February 2015

Master's Degree Thesis

# Image authentication algorithm via photon-counting double random phase encoding

Graduate School of Chosun University

Department of Computer Engineering

Han Min Gu

# Image authentication algorithm via photon-counting double random phase encoding

광자계수 이중랜덤위상부호화 기반
영상 인증 알고리즘 연구

February 2015

Graduate School of Chosun University

Department of Computer Engineering

Han Min Gu

# Image authentication algorithm via photon-counting double random phase encoding

Advisor : Dr. Inkyu Moon

A thesis submitted in partial fulfillment of
the requirements for Master's degree
February 2015

Graduate School of Chosun University

Department of Computer Engineering

Han Min Gu

# 한민구의 석사학위논문을 인준함

위 원 장 조선대학교 교수 이 상 웅 (인)

위 원 조선대학교 교수 양 희 덕 (인)

위 원 조선대학교 교수 문 인 규 (인)

2014년 11월

조선대학교 대학원

# Contents

# List of Figures

# List of Tables

# 한글요약

## 광자계수 이중랜덤위상부호화 기반 영상 인증 알고리즘 연구

한민구
지도교수 : 문인규
컴퓨터공학과
대학원, 조선대학교

푸리에 변환 도메인을 기반으로 하는 광학 이미지 암호화 시스템(즉, 이중 임의위상 암호화,DRPE)은 불법 침입자의 알려진 암호문 공격에 대해서 약점을 가지고 있다. 최근에 이진 이미지의 광자 계수 이미징(PCI) 기술과 이중 임의위상 암호화(DRPE)의 통합이 제안되었고 그 결과는 불법 침입자의 공격에 대한 정보 인증에 강점을 가지고 있다. 그러나 여전히 키 관리와 분배의 문제 등과 같은 취약점들을 가지고 있다. 이 논문에서, 우리는 더욱 보안이 강화된 정보의 인증을 위해서 대칭키 기반 암호화 기술과 공개키 기반 암호화 기술이 조합된 암호화 기술과 광자 계수 이미징 기술의 통합을 제안했다. 제안된 기법을 위해서 기본 이미지가 이중 임의위상 암호화 기술로 암호화된다. 이 절차에서 두 번째 랜덤 페이즈 마스크 키가 RSA로 암호화된다. 그 후에 암호화된 데이터인 복소수 정보가 광자 계수 이미징 시스템에 입력된다. 마지막으로 정수화된 결과가 다시 RSA알고리즘으로 암호화된다. 인증을 위한 과정에서 암호화된 이미지는 RSA에 대해서 다시 복호화된다. 복호화된 이미지는 원래의 기본이미지와 전혀 비슷하지 않으므로 공격자는 원래의 기본이미지를 전혀 예측할 수 없다. 인증을 시도

할 때 새로운 이미지가 입력되고 기본이미지와 같은 암호화 및 복호화 절차를 거친 후 저장된 기본이미지와 비교한다. 우리는 이 때 비선형 상관계수를 이용하여 각각 암호화되고 복호화된 기본이미지와 입력된 이미지가 통계적으로 비슷함을 이용하여 인증하는 방법을 제안한다. 우리는 차별화된 측정방법을 사용하여 차별화된 결과를 보여줄 것이다. 실험의 결과는 암호화된 더 적은 양의 데이터가 원래의 정보와 같다는 것을 인증하기에 충분하다는 것을 증명할 것이다. 우리는 이 제안을 통하여 더 좋은 영상 인증 시스템을 얻을 수 있을 것이다.

# 1. Introduction

Since Refrégier and Javidi proposed the method of double random phase encoding(DRPE), research interest based on optical cryptography has been increased [1]. This is due to the excellent performance of optical encryption system regarding parallel processing and high-freedom encoding. The original DRPE is conducted on Fourier domain. Later, DRPE technique has been extended to other domains such as Fresnel domain. However recently, Carnicer et al have proved the weakness of DRPE to chosen cipher attacks. They demonstrated that decryption random key could be reproduced by an unauthorized user who has repeated access.

Photon-counting imaging(PCI) technique is not a cryptography algorithm. It can obtain image at a low light level. Usually, the photon-counting image cannot be visually recognized, especially under a low light level. Thus, the cryptography system can be enhanced when the PCI technique is introduced and integrated. In addition, PCI algorithm has the advantage of reducing the data size which will be helpful for the data transmission on the internet channel. However PCI result cannot be reconstructed perfectly. In other words integration encryption system including PCI cannot be decrypted to original information.

Nevertheless Perez et al have demonstrated the robustness against intruder attacks by integration system of photon-counting imaging technique to the conventional double random phase encryption. Since photon-counting encrypted information is kept for decryption process, reconstructed information look different with original information.

However most of the optical cryptosystems are developed by symmetric cryptosystem likes DRPE, in which the same keys are used for process of encryption and decryption. Consequently, the symmetric optical encryption would lead to security problems regarding key management and distribution.

On the contrary, public-key cryptography such as RSA is asymmetric algorithm that uses two separate keys consisting of private key and public key. The asymmetric system can reduce the security problem existed in symmetric system.

Also, it is possible for the public key system to achieve personal authentication and safe key distribution. Even though, the asymmetric algorithm has weakness in terms of long execution time, especially, when a large size of data need to be processed. Still we can use RSA to exchange the keys used in DRPE in order to solve key distribution problem.

In this thesis, we propose an authentication method from alternative hybrid optical cryptosystem, which combines photon counting DRPE and RSA. As a result, the security of this system is improved compared with that by only using any one of the techniques.

## 2. Photon Counting Imaging

Photon-counting imaging in which an especial class of optical imaging technique has been implemented in areas such as 3D optical imaging and 2D/3D object identification in photon limited dark situations. Photon-counting imaging systems are designed for optical processing of low light levels(condition of unique photon) or night vision, situations in which a limited quantity of photons reach the image sensors. Monochromatic photon counting imaging could be accomplished by allowing only a limited quantity of incident photons to the captured image scene. This scheme includes the estimation that the probability of counted photons number where any arbitrary pixels in a utilized image follows a Poisson distribution.

To generate the photon counted image from gray image on computer, the gray image is normalized and multiplied with the number of photons. The resultant values would follow Poisson distribution. Thus, a new photon-counted image can be achieved by using the following equation (1) :

$$C_w(x,y) = Poisson(\lambda_w = f_w(x,y) \times N_p) \qquad (1)$$

Here, $N_p$ is the number of photon and Poisson means Poisson distribution.[18]

$$f_w(x,y) = \frac{f_w(x,y)}{\sum_{x=1}^{M}\sum_{y=1}^{N} f(x,y)} \qquad (2)$$

where $f(x,y)$ is the input gray image, and M and N are total number of pixels in input gray image in the x and y directions. In this process, data which have very small values are discarded by high pass filter. Then, the photon-limited image $f_{ph}(x,y,w)$ is obtained as follows :

$$f_{ph}(x,y,w) = Poissrnd(\lambda_w(x,y) = N_P \times f_w(x,y)) \quad (3)$$

where the function Poissrnd( ) generate arbitrary numbers from the Poisson distribution with regard to Poisson parameter $\lambda_w(x,y)$[28]

# 3. Double Random Phase Encryption

Optical and digital information security system based on double random phase encryption (DRPE) technique had shown predominant role in information security. According to DRPE principle, the primary image $f(x,y)$ which expresses spatial coordinates of a two dimensional signal or a 2D image, is being encrypted as static white noise using two random phase masks. which does not leak to manufacture or disclose any content of the original image. The random phase masks(RPMs) of spatial and frequency domain, $\exp[i2\pi p(x,y)]$ and $\exp[i2\pi b(\mu,\eta)]$ respectively, are statistically independent and uniformly distributed over [0,2π], The decryption procedure is the reverse process of encryption process.

In our experiment, the input image is used for encryption and the procedure is defined as follows; first, the original images are multiplied with spatial phase mask p(x,y) and transform into frequency domain (i.e., Fourier transform) subsequently. Later, the transformed image are multiplied with frequency domain phase mask $b(\mu,\eta)$. Eventually, an inverse Fourier transform is performed to get encryption result. In general, the encrypted data are complex-amplitude and white noise. Mathematically this process can be defined as follows equation (4).

$$\begin{aligned} R_w(\mu,\eta) &= FFT(f_w(x,y) \bullet p(x,y)) \\ en_w(x,y) &= IFFT(R_w(\mu,\eta) \bullet b(\mu,\eta)) \end{aligned} \quad (4)$$

where, FFT and IFFT represent the Fourier transform and inverse Fourier transform respectively, and the term $en_w(x,y)$ denotes the encrypted image. The

same values of spatial and Fourier phase masks are used in all process. Following Figure. 1. represent encryption process of DRPE system.

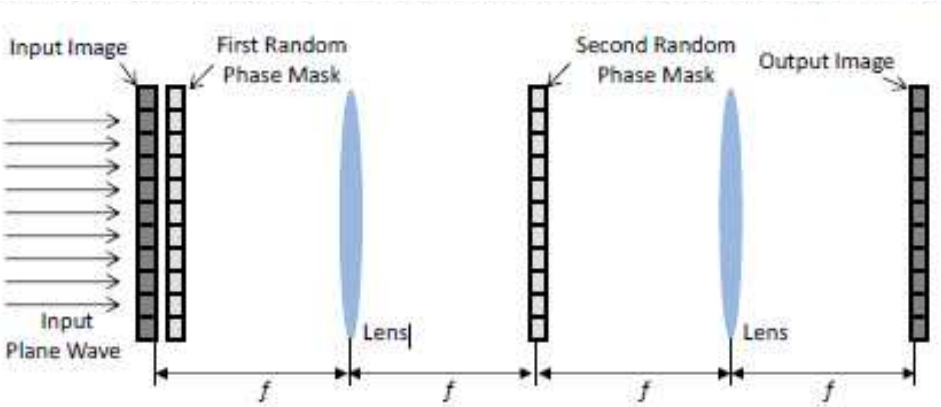



Figure. 1. Schematic diagram of the DRPE system
(f is focal length of the lens)

In order to decrypt the original channels, the inverse procedure of encryption process need to be used . At first, the encrypted images are transformed to Fourier domain and then the result of Fourier transform multiplied with inverse Fourier masks. After that, inverse Fourier transform is performed. Lastly, the resultant image multiplied with inverse spatial phase mask in order to generate the decrypted image. It can be mathematically represented as follows :

$$R_w(\mu,\eta) = FFT(en_w(x,y) \bullet b^*(x,y))$$
$$f_w(x,y) = IFFT(R_w(\mu,\eta) \bullet p^*(\mu,\eta)) \quad (5)$$

where '*' symbol denotes complex conjugate operation. It is been proven that, knowing phase masks are useful for decrypting the original information. Thus DRPE technique can leads to a good reconstruction result of an input image. However, some researchers have substantiated the weakness against known and chosen cipher-text attacks about implementation of DRPE techniques on digital signal processing

This consequence of research brings the necessity to find a specialized solution in order to improve the security of an encrypted result. Enough new

methods have been proposed recently, among them, the integration of PCI and DRPE based on binary images have proven the robustness against previous attacks by providing double process of protection.

