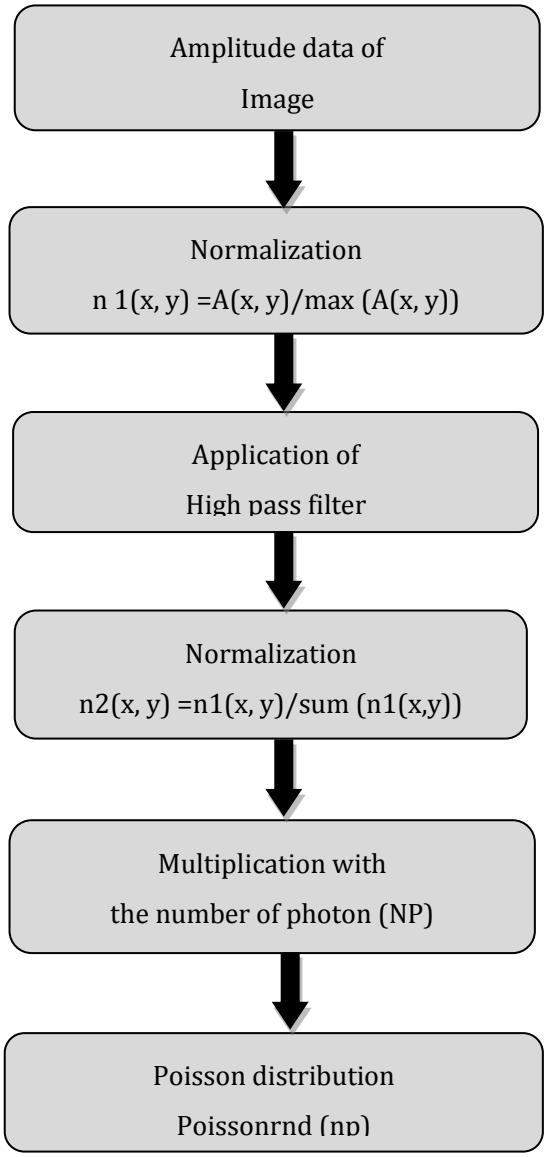
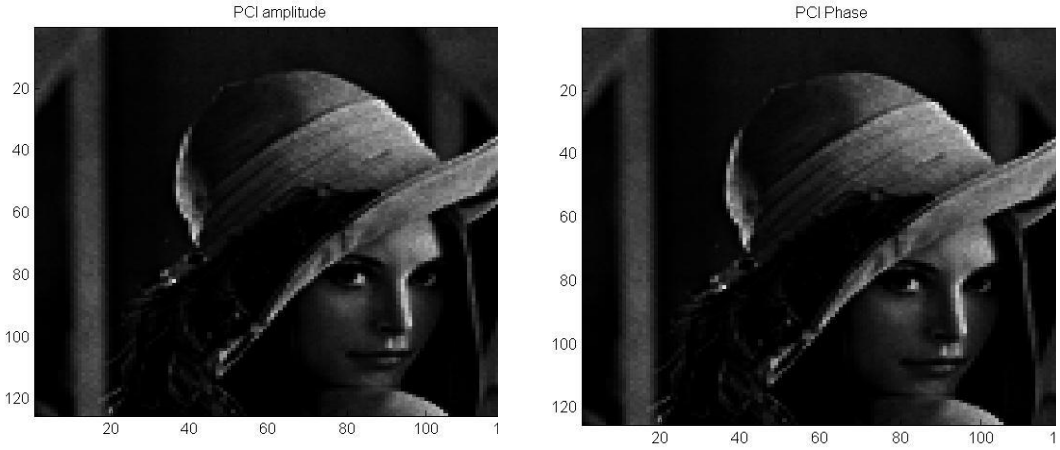


Fig 2.3: Flowchart Diagram for PCI

The photon counting method can be used by normalizing the image amplitude and passing the result through a high pass filter. Then that image is multiplied with the number of photon. After that it generates a photon limited encrypted image by Poisson random distribution. Figure 2.4(a) shows a 125×125 pixel gray image and fig 2.4(b) and fig 2.4(c) are the amplitude and phase value of PCI, where the number of photon is 10^7.

(a)



(b) (c)

Fig 2.4:(a) Original Image , (b) Amplitude of PCI image, (c) Phase value of PCI image

2.2.2 Advantages and Limitations

Using PCI an image can be totally encrypted as well as compressed. However, since the image has been compressed so there is no way that it can be recovered totally after going through the process of PCI.

CHAPTER 3

HASH FUNCTION FOR CRYPTOGRAPHY

3.1 Basic Concept

Hash function is one of the commonly used cryptographic primitive used in image encryption. The other two widely used cryptographic algorithms are block ciphers and pseudo-random number generators. It basically converts an arbitrary large input message into a fixed length message digest. It can generate a fixed output regardless of the size of the input message. This fixed length message is different for every input message so it works like a fingerprint of a message. This fingerprint is called hash value of the hash function. The main difference of hash function from other crypto algorithm is, it does not have a key for encryption [28-33].

The principal input and output behavior of a hash function is shown in Fig .3.1. Hash function has many applications. However, it's best known for its application as digital signatures. Hash function has some security requirements which are shown in Fig 3.2.

