August 2013,

Master's Degree Thesis

Multispectral image authentication method via Photon Counting Fourier Optics

Graduate School of Chosun University

Department of Computer Engineering

Muniraj Inbarasan

Multispectral image authentication method via Photon Counting Fourier Optics

포톤 카운팅 푸리어 광학 기반 칼라영상 인증 기법

August 2013

Graduate School of Chosun University

Department of Computer Engineering

Muniraj Inbarasan

Multispectral image authentication method via Photon Counting Fourier Optics

Advisor: Dr. Inkyu Moon

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

April 2013

Graduate School of Chosun University

Department of Computer Engineering

Muniraj Inbarasan

무니라흐 인바라산의 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)

2013년 5월

조선대학교 대학원

Table of Contents

Contents····· i

List of Figures····· iii

List of Tables····· iv

ABSTRACT····· v

한글 요약····· vii

1. Introduction····· 1

2. Background····· 3

2.1 Bayer Image····· 3

2.2 Image Downsampling····· 4

3. Image interpolation algorithms····· 5

3.1 Nearest Neighbor Interpolation····· 6

3.2 Bilinear Interpolation····· 6

3.3 Constant Hue-Based Interpolation····· 7

3.4 Gradient Based Interpolation····· 8

3.5 Adaptive Color Plane Interpolation····· 10

3.6 Gradient Corrected Linear Interpolation····· 11

4. Photon Counted Imaging (PCI)····· 13

5. Double Random Phase Encryption (DRPE)····· 14

6. Proposed Integration Approaches····· 16
6.1 PCI + DRPE (Procedure I)····· 16
6.2 DRPE + PCI (Procedure II)····· 17

7. Image Authentication····· 19

8. Experimental Results····· 20

9. Conclusion····· 38

10. References····· 39

LIST OF FIGURES

Figure 1. Bayer mosaic (GRBG pattern) from CCD sensor ····· 4
Figure 2. Schematic representation of Image Downsampling ····· 5
Figure 3. Schematic representation of Double Random Phase Encoding ····· 15
Figure 4. Schematic representation of Procedure I ····· 17
Figure 5. Schematic representation of Procedure II ····· 18
Figure 6. Reference and Primary images used ····· 21
Figure 7. Retrieved images by Procedure I ····· 26
Figure 8. Retrieved images by Procedure II ····· 27
Figure 9. Discrimination Metrics ····· 28
Figure 10. Nonlinear Cross-Correlation values for Procedure I ····· 29
Figure 11. Nonlinear Cross-Correlation values for Procedure II ····· 29
Figure 12. Discrimination capability test values ····· 30
Figure 13. Nonlinear correlation with different k values for Procedure I ····· 32
Figure 14. Nonlinear correlation with different k values for Procedure II ···· 32
Figure 15. Nonlinear correlation versus partial decryption data ····· 33
Figure 16. Retrieved image with partial decryption using Procedure I ····· 33
Figure 17. Retrieved image with partial decryption using Procedure II ····· 34
Figure 18. Nonlinear Cross-Correlation values in HSI color space ····· 35
Figure 19. Demosaicing Comparison Results ····· 36

LIST OF TABLES

Table 1. Cross correlation with perturbed image pixels ····· 25
Table 2. Demosaicing with different algorithms ····· 37

ABSTRACT

Multispectral Image authentication method via Photon Counting Fourier Optics

Muniraj Inbarasan

Advisor : Dr. Inkyu Moon, Ph.D.

Department of Computer Science

Graduate School of Chosun University

Optical image encryption algorithms based on Fourier plane encoding (i.e., double random phase encryption) systems shown vulnerability against intruder attacks. Recently, the integration of photon-counting imaging (PCI) techniques to the double random encryption (DRPE) systems based on binary images had demonstrated the robustness of information authentication against those attacks. In this thesis, we have proposed integration of optical encryption systems with the photon counting imaging systems for multispectral information authentication. The proposed approaches has two possible combinations of integrating PCI and DRPE systems for multispectral image authentication based on Bayer patterned color filter array (CFA) images. On the one hand, the primary multispectral images are photon-counted subsequently the sparse distributed information being encrypted by DRPE systems which yields sparse encrypted data, eventually it retrieved as sparse distributed photon-limited

version of primary images. Whereas in the second procedure, the reference multispectral images are first encrypted by DRPE systems and the encrypted complex information brought to the photon-counted imaging systems, thus the noisy and high intensity images retrieved. Both the decrypted images do not resemble its original counterpart. Nevertheless, we validate our proposed approaches through statistical nonlinear correlations. We also have displayed our proposed system's discrimination capability using discrimination metric. Experimental results demonstrate that the fewer encrypted distributions are adequate in order to decrypt and authenticate the original information. Since the multispectral information is introduced in optical imaging systems, better authentication and recognition could be achieved.

한글 요약

포톤 카운팅 푸리어 광학 기반 칼라영상 인증 기법

무니라흐 인파라산

지도 교수 : 문 인규.

컴퓨터공학과

대학원, 조선대학교

푸리에 평면 인코딩 (즉, 이중 임의 위상 암호화)를 기반으로 광학 이미지 암호화 알고리즘 시스템은 불법 침입자의 공격에 대한 취약점을 보인다. 최근의 광자 계수 바이너리 이미징(PCI) 기술과 이중 임의 암호화 (DRPE) 시스템의 통합은 이러한 공격에 대해 정보 인증의 견고성이 입증된 이진이미지를 기반으로 한다. 이 논문에서, 우리는 멀티 스펙트럼 정보 인증을 위한 광자 계수 이미징 시스템과 광학 암호화 시스템의 통합을 제안했다. 제안된 방법은 바이엘 패턴 컬러 필터 배열 (CFA) 이미지를 기반으로 다중 스펙트럼 이미지 인증을 위한 DRPE 시스템과 PCI를 통합하기 위한 두 가지 가능한 조합을 가진다. 한편, 기본 다중 스펙트럼 이미지는 희박하게 분산된 정보가 희박한 암호화 데이터가 산출되는 DRPE 시스템을 통해 암호화된 후에 광자가 계수된다. 두 번째 절차에서, 참조 다중 스펙트럼 이미지가 DRPE 시스템에서 처음으로 암호화되고 암호화 된 복잡한 정보는 광자 계수 이미징 시스템으로 가지고 온다. 더하여 잡음이 있고 고강도의 이미지들이 검색된다. 암호가 해독된 두 이미지 모두 원래의 상대와 비슷하지 않다. 그럼에도 불구하고, 우리는 통계 비선형 상관관계를 통해 제안 된 방법을 검증한다. 우리는 또한 식별 메트릭을 사용하여 제안한

시스템의 식별 능력을 표시했다. 실험 결과는 적은 암호화 된 분포가 원래의 정보를 해독하고 인증하는 데적절하다는 것을 검증한다. 광학 이미징 시스템에서 다중 스펙트럼 정보가 알려진 이래로 더 좋은 인증과 인식이 성취될 수 있다.

1. Introduction

With the extensive growth in multimedia techniques, the digital information security has gaining more and more attention since last two decades. In order to protect the transmitted information several optical as well as digital encryption techniques have been proposed to show the robustness against unauthorized attacks [1]. Among them, one of the most powerful and widely used techniques is double random phase encryption (DRPE) or 4f optical encryption processer [2] which turns the intensity image into stationary white noise, by using two statistically independent random phase masks in spatial and Fourier domains; eventually, hence, it does not reveal any content of primary information. The digital implementation of conventional DRPE approaches have shown to be vulnerable against intruder attacks. Recently, Carnicer et al have demonstrated the vulnerability of DRPE to chosen-cipher text attacks [3-4]. They demonstrated that decryption random key could be reproduced by an intruder who has repeated access of encryption or decryption systems. Recently, Perez et al have proven the robustness against unauthorized attacks by integrating photon-counting imaging technique (PCI) to the conventional double random phase encryption (DRPE) technique based on binary images [5]. The photon-counted encrypted (i.e., sparse distribution) information is kept for the decryption process thus the retrieved information would not resemble its original counterpart. Thus this approach demonstrated the robustness against unauthorized attacks and also provides the double layer protection (i.e., information authentication as well as impossible visual recognition) to the encrypted information. However, the intention of this proposed technique was only information authentication, but not visualization [5].

In general, for security applications, the multispectral or color images are more appropriate and it has shown ameliorates advantage than the monochrome or

gray-scale images [6-7]. So far, numerous approaches have been proposed and implemented on multispectral image encryption which could be utilized in many security applications such as intrusion detections, color object recognition, remote sensing image detection and moreover to achieve actual human perception system [7-15]. Despite, the multichannel processing said to be increases the system complexity and diminishes the reliability of the optical systems [13, 16]. Thence, the single channel encryption based on double random phase encryption technique, which was simplest and robust approach, proposed by Zhang et al by using indexed images [16]. Other DRPE based authentication techniques that utilize multiple images, biometric information and near-infrared remote sensing have been developed for a secure multifactor verification. Recently, Moon et al have proposed an approach for multispectal 3D object visualization in Photon starved environment.

To date, no one has introduced multispectral information to the integration procedures of optical encryption and photon-counted imaging systems. By taking this into an account, in this paper, we propose the possible combinations of integrating the photon counting imaging (PCI) systems and double random phase encryption (DRPE) systems for secured multispectral image authentication using Bayer images, which is more reliable and also utilizes the single channel compactness. Eventually, the Bayer image would be interpolated to represent as multispectral images. We believe that this approach would be beneficial in broad spectrum of optical security applications.

This paper is organized as follows. In section 2, the background of Bayer image and downsampling are described. In section 3, we briefly describe the principle of interpolation algorithms. In section 4, the procedure of the Photon counted imaging is presented. Standard Double Random Phase Encryption is described in section 5. In section 6 our proposed procedures are explained. In section 7, image authentication metrics described. Then, in section 8, we show our experimental results. Finally, we conclude our paper in section 9.

2. Background

2.1 Bayer Image

Nowadays, the digital still cameras (DSCs) are gaining much more attention. One of the eminent and most cost effective solutions to capture color images is using single-sensor cameras, made off charge coupled device (CCD) or complementary metal oxide semiconductors (CMOS) coated with color filter arrays (CFA). The popular color filter array (CFA) is known as Bayer CFA invented by Bryce E. Bayer [17]. The Bayer CFA sensor pixels can allow or capture only one of the primary color samples of visible spectrum, i.e., R or G or B at each pixel or photosite locations. Figure. 1 shows the conventional Bayer CFA (mosaic) pattern. Thus the captured images are known as Bayer image or mosaic images.