# 4. RSA

RSA algorithm was developed by Ron Rivest, Adi Shamir, and Len Adleman at MIT in 1977, and first published in 1978. The Rivest-Shamir-Adleman(RSA) scheme has been utilized to general purpose approach to public key encryption.

On the contrary to symmetric cryptosystems, where the key for encryption and the key for decryption are same secret key or same session key; an asymmetric cryptosystem has two keys which are referred to as the public key KU and the private key KR, individually. A simple framework of an asymmetric cryptosystem using this pair of keys can be briefly stated as follows:

the message X in the source A is intended for the destination B where the receiver has generated a pair of keys: a public key $KU_b$ and a private key $KR_b$. During the communication between A and B, the sender A uses $KU_b$ to encrypt message X to create a cipher-text Y and the receiver B decrypts the cipher-text with the private key $KR_b$ to recover the message X. In this framework of an asymmetric cryptosystem, even if an opponent can intercept the cipher-text Y and is able to obtain the public key KUb, he is still unable to discover the private key $KR_b$. Attempting to recover X and KRb, the opponent has to generate two estimates $\hat{X}$ and $\widehat{KR_b}$.

The RSA algorithm was proposed as an asymmetric cryptographic technique. The invention of the RSA was based on the fact that the factorization of integers into their prime factors would be very difficult and it is now widely used in asymmetric cryptosystems.

$$n = p \times q \tag{6}$$

As like this equation (6), if we knows p and q, n has found easily. Contrastively if we knows n just only, it is difficult to guess the n.

The implementation of the RSA algorithm is simply summarized as follows and then more detailed descriptions can be found in the procedure part.

•. Key generation:

* Select two random prime numbers p and q;
* Calculate N = p × q, let $\phi$ = (p −. 1)(q −. 1);
* Select an integer e which satisfies 1 < e < $\phi$
  and relatively prime to (gcd($\phi$, e) = 1),
  where the operator 'gcd' denotes greatest common divisor operation
* Determine d such that ed = 1 mod ($\phi$), where the
  operator ''mod'' denotes the modular operation;
* N and e make up the public key, $KU_b$ = {e, N};
* d and N make up the private key $KR_b$ = {d, N};
* p and q are discarded.

•. Encryption: the encryption rule is

$$C = M^e (\mathrm{mod}\ N)\ (M < N), \qquad (7)$$

•. Decryption: the decryption rule is

$$M = C^d (\mathrm{mod}\ N). \qquad (8)$$

Among two keys, one key is used for encryption, the other key is used for decryption. this fact takes advantage of other cryptographic methods as digital signature or key distribution. In digital signature case, A generates a message for B and encrypts by private key of A. B can decrypt the message using public key of A. Because the message was encrypted by private key of A, only A could prepare the message. So cipher message provides digital signature. In key distribution case, A makes a message and encrypts by symmetric cryptography algorithm. And A encrypts symmetric secret key of symmetric cryptography algorithm using public key of B. A transmits the cipher message and encrypted secret key to B. B can decrypt message after decrypt secret key from private key of B.

# 5. Proposed integration approach

## 5.1 DRPE + RSA

Suppose that the source A utilizes two RPMs ψ1 and ψ2 to encrypt an image in the Fourier domain. ψ1 and ψ2 are generated same size with plain image and used as secret keys. The first RPM ψ1 is white noise and uniformly distributed in an interval [0, 1], however the second RPM ψ2 has a decisive effect on DRPE cryptosystem. Because of that, ψ2 needs to be encrypted and decrypted by the RSA algorithm and RSA algorithm only works for integers, the distribution of the second RPM ψ2 is uniformly quantized to the integers 0–9. it is possible to quantize to other integer ranges, such as 0–63, 0–127, etc. However, in this thesis, we just utilize the range of 0–9 as an example, to confirm the proposed method. The complex amplitudes of the two RPMs can be expressed as exp(i2π ψ1) and exp(i0.2πψ2).[27] Generally the first RPM ψ1 and second RPM ψ2 are multiplied with 2π, however range of ψ2 is decuple number than original range. So we multiply with 0.2π and ψ2 to make same interval data. DRPE process can be mathematically represented as follows :

$$U(x,y) = iFFT(FFT(f(x_0,y_0)\exp[i2\pi\psi_1(x_0,y_0)]) \times \exp[i0.2\pi\psi_2(x_t,y_t)]) \quad (9)$$

On the other hand, ψ2 is encrypted using RSA public key. Because a pixel value of second RPM ψ2 has digit, in each row of the ψ2 are regrouped with 4digits to achieve better performance to encryption process. ψ2 is stored in an encrypted state and it is decrypted when user encrypts image again for authentication. Figure. 2. represent RSA encryption and decryption process of second RPM ψ2.

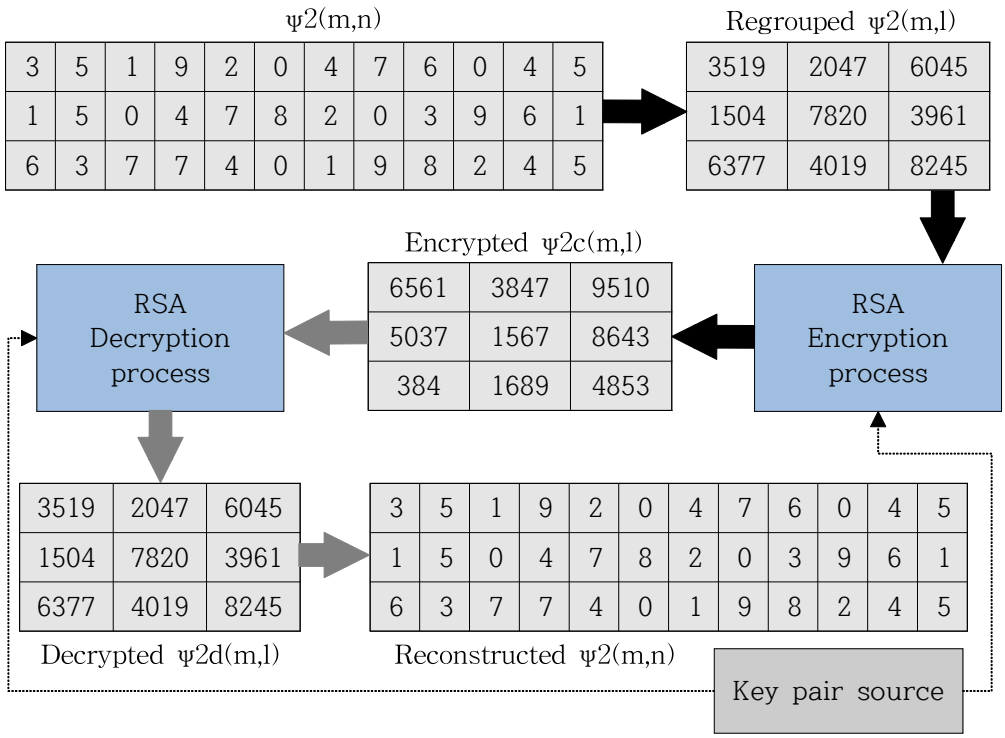



Figure. 2. RSA Example of Second RPM ψ2

## 5.2 DRPE + PCI and Quantization

The each pixel value of encrypted image by DRPE would be a complex number including amplitude value and phase angle information. Since the phase angle information should be used in the authentication process with amplitude together, they cannot all be discarded and be processed separately. If they do not exist, it would be impossible to generate the information of the image which used for authentication. In this procedure, the photon-counting technique is only applied to the amplitude image A(x,y) obtained from DRPE. Amplitude image A(x,y) are photon-counted individually. PCI technique makes the pixel values of low data in A(x,y) to zero using high pass filter, and we only keep the phase

angle information for pixels with non-zero amplitude value. This encrypted image is performed normalization over the sum of all data of encrypted image. The last procedure of PCI is Poisson distribution and the result value of Poisson distribution is integer of an interval [0,∞]. So PCI result is quantized result of amplitude information and that result can be used for RSA encryption. In addition That result data will be rarely distributed and it can be appropriate for data compression, which means to reduce the data size needed for data encryption by RSA algorithm. The other words performance time of RSA will decrease.

In quantization procedure, phase angle information P(x,y) of DRPE result has radian value about range of [-π,π]. If we focus on image encryption and decryption, we should keep phase angle information intact. However we will uniformly quantize and encrypt the data, because authentication does not need decryption process and we need to protect the phase information. The number of bits for quantization decides quantized integer range. i.e. for an one bit quantization, the range from -π to 0 can be refer to as 1 and range from 0 to π can be refer to as 2. In this thesis we will test about 1bit to 4bit quantization. This procedure is represented in Figure. 3. and Figure. 4.