1

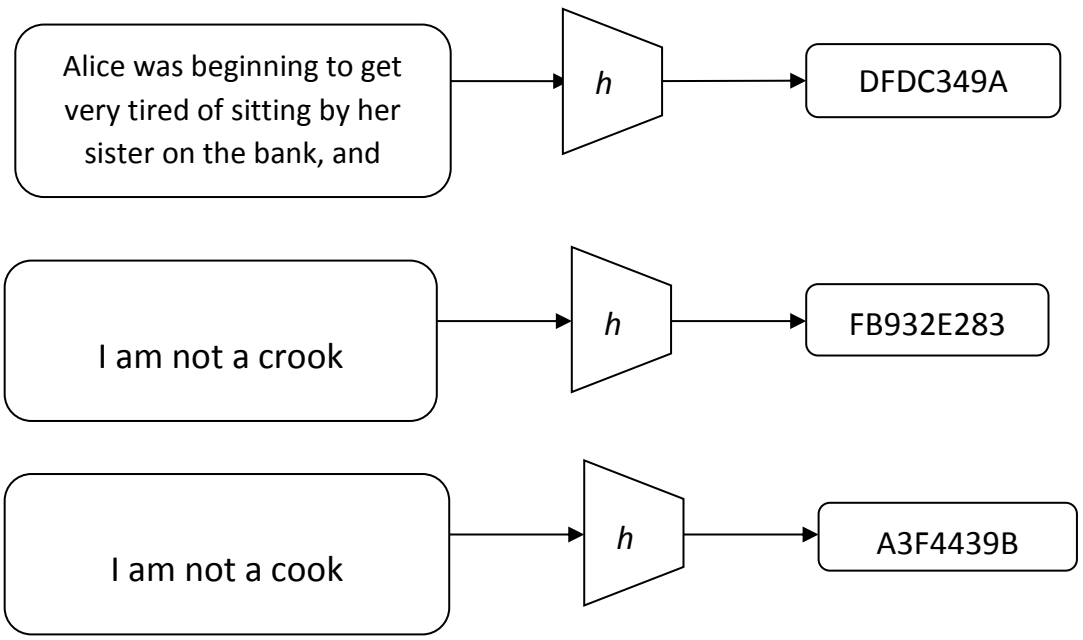


Fig 3.1: Basic input and output behavior of hash function

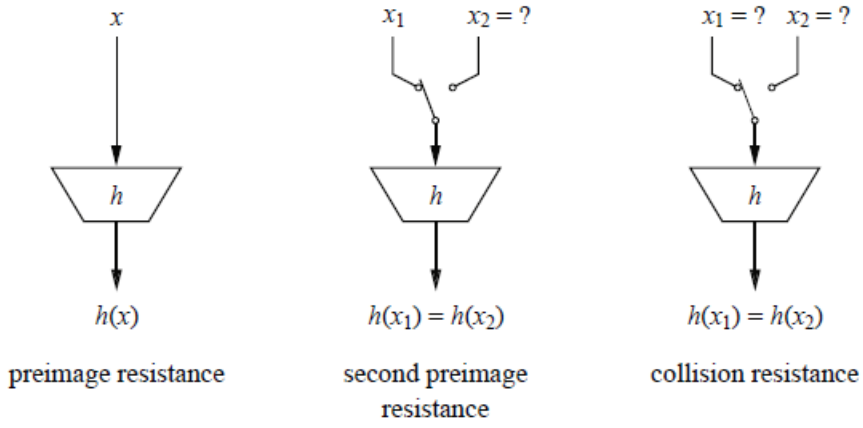


Fig 3.2: Security requirements of hash function

3.2 Hash Function Properties

Property-1: **Arbitrary Message size**

Hash function $h(x)$ can be applied to any kind of input message regardless of size of the message.

Property-2: **Fixed output length**

If the input1 has a length of z_1 and input2 has a length of z_2 both will produce output of the same length z.

Property-3**: Efficiency**

Hash functions are easy to calculate. It has less complexity and does not consume a lot of time**.**

Property-4***:*** **Preimage resistance**

For a given output *z*, it is impossible to find any impit *x* such that $h(x) = z$**,** i.e. $h(x)$is one way

Property-5**: Second Preimage resistance**

Given x_1,and thus $h(x_1)$,it is a computationally infeasible to find any x_2 such that $h(x_1) = h(x_2)$

Property-6**: Collision resistance**

It is computationally infeasible to find any pairs $x_1 \neq x_2$ such that $h(x_1) = h(x_2)$

3.3Birthday Paradox

If n items are put in m containers, where $n > m$. The it is obvious that some of the containers will have more than one item. This theory is known as pigeonhole theory. Due to this theory we can come to a conclusion that collision always exist. But our concern is how often does it occur and how difficult to find them. Though we think that it is as difficult as finding second preimage resistance, but in reality it is half of the number of attacks we presumed. This is due to a theory called birthday paradox which is explained below.

How many people are needed at a party such that there is a reasonable chance that at least two people have the same birthday?

$$P(no\ collision\ among\ 2people) = (1 - \frac{1}{365})$$

$$P(no\ collision\ among\ 3people) = (1 - \frac{1}{365})(1 - \frac{2}{365})$$

Therefore, For t people having no birthday collision:

$$P\left(no\ collision\ among\ 3people\right) = \left(1 - \tfrac{1}{365}\right).(1 - \tfrac{2}{365})\ldots(1 - \tfrac{t-1}{365})$$

To figure out the probability of having 50% chance of two colliding birthdays, we need to do some calculations.

$$P(at\ least\ one\ collision) = 1 - P(no\ collision)$$

$$= 1 - \left(1 - \frac{1}{365}\right).(1 - \frac{2}{365}) \ldots (1 - \frac{t-1}{365})$$

For example, if $t = 23$ the probability of having at least one collision is

$$P(at\ least\ one\ collision) = 1 - \left(1 - \frac{1}{365}\right).(1 - \frac{2}{365}) \ldots (1 - \frac{23-1}{365})$$

$$=0.507 \approx\ 50\%$$

Number of values each element can take=2^n

Here, n is the output width of hash value $h()$

Let's now calculate, how many messagesthe attacker needs to Hash until he has a reasonable chance that $h(x_i) = h(x_j)$ for some x_i and x_j as two input values.

Probability for no collisions among *t* hash values

$$P\left(no\ collision\right) = \left(1 - \frac{1}{2^n}\right).(1 - \frac{2}{2^n}) \ldots \left(1 - \frac{t-1}{2^n}\right)$$

$$= \prod_{i=1}^{t-1} \left(1 - \frac{i}{2^n}\right)$$

$$\approx \prod_{i=1}^{t-1} \left(1 - e^{-i/2^n}\right) \quad [\because e^{-x} = 1 - x \& i/2^n << 1]$$

$$\approx e^{-\frac{t(t-1)}{2^n.2}} \qquad [\because 1+2+3+\cdots+t-1=\frac{t(t-1)}{2}]$$

Let, $\lambda = P(at\ least\ one\ collision)$

$$\Rightarrow \lambda = 1 - P(no\ collision)$$

$$\Rightarrow \lambda \approx 1 - e^{-\frac{t(t-1)}{2^{n+1}}}$$

$$\Rightarrow \ln(1-\lambda) \approx -\frac{t(t-1)}{2^{n+1}}$$

$$\Rightarrow t(t-1) \approx 2^{n+1} \ln(\frac{1}{1-\lambda})$$

$$\Rightarrow t \approx \sqrt{2^{n+1}\ \ln(\frac{1}{1-\lambda})} [\because t \gg 1]$$

$$\Rightarrow t \approx 2^{\frac{n+1}{2}} \sqrt{\ln(\frac{1}{1-\lambda})}$$

Equation to describe the relationship between the number of hashed messages t needed for collision probability λ

Thus, for a success probability of 50% with 80bit hash output, we expect to hash about

$$t \approx 2^{\frac{80+1}{2}} \sqrt{\ln\left(\frac{1}{1-0.5}\right)} \approx 2^{40.2}$$

So, it means the attacker has to generate only around 2^{40} hash values to find a collision. This is half of the values we expected. Due to this birthday paradox the collision resistance property becomes vulnerable for the attacker. If we consider

minimum of 128bit as the output length of a hash function which is the minimum output length of a hash function, then the attacker needs to try 2^{65} types of hash values to find a collision. The following table 1 shows the different hash values needed for collision in different collision likelihood.

Table 1: No. of hash values needed for a collision for different hash function output lengths

	Hash output length				
λ	128bit	160bit	256 bit	384bit	512bit
0.5	2^{65}	2^{81}	2^{129}	2^{193}	2^{257}
0.9	2^{67}	2^{82}	2^{130}	2^{194}	2^{258}

3.4 Conventional Hash functions

The basic algorithm of hash function is known as Merkle-Damgård construction for hash function. This basically divides the whole data into series of blocks of equal size and passes through a hash function sequentially. The hash function has a compression algorithm at its center. The hash value is defined by the cumulative sum of all the output of the compression function.

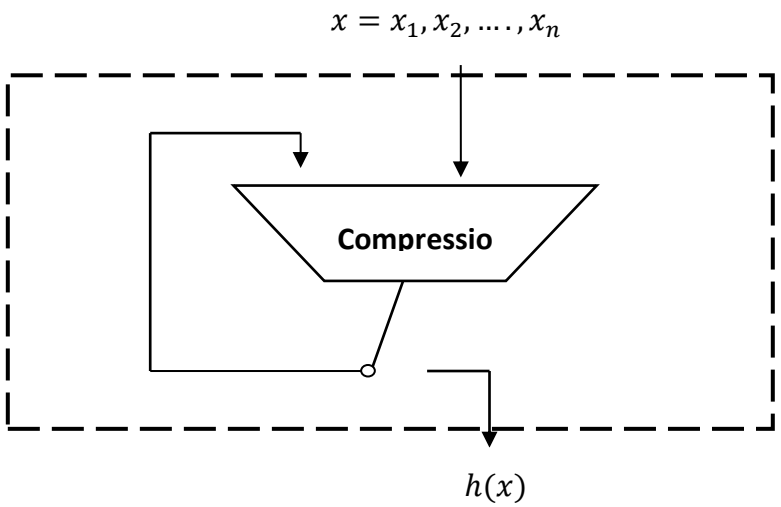


Fig 3.3 : Merkle-Damgård construction for hash function

There are two general types of hash functions. One is called dedicated hash function and another one is based on block cipher.