In Bayer patterned mosaic image, the green (G) samples (luminance sensitive elements) are arranged in a checkerboard pattern, and red (R) and blue (B) samples (chrominance sensitive elements) are arranged in rectangular grid pattern. The green pixels, which contribute remarkably to luminance signals requiring high resolution, are more in numbers and the red and blue pixels, each of which accounts half of the total number of green pixels, Additionally, the spectral response of a green channel is similar with the spectral response of human eye's luminance channel; thence, the Green pixels are more in counts [17]. Commonly, the multispectral or color images are represents by combining three monochromatic (i.e., R, G and B) image channels. In order to generate the multispectral image from Bayer image samples, the missing two colors at each pixels should be estimated from the existing mosaic data. The process of estimating or interpolating the missing color components from sparsely distributed samples is known as demosaicing [18]. In the literatures, plenty of interpolation algorithms have been proposed to estimate the missing color values and those methods has its unique strengths and weaknesses. Among them,

one of the best adaptive approaches called Gradient Corrected Linear Interpolation algorithm by Malvar [19] is implemented in our experiments to visualize multispectral decrypted images from Bayer patterned images.

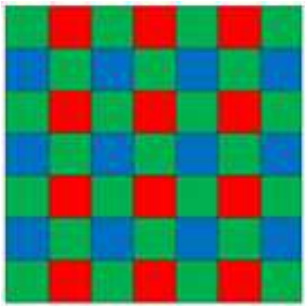


Figure. 1. Conventional Bayer mosaic (GRBG sensor)

2.2 Image Downsampling

Image downsampling is a process of shrinking a digital image by removing unwanted pixels at some pixel locations. Generally, the multispectral images are represented by setting specific (RGB) values of the color space coordinates for each pixels. Such an image has three colors at each photosite locations. These images could be downsampled (i.e., limiting one color value for each pixel) according to Bayer CFA samples to achieve single channel compactness [20]. Figure 2 shows the multispectral image downsampling process. On the other hand, upsampling or interpolation is said to be the reverse process of making a digital image larger. In general, an image downsampling is usually manipulated in spatial or frequency domains. In the spatial domain, downsampling can be performed by uniformly retaining the corresponding pixels within the input image. It is also referred to as direct downsampling, which is the easiest downsampling algorithm. Whereas, in the frequency domain, wavelet transforms, and discrete cosine transforms (DCTs) are usually employed for image downsampling, where the transformed coefficients of low frequencies

are maintained, while the other coefficients are discarded.

Both the image downsampling and interpolation have wide applications in image, video processing techniques. In addition to the conversion between different image sizes, downsampling and interpolation are alternative approaches to achieve better performance for low-bit-rate image coding, where the images are downsampled prior to compression, and then, the missing portions are interpolated after decompression. Image downsampling can be also utilized in SD/HD video coding, where an HD sequence is downsampled to SD before encoding, and then, the decoded SD sequence can be used for an SD-display device or converted to HD via interpolation for an HD-display device.

Figure. 2. Image Downsampling Process (GRBG Pattern)

3. Image Interpolation Algorithms

Mathematically, interpolation means that the construction of a new data within the range of the existing data. This same idea can be used to estimate the missing pixels in the Bayer image in order to generate the true color image (RGB at each pixel). This process of estimation is known as demosaicing [18]. There are varieties of methods available; among those the simplest method,

linear interpolation was widely recommended. Although, there was a problem with this method, that produces visible artifacts at the edges in an image. This result motivates the necessity to find a best technique for interpolation. Many algorithms were emerged. Such algorithms can be classified into two distinct groups as non-adaptive algorithms and adaptive algorithms. As their names suggest, the non-adaptive algorithms performs the interpolation in a fixed pattern on every pixel in an image (within a fixed band or group). It fails to maintain the edge information and it causes an artifact known as the zipper effect [18]. Whereas the adaptive algorithms can detect the local spatial features present in the neighborhood pixel of an input image and then make an effective choice to predict the missing pixels. Thus the adaptive algorithm provides the stupendous results compared to the non adaptive algorithms. We have also made a short comparison analysis on the interpolation algorithms.

3.1 Nearest Neighbor Interpolation

This is well known non adaptive algorithm and it is very simple to implement. In this interpolation method, the interpolated output pixel is assigned to have the same value of the nearest (neighbor) pixel in the input image. The programmer can select any one of the left, right, upper and lower four pixels from the input image [18]. Although this algorithm can provide satisfactory result in the smooth regions of an image, they fail to produce better results in the high frequency regions (especially along edges).

3.2 Bilinear Interpolation

Bilinear interpolation is the most popular non adaptive algorithm used to interpolate the CFA images [18]. To interpolate any pixel in the Bayer CFA, it considers its direct neighbors and then it determines the two missing colors samples on each pixel location. For an example, if we want to estimate the

missing values on B_{43}, it neighbours are averaged to compute the missing pixels as shown in following Equation.

$$G_{43} = \frac{G_{33} + G_{42} + G_{44} + G_{53}}{4}$$

$$R_{43} = \frac{R_{32} + R_{34} + R_{52} + R_{54}}{4}$$

It's clear from the Eq.1 that the output values would have the same range as input. Similarly for estimating of the missing values on red pixel, the green and blue should be utilized accordingly. Whereas, to estimate the missing chrominance samples on luminance samples it averages it two immediate neighbors of the chrominance samples. By performing this estimation on every pixel we can generate the interpolated output (color) image. The band limiting nature of this technique would leads to significant artifacts (known as Zipper effect) especially across the edges [18].

3.3 Constant Hue-Based Interpolation

Constant Hue-Based Interpolation was proposed by David R. Cok [18]. Commonly, the hue is defined as the gradation of color. It represents the dominant wavelength of light (ranging from red through yellow, green and blue) as perceived by an observer. It denoted by a vector of ratios as (R/G, B/G). The color fringes (artifacts) can be reduced by interpolating chrominance values based on interpolated hue values and interpolated luminance values. As a first step, this algorithm approaches the interpolation of luminance channel using standard bilinear interpolation. Later, the chrominance channels are interpolated as expressed as follows,

$$R_{43} = \boldsymbol{G}_{43} . \frac{\frac{R_{32}}{\boldsymbol{G}_{32}} + \frac{R_{34}}{\boldsymbol{G}_{34}} + \frac{R_{52}}{\boldsymbol{G}_{52}} + \frac{R_{54}}{\boldsymbol{G}_{54}}}{4}$$

$$B_{32} = \boldsymbol{G}_{32} . \frac{\frac{B_{21}}{\boldsymbol{G}_{21}} + \frac{B_{23}}{\boldsymbol{G}_{23}} + \frac{B_{41}}{\boldsymbol{G}_{41}} + \frac{B_{43}}{\boldsymbol{G}_{43}}}{4} \quad (2)$$

The boldface 'G' value refers to the estimated (bilinear interpolated) values from the first pass of this algorithm. Further, by using this algorithm the color fringes are reduced without introducing unwanted hue shifts in the interpolated output image.

3.4 Gradient Based Interpolation

This method was proposed by Claude A. Laroche and Mark A. Prescott [18]. This method takes an advantage that the human eyes are more sensitive to the luminance changes. This algorithm employs a three steps process. As a first step, the luminance channel is being interpolated, then the second and third steps involves in interpolating the gradient value, which can be obtained as the color differences (R-G, B-G) in horizontal and vertical directions. Corresponding interpolated gradient vaules are then used to reconstruct the chrominance channels. For example if we need to estimate G_{43}, this can be calculated using the following equations.

$$\boldsymbol{G}_{43} = \begin{cases} \frac{G_{42} + G_{44}}{2}, & \text{if } \alpha < \beta \\ \frac{G_{33} + G_{53}}{2}, & \text{if } \alpha > \beta \\ \frac{G_{33} + G_{42} + G_{44} + G_{53}}{4}, & \text{if } \alpha = \beta \end{cases}$$

$$\alpha = \text{abs}\left[\left(B_{41} + B_{45} \right) / 2 - B_{43} \right] \quad , \quad \beta = \text{abs}\left[\left(B_{23} + B_{63} \right) / 2 - B_{43} \right]$$

Where the α and β referred to the gradient values (also known as

classifiers). Similarly, for estimating G_{34} the following classifiers are used,

$$\alpha = \mathrm{abs}\left[\left(R_{32} + R_{36}\right)/2 - R_{34}\right] \quad , \quad \beta = \mathrm{abs}\left[\left(R_{14} + R_{54}\right)/2 - R_{34}\right] \quad .$$

$$\boldsymbol{G}_{34} = \begin{cases} \dfrac{G_{33} + G_{35}}{2}, & \text{if} \quad \alpha < \beta \\ \dfrac{G_{24} + G_{44}}{2}, & \text{if} \quad \alpha > \beta \\ \dfrac{G_{24} + G_{33} + G_{35} + G_{44}}{4}, & \text{if} \quad \alpha = \beta \end{cases}$$

After this step the chrominance values are interpolated from the differences between color and luminance channels (R-G and B-G). This can be expressed as follows,

$$R_{33} = \frac{(R_{32} - \boldsymbol{G}_{32}) + (R_{34} - \boldsymbol{G}_{34})}{2} + G_{33},$$
$$R_{44} = \frac{(R_{34} - \boldsymbol{G}_{34}) + (R_{54} - \boldsymbol{G}_{54})}{2} + G_{44},$$
$$R_{43} = \frac{(R_{32} - \boldsymbol{G}_{32}) + (R_{34} - \boldsymbol{G}_{34}) + (R_{52} - \boldsymbol{G}_{52}) + (R_{54} - \boldsymbol{G}_{54})}{4} + G_{43}.$$

Note that the luminance channel should completely estimated before this process (it's indicated as boldface values of **G**). The same procedure can also be used to derive for the blue channels. Besides, this algorithm minimizes the color artifacts without adding unnecessary complexity to the interpolation process.