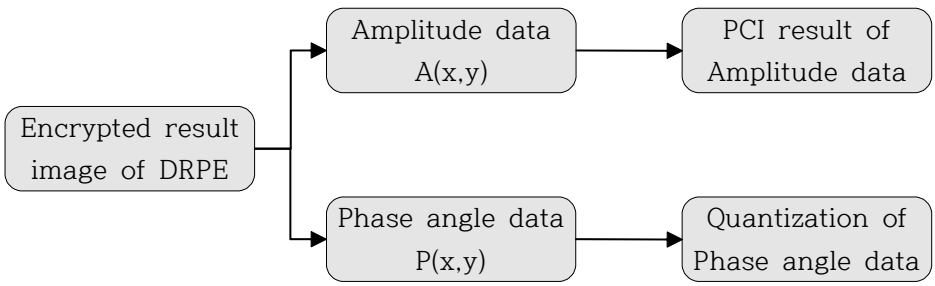



Figure. 3. Flow Chart of DRPE + PCI and Quantization

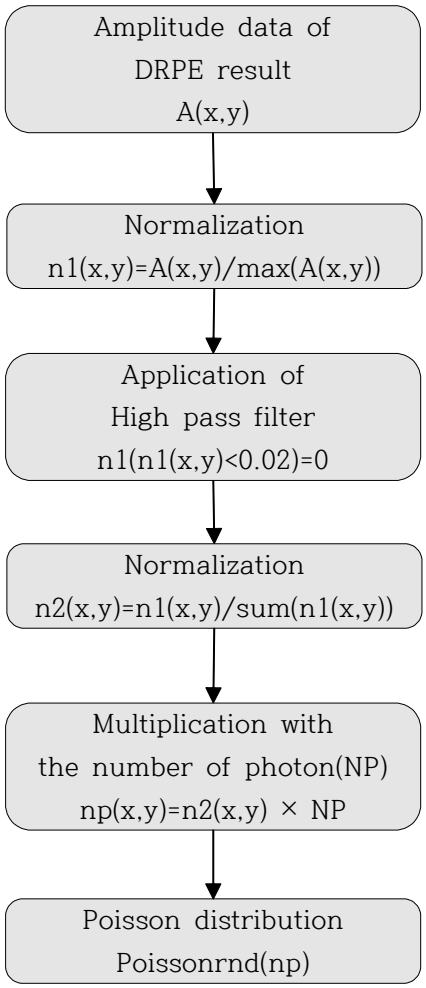
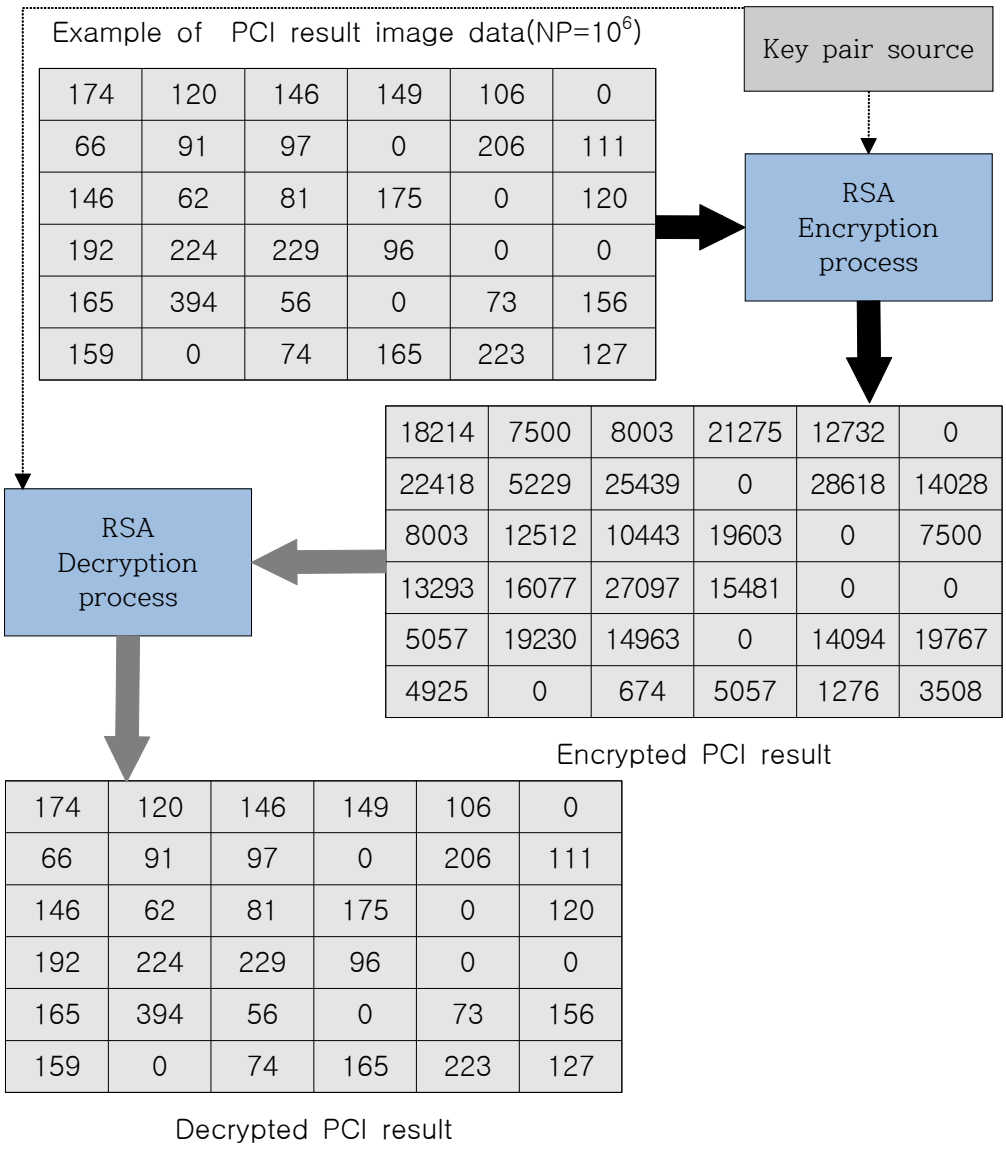



Figure 4. A schematic representation of PCI

## 5.3. RSA

In this cryptosystem, we use two pairs of public key and private key set. One set(KU1, KR1) used for symmetric key distribution as mentioned in DRPE + RSA procedure. They are generated in user level and share public key KU1 at key pair source.

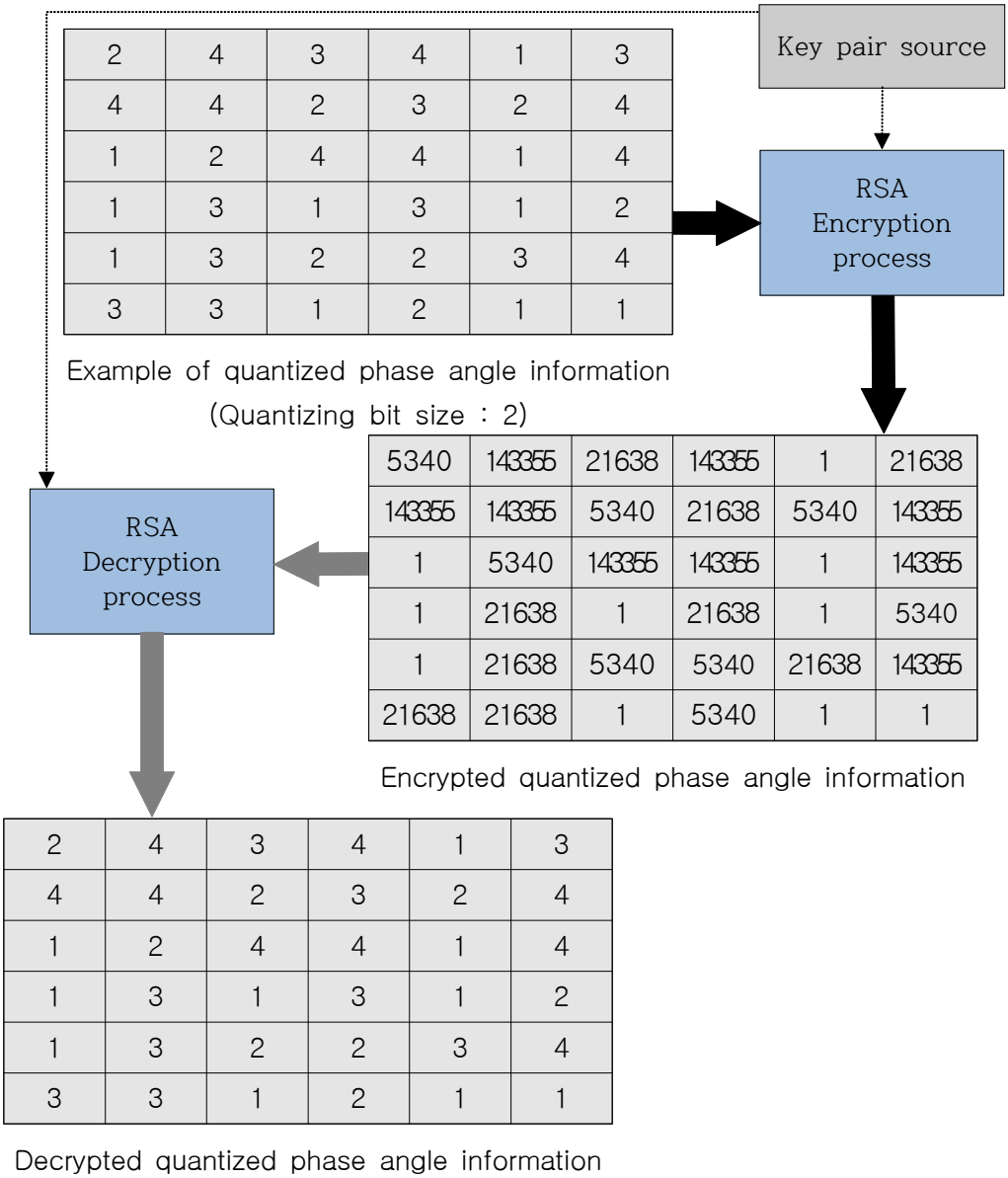



| | | | | | |
|---|---|---|---|---|---|
| 174 | 120 | 146 | 149 | 106 | 0 |
| 66 | 91 | 97 | 0 | 206 | 111 |
| 146 | 62 | 81 | 175 | 0 | 120 |
| 192 | 224 | 229 | 96 | 0 | 0 |
| 165 | 394 | 56 | 0 | 73 | 156 |
| 159 | 0 | 74 | 165 | 223 | 127 |

| | | | | | |
|---|---|---|---|---|---|
| 18214 | 7500 | 8003 | 21275 | 12732 | 0 |
| 22418 | 5229 | 25439 | 0 | 28618 | 14028 |
| 8003 | 12512 | 10443 | 19603 | 0 | 7500 |
| 13293 | 16077 | 27097 | 15481 | 0 | 0 |
| 5057 | 19230 | 14963 | 0 | 14094 | 19767 |
| 4925 | 0 | 674 | 5057 | 1276 | 3508 |

| | | | | | |
|---|---|---|---|---|---|
| 174 | 120 | 146 | 149 | 106 | 0 |
| 66 | 91 | 97 | 0 | 206 | 111 |
| 146 | 62 | 81 | 175 | 0 | 120 |
| 192 | 224 | 229 | 96 | 0 | 0 |
| 165 | 394 | 56 | 0 | 73 | 156 |
| 159 | 0 | 74 | 165 | 223 | 127 |