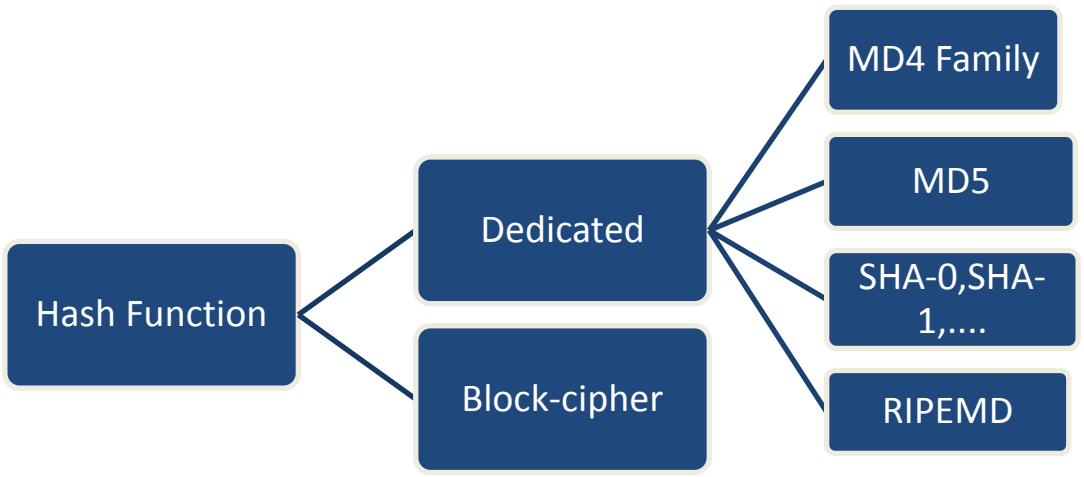


Fig 3.4: Classification of conventional hash functions

3.4.1 Dedicated hash function

Dedicated hash functions are algorithms that have been custom designed. A large number of such constructions have been proposed over the last two decades. In practice, by far the most popular ones have been the hash functions of what is called the MD4 family. MD5, the SHA family and RIPEMD are all based on the principles of MD4. MD4 was an innovative idea because it was especially designed to allow very efficient software implementation. It uses 32-bit variables, and all operations are bitwise Boolean functions such as logical AND, OR, XOR and negation. A strengthened version of MD4, named MD5, was proposed by Rivest in 1991 [1].

Both hash functions compute a 128-bit output, i.e., they possess a collision resistance of about 264. MD5 became extremely widely used, e.g., in Internet security protocols, for computing checksums of files or for storing of password hashes. There were, however, early signs of potential weaknesses. Thus, the US NIST published a new message digest standard, which was coined the Secure Hash Algorithm (SHA), in 1993. This is the first member of the SHA family and is officially called SHA, even though it is nowadays commonly referred to as SHA-0. In the absence of analytical attacks, the maximum collision resistance of SHA- 0 and SHA-1 is about 280, which is not a good fit if they are used in protocols together with algorithms such as AES, which has a security level of 128–256 bits. Thus, in 2001 NIST introduced three more variants of SHA-1: SHA-256, SHA-384 and SHA-512, with message digest lengths of 256, 384 and 512 bits, respectively. A further modification, SHA-224, was introduced in 2004 in order to fit the security level of 3DES. These four hash functions are often referred to as SHA-2.

The Secure Hash Function algorithm SHA-1 is the most widely used message digest function of the MD4 family. Stronger versions of SHA family have the similar internal structure such as SHA-1. SHA-1 produces a 160-bit output of a message with a maximum length of 264 bit. Before the hash computation, the algorithm has to preprocess the message. During the actual computation, the compression function processes the message in 512-bit chunks. The compression function consists of 80 rounds which are divided into four stages of 20 rounds each.

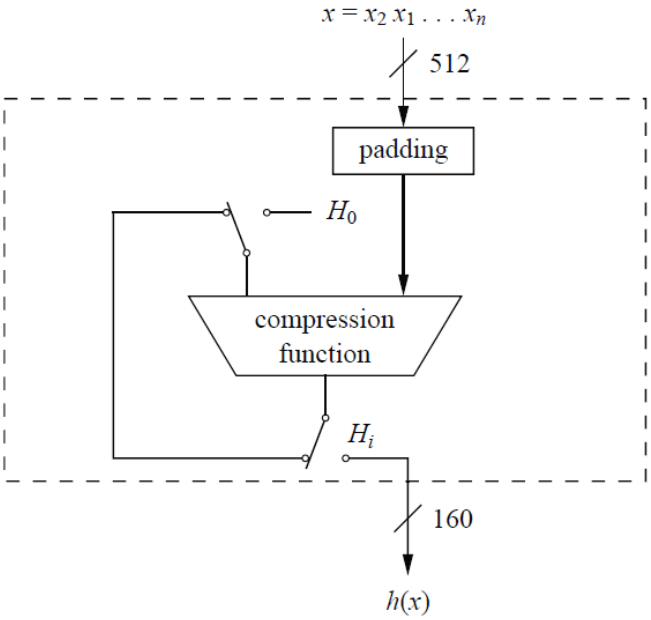


Fig 3.5: Diagram of SHA-1

The input-output behavior and the collision resistance of different dedicated hash function can be summarized as table 2.

Table 2: The MD4 family of Hash function

Algorithm		**Output[bit]**	**Input [bit]**	**No. of rounds**	**Collisions found**
MD5		128	512	64	Yes
SHA-1		160	512	80	Not yet
SHA-2	SHA-224	224	512	64	No
	SHA-256	256	512	64	No
	SHA-384	984	1024	80	No
	SHA-512	512	1024	80	no

3.4.2 Block-cipher based hash function

Hash functions can also be constructed using block cipher chaining techniques. As in the case of dedicated hash functions like SHA-1, we divide the message *x* into blocks *xi* of a fixed size. Figure 3.6 shows a construction of such a hash function: The message chunks *xi* are encrypted with a block cipher *e* of block size *b*. As *m*-bit key input to the cipher, we use a mapping *g* from the previous output *Hi*−1, which is a *b*-to-*m*-bit mapping. In the case of *b* = *m*, which is, for instance, given if AES with a 128-bit key is being used, the function *g* can be the identity mapping. After the encryption of the message block *xi*, we XOR the result to the original message block. The last output value computed is the hash of the whole message *x*1,*x*2,. . .,*xn*, i.e., *Hn* = *h*(*x*).