3.5 Adaptive Color Plane Interpolation

This method was proposed by Hamilton and Adams [18]. It is just an extension of the algorithm proposed by Laroche and Prescott. This method estimates the missing values based on similar classifier used in Laroche et. al method. As a first pass, the adaptive interpolation method is used to estimate the luminance value horizontally, vertically or diagonally depending upon the gradient value. The gradient values are calculated between the chrominance pixel locations in the vertical and horizontal direction. By the second pass, the chrominance channels are being interpolated. The classifiers are calculated as follows,

$$\alpha = \mathrm{abs}\left(-R_{32} + 2R_{34} - R_{36}\right) + \mathrm{abs}\left(G_{33} - G_{35}\right)$$
$$\beta = \mathrm{abs}\left(-R_{14} + 2R_{34} - R_{54}\right) + \mathrm{abs}\left(G_{24} - G_{44}\right)$$

These classifiers are composed of Laplacian second derivative terms for the R and B channels and gradients for G channel. These classifiers can sense the high frequency information in the neighborhood pixels in both the horizontal and vertical directions. Consider, that we need to estimate G_{34}, the interpolation estimates are determined as in Eq.7,

$$\boldsymbol{G}_{34} = \begin{cases} \dfrac{G_{33} + G_{35}}{2} + \dfrac{\left(-R_{32} + 2R_{34} - R_{36}\right)}{4}, & \text{if} \quad \alpha < \beta \\ \dfrac{G_{24} + G_{44}}{2} + \dfrac{\left(-R_{14} + 2R_{34} - R_{54}\right)}{4}, & \text{if} \quad \alpha > \beta \\ \dfrac{G_{24} + G_{33} + G_{35} + G_{44}}{4} + \dfrac{\left(-R_{14} - R_{32} + 4R_{34} - R_{36} - R_{54}\right)}{8}, & \text{if} \quad \alpha = \beta \end{cases}$$

This process comprises the first step of the interpolation algorithm. As a second pass the chrominance channels are interpolated. For example, if we need to estimate R_{33} and R_{42} the following expressions can be used.

$$R_{33} = \frac{(R_{32} + R_{34})}{2} + \frac{(-\boldsymbol{G}_{32} + 2G_{33} - \boldsymbol{G}_{34})}{2}$$
$$R_{42} = \frac{(R_{32} + R_{52})}{2} + \frac{(-\boldsymbol{G}_{32} + 2G_{42} - \boldsymbol{G}_{52})}{2}$$

But to estimate the R_{43}, it employs the similar method used for luminance channel. First it finds the classifiers and then it interpolated the chrominance data. Let,

$$\alpha = \mathrm{abs}\left(-\boldsymbol{G}_{34} + 2\boldsymbol{G}_{44} - \boldsymbol{G}_{52}\right) + \mathrm{abs}\left(R_{34} - R_{52}\right)$$
$$\beta = \mathrm{abs}\left(-\boldsymbol{G}_{32} + 2\boldsymbol{G}_{43} - \boldsymbol{G}_{54}\right) + \mathrm{abs}\left(R_{32} - R_{54}\right)$$

$$R_{43} = \begin{cases} \dfrac{(R_{34} + R_{52})}{2} + \dfrac{(-\boldsymbol{G}_{34} + 2\boldsymbol{G}_{43} - \boldsymbol{G}_{52})}{2}, & \text{if} \quad \alpha < \beta \\ \dfrac{(R_{32} + R_{54})}{2} + \dfrac{(-\boldsymbol{G}_{32} + 2\boldsymbol{G}_{43} - \boldsymbol{G}_{54})}{2}, & \text{if} \quad \alpha > \beta \\ \dfrac{(R_{32} + R_{34} + R_{52} + R_{54})}{4} + \dfrac{(-\boldsymbol{G}_{32} - \boldsymbol{G}_{34} + 4\boldsymbol{G}_{43} - \boldsymbol{G}_{52} - \boldsymbol{G}_{54}}{4}, & \text{if} \quad \alpha = \beta \end{cases}$$

These estimates are composed of arithmetic averages for the chromaticity (red or blue) samples and appropriately scaled Laplacian second order derivative terms for the luminance (green) samples. Further, the visible artifacts will be reduced effectively by using gradient values and second order derivative values.

3.6 Gradient Corrected Linear Interpolation

This algorithm recently proposed by Henrique S. Malvar [19]. The bilinear interpolation generates some visible artifacts since it does not consider the statistical correlation among the RGB values in a color image. It's said that in [18] the gradient based algorithms can produce the better interpolated results. To estimate the value of missing pixel, this algorithm combines the

calculated gradient information with the bilinear interpolated value of a given pixel. The combination of such calculated gradient values and the linear interpolation technique ameliorate the quality of the interpolated output data [19]. In such a way, this adaptive technique corrects the artifacts produced by symmetric bilinear interpolation algorithm. Thus, it termed as Gradient Corrected Linear Interpolation. For example, to interpolate the G value at location R pixel location the following expression is used,

$$\hat{g}(x,y) = \hat{g}_B(x,y) + \alpha\Delta_R(x,y)$$

Where the subscript B means bilinear interpolated and $\triangle_R(x,y)$ is the calculated gradient value of R at that pixel location, it can be computed as follows,

$$\Delta_R(x,y) \square\ r(x,y) - \frac{1}{4}\sum r(x+m, y+n)$$

Where the boundaries are $(m,n) = \{(0,-2),(0,2),(-2,0),(2,0)\}$. The gain factor α controls the intensity of correction values. Similarly for interpolating G at blue pixels, the same equation can be used with the correction (gradient) value $\triangle_{Blue}(x,y)$. To interpolate R at G pixel locations, the following expression is used, with $\triangle_G(x,y)$ determined by a 9-point region as defined in [19].

$$\hat{r}(x,y) = \hat{r}_B(x,y) + \beta\Delta_G(x,y)$$

Whereas interpolating R value at B pixels can be denoted as follows,

$$\hat{r}(x,y) = \hat{r}_B(x,y) + \gamma\Delta_{Blue}(x,y)$$

With $\triangle_{Blue}(x,y)$ is computed on a 5-point region as defined in [19]. Similar expressions can be used for interpolating blue pixel. The values of gain

parameters $\{\alpha,\beta,\gamma\}$ were determined by Wiener approach. The approximated final values are $\{\alpha=1/2,\beta=5/8,\gamma=3/4\}$. On the whole, this method takes an advantage of reduced computational complexity than others.

4. Photon Counting Imaging (PCI)

Photon-counting imaging (PCI) systems are special class of imaging system, designed for low light level (photon-starved conditions) or night vision, where only the limited number photons would reach the image sensors [21-22]. In general, photon-counted image has lesser information than its counterpart. Similar effect could be computed digitally by allowing a limited number of incident photons (N_p) to the captured image scene. Thus the photon counted images would carry less information than the primary image. Recently, we have proposed a multispectral photon-counting integral imaging system based on Bayer images for 3D low light visualization [22]. We assumed that the probability of counting photons at any arbitrary pixels in a captured Bayer image follows Poisson distribution [23]. To generate the photon counted multispectral images from Bayer samples, the captured primary color images are first down sampled according to the Bayer image and then the Bayer samples are individually (i.e., R, G and B) Poisson distributed. We generate the Poisson random numbers at arbitrary pixels for each spectral element (channel) in a given Bayer image with corresponding Poisson parameter λ_w.

$$C_w(x,y) \approx Poisson(\lambda_w = \overline{f_w}(x,y) \times N_p)$$

Where the terms $w, N_p, \overline{f_w}(x,y)$ are denotes red (R), green (G) and blue (B) channels, average number of expected photons per Bayer image and normalized Bayer image respectively [21]. The term $Poisson[.]$ denotes random numbers generated using the Poisson distribution. To epitomize, in general, the

photon-counted images would have lesser information than the input images [24-25].

5. Double Random Phase Encoding (DRPE)

Optical and digital information security systems based on double random phase encoding (DRPE) [1-5] technique had shown predominant role in information security. According to DRPE principle, the primary image $f(x,y)$ represents spatial coordinates of a two dimensional signal or an image, is being encrypted as stationary white noise using two random phase masks, which does not lead to fabricate or reveal any content of the original image. The random phase masks 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 $[0,2\pi]$. The decryption procedure is said to be the reverse or inverse process of encryption. Figure 3 shows the complete image encryption and decryption processes. In our experiments, the Bayer image is used for encryption and it is defined as follows; first, the original multispectral images are down sampled according to Bayer samples $f(x,y)$. Since the color samples (i.e., R, G and B), shows different attributes in visible spectrum, it processed independently as monochrome channels [22]. The segregated channels are multiplied with spatial phase mask $p(x,y)$ and transform into frequency domain (i.e., Fourier transform) subsequently. Later, the transformed images are multiplied with frequency domain phase masks $b(\mu,\eta)$. Eventually, an inverse Fourier transform is then performed on color channels individually to get the encrypted channels. In general, the encrypted data are complex-amplitude and white noise [2]. Mathematically this process can be defined as follows,

$$R_w(\mu,\eta) = FFT\{f_w(x,y).p(x,y)\}$$

$$en_w(x,y) = IFFT\{R_w(\mu,\eta).b(\mu,\eta)\}$$

Where, the subscript $w=(0,1,2)$ denotes red, green or blue channels.FFTandIFFTrepresenttheFourierandinverseFouriertransformsrespectively, andthetermdenotes the encrypted Bayer image. The spatial and Fourier phase masks values are same for all three monochromatic channels.

The reverse procedure of encryption process is to be employed in order decrypt the original channels. At first, the encrypted Bayer images are transformed into the Fourier domain individually and then multiplied with inverse (i.e., complex conjugate) Fourier phase masks. The resultants are then inverse Fourier transformed and multiplied with inverse spatial phase mask in order to obtain the decrypted (original) image. It can be mathematically represented as follows,

$$R_w(\mu,\eta) = FFT\{en_w(x,y).b^*(x,y)\}$$

$$f_w(x,y) = IFFT\{R_w(\mu,\eta).p^*(\mu,\eta)\}$$

Where '*' symbol denotes complex conjugate operation. It is been proven that the decrypting the original information without knowing phase masks would lead to futile. Thus this technique leads to a robust reconstruction of an input image. However, some researchers have demonstrated the vulnerability against known and chosen cipher-text attacks on digital implementation of DRPE techniques [3-4].

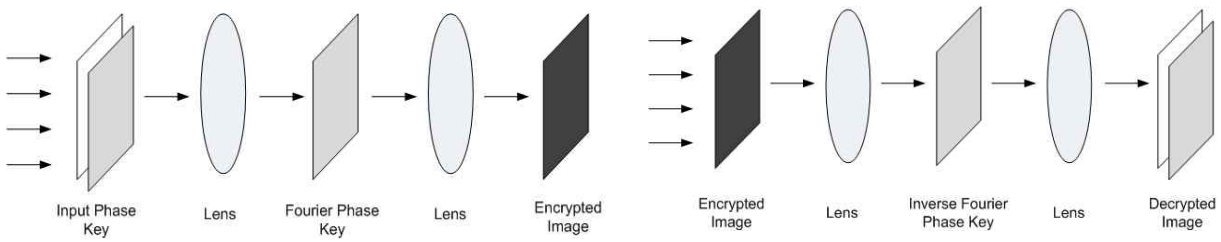


Figure. 3. A schematic representation of DRPE.