Figure. 5. Example of RSA using PCI result of amplitude data




| | | | | | |
|---|---|---|---|---|---|
| 2 | 4 | 3 | 4 | 1 | 3 |
| 4 | 4 | 2 | 3 | 2 | 4 |
| 1 | 2 | 4 | 4 | 1 | 4 |
| 1 | 3 | 1 | 3 | 1 | 2 |
| 1 | 3 | 2 | 2 | 3 | 4 |
| 3 | 3 | 1 | 2 | 1 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| 5340 | 143355 | 21638 | 143355 | 1 | 21638 |
| 143355 | 143355 | 5340 | 21638 | 5340 | 143355 |
| 1 | 5340 | 143355 | 143355 | 1 | 143355 |
| 1 | 21638 | 1 | 21638 | 1 | 5340 |
| 1 | 21638 | 5340 | 5340 | 21638 | 143355 |
| 21638 | 21638 | 1 | 5340 | 1 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| 2 | 4 | 3 | 4 | 1 | 3 |
| 4 | 4 | 2 | 3 | 2 | 4 |
| 1 | 2 | 4 | 4 | 1 | 4 |
| 1 | 3 | 1 | 3 | 1 | 2 |
| 1 | 3 | 2 | 2 | 3 | 4 |
| 3 | 3 | 1 | 2 | 1 | 1 |

Figure. 6. Example of RSA using PCI phase angle information

The public key KU1 can be accessed by authorized authentication system and The private key KR1 are saved privately only to user level. Then authentication system utilize the public key KU1 of user to encrypt the secret key(second RPM) as Figure. 2, and transfer to user. The other set(KU2, KR2) is used to encrypt PCI result of amplitude and quantized phase angle. RSA encryption and

decryption process of data of PCI result image are represented by Figure. 5. and quantized phase angle information are represented by Figure. 6. In Figure. 6. case, all quantization result data are less than ten due to quantization bit size of less than four. If quantization bit size is greater than or equal to four, however, some data will be bigger than ten. Because of that, we didn't merge bits in order to RSA encryption same as DRPE secret key. And we mention that we only keep the phase angle information for pixels with non-zero amplitude value, but corresponding phase angle pixels has some values. These values does not have effect on authentication result, because PCI result and phase angle information will be multiplied in authentication procedure. The RSA encryption and decryption process can be shown as :

• Encryption and decryption of second RPM-key :

For simplicity, we have 3 × 12 pixels from the second RPM ψ2 to show the concept of the encryption process illustrated in Figure. 2. First, we generate the integer range of ψ2 of [0, 9] in order to facilitate the encryption. Furthermore, the pixel values in each row of the ψ2 are regrouped with four digits, resulting in a new 3 × 3 matrix ψ2 to obtain a block ciphering. the authentication system can generate a pair of public key and private key with the following procedure :

* p1 = 11, q1 = 9091, N1 = p2×q2 = 100,001
  ϕ1 = (p1 −1)(q1 −1) = 90,900
* e1 = 131, d1 = 71,471
* Public key: KU1 = (e1 N1) = (131 100,001)
  Private key: KR1 = (d1 N1) = (71,471 10,001)

With equation (7), the user utilizes the public key KU1 (e1, N1) to encrypt regrouped ψ2 to obtain an encrypted RPM ψ2c with 3 × 3 pixel matrix. Authentication system receives the encrypted RPM ψ2c and makes use of the private key KR1 (d1, N1) to decrypt it according to equation (8). Result of decrypted RPM ψ2d is converted to 3 × 12 reconstructed ψ2.

• Encryption and decryption of PCI result and quantized phase angle

The pixel values in the PCI are less than 10,000 when NP value is $10^6$. Authentication system should generate N of second RSA key set to bigger than 10,000 for stable encryption and decryption. The authentication system can construct a pair of public-rivate keys with the following procedure :

* p2 = 101, q2 = 123, N2 = p2 × q2 = 12,423
  ϕ2 = (p2 − 1)(q2 − 1) = 12,200
* e2 = 19, d2 = 29,755
* Public key: KU2 = (e2 N2) = (19 12,423)
  Private key: KR2 = (d2 N2) = (29,755 12,423)

With equation (7), the user encrypt both PCI result and quantized phase angle by public key KU2 and transmit to authentication system. The authentication system receive and decrypt by using private key KR2.

# 6. Image Authentication

In this thesis, nonlinear cross-correlation nonlinear cross-correlation cc(x, y) between the encrypted reference image and the encrypted image produced from the input test image for verification is defined as follows[11] :

$$cc(x,y) = \xi^{-1}(|D(\mu,\eta)F(\mu,\eta)|^k \exp[i(\phi_p(\mu,\eta) - \phi_F(\mu,\eta])) \qquad (10)$$

where D(μ,η) and F(μ,η) are 2D Fourier transforms result of the encrypted input image and encrypted reference images, $\phi_D(\mu,\eta)$ and
$\phi_F(\mu,\eta)$ are the phase angle parts of D(μ,η) and F(μ,η), respectively, and parameter k defines the density of the applied nonlinearity. When k is close to

0, the nonlinear cross-correlation equation is the phase extractor leading to improve the high frequency content. When k is 1, the equation decline to a linear filtering method. Different numbers of k produces different cross-correlation values in its train. The appropriate parameter k can be decided with the PCE(best peak-to-correlation energy) value[28], following as :

$$PCE = \frac{\max[|cc(x,y)|^2]}{\sum_{i=1}^{M}\sum_{j=1}^{N}|cc(x_i,y_j)^2|} \qquad (11)$$

where $cc(x_i,y_j)$ is the nonlinear cross-correlation value between the encrypted input image and the encrypted reference image. In addition M and N are the image size along the x and y axes in each. Since PCE is defined as the ratio of the maximum peak cross-correlation result over the total energy of the nonlinear cross-correlation image. If the PCE value close to 1, it is a good nonlinear cross-correlation result.

Procedure of image authentication is as follow :

• Reference image registration class

* Sender and authentication system produces keys respectively.
  Sender : one pair of RSA key set(KU1, KR1)
  Authentication system : Two RPMs (ψ1, ψ2) and the other pair of RSA key set(KU2, KR2)
* Authentication system encrypts second RPM ψ2 and shares with sender.
* Sender encrypts reference image according to hybrid cryptosystem with shared two RPMs and public key KU2.
* Sender transmits encrypted amplitude data and encrypted phase angle to the authentication system.
* The authentication system registers received two encrypted data.

This procedure is represented in Figure. 7.

• Image Authentication class

* Sender encrypts input test image depending on same process of reference image encryption and transmit to the authentication-system.
* The received images are decrypted by RSA with private key KR2.
* Decrypted amplitude data are quantized to binary data. non-zero dataes are convert to 1 in order to better nonlinear-cross-correlation result.
* Result image are generated from multiplication of Decrypted phase-angle information and quantized binary amplitude.
* Same process are performed about registered data set.
* The nonlinear cross-correlation cc(x, y) and PCE are calculated between the two result image.

This procedure is represented in Figure. 8.

In this procedure, each PCI results has little difference because of poissonrnd function, although reference image and input test image are same. However if we utilize same image, PCE value will be close to 1. So we can recognize that same image data are inputed.