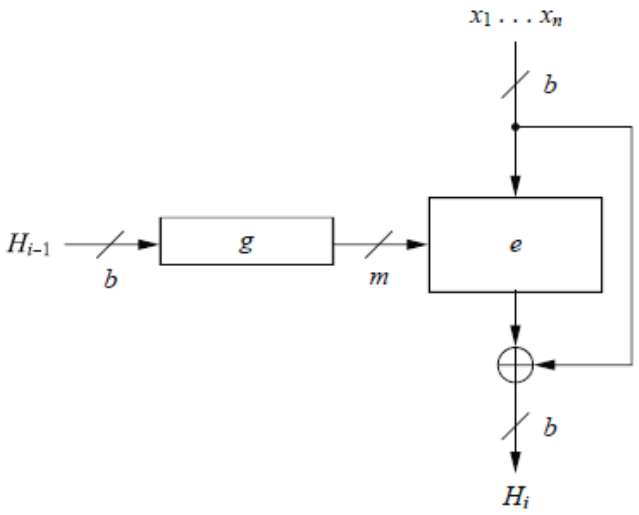


Fig 3.6: Diagram of block-cipher based hash function

The function can be expressed as:

$$H_i = e_{g(H_{i-1})}(x_i) \oplus x_i \ldots\ldots\ldots\ldots (3)$$

This construction, which is named after its inventors, is called the Matyas–Meyer–Oseas hash function. All the Hash functions based on block cipher needs to have an initial value H_0. The Bit size if the hash output is equal to block width of cipher used in that diagram. In situations where only preimage and second preimage resistance is required, block ciphers like AES with 128-bit block width can be used, because they provide a security level of 128 bit against those attacks.

CHAPTER 4

HASH FUNCTION FOR IMAGE CIPHER

We proposed a new Hash function algorithm based on image ciphers. As images are different than plain text, sometimes using block cipher based Hash function can be complicated for image authentication. However the proposed method proves all the properties of a hash based encryption method and shows better results for collision resistance than conventional hash algorithm such as block cipher and dedicated hash functions.

We all familiar to the Merkle-Damgård construction for hash function (Ch-3).

However in the case of image; the inputs are two dimensional. As a result dividing the image in block message and process them is lot more complicated. Instead of following the conventional method, a new approach is proposed here. As mentioned in chapter 3, the aim of hash function is to process an arbitrary-length message to a fixed length random output. It is done to get disguised while sending through a common media such as internet to hide the original image from the attacker. The proposed method also encrypts the image and compresses as it requires less bits to transmit the image. The basic operation of the proposed method is shown in figure 4.2. This new method for hash function shows very strong avalanche effect, which is a very strong cryptographic property.

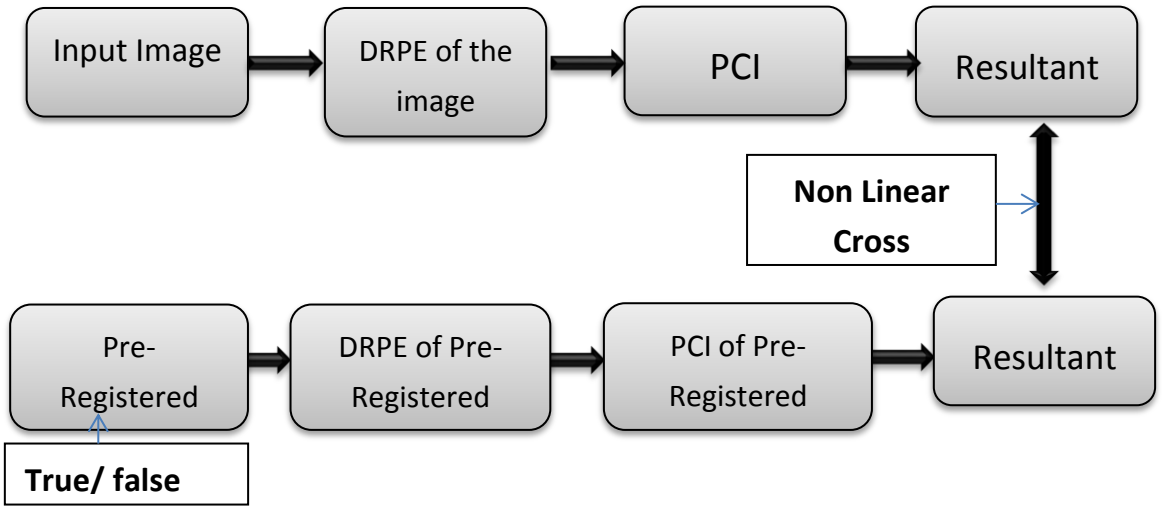


Fig4.1: Block diagram for the proposed image-cipher based hash function

In this procedure, an input image is encrypted using double random phase encryption. Further the amplitude of the encrypted image is sent through the procedure of photon counting imaging for further encryption and compression. DRPE and PCI together can exhibit strong resistance against intruder attacks based on binary, gray as well as RGB images. As PCI compresses the image, so it makes some of the pixel values zero. We only need the phase information of the pixels with non -zero amplitude value. It produces an image which cannot be visually recognized by human eye. It looks like a noisy image. This noisy image can be compared with reference image using non-linear correlation, which also went through the same procedure of encryption and compression. The authenticated image shows non-linear correlation result closer to one. Having a correlation value near zero means it was compared with a false class of images.

4.1 Mathematical Model

Equation 2 from chapter two can be applied to the amplitude of equation 1. Eq 1 can be rewritten as,

$$\psi(x,y) = |\psi(x,y)| \exp[j\emptyset(x,y)] \text{..... (4)}$$

Here, $\emptyset(x,y)$ denotes the phase information of the DRPE image whereas$|\psi(x,y)|$ denotes the amplitude data.

For generating photon counting image, the amplitude of eq 3 needs to normalize. This can be expressed as,

$$\Gamma(x,y) = \frac{|\psi(x_i,y_i)|}{\sum_{i=1}^{M}\sum_{j=1}^{N}|\psi(x_i,y_i)|} \text{.....(5)}$$

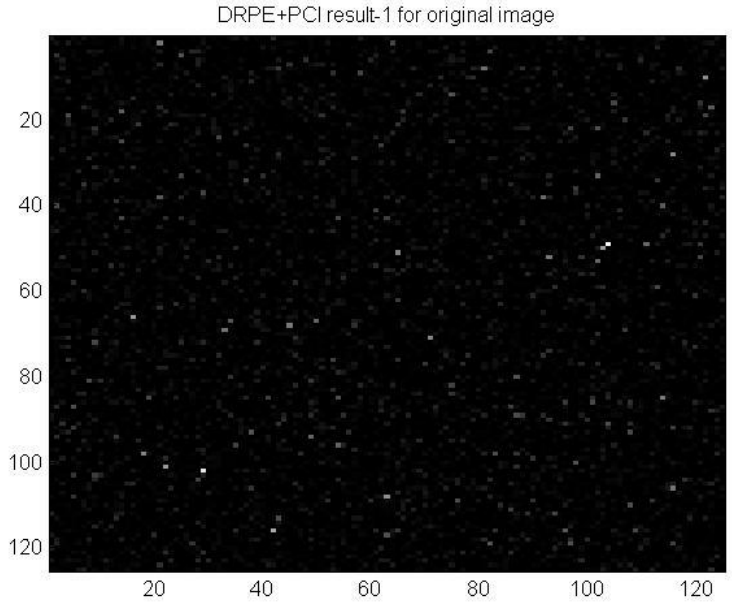
Here, M and N are the total number of pixels in the x and y directions respectively.

$\Gamma(x,y)$ is multiplied by N_p to calculate the Poisson parameter in eq 2. So the final expression for the resultant image which can also be called as image cipher based hash function can be expressed as,

$$h_{im}(x,y) = \Gamma(x,y) * N_p \text{..... (6)}$$

Here, $h_{im}()$ is the expression for hash value based on image cipher. For a given N_p, a photon limited encrypted image for a double random phase encryption with photon counting imaging $\psi_{ph}(x,y)$ can be shown in figure 4.3.

(a)



(b)

Fig 4.2: DRPE+PCI image output

4.2 Proof of Hash Algorithm for Image Cipher Hash Function

As we can recall the properties from chapter 3 of hash function, we can prove the properties for image cipher based hash function as well.

Property-1: **Arbitrary Message size**

Image cipher based hash function can be used for any size of image.