This result motivates the need to find a specialized approach in order to increase the security of an encrypted data. Plenty of new approaches have been proposed in recent years, among them, the integration of PCI and DRPE based on binary images have demonstrated the robustness against those attacks by providing double layer of protection [5].

6. Proposed Integration Approaches

6.1 Procedure I (PCI + DRPE)

The integration photon-counting imaging (PCI) with double random phase encryption (DRPE) techniques can be processed in two different ways by associating both the techniques in different orders. One of the procedures is discussed in this section. On this approach, the multispectral reference images are photon-counted and given to the DRPE systems for further security. The photon-counted decrypted images do not resemble and reveal any content of its original information, at any cost. Thus, this procedure achieves additional security as compared to conventional DRPE systems. Figure 4 shows a schematic representation of our procedure I. In our experiments, the primary multispectral (i.e., reference) images are first down sampled according to the Bayer samples. Later, the photon-counted Bayer image $f_{ph}(x,y)$ is obtained by employing PCI procedures individually on normalized three color samples as mentioned earlier in section 3. Subsequently, the photon-counted (i.e., sparse distributed) Bayer images are kept for encryption using conventional DPRE technique and it would be processed as explained in section 4. Eventually the decrypted Bayer image retrieved and it would be a sparse distribution of the primary image and hence it cannot be visualized or recognize by ordinary human eyes. We represent such decrypted Bayer information by this procedure as

$d_{fph}(x,y)$. Remember the fact that the integration PCI and DRPE systems intended for only image authentication, but not for image visualization [5]. Since the decrypted images make possible to authenticate the information by nonlinear correlations also with impossible human visual recognition, the integration procedures can said to be providing additional layer of protection to the primary data.

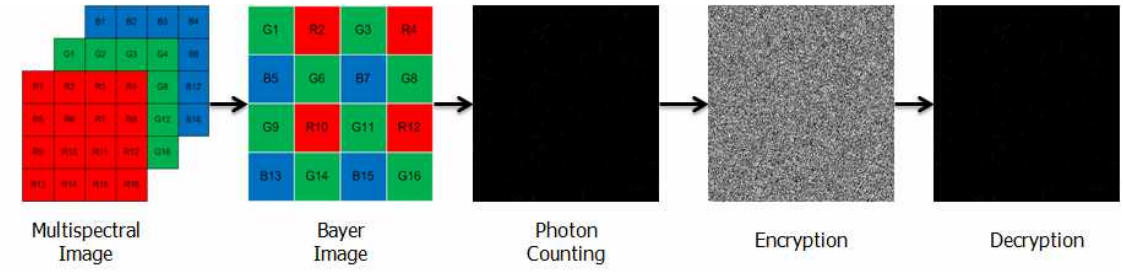


Figure. 4. A schematic representation of Procedure I (PCI + DRPE).

6.2 Procedure II (DRPE + PCI)

On the other hand, in this approach, the multispectral reference images are first encrypted using DPRE technique and then photon-counted. In our experiments, the down sampled Bayer images are encrypted individually using DRPE as explained in section 4. In general, the encrypted Bayer distributions $\psi(x,y)$ are complex-amplitude; hence both the amplitude and phase values must be given to decryption process. At first, the photon-counting imaging (PCI) technique is applied only on the amplitude or magnitude information of the Bayer encrypted complex data. Thus, the photon-counted Bayer amplitude encrypted distributions $|\psi_{ph}(x,y)|$ are generated. Later, the pixels which have non-zero amplitude (intensity) would keep for the decryption process including their corresponding phase information. This decrypted image would

looks like a noisy image with much higher intensity, on average, than the primary image. We represent such decrypted Bayer image as $d_{\psi ph}(x,y)$. Figure 5 shows the schematic representation of our procedure II. Since, only few samples (i.e., non-zero pixels) of encrypted Bayer images are utilized for decryption, it is worth to state that the bandwidth reduction is achieved only by this procedure [26]. Whereas by the procedure I (i.e., PCI +DRPE), the primary image is photon-counted and then the photon-counted primary image encrypted using DPRE systems, in such cases no compression is achieved. However, the number of photons could only be reduced for decrypting the information by procedure I (PCI+ DRPE) when compared to the procedure II (DRPE + PCI), as the noisy-like appearance would require larger number of photons [5].

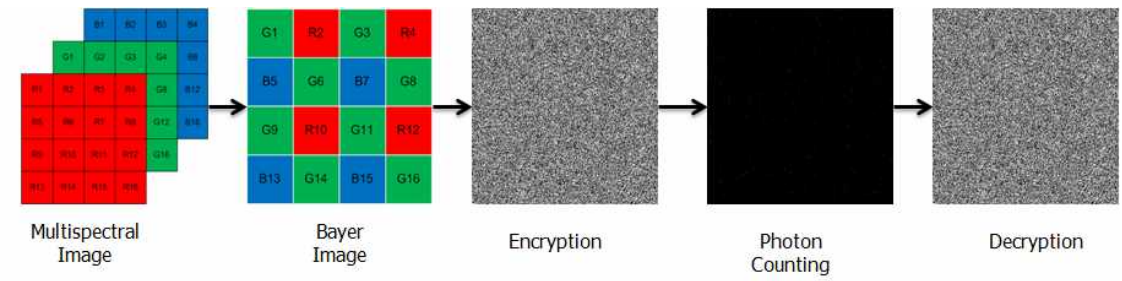


Figure. 5. A schematic representation of Procedure II (DRPE + PCI).

Further, the outcomes (i.e., decrypted images) of both the procedures $(d_{\psi ph}(x,y), d_{\psi ph}(x,y))$ would not resemble its original primary image. To reiterate, the integration of Photon-counting Imaging (PCI) technique and Double Random Phase Encryption (DRPE) systems is introduced only for image authentication or verification, not for the image visualization [5].

7. Image Authentication

The integration of PCI and DRPE procedures decrypts the image, which cannot be recognize by direct visualization [5]. Nevertheless, the decrypted or retrieved image authentication might be verified through statistical correlation techniques [27-30]. One of the widely used metrics to calculate similarity between two signals is nonlinear correlation. In this procedure the signals or images are transformed from time or spatial domain to frequency domain (i.e., Fourier transform), then the signals are nonlinearly modified and multiplied. Eventually by taking inverse Fourier transform of the multiplied product yields the nonlinear correlation between reference and probe images [27]. Such nonlinear cross-correlation operation between reference and probe images can be expressed as follows,

$$c(x,y) = FT^{-1}\left\{ \left| D_{fph/\varphi h}(\mu,\eta).F(\mu,\eta) \right|^{k} . \exp\left[i\left(\phi_D(\mu,\eta) - \phi_F(\mu,\eta)\right)\right] \right\}$$

Where $D(\mu,\eta), F(\mu,\eta)$ represents 2D Fourier transform of decrypted and reference images respectively. The parameter k defines applied nonlinearity in the nonlinear cross-correlation and we estimated the best suited value for k is 0.3 which achieves sharp intensity peak value in our experiments. In addition to this, we have calculated the Discrimination Metric (DM) in order to verify the performance of our proposed methods [5]. It is computed as the ratio between maximum intensity value of cross-correlation output and maximum intensity value auto-correlation and it's expressed as follows,

$$DM = \left| \frac{CC}{AC} \right|$$

Where, CC, cross correlation, refers to the maximum cross-correlation

intensity value when the decrypted image (by both the procedures) is correlated with reference multispectral image and AC, autocorrelation, is computed when the reference images are correlated with themselves. In order to estimate the better discrimination and nonlinear correlation values, the maximum values are considered as unity. Also, in our experiments, we have arbitrarily selected some threshold (0.5) value to estimate a good discrimination. When the calculated DM value is greater than the threshold (>0.5), the decrypted image is said to be authorized or sought image, whereas the lesser DM values (<0.5) indicates unauthorized or imposter decrypted image. In our experiments, DM is measured for all three monochromatic channels (i.e., R, G and B) individually and the results are averaged then.

8. Experimental Results

Experimental results are illustrated here to validate of our proposed systems. Figure 6 (a-c) shows three standard multispectral reference images taken from Kodak true color image data sets, each with the size of 512x512x3 pixels. As mentioned earlier, at first, the multispectral reference images are down sampled according to Bayer samples and the Bayer images are manipulated in both the procedures (I and II) in order to examine our proposed approaches. Figure 6 (d-f) shows the corresponding down sampled Bayer images (8 bits) in GRBG pattern which are manipulated in our experiments. The spatial and Fourier random phase masks are generated using MATLAB random number generator. In our experiments, we have implemented one of the best demosaicing algorithms the Gradient corrected linear interpolation proposed by Henrique S. Malvar, on retrieved Bayer images to visualize the multispectral or RGB decrypted images. The missing color samples from the Bayer decrypted images are interpolated and visualized as multispectral decrypted images. Additionally this method said to

be reducing the computational complexity and it outperforms all other adaptive demosaicing approaches [19, 22].

(a) (b) (c)

(d) (e) (f)

Figure. 6. Images used in our experiments; (a)-(c) original (reference) multispectral images (d) - (f) Corresponding down sampled Bayer patterned (GRBG format) mosaic images.

According to the procedure I (PCI + DRPE), the down sampled Bayer images are first photon counted as explained in section 5.1, following that the photon-counted Bayer images are encrypted using DRPE technique. Eventually,

the encrypted sparse Bayer samples are decrypted. Figure 7 (a-c) shows such the Bayer patterned retrieved images (sparse distribution) by procedure I, $d_{fph}(x,y)$, when the photon numbers 10^3 (or equivalently 0.38% of image pixels) is considered. Figure 7 (d-f) shows corresponding decrypted images in RGB format (i.e., after Malvar's demosaicing) while the photons are same in count. On the other hand, for the procedure II (DRPE + PCI) the sampled Bayer images are first encrypted as explained in section 5.2, and then the encrypted Bayer images are photon-counted. Figure 8 (a-c) shows the retrieved images (noisy distribution) off procedure II in Bayer format, $d_{\psi ph}(x,y)$ with photon numbers 10^4 (or equivalently 3.8% of image size). Figure 8 (d-f) shows the corresponding decrypted images, after Malvar's demosaicing, in RGB format at the same photons as in Bayer image. It is precise from figures 7 and 8 that, neither the sparse distribution images of procedure I nor the noisy-like images of procedure II do allow us for authenticating the decrypted images by direct visual inspection. Thus the proposed approaches produce additional layer of information protection. To reiterate, the proposed integration procedures only for image authentication but not for image visualization.