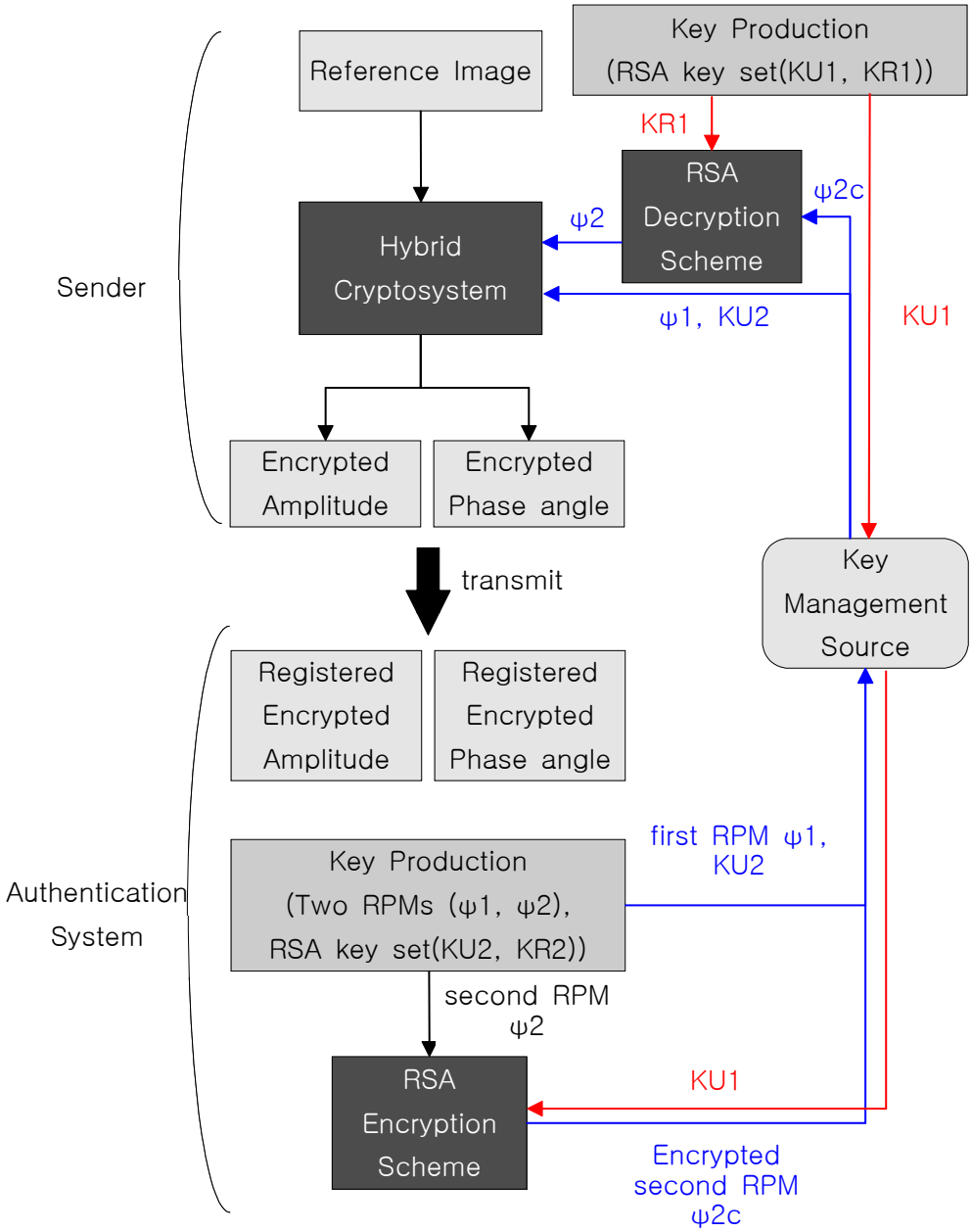



Figure. 7. Reference image registration procedure

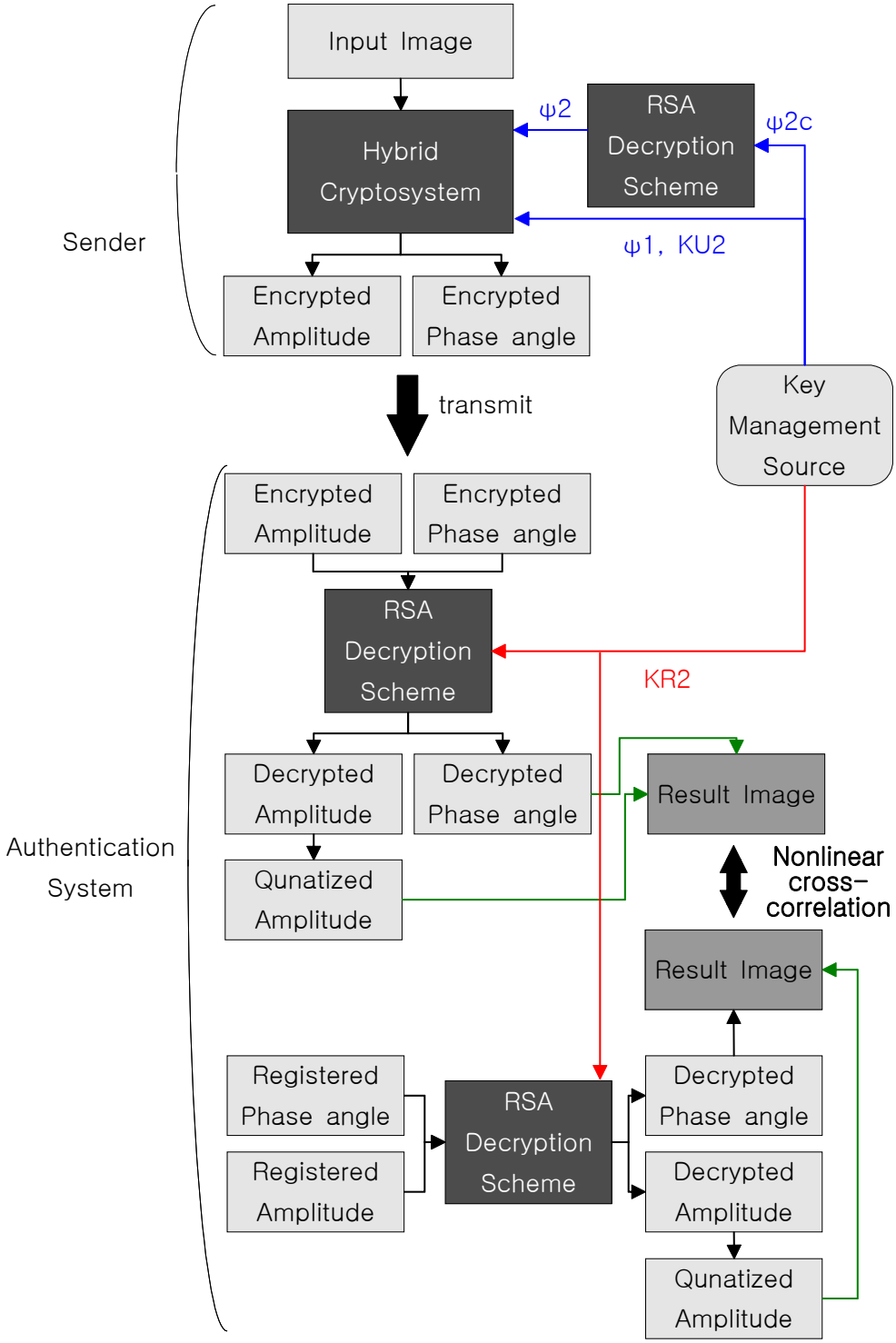



Figure. 8. Image Authentication procedure

# 7. Computer Simulation Results

In this paper, all of the results are obtaind from Matlab (R2013a) that is executed on a 64-bits windows 7 Enterprise OS computer which include an Intel(R) Core(TM) i5-3330 processor of 3.00GHz and the RAM is 4.00GB. All of used images are 100 × 100 pixels 256 grayscale quantization level and all processing data are digitally recorded on computer without optical processing configurations.


Figure. 9. Utilized image in simulation
(a) Lena image for true class; (b) Different woman image for false class

The case of that input image is same with reference image is true class, other case is false class. Images of Figure. 9. are utilized for the computer simulation.

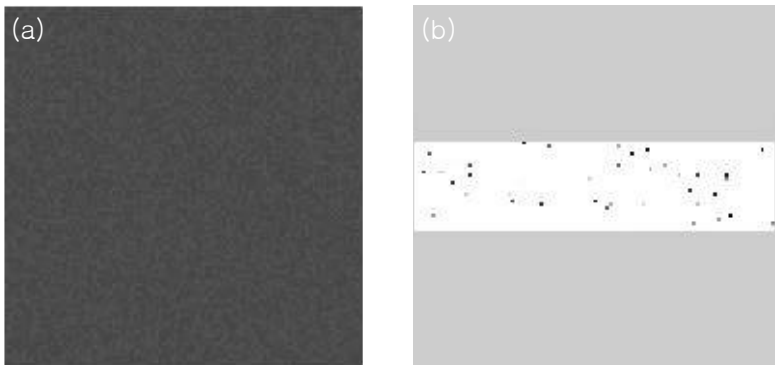


Figure. 10. represent secret key of DRPE and regrouped and encrypted secret key of DRPE. In order to one pixel of 10(b) has four pixel of 10(a), 10(b) image is more bright and small

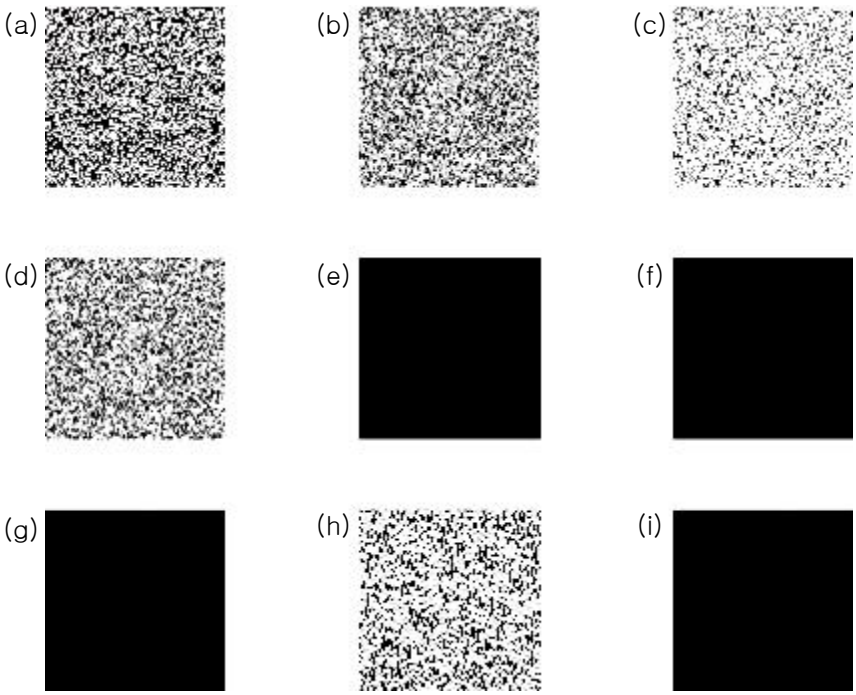



Figure. 11. Reference image processing
(a) DRPE result; (b) PCI result of amplitude; (c) RSA encryption result of (d); (d) RSA decryption result of (c); (e) Quantized amplitude; (f) Result image; (g) Quantized angle; (h) RSA encryption result of (g); (i) RSA decryption result of (h);

where Figure. 11. images of all encryption and decryption process about reference image are represented. images of all process can not visually recognized. 11(c) RSA encryption result of amplitude and 11(h) RSA encryption result of quantized phase angle are registered at authentication, and whenever user want authenticate, 11(f) result image is generated for calculation of nonlinear cross-correlation and PCE.