Property-2: **Fixed output length**

As DRPE always produces a fixed length of output message that means image cipher based hash function produces a fixed length output message for any size of input message.

Property-3**: Efficiency**

Image cipher based hash function takes only couple of seconds to generate the output result. The algorithm is very simple and effective.

Property-4***:*** **Preimage resistance**

After the image goes through the procedure of DRPE followed by PCI, it is impossible to retrieve the input image $f(x)$. Thus $h_{im}()$ is one way.

Property-5**: Second Preimage resistance**

Avalanche effect is one of the major properties of cryptography. If there is an avalanche effect of around 50% that means the system is robust and is unlikely to

have two outputs of same values. As image cipher based hash function has very strong avalanche which is shown in next chapter so we can say that it is infeasible to find $h_{im}(x_1) = h_{im}(x_2)$ where $h_{im}(x_1)$ is the hash value based on image cipher for x_1 and $h_{im}(x_2)$ is the hash value based on image cipher for x_2.

Property-6**: Collision resistance**

It is computationally in feasible to find any pairs $x_1 \neq x_2$ such that $h_{im}(x_1) = h_{im}(x_2)$.

The table 2 shows the different image cipher based hash values needed for collision in different collision likelihood. As we are converting the 8bit output to 64bit output for our case, so the output width n is very large.

Table 3: No. of image cipher based hash values needed for a collision for different hash function output lengths

	Image cipher based hash output length		
λ	$64 \times 50 \times 50$	$64 \times 125 \times 125$	$64 \times 240 \times 240$
0.5	2^{80001}	2^{500000}	$2^{1843201}$
0.9	2^{80002}	2^{500001}	$2^{1843202}$

As we can see that the numbers are tends to the infinity so we can say it is impossible to find a collision between two inputs such that both have the same image cipher based hash value.

CHAPTER 5

PERFORMANCE ANALYSIS

This chapter is consisted of two main sections. One is the familiarization of the fundamental simulation parameters for image encryption and the second chapter is for numerical result analysis of hash function based on image cipher.

5.1 Fundamental Simulation Parameter

For simulation of this proposed technique, we use some parameters. These parameters help us to understand the performance of a technique and analyze the technique. These parameters are briefly described below:

5.1.1 Avalanche Effect

Avalanche effect is a desirable property of cryptographic algorithm and cryptographic hash function. It was first used by Feistel[5]. If an input is changed slightly (for example, flipping a single bit) the output changes significantly (e.g., more than half the output bits flip). Having a small change in input bit; either in plain text or the key, the output changes drastically. Having an avalanche effect of around 50% means the method is satisfactory.

The avalanche effect is calculated as,

$$Avalanche\ Effect = \frac{No.of\ flipped\ bits\ in\ the\ ciphertext}{Total\ no.of\ bits\ in\ the\ cipher\ text} \times 100\%$$

The number of flipped bits in the cipher text is calculated by the hamming distance between the first encrypted cipher text and the cipher text after changing bit.

5.1.2 Cross- Correlation Process for Image Verification

Since the images after going through DRPE and PCI are not visually recognizable, so we have to adopt a comparison parameter for image recognition. A lot of image pattern recognition and authentication processors are there to authenticate the decrypted image; the linear and non-linear cross correlation processor produces the optimum result for image verification. Basically we are going to use non-linear cross correlation of the original image with true set of images as well as false set of images [8,18]. The non-linear cross correlation $cc(x, y)$ can be defined as,

$$cc(x, y) = \Im^{-1}\{|D(\mu, \eta)F(\mu, \eta)|^{k}\exp[i(\phi_D(\mu, \eta) - \phi_F(\mu, \eta)\}]\} \ldots\ldots\ldots (7)$$

Here, $D(\mu, \eta)$ and $F(\mu, \eta)$ are 2 dimensional Fourier transform of the resultant and reference images. Whereas, $\phi_D(\mu, \eta)$ and $\phi_F(\mu, \eta)$ denotes the phase values of $D(\mu, \eta)$ and $F(\mu, \eta)$ respectively. Parameter k defines the strength of the applied non-linearity. $k = 0$ makes the non-linear cross correlation as phase extractor which enhances the high-frequency content. When $k = 1$, the equation degenerate itself to a linear cross correlation. Changing the value of k can generate different results. The appropriate parameter of k can be found by analyzing the best peak-to-correlation energy (PCE). It can be expressed as,

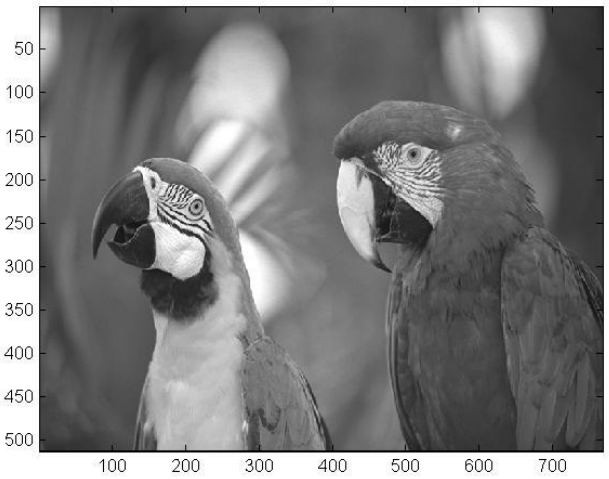
$$PCE = \frac{\max[|cc(x,y)|^2]}{\sum_{i=1}^{M}\sum_{j=1}^{N}|cc(x,y)|^2} \ldots\ldots\ldots (8)$$

Here $cc(x,y)$ is the output of eq 6. M and N are the image sizes x and y axes. A higher value of PCE results to a better non-linear cross correlation result.

5.2 NUMERCIAL RESULT ANALYSIS

All of the results are obtained by using Matlab R2013a. The computer which was used to execute the results is a 32bit windows 7 OS with a Intel(R) Core(TM) i3-3330 processor of 3.07GHz and the RAM is 3.00GB. The images used here are 500 × 500 pixels 256 grayscale which were later on down sampled to 125 × 125pixels. All processing data are digitally recorded on computer without optical processing configurations.

(a)

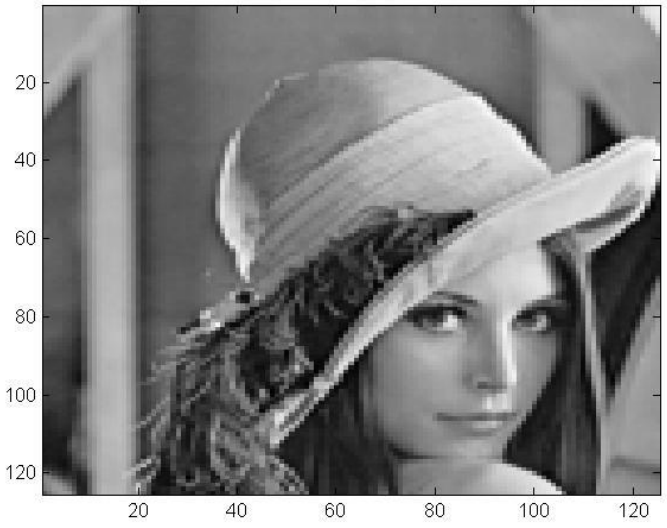


(b)