Figure 9 (a-b) and (c-d) shows the calculated DM results for both the procedures using Bayer and RGB Images respectively. It is precise from Figure 9 that, it's possible to significantly reduce the number photons in procedure I (PCI + DRPE) as compared to procedure II (DRPE+ PCI) to get successful authentication. For instance, a good trade-off between photons and approached procedures on Bayer images are Np= 10^3.3 which gives DM>0.7 for procedure I and Np= 10^5.3 which gives DM>0.7 for procedure II. Similarly, demosaiced multispectral images provide good recognition results at Np=10^3.6 for procedure I (i.e., DM>0.7) and Np=10^5.4 for procedure II provides DM>0.7. The corresponding intensity nonlinear cross-correlation outputs (the sharp peak over noisy background) for both the procedures based on Bayer images when the parameter value k=0.3 (applied nonlinearity) are depicted in Figures 10&11.

Additionally, to validate the discrimination capability of the proposed systems, different and non-authorized multispectral image have been tested. Figure 12 (a-c) shows the non-authorized multispectral images and Figure 12 (d-f) shows corresponding Bayer images, a plane with noisy background is obtained without any remarkable peak (Figure 12 (g-h) and (i-j)) in the nonlinear cross-correlation when these images correlated with the authorized images. Figure 13 (a-c) and 14 (a-c) shows the nonlinear cross correlation values calculated between primary and decrypted images for both the procedures. As depicted, the intermediate values of parameter k, $k\epsilon[0.2,0.4]$ provides satisfactory results in terms of good correlation values. Hence, in our experiments, we select the intermediate nonlinearity value (i.e., k=0.3), which offers an intense correlation peak and good discrimination results. Besides, we also tested the robustness of the proposed procedures by partial encryption. In this approach, we have arbitrarily selected and kept some percentages of encrypted pixels for the decryption process. Figure 15 shows the computed nonlinear correlation values for both the procedures when the partial encryption values were used in the decryption. The procedure I (PCI + DRPE) gives some satisfactory results when the portion of encrypted pixels was larger than 25%. Similarly, for the procedure II (DRPE + PCI) the retrieved image was recognizable when the 35% of original encrypted information is being kept for decryption process. It's very clear from the graph that the correlation increases as the encrypted pixels increased. Figures 16 (a-c) and 17 (a-c) shows retrieved images (1%, 5% and 10% respectively) when the partial encryption values were used in the decryption process. Besides, we also have examined the key sensitivity by changing a single phase key value in the encryption process. It is well known fact that the ideal image encryption scheme is key sensitive with respect to the secret phase key and should also produce totally different encrypted image when the secret key has been changed or damaged. Table 1 show the cross correlation value between the cipher image

with original phase key and with the phase key perturbed. These results would guarantees the security of the proposed method against Brute-force attacks. Additionally, we have estimated the proposed system's strength in HSI (Hue, Saturation and Intensity) color spaces. The input and decrypted images are first brought to the HSI color spaces and then the correlation carried out individually for all three channels. Figure 18 (a-b) shows the computed nonlinear correlation values in HSI color space. Since the photon-limited image has less color information and correlation values than the original (RGB) one the Hue (color) values provided lower correlation results and thus the averaged correlation value in HSI space is lesser than in RGB color space. We also have compared and analyzed the superior technique to convert our Bayer retrieved images into multispectral retrieved images. From our experiments (Table 2 and Figure 19), we have found that the adaptive algorithms provide good results than the non-adaptive algorithms. Especially, Hamilton-Adams interpolation algorithm and Laroche-Prescott algorithm, that uses similar algorithms to interpolate the Bayer CFA images, considerably reduces the artifacts and enhances the image quality of interpolated retrieved image. It is clear from the figure 19 that the Malvar's interpolation technique consistently provides better results for both the procedures. Besides, the computational time is one of the important factors for demosaicing algorithms when implemented in the real-time systems. Hence, we also have measured the computational time required for interpolation of Bayer CFA samples. Among all the methods, the Malvar's technique takes the reduced computational advantages. On the whole, thence, Malvar's demosaicing technique would be an adequate technique (both in accuracy and computational time) to convert our retrieved Bayer images into multispectral decrypted images. Hence, we have implemented the Gradient Corrected Linear Interpolation technique to estimate the missing pixels from the Bayer CFA images.

These results are in accordance with the fact that integration of PCI and

DRPE systems are robust and it would produce additional layer of information security, by not allowing the intruder for direct image visualization, as compared to the conventional approaches also it is capable of discriminating the decrypted images from other similar and non-authorized images. In our experiments, the maximum nonlinear correlation and DM values are considered as one (i.e., unity) to make comparison simpler. Additionally, the nonlinear correlation and discrimination metrics are computed from 10 numerical simulations, in order to select most appropriate results. By using our experiments, not only the image verification have been achieved also the retrieval of an original image has been demonstrated based on correlation output values.

Encryption Procedures	Cross Correlation
PCI + DRPE	9.55X10-7
DRPE + PCI	9.52X10-7

Table 1. Cross correlation between original & perturbed key encrypted image

(a) (b) (c)

(d) (e) (f)

Figure. 7. Decrypted images (Lena, Parrots, Flowers)(Np=10^3.5); (a-c) decrypted Bayer images.(d)-(f)Corresponding decrypted multispectral images.

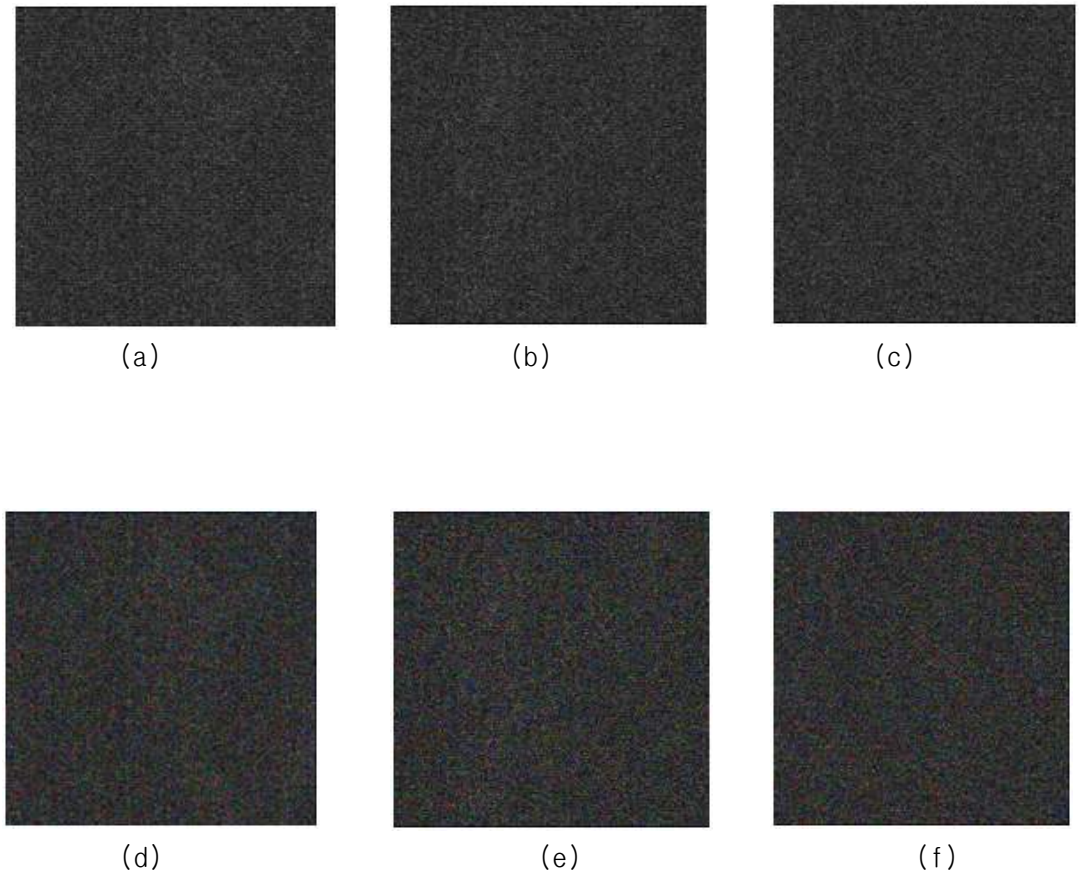


Figure .8. Decrypted images (Lena, Parrots, Flowers) (Np=10^4); (a)-(c) decrypted Bayer images(d)-(f)Corresponding decrypted multispectral images