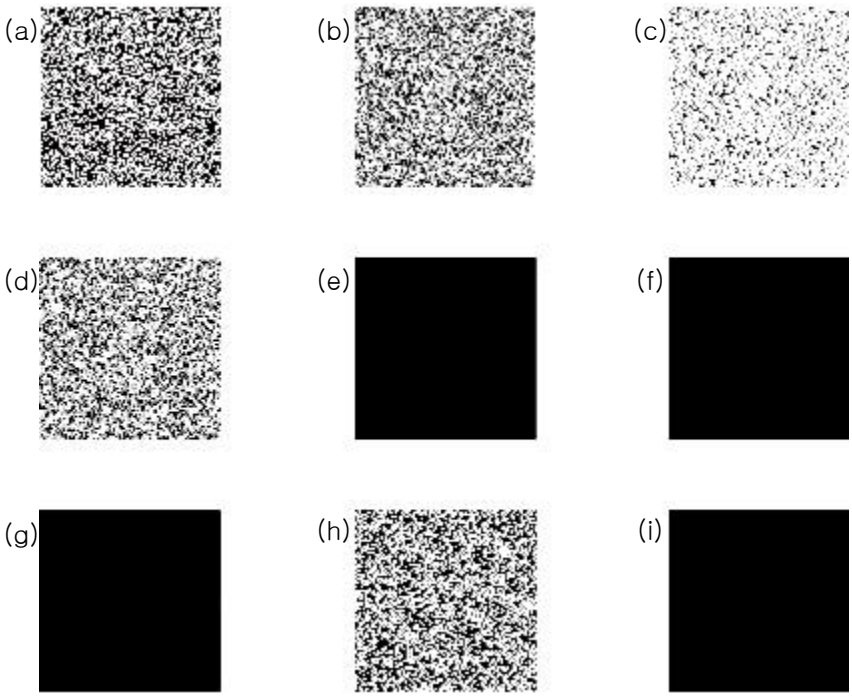



Figure. 12. True class image processing
(a) DRPE result; (b) PCI result of amplitude; (c) RSA encryption result of (d); (d) RSA decryption result of (c); (e) Quantized amplitude; (f) Result image; (g) Quantized angle; (h) RSA encryption result of (g); (i) RSA decryption result of (h);

Figure. 12. and Figure. 13. show us true class image processing and false class image processing. They look similar. True class means that input image is same with reference image. In this class, system grants authentication to user. False class means that input image is different with reference image. And system does not allow access to user.

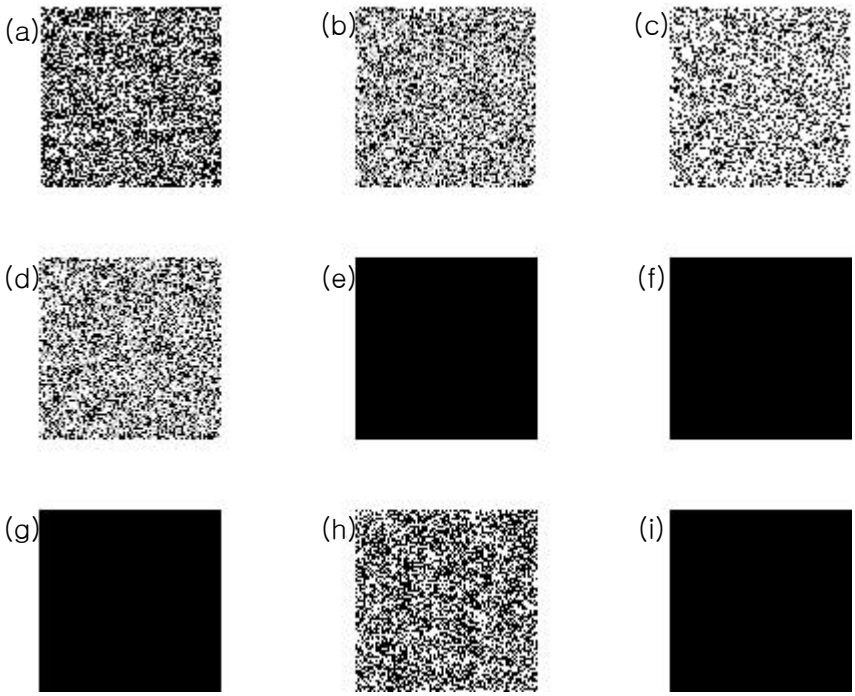



Figure. 13. False class image processing
(a) DRPE result; (b) PCI result of amplitude; (c) RSA encryption result of (d); (d) RSA decryption result of (c); (e) Quantized amplitude; (f) Result image; (g) Quantized angle; (h) RSA encryption result of (g); (i) RSA decryption result of (h);

Figure. 14. show us PCE value with various k value where quantization bit size is 2bit. PCE values are given against change of the expected number of photons for different parameters k, using resultant image of reference and resultant image of input test images. We realize, from Figure 14(a), that PCE values increase with an increasing in the number of photons. Especially, when parameter k is within a range from 0.0 to 0.3, good PCE values are obtained for true-class images. Consequently, k = 0.0 or k = 0.1 can selected for best result of simulations. It is also confirmed that the number of photon Np=10^4 is the watershed to achieve a better nonlinear correlation plane.

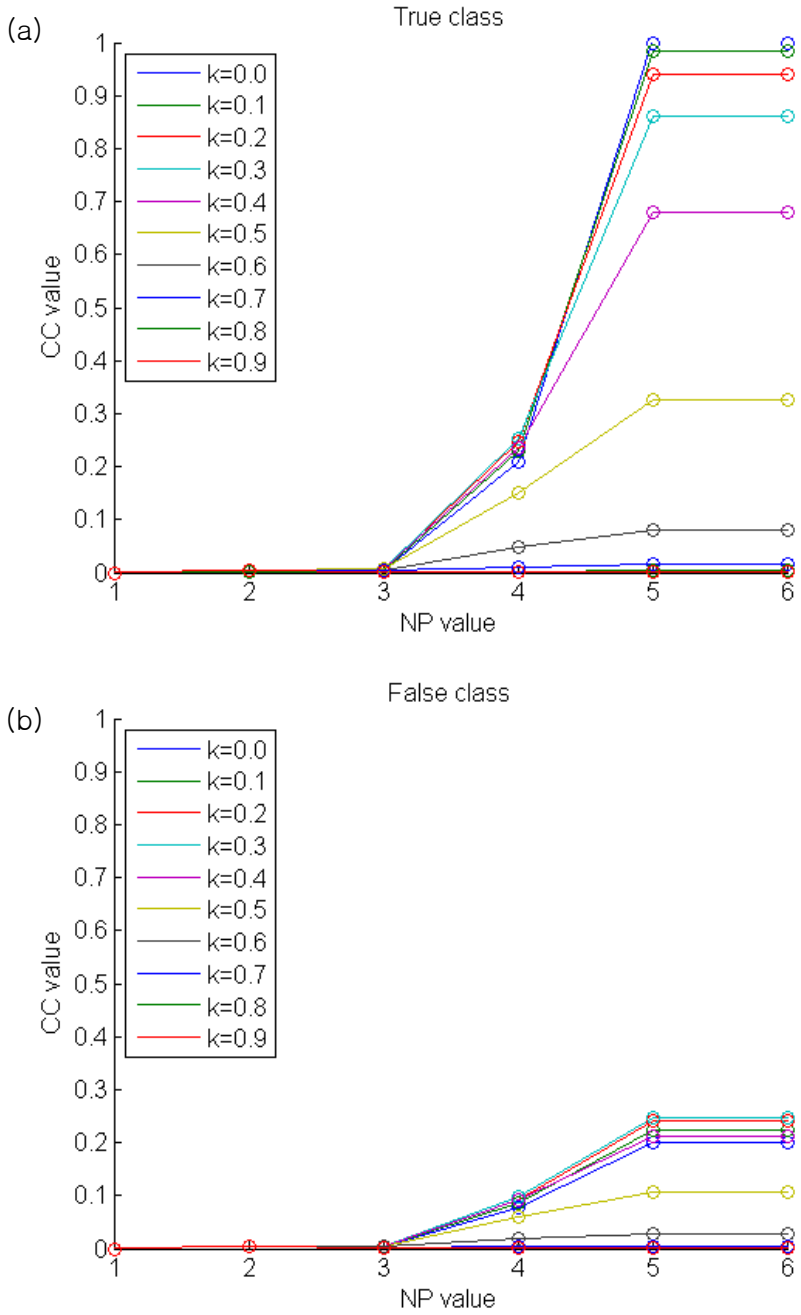



Figure. 14. PCE values with various k and NP
(a) result of true class; (b) result of false class

We simulate this process about fifty times, and the data of Figure. 14. are maximum data. Numerical results are as follow tables.