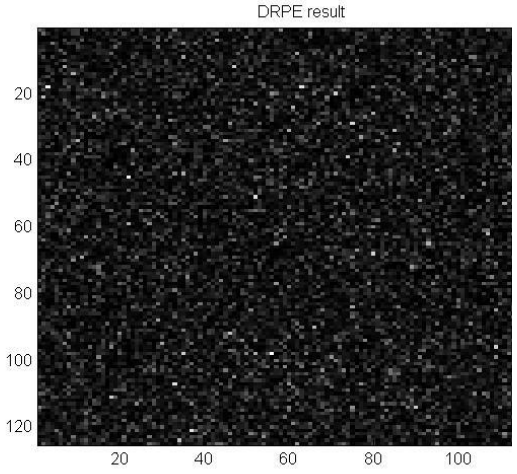
Fig 5.1: (a) True class image lena, (b) False class image parrot

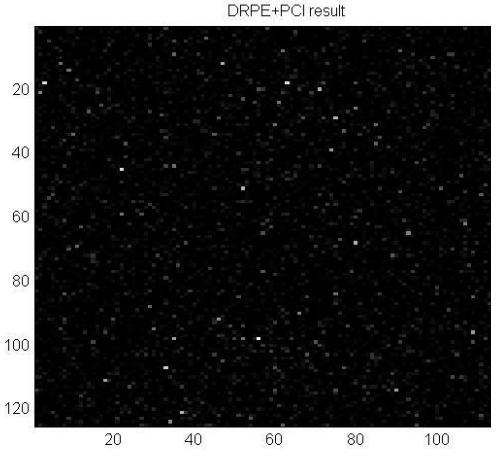
5.2.1 Image-Cipher Based Hash Outputs

The 125 × 125 grayscale image is shown in Fig 5.2 (a). This image was processed through DRPE and the output image is shown Fig 5.2 (b). Fig 5.2 (c) shows the final DRPE and Photon Counted Image. As we can see the image looks like a noisy image and it is almost impossible to find out the content of the image. Therefore, it is safe to transmit through any channel or medium. If an attacker does not have a true set of images it cannot be verified.



(a)





(b) (c)

Fig 5.2: (a) Input image lena, (b) DRPE result, (c) Image cipher based hash output

5.2.2 Avalanche Effect Analysis

Figure 5.3 shows output of avalanche effect in bit unit and pixel unit when some bits are changed in plain text. As it is visible from the figure, when 1 bit gets change the avalanche effect is around 40%. Later on, as the number of bits gets increased the result shows almost 50% avalanche effect. Figure 5.4 and figure 5.5 shows the avalanche effect for number of changed bits in first key and second key respectively. For all the cases image cipher based hash function has achieved reasonable avalanche effect since all the results in pixel unit are closer to 50% and in bit unit 100%. All the outputs are in Fourier domain.

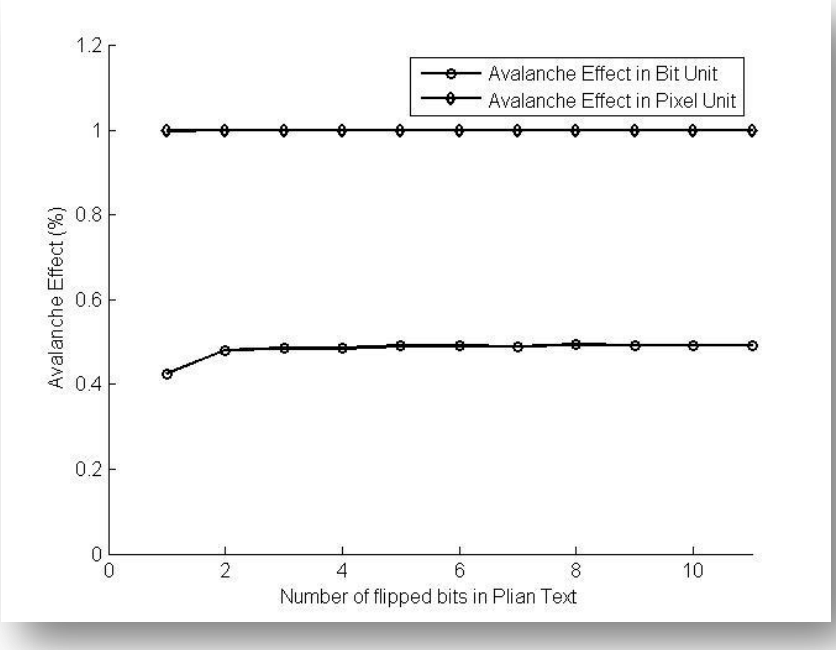


Fig 5.3: Avalanche effect with some bits in the plaintext gets inverted with input grayscale image

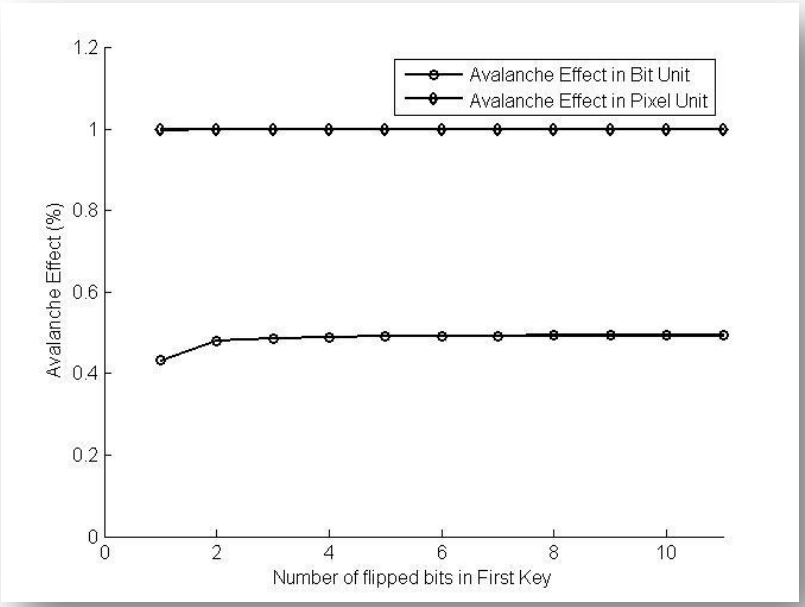


Fig 5.4: Avalanche effect with some bits in the first phase key gets inverted with input grayscale image

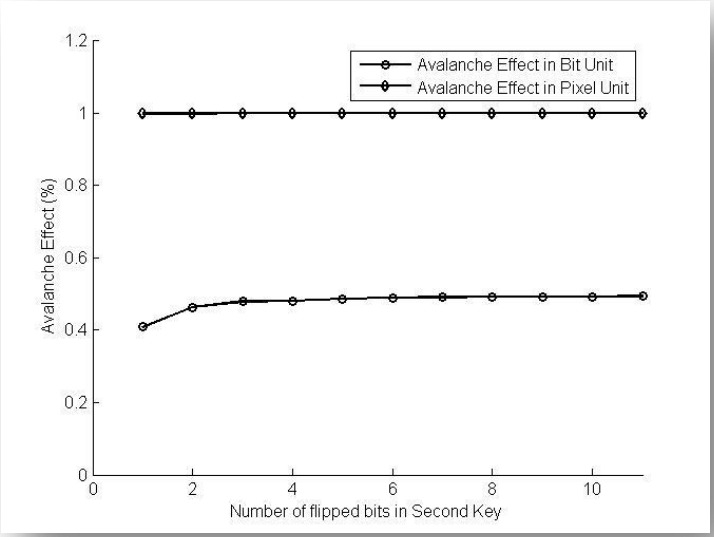


Fig 5.5: Avalanche effect with some bits in the second phase key gets inverted with input grayscale image

These results also mean that image cipher based hash function has good bit independence characteristics.