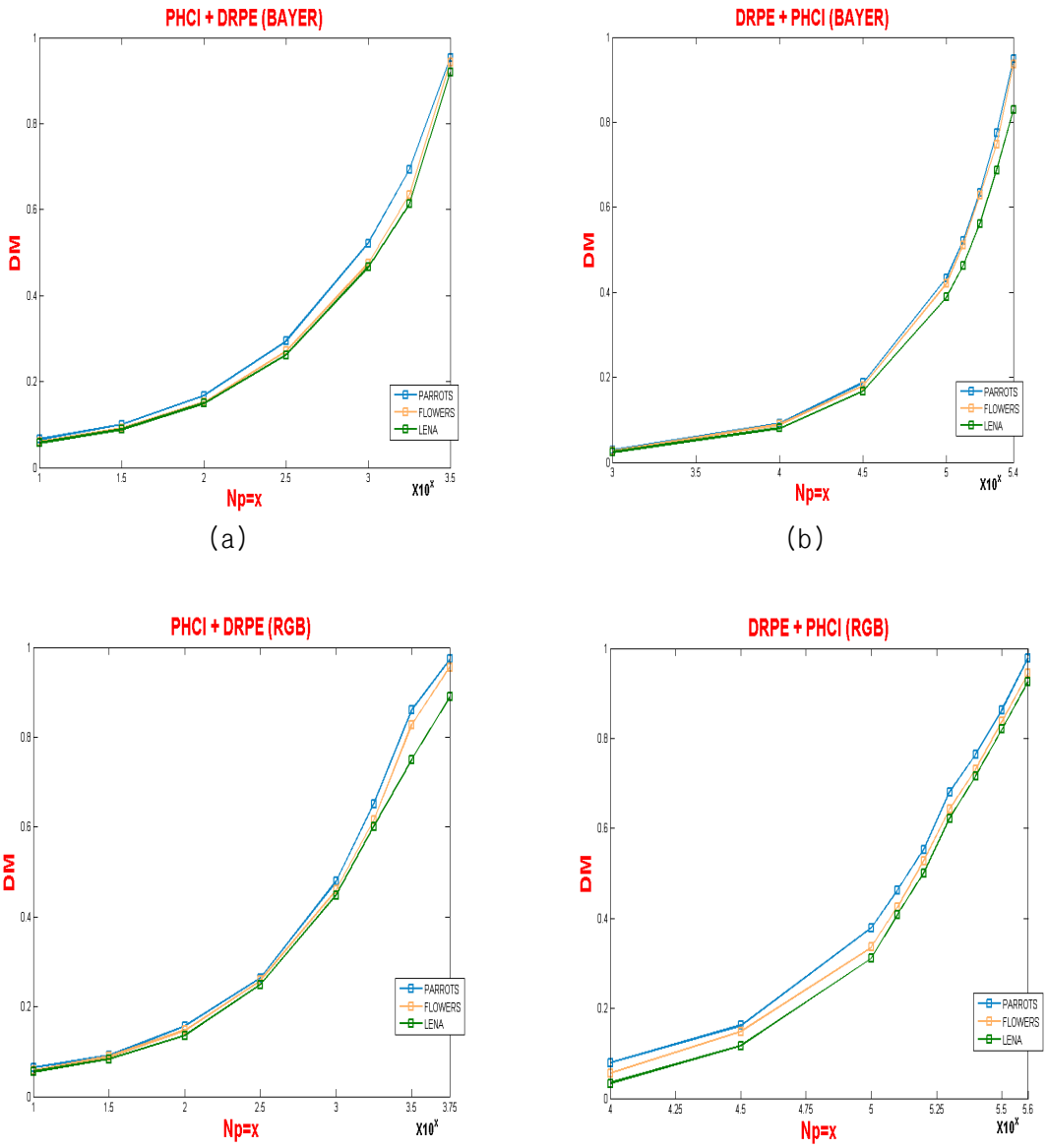


Figure.9. Discrimination Metric (DM) Values

(a) Procedure I (PCI + DRPE) & (b) Procedure II (DRPE + PCI) on Bayer Images

(c) Procedure I (PCI + DRPE) & (d) Procedure II (DRPE + PCI) on RGB Images.

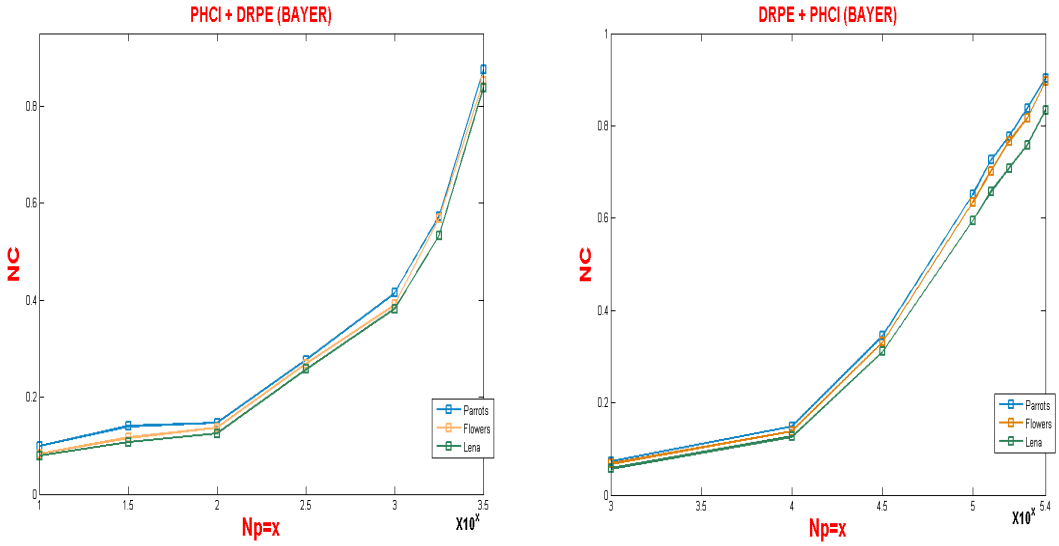


Figure. 10. Nonlinear Cross-Correlation output on Bayer images.

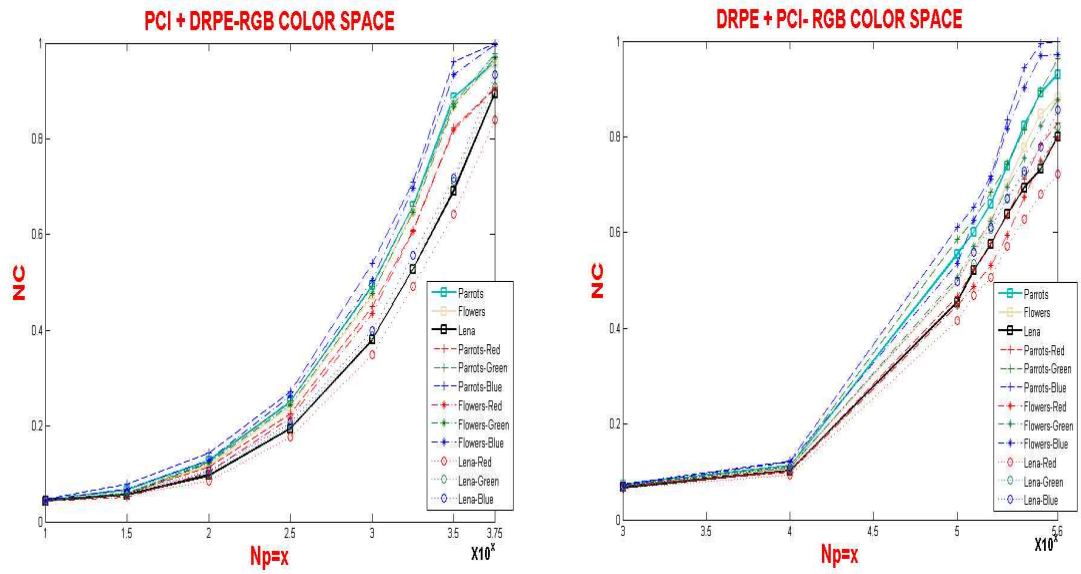


Figure.11. Nonlinear Cross-Correlation output on Multispectral images.

(a)

(b)

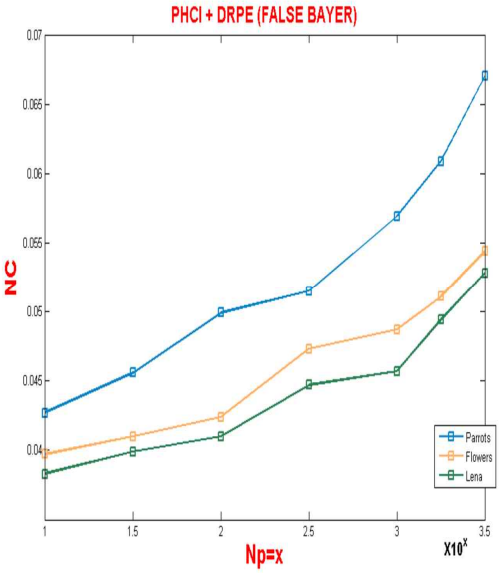
(c)

(d)

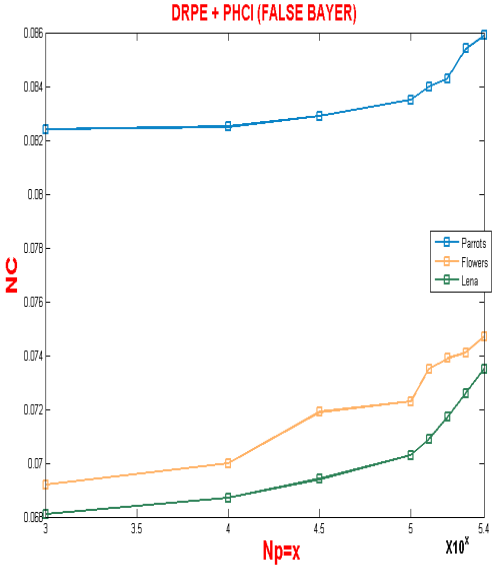
(e)

(f)

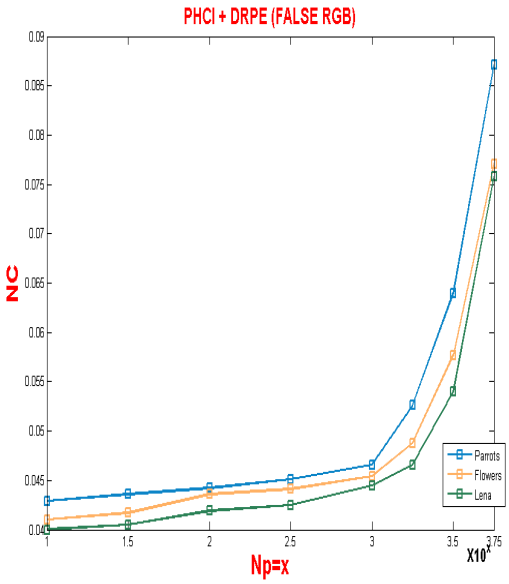
Figure.12. Discrimination Test. (a-c) Multispectral Non-authorized images, (d-f) corresponding Non-authorized Bayer Images. (g-h) and (i-j) Nonlinear Cross Correlation output on Bayer images and Multispectral images respectively, for both the procedures.