PCE value of True class

| | 0.0 | 0.1 | 0.2 | 0.3 | 0.4 |
|---|---|---|---|---|---|
| $10^2$ | 0.002399 | 0.002704 | 0.002983 | 0.003235 | 0.003458 |
| $10^3$ | 0.00503 | 0.005491 | 0.005918 | 0.00631 | 0.00662 |
| $10^4$ | 0.208466 | 0.229584 | 0.24601 | 0.253803 | 0.234736 |
| $10^5$ | 0.998771 | 0.983004 | 0.939491 | 0.860233 | 0.678451 |
| $10^6$ | 1 | 0.983803 | 0.940031 | 0.860602 | 0.678657 |
| | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
| $10^2$ | 0.003648 | 0.003796 | 0.003874 | 0.003825 | 0.003561 |
| $10^3$ | 0.006636 | 0.005779 | 0.003755 | 0.001821 | 0.000815 |
| $10^4$ | 0.149292 | 0.049686 | 0.011549 | 0.002722 | 0.00079 |
| $10^5$ | 0.325513 | 0.079468 | 0.01498 | 0.003037 | 0.000792 |
| $10^6$ | 0.325554 | 0.079465 | 0.014978 | 0.003036 | 0.000792 |

PCE value of False class

| | 0.0 | 0.1 | 0.2 | 0.3 | 0.4 |
|---|---|---|---|---|---|
| $10^2$ | 0.002949 | 0.003201 | 0.003417 | 0.003597 | 0.003743 |
| $10^3$ | 0.003525 | 0.00396 | 0.004344 | 0.004673 | 0.004914 |
| $10^4$ | 0.076532 | 0.085282 | 0.092866 | 0.097781 | 0.092534 |
| $10^5$ | 0.200876 | 0.223166 | 0.240314 | 0.246209 | 0.212512 |
| $10^6$ | 0.201081 | 0.223275 | 0.240364 | 0.246225 | 0.212509 |
| | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
| $10^2$ | 0.003852 | 0.003917 | 0.003914 | 0.003788 | 0.003459 |
| $10^3$ | 0.004926 | 0.004309 | 0.002844 | 0.001413 | 0.000653 |
| $10^4$ | 0.059943 | 0.020406 | 0.005034 | 0.001331 | 0.000459 |
| $10^5$ | 0.105606 | 0.026557 | 0.005463 | 0.001295 | 0.000423 |
| $10^6$ | 0.105598 | 0.026554 | 0.005462 | 0.001295 | 0.000423 |

Table. 1. PCE values with respect to change in NP value

Every times results of true class are similar, but max PCE results of false where NP is $10^6$ and k value range are 0.0 to 0.2 are in range (0.15 to 0.25). Those results are realized to us, distinction standard of PCE = 0.3 for authentication is appropriate.

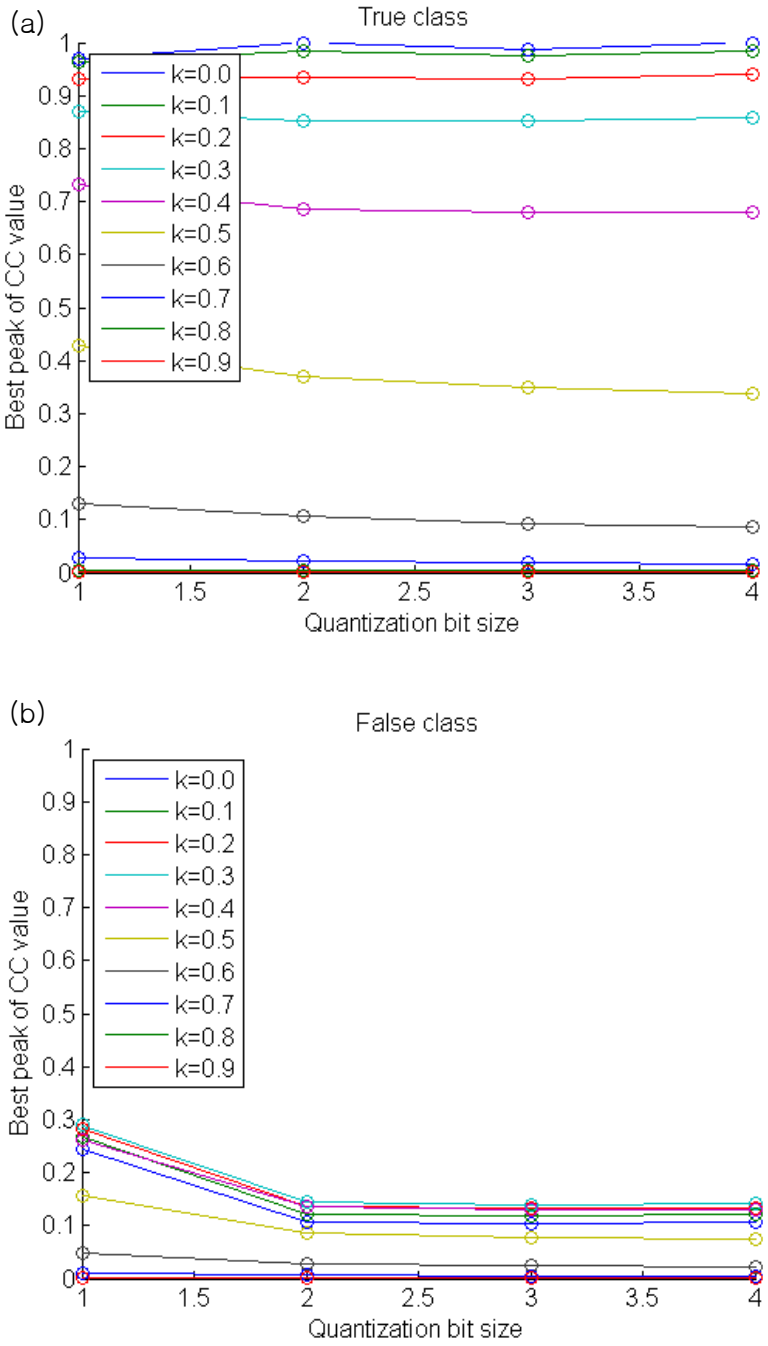



Figure. 15. PCE values with various k and quantization bit (a) result of true class; (b) result of false class

PCE value of True class

| | 0.0 | 0.1 | 0.2 | 0.3 | 0.4 |
|---|---|---|---|---|---|
| 1 | 0.970292 | 0.963809 | 0.931601 | 0.870883 | 0.73388 |
| 2 | 1 | 0.982582 | 0.934746 | 0.851534 | 0.685504 |
| 3 | 0.98788 | 0.975163 | 0.932244 | 0.852985 | 0.681237 |
| 4 | 1 | 0.983626 | 0.93887 | 0.858279 | 0.681137 |
| | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
| 1 | 0.427276 | 0.130308 | 0.02743 | 0.005688 | 0.001395 |
| 2 | 0.370879 | 0.107042 | 0.022306 | 0.004706 | 0.0012 |
| 3 | 0.348655 | 0.092664 | 0.018348 | 0.003789 | 0.000974 |
| 4 | 0.339112 | 0.08692 | 0.016852 | 0.003452 | 0.000893 |

PCE value of False class

| | 0.0 | 0.1 | 0.2 | 0.3 | 0.4 |
|---|---|---|---|---|---|
| 1 | 0.244558 | 0.266856 | 0.283371 | 0.289579 | 0.262718 |
| 2 | 0.105352 | 0.121609 | 0.13586 | 0.144894 | 0.136042 |
| 3 | 0.102737 | 0.118149 | 0.131609 | 0.140006 | 0.129776 |
| 4 | 0.105881 | 0.120426 | 0.133058 | 0.140629 | 0.128938 |
| | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
| 1 | 0.157515 | 0.048176 | 0.010591 | 0.002425 | 0.000701 |
| 2 | 0.085281 | 0.028384 | 0.00695 | 0.001795 | 0.000587 |
| 3 | 0.076808 | 0.023558 | 0.005514 | 0.001416 | 0.000477 |
| 4 | 0.073957 | 0.021828 | 0.005009 | 0.001284 | 0.000439 |

Table. 2. PCE values in terms oft quantization bit size

PCE values against variation of quantization bit size in terms of phase angle information show in Figure. 15. and Table. 2. In this thesis, we experiment on 1bit to 4bit at $10^5$ of NP value. The number of classification is decided by $10^{quantization\_bit\_size}$, where quantization bit size is just 1bit, all of quantized phase angle information are 1 or 2. As a result, that brings a simple result image in its train and PCE value is also not good. If quantization bit size is bigger than or equal to 2bit, however, results do not show a significant difference. We can select quantization bit size of 2bit or 3bit for efficiency of operation.

Following contents are integration system of DRPE and RSA without PCI technique. This procedure is performed in order to compare with performance of the proposed method. In this procedure, we obtain amplitude data from DRPE encryption result. Because this amplitude data is large real number, we should quantize to integer range for RSA process. Quantization method is division operation and rounding up operation. we calculate division operation by $10^{48}$ in order to reduce data loss. Surely, indices of a smaller number also possible and it is easier to decrypt, however smaller indices needs bigger numbers of RSA key set that can result in longer execution time. Division result by $10^{48}$ of amplitude are data of numbers in the ten thousand. In this case, we must select n value of RSA key bigger than one hundred thousand.