TABLE 4: Avalanche Effect

		Change Bit in		
	No of changed bits *n*	Plain Text	First Phase Key	Second Phase Key
Avalanche Effect	1	0.4260	0.4328	0.4093
	5	0.4814	0.4813	0.4642
	10	0.4854	0.4868	0.4798
	15	0.4850	0.4894	0.4804
	20	0.4908	0.4923	0.4872
	25	0.4908	0.4924	0.4896
	30	0.4900	0.4922	0.4911
	35	0.4937	0.4936	0.4931
	40	0.4925	0.4945	0.4927
	45	0.4926	0.4945	0.4933
	50	0.4931	0.4948	0.4935

The statistical analysis is shown in table 4. All the avalanche value with changes in plaintext, first key and second key for image cipher based hash function has been stored in this table. These results can be compared to the DRPE output value and it will give better avalanche result than DRPE [5].

5.2.3 Compression Rate

In image authentication, compression is an important factor. In this case, to find the compression rate of image cipher based hash algorithm, entropy is being used as the compression ratio measurement parameter. Entropy is a statistical measurement of randomness that can be used to characterize the texture of the input image [39]. The entropy is expressed as,

$$E = -\sum\{P.log_2 P\}\ldots.. (9)$$

Here, E denotes the entropy and P is the probability massive function. Having a smaller entropy means the image is more compressed.

In the experiment the entropy of the original image and image cipher based hash function is 0.1803 and 0.0458 respectively. As a result we can clearly say that the image cipher based hash function is quite compressed in compare to the original image.

5.2.4Authentication

As previously discussed, there are two types of cross correlation. These are linear cross correlation and non-linear cross correlation. Both are evaluated using true and false class of image to validate the discrimination property of the proposed algorithm. Fig 5.6 shows output of linear cross correlation of the image cipher based hash for the original image with the image cipher based hash for the true and false class image. In this case of true class image, the random phase keys for DRPE are same for the original image and true class image. In the other hand, for false class image; we had to generate two new random phase keys for DRPE. We kept the value of k as 0.3.

Fig 5.7 shows maximum non-linear cross correlation values between the image cipher based hash function for the original image and the image cipher based hash function for the true and false class image. Comparing the true class image maximum non-linear cross correlation has been achieved. We note that the proposed method can appropriately distinguish between true class and false class image. However, the number of photons at least has to be 10^4 or higher for a satisfactory output.

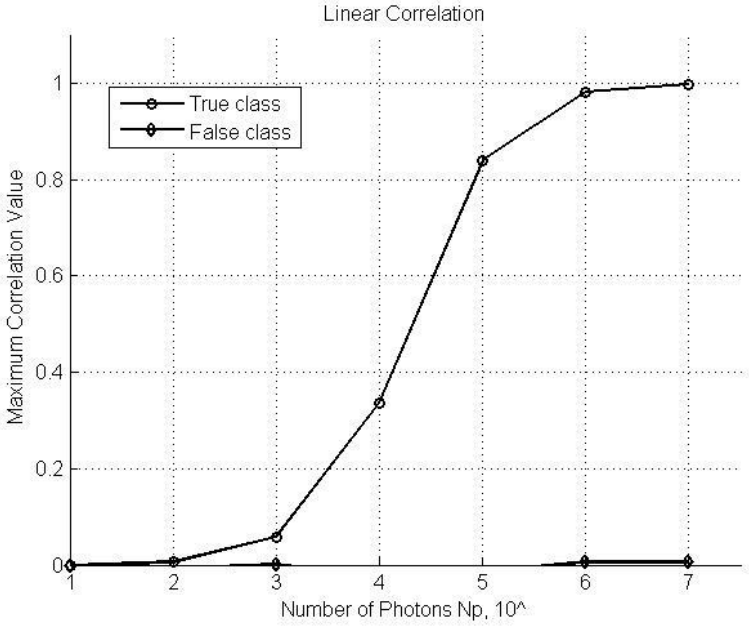


Fig 5.6: Linear correlation values between image cipher based hash image and reference image

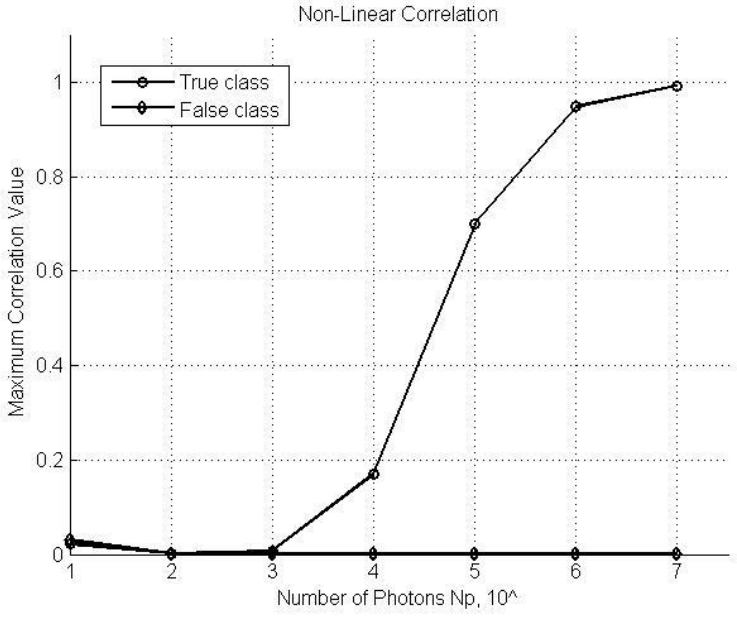


Fig 5.7: Non-linear correlation values between image cipher based hash image and reference image

5.2.5 Comparison with Conventional Hash Functions

For comparing the proposed method with the conventional hash functions, we used an image of 64×64pixels. Each pixel is consisting of 8bit which gives 512bit in one row. Consider 512bit as a block, we evaluated the following results. Here to be noticed that, the non-linear correlation is used to verify an image whether it is a false class image or a true class. Usually, in the case of false class image we get result closer to zero. However, in our case the result is 0.7 which means it can be easily differentiated from the false class image as true class image. As a result we can consider 0.7 as 1.

Table 5: Comparison between different hash function algorithm

Algorithm	SHA-1	MD5	Image Hash ($\boldsymbol{No.of\ photons10^{3.5}}$)
Input (bit)	512×64	512×64	512×64
Output (bit)	160×64≅ 10K	128×64≅8k	$10^{3.5} + 2 \times 10^{3.5}$ ≅ 9.5k
Non-linear Correlation	1	1	0.7
No of hash value needed for one collision	2^{81}	2^{65}	2^{16384}

CHAPTER 6

CONCLUSION

A new hash function based on image cipher is an effective tool for image encryption and authentication and can be used as new algorithm of hash function. It has better performance than conventional hash function as easy implementation. So we can use it for authenticating image through non secure channel. It can be added as another new technique for hash function along with dedicated hash functions and block-cipher hash functions. Since images are frame data so it is easier to encrypt it using this method rather than using block cipher hash function. The numerical results prove that it is a novel technique for hashing along with better collision resistance and compression. This technique should be widely accepted as hash function algorithm as should be used in real life implementation.

BIBLIOGRAPHY

[1] Understanding Cryptography by Cristof Paar and Jan Pelzl

[2] Adam Markman, “Optical Security using Double Random Phase Encryption with Photon Counting”

[3] T. Nomura and B. Javidi, “Optical encryption using a joint transform cor-relator architecture,” Opt. Eng.39, 2031–2035 (2000).

[4] E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double random- phase encrypted images," Opt. Lett. 36, 22-24 (2011).