PHCI + DRPE (FALSE BAYER)
NC
Np=x
X10^x
Parrots
Flowers
Lena

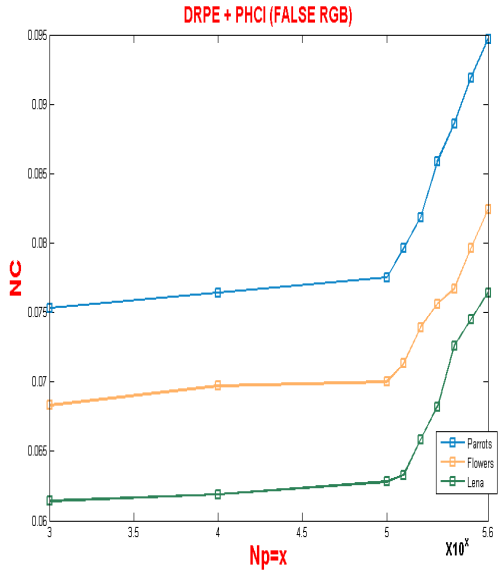
(g)


DRPE + PHCI (FALSE BAYER)
NC
Np=x
X10^x
Parrots
Flowers
Lena

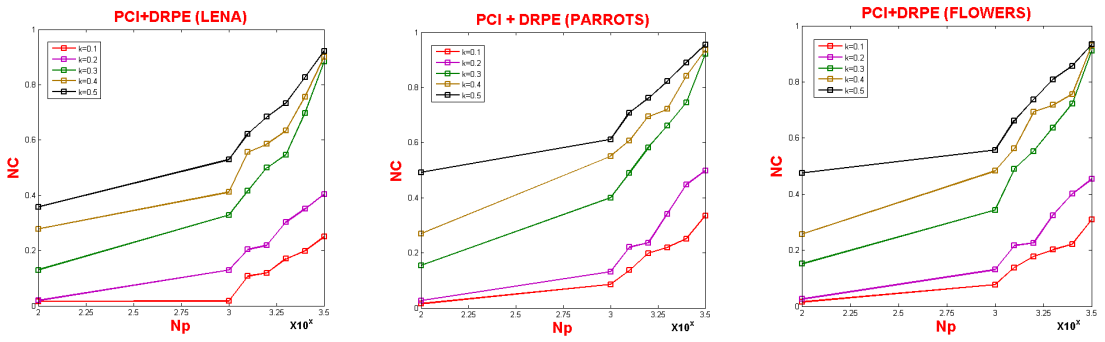
(h)


PHCI + DRPE (FALSE RGB)
NC
Np=x
X10^x
Parrots
Flowers
Lena

(i)

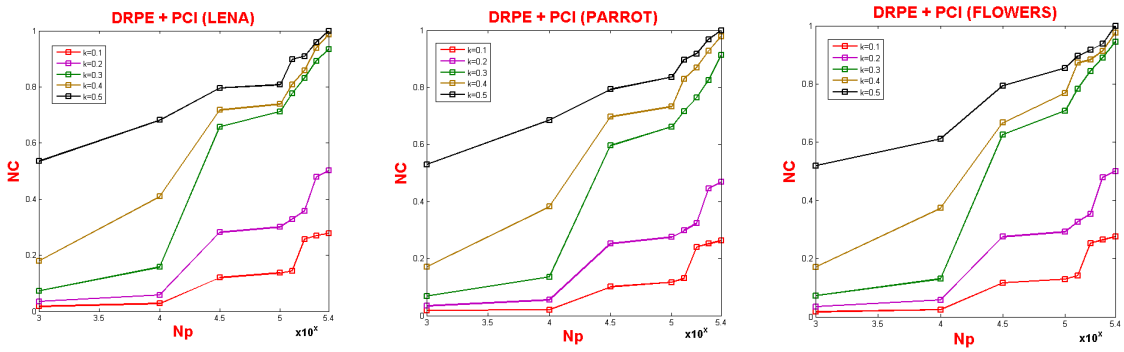

DRPE + PHCI (FALSE RGB)
NC
Np=x
X10^x
Parrots
Flowers
Lena

(j)



(a) (b) (c)

Figure.13. Nonlinear Cross-Correlation output on Bayer images with different k values, Procedure I (PCI + DRPE) (a) Lena (b) Parrots (c) Flowers.



(a) (b) ©

Figure.14. Nonlinear Cross-Correlation output on Bayer images with different k values, Procedure II (DRPE + PCI) (a) Lena (b) Parrots (c) Flowers.

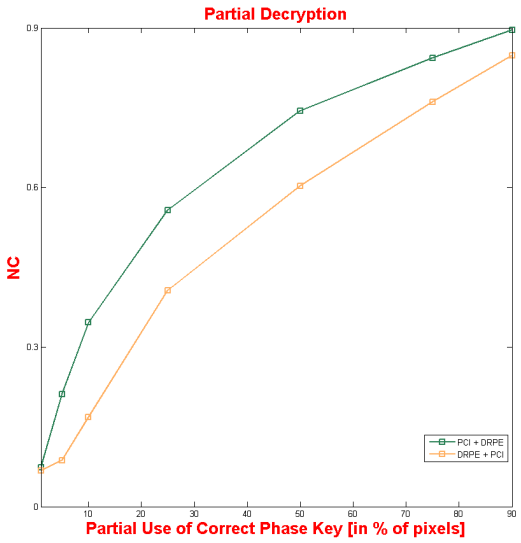
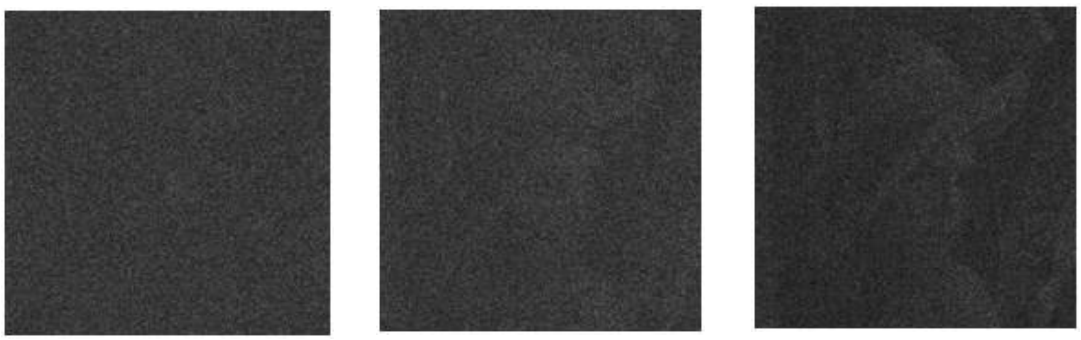
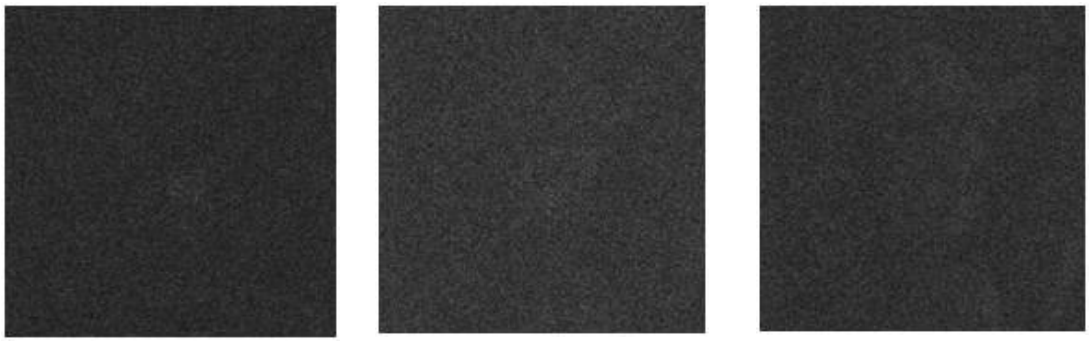


Figure 15. Nonlinear Correlation value versus partial decryption data.



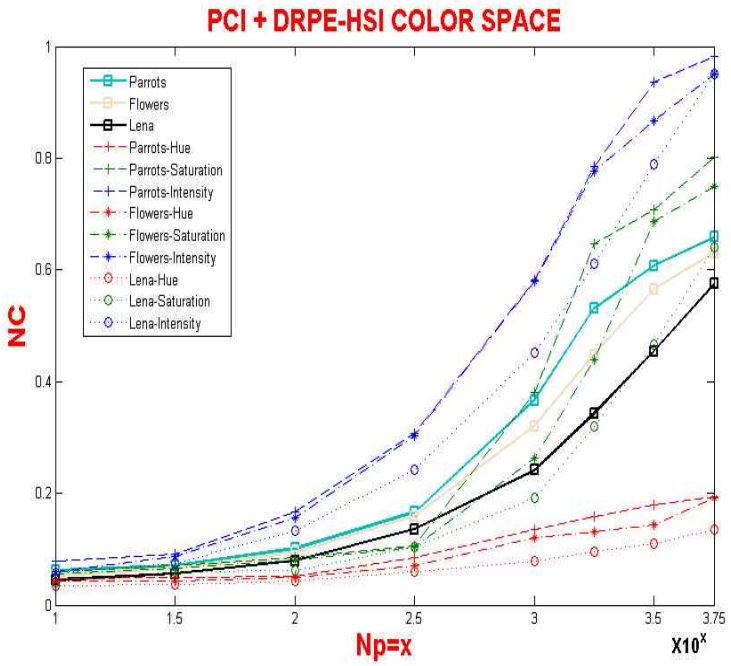
(a) (b) (c)

Figure 16. Retrieved Lena image when the portion of the encrypted image used in the procedure I (PCI + DRPE). (a) 1%, (b) 5%, and (c) 10%.

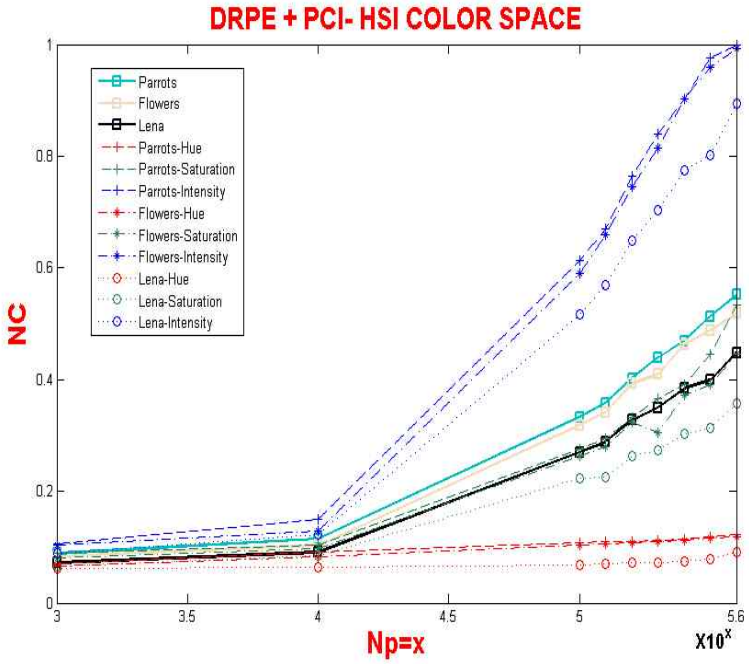


(a) (b) (c)

Figure 17. Retrieved Lena image when the portion of the encrypted image used in the procedure II (DRPE + PCI). (a) 1%, (b) 5%, and (c) 10%.