PCE value of True class

| | 0.0 | 0.1 | 0.2 | 0.3 | 0.4 |
|---|---|---|---|---|---|
| 1 | 1 | 0.985675 | 0.948538 | 0.887711 | 0.769677 |
| 2 | 1 | 0.983395 | 0.938798 | 0.86248 | 0.707119 |
| 3 | 1 | 0.983549 | 0.939923 | 0.86415 | 0.700591 |
| 4 | 1 | 0.983825 | 0.940803 | 0.864928 | 0.696388 |
| | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
| 1 | 0.509649 | 0.192309 | 0.046566 | 0.010236 | 0.002485 |
| 2 | 0.395142 | 0.117019 | 0.024529 | 0.00514 | 0.001289 |
| 3 | 0.369645 | 0.10072 | 0.020076 | 0.004123 | 0.001043 |
| 4 | 0.356592 | 0.093465 | 0.018231 | 0.003717 | 0.000947 |

PCE value of False class

| | 0.0 | 0.1 | 0.2 | 0.3 | 0.4 |
|---|---|---|---|---|---|
| 1 | 0.076725 | 0.086229 | 0.094587 | 0.1005 | 0.097613 |
| 2 | 0.025758 | 0.030295 | 0.034806 | 0.038553 | 0.037736 |
| 3 | 0.020242 | 0.023977 | 0.027671 | 0.030716 | 0.02972 |
| 4 | 0.018751 | 0.022222 | 0.025635 | 0.028419 | 0.027267 |
| | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
| 1 | 0.068916 | 0.026379 | 0.006863 | 0.001801 | 0.000589 |
| 2 | 0.024077 | 0.00814 | 0.002185 | 0.000682 | 0.000291 |
| 3 | 0.017885 | 0.005672 | 0.00152 | 0.000502 | 0.000234 |
| 4 | 0.015908 | 0.004899 | 0.001314 | 0.000446 | 0.000216 |

Table. 3. PCE values about quantization bit size

(System of DRPE-RSA class)

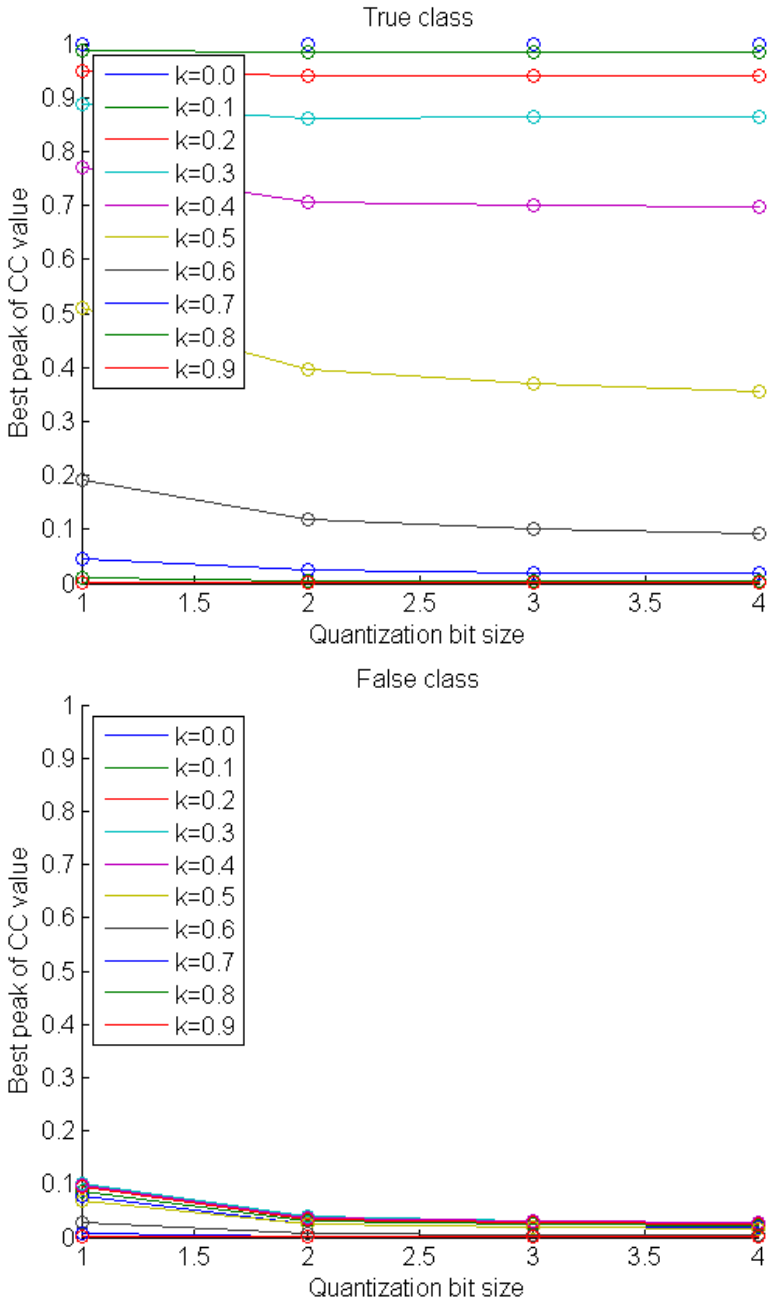



Figure. 16. PCE values with various k and quantization bit (System of DRPE-RSA class)

In Procedure for Table. 3 and Figure 16. NP parameter is not exist due to excepted PCI technique, therefore we experiment against quantization bit size.

And We can show very good result of Authentication. If k value is 0, true class result is always 1. Though this procedure produces good results, however the problem is performance time due to big number RSA key. Performance time per one time execution of this method and proposed method are shown in the following table in terms of second:

| | 1st | 2nd | 3rd | 4th | 5th | 6th | 7th | 8th | 9th | 10th |
|---|---|---|---|---|---|---|---|---|---|---|
| DRPE +RSA | 10.43 | 21.26 | 17.04 | 30.98 | 12.65 | 18.25 | 26.11 | 22.34 | 11.34 | 15.5 |
| Proposed Method | 1.10 | 1.06 | 1.17 | 1.14 | 1.26 | 1.31 | 1.17 | 1.08 | 1.46 | 1.13 |

Table. 4. Comparing execution time(measure : sec)

In Table. 4. integration of DRPE and RSA without PCI needs more than 10sec execution time and that has big difference, because of selected big arbitrary number of RSA key set. On the other hand, proposed method has fast execution time of around 1.188sec in order to select moderate sized number of RSA key set.

# 6. Conclusions

In this thesis, we have proposed an integration of RSA and Photon Counted Imaging(PCI) and Double Random Phase Encoding (DRPE) for image authentication. Experimental results showed that the encrypted or decrypted images from the proposed process cannot be visually recognized with a limited number of photons. And we also achieved security of key management and distribution from RSA algorithm. Nevertheless, the input image can be authenticated with the registered image using nonlinear cross-correlation matrices. The procedure can also achieve better performance time than existing hybrid cryptosystem of DRPE and RSA through the integration of PCI and RSA. Performance time that include all process like key generation process is average 1.188sec on PC environment. In addition, the proposed system have robustness against partial encryption and brute-force attacks. When the encrypted images are partially changed or losed, good authentication results can be achieved.

# References

1. Réréier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. 1995, 20, 767-769.

2. Liu, Z.; Li, S.; Liu, W.; Wang, Y.; Liu, S. Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. Opt. Laser Eng. 2013, 51, 8-14.

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

4. Yao-yao, C.; Xin, Z.; Yong-liang, X.; Sheng, Y.; Xiu-ling, W. An improved watermarking method based on double random phase encoding technique. Opt. Laser Technol. 2010, 42, 617-623.

5. 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.

6. Javidi, B.; Sergent, A.; Zhang, G.; Guibert, L. Fault tolerance properties of a double phase encoding encryption technique. Opt. Eng. 1997, 36, 992-998.

7. 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.

8. Frauel, Y.; Castro, A.; Naughton, T.J.; Javidi, B. Resistance of the double random phase encryption against various attacks. Opt. Express 2007, 15, 10253-10265.

9. Carnicer, A.; Montes-Usategui, M.; Arcos, S.; Juvells, I. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. Opt. Lett. 2005, 30, 1644-1646.

10. Péez-Cabré E.; Abril, H.; Millá, M.; Javidi, B. Photon-counting double-random-phase encoding for secure image verification and retrieval. J. Opt. 2012, 14, 094001.

11. Péez-Cabré E.; Cho, M.; Javidi, B. Information authentication using

photon-counting double-random-phase encrypted images. Opt. Lett. 2011, 36, 22-24.

12. Liu, S.; Guo, C.; Sheridan, J.T. A review of optical image encryption techniques. Opt. Laser Technol. 2014, 57, 327-342.

13. Millá Garcí-varela, M.S.; Péez-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.

14. Alfalou, A.; Brosseau, C. Optical image compression and encryption methods. Adv. Opt. Photon. 2009, 1, 589-636.

15. Javidi, B. Nonlinear joint power spectrum based optical correlation. Appl. Opt. 1989, 28 2358-2367.

16. Cho, M.; Javidi, B. Three-dimensional photon counting double-random-phase encryption. Opt. Lett. 2013, 38, 3198-3201.

17. Mendlovic, D.; Garcia-Martinez, P.; Garcia, J.; Ferreira, C. Color encoding for polychromatic single-channel optical pattern recognition. Appl. Opt. 1995, 34, 7538-7543.

18. Moon, I.; Muniraj, I.; Javidi, B. 3D Visualization at Low Light Levels Using Multispectral Photon Counting Integral Imaging. J. Disp. Technol. 2013, 9, 51-55.

20. Tan, X.; Matoba, O.; Okada-Shudo, Y.; Ide, M.; Shimura, T.; Kuroda, K. Secure Optical Memory System with Polarization Encryption. Appl. Opt. 2001, 40, 2310-2315.

21. Sang, J.; Ling, S.; Alam, M. Efficient Text Encryption and Hiding with Double-Random Phase-Encoding. Sensors 2012, 12, 13441-13457.

22. Chen, W.; Chen, X. Space-based optical image encryption. Opt. Express 2010, 18, 27095-27104.

23. Tashima, H.; Takeda, M.; Suzuki, H.; Obi, T.; Yamaguchi, M.; Ohyama, N. Known plaintext attack on double-random-phase encoding using fingerprint as key and a method for avoiding the attack. Opt. Express 2010, 18, 13772-13781.

24. Peng X, Wei H and Zhang P 2006 Asymmetric cryptography based on wavefront sensing Opt. Lett. 31 3579-81

25. Rivest R, Shamir A and Adleman L 1978 A method for obtaining digital

signatures and public key cryptosystems Commun. ACM 21 120-6
26. Lin G S, Chang H T, Lie W N and Chuang C H 2003 Public-key-based optical image cryptosystem based on data embedding techniques Opt. Eng. 42 2331-9
27. X FMeng, X Peng, L Z Cai, A M Li1, Z Gao and Y R Wang Cryptosystem based on two-step phase-shifting interferometry and the RSA public-key encryption algorithm J. Opt. A: Pure Appl. Opt. 11 (2009) 085402 (9pp)
28. Faliu Yi, Inkyu Moon and Yeon H. Lee A Multispectral Photon-Counting Double Random Phase Encoding Scheme for Image Authentication Sensors 2014, 14, ISSN 1424-8220