[5] I. Moon, F. Yi, Y. H. Lee, B. Javidi, “Avalanche and bit independence characteristics of double random phase encoding in the” J. Opt. Spc. Am. A; Vol 31 No 5; May 2014

[6] Y. Qin & Q.Gong & A. Wang, “Image encoding and watermarking in the double random phase encoding scheme with sparse representation strategy” J Opt (January–March 2015) 44(1):45–52; DOI 10.1007/s12596-014-0226-5

[7] E. Pérez-Cabré, M. Cho, and B. Javidi, “Information authentication using photon- counting double-random-phase encrypted images” OPTICS LETTERS / Vol. 36, No. 1 / January 1, 2011

[8] Pérez-Cabré, E.; Abril, H.; Millán, M.; Javidi, B. Photon-counting double-random-phase encoding for secure image verification and retrieval. *J. Opt.* **2012**, *14*, 094001.

[9] F. Yi 1, I. Moon , and Y. H. Lee, "A Multispectral Photon-Counting Double Random Phase Encoding Scheme for Image Authentication" Sensors 2014, 14, 8877-8894; doi:10.3390/s140508877

[10] S. M. Seyedzade, R. E. Atani, S. Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Hash Function" 2010 IEEE

[11] Adil Haouzia & Rita Noumeir, "Methods for image authentication: a survey"; Multimed Tools Appl (2008) 39:1–46

[12] Zhang, Y.; Wang, B.; Dong, Z. Enhancement of image hiding by exchanging two phase masks. *J. Opt. A Pure Appl. Opt.* **2009**, *11*, 125406.

[13] Réfrégier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769.

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

[15] Monaghan, D.; Gopinathan, U.; Situ, G.; Naughton, T.; Sheridan, J. Statistical investigation of the double random phase encoding technique. *JOSA A* 2009, *26*, 2033–2042.

[16] Millán García-varela, M.S.; Pérez-Cabré, E. Optical data encryption. In *Optical and Digital Image Processing: Fundamentals and Applications*; John Wiley & Sons: New York, NY, USA, 2011; pp. 739–767.

[17]Alfalou, A.; Brosseau, C. Optical image compression and encryption methods. *Adv. Opt. Photon.* 2009, *1*, 589–636.

[18] Javidi, B. Nonlinear joint power spectrum based optical correlation. *Appl. Opt.* 1989, *28* 2358–2367.

[19] Cho, M.; Javidi, B. Three-dimensional photon counting double-random-phase encryption. *Opt. Lett*. 2013, *38*, 3198–3201.

[20] Moon, I.; Javidi, B. Three dimensional imaging and recognition using truncated photon counting model and parametric maximum likelihood estimator. *Opt. Express* 2009, *17*, 15709–15715.

[21] Moon, I.; Javidi, B. Three-dimensional recognition of photon-starved events using computational integral imaging and statistical sampling. *Opt. Lett*. 2009, *34*, 731–733.

[22] Goodman J W 2000 Statistical Optics (New York: Wiley)

[23] Refregier P and Javidi B 1995 Optical image encryption based on input plane and Fourier plane random encoding Opt. Lett. 20 767–9

[24] Wolfgang RB, Delp EJ (1997) Techniques for watermarking digital imagery: further studies. In: Proceedings of the international conference on imaging science, systems, and technology, vol 1. Las Vegas, Nevada, USA, pp 279–287

[25] Schneider M, Chang SF (1996) A robust content based digital signature for image authentication. IEEE International conference on image processing, Lausanne, Switzerland

[26] Wolfgang RB, Delp EJ (1996) A watermark for digital images. In: Proceedings of the IEEE international conference on image processing, vol 3, pp 219–222

[27] Yeung M, Mintzer F (1997) An invisible watermarking technique for image verification. In: Proceedings of the ICIP‘97, Santa Barbara, CA

[28] R. L. Rivest, “The MD4 message-digest algorithm”, proceeding of Crypto’90, LNCS 537, (1991), pp. 303- 311.

[29] Federal Information Processing Standard (FIPS) Publication 180-2, Secure Hash Standard (SHS), U.S. Doc/NIST, Available from *http://csrc.nist.gov/publications/fips/fips180-2/fips 180-2.pdf*.

[30] J. Daemen, R. Govaerts and J. Vandewalle, “A Framework for the Design of One-Way Hash Functions Including Cryptanalysis of Damgard’s One-Way Function Based on a Cellular Automaton”, proceeding of Asiacrypto’91, LNCS 739, (1993), pp. 82-96.

[31] I. B. Damgarrd, “A Design Principle for Hash Functions”, proceeding of Crypto’89, LNCS 435, (1989), pp. 416-442.

[32] Mohammad A. AlAhmad , Imad Fakhri Alshaikhli, “Broad View of Cryptographic Hash Functions” IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013

[33] Milan Tuba , Nadezda Stanarevic , Perica Strbac , Jasmina Novakovic, “Impact of Hash function non-uniformity on digital signature security.” Novi Sad J. Math. Vol. 38, No. 3, 2008, 201-208

[34] B. Javidi, G. Zhang, J. Li, Encrypted optical memory using double random phase encoding. Appl. Opt. 36, 1054–1058 (1997)

[35] X. Peng, P. Zhang, H.Wei, B. Yu, Known-plaintext attack on optical encryption based on double random phase keys. Opt. Lett. 31, 1044– 1046 (2006)

[36] X. Peng, H. Wei, P. Zhang, Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. Opt. Lett. 31, 3261–3263 (2006)

[37] Morris G M 1984 Scene matching using photon-limited images J. Opt. Soc. Am. A 1

[38] Tavakoli B, Javidi B and Watson E 2008 Three-dimensional visualization by photon counting computational integral imaging Opt. Express 16

[39] Theory of data compression. Available from: *http://www.data-compression.com/theory.shtml*

ACKNOWLEDGEMENTS

I am using this opportunity to express my gratitude to everyone who supported me throughout the journey of my master's degree. There were so many meaningful moments I cannot forget and so many people I have to thank.

At first and at most I want to thank my great supervisor Professor Inkyu Moon. He is an extraordinary human being who can guide a student with patience and perseverance. Without his consistent and illuminating instruction, this dissertation could not have reached its present form. In addition, Prof. Moon often helped me buy the air ticket when I went back to China for Chinese New Year. Most importantly, Prof. Moon trusts me very much, which lets me feel free to do any researches. He is also concerned about my future and supports me to do any programs that are beneficial to my future.

I am greatly indebted to my parents, Md. Ishaque Ali and Flora Nasrin Ali, who are the greatest persons in my heart. Their unconditional love and encouragement have always been the invariants of my life. I also give my thanks to my only brother Sabbir Hasan who hasshared uncountable hours of laughter and joy with me. I feel grateful to all the professors at Chosun University who once offered me valuable courses and advice during my study. These professors include Prof. Moon Inkyu, Prof. Lee Sangwoong, Prof. Kwon Gu Rak, Prof. Cho Beomjoon, Prof. Shin Seok Ju, Prof Chung Hyun Sook. I also wish to thank my colleagues who made my experience a joyful one. These colleagues consist of 정유선, Yi Faliu, Han Minggu, We Jonggob, Keyvan, Samaneh, Nishat Sultana and Ayesha Akhter Lata. Senior colleague Yi Faliu is like my brother and helps me every time I face a problem.

My gratitude also extends to my friends, who are a great support for me in Korea,

especially, Ashik Rahman Ruso who helped me in every step during my dissertation writing. It is they who let me know Korea better and make my spare time rich and colorful. I will never forget the happy time we spent together in Korea. I also want to express my thanks to my undergrad super visor and the mentor of my life who showed me to aim a higher goal in my life.

Last but not the least; nothing was possible without the command of Allah. He showed me the path to success and I am walking on that path. In brief, I deeply appreciate all of the professors, relatives, colleagues, and friends who have helped me a lot. I sincerely wish them all the best in their lives.