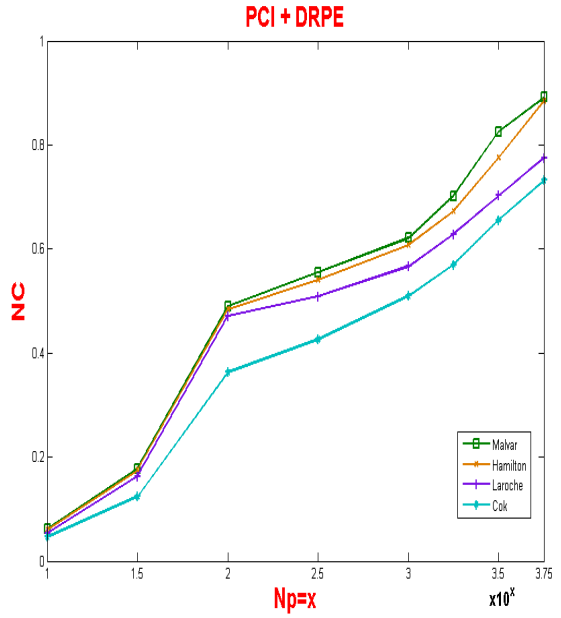


(a)

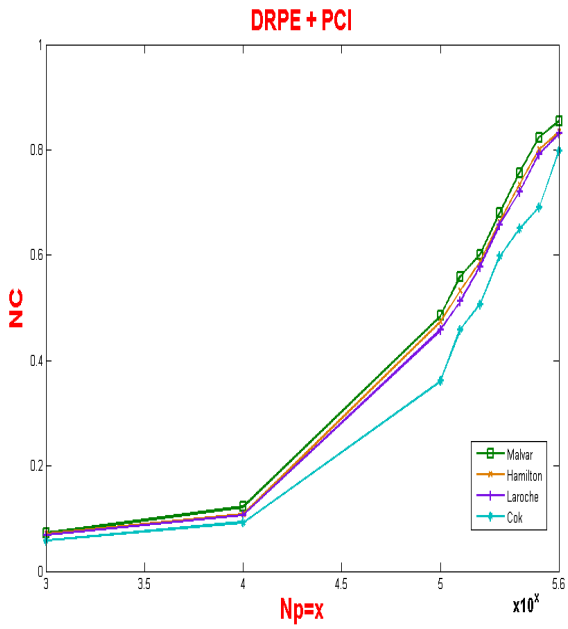


(b)

Figure 18. Nonlinear Correlation Values in Hue, Saturation and Intensity (HSI) Color Space.(a) Non linear Correlation Value in Procedure I (PCI + DRPE) and (b) Non linear Correlation Values for Procedure II (DRPE + PCI).



(a)



(b)

Figure 19. Demosaicing Comparisons (a) Procedure I and (b) Procedure II

DRPE + PCI		MALVAR	HAMILTON ADAMS	LAROCHE PRESCOTT	COK	NEAREST NEIGHBOR
3	R	0.0723	0.0711	0.0676	0.0657	0.0551
	G	0.0741	0.0716	0.0689	0.0664	0.0592
	B	0.0769	0.0731	0.0712	0.0680	0.0627
5	R	0.4436	0.3914	0.3881	0.3605	0.2754
	G	0.5669	0.5277	0.5041	0.4803	0.4388
	B	0.5979	0.5587	0.5490	0.5244	0.5161
5.6	R	0.8015	0.6953	0.6835	0.6789	0.5864
	G	0.9606	0.8474	0.8419	0.8408	0.6327
	B	0.9951	0.9917	0.9859	0.9329	0.9134
Time in Seconds		0.0297	0.1239	0.1195	0.1117	0.0524

(a)

PCI + DRPE		MALVAR	HAMILTON ADAMS	LAROCHE PRESCOTT	COK	NEAREST NEIGHBOR
3	R	0.0619	0.0609	0.0573	0.0478	0.0445
	G	0.0685	0.0669	0.0595	0.0531	0.0458
	B	0.0696	0.0672	0.0605	0.0535	0.0486
5	R	0.5090	0.5038	0.4865	0.3830	0.3175
	G	0.5497	0.5430	0.5250	0.5140	0.4047
	B	0.6153	0.5835	0.5664	0.5332	0.4566
5.6	R	0.8144	0.7308	0.7267	0.5473	0.4699
	G	0.8619	0.8351	0.7982	0.7607	0.5958
	B	0.9471	0.9055	0.8535	0.8119	0.7924
Time in Seconds		0.0311	0.1321	0.1210	0.1144	0.0531

(b)

Table 2. Demosaicing Comparison between adaptive and non adaptive algorithms.

9. Conclusion

Conventional optical image encryption algorithms based on double random phase encoding are vulnerable to an organized chosen-cipher text attack. Recently proposed integration of Photon Counting Imaging (PCI) systems with cryptographic algorithms (DRPE), although it fails to achieve better visualization, it has demonstrated the additional layer of security against intruder attacks. In this paper, we have proposed two possible combinations of integrating PCI and DRPE systems for multispectral images authentication based on Bayer CFA images. In the procedure I, the primary down sampled Bayer images first photon-counted and the resultant sparse distributed data encrypted by DPRE techniques, eventually it decrypts sparse distributed Bayer images. The procedure II, the Bayer images are first encrypted by DRPE and the encrypted complex samples are photon-counted eventually produces noisy-like images, both the decrypted images do not reveal any information of the original content by the direct visual recognition. It's worth mentioning the fact that, the photon number reduction gives more satisfactory results in procedure I (i.e., PCI + DRPE) but no compression could be achieved in this case, whereas bandwidth reduction is only achieved by procedure II (DRPE + PCI) however it requires larger amount of photons to authenticate the retrieved images. Further, the decrypted image authentication demonstrated by statistical nonlinear cross-correlations. In our experiments, we also calculated discrimination metric in order to measure the proposed system's discrimination capacity. The proposed system was shown to be more sensitive to an error in encryption data. Experimental results are displayed using three standard authorized and non authorized test images. The proposed system shows the robustness against intruder attacks by producing the decrypted information as sparse distribution and a noisy appearance, which makes direct visual recognition impossible.

References

[1] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi, “Optical Techniques for Information Security,” Proceedings of the IEEE 97, 1128-1148 (2009).

[2] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding” Opt. Lett 20, 767 (1995).

[3] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, “Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys,” Opt. Lett 30, 1644-1646 (2005).

[4] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, “Resistance of the double random phase encryption against various attacks,” Opt. Expr 15, 10253-10265 (2007).

[5] E. Perez-Cabre, M. Cho and B. Javidi, “Information authentication using photon-counting double-random-phase encrypted images,” Opt. Lett 36, 22-24 (2011).

[6] A. Yip and P. Sinha, "Contribution of color to face recognition,” Perception, 31, 995-1003 (2002).

[7] F.T.S. Yu, “Color image recognition by a spectral-spatial matched filtering,” Opt. Eng 23, 690-695(1984).

[8] J. C. Hou, “Visual cryptography for color images,” Pattern Recognition 36, 1619(2003).

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

[10] K. Martin, R. Lukac, and K. N. Plataniotis, “Efficient encryption of wavelet-based coded color images,” Pattern Recognition 38, 1111(2005).

[11] R. Lukac and K. N. Plataniotis, “A cost-effective encryption scheme for color images,” Real-Time Imaging 11, 454(2005).

[12] L. Chen, D. Zhao, “Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms,” Optics Express 14, 8552-8560 (2006).

[13] M. Joshi, Chandrashakher, and K. Singh, “Color image encryption and decryption using fractional Fourier transform,” Opt.Com 279, 35-42 (2007).

[14] D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, “Digital color encryption using a multi-wavelength approach and a joint transform correlator,” J. Opt. A 10, 104031(2008).

[15] M. Joshi, C. Shakher, and K. Singh, “Phase Image Encryption of Colored Images Using Double Random Phase Encoding Technique in HSV Color Space,” Optical Review 16, 511 -516 (2009).

[16] S. Zhang and M.A. Karim, “Color Image Encryption Using Double Random Phase Encoding,” Microwave and Optical Technology Letters 21, 318 (1999).

[17] B. E. Bayer, “Color imaging array,” U.S. Patent, 3,971,065.

[18] B. Gunturk, J. Glotzbach, Y. Altunbasak, R. Schafer and R. Mersereau, "Demosaicking: Color filter array interpolation," IEEE Signal Proceeding. Magazine 22, 44-54 (2005).

[19] H. Malvar, L. He and R. Cutler, "High-quality linear interpolation for demosaicing of Bayer-patterned color images," IEEE International Conference on Acoustics, Speech and Signal Proceeding. 3, 485-488 (2004).

[20] Y. Zhang, D. Zhao, J. Zhang, R. Xiong and W. Gao, "Interpolation Dependent Image Downsampling," IEEE transactions on image processing, Vol.20, no.11, 3291-3296 (2011).

[21] I. Moon and B. Javidi, “Three-dimensional recognition of photon-starved events using computational integral imaging and statistical sampling,” Opt. Lett. 34(6), 731-733 (2009).

[22] I. Moon, I. Muniraj, and B. Javidi, “3D Visualization at Low Light Levels Using Multispectral Photon Counting Integral Imaging,” Journal of Display technology 9 (1), 51-55 (2013).

[23] J. W. Goodman, Statistical Optics (Wiley-Interscience, New York, 1985).

[24] B. Tavakoli, B. Javidi and E. Watson, "Three dimensional visualization by photon counting computational integral imaging," Optics Express 16, 4426-4436 (2008).

[25] S. Yeom, B. Javidi and E. Watson, "Photon counting passive 3D image sensing for automatic target recognition," Optics Express 13, 9310-9331 (2005).

[26] P. Memmolo, M. Paturzo, A. Pelagotti, A. Finizio, P. Ferraro, and B. Javidi, “Compression of digital holograms via adaptive-sparse representation,” Opt. Lett., 35, 3883-3885 (2010).

[27] B. Javidi, "Nonlinear joint power spectrum based optical correlation," Appl. Opt., 28, 2358-2367 (1989).

[28] F. Sadjadi, B. Javidi, Physicsoftheautomatictargetrecognition,Springer,2007.

[29] F. Dubios,"Automatic spatialfrequency selection algorithm for pattern recognition by correlation," Appl. Opt. 32, 4365-4371, (1993).

[30] A. Mahalanobis, "Object specific image reconstruction using a compressive sensing architecture for application in surveillance systems," IEEE Trans. AES, 45, 1167-1180, (2009).