High Security Optical Encryption based on Sweeping Computational Ghost Imaging

Sajjad Rajabi-ghaleh
University of Tabriz
Babak Olyaeefar (olyaeefar@tabrizu.ac.ir)
University of Tabriz
Reza Kheradmand
University of Tabriz
Sohrab Ahmadi-kandjani
University of Tabriz

Research Article

Keywords: CCD, BBO-crystal, Ghost Imaging, NPCR

Posted Date: December 28th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-132235/v1

High Security Optical Encryption based on Sweeping Computational Ghost Imaging

Sajjad Rajabi-Ghaleh[1], Babak Olyaeefar[1*], Reza Kheradmand[1,2], and Sohrab Ahmadi-Kandjani[1,2]

[1]Research Institute for Applied Physics and Astronomy, University of Tabriz, Tabriz, Iran
[2]Photonics and plasma technology group, Faculty of Physics, University of Tabriz, Tabriz, Iran
[*]Olyaeefar@tabrizu.ac.ir

ABSTRACT

A method for the optical data encryption and decryption based on the sweeping computational ghost imaging is proposed. This method is governed on reconstructing the ghost imaging by one-by-one sweeping of rows or columns of the random generated matrices. Proposed encryption in this paper is defined by these sweeping row and column matrices and basic mathematical operators between them. Introduced encryption can be employed as symmetric and asymmetric encryptions. In the symmetric system, cross-operator and the row and column matrices were assumed as private keys, defining the four basic operators as decryption keys. Whereas, in the asymmetric system, permutation of three possible cases was considered as private keys, leaving cross-operator and row and column selection sequence as public keys. The number of pixel changing Rate (NPCR) as a parameter that evaluates the strength of image encryption versus differential attacks was calculated for each case which show high security data transfer to the user. In the asymmetric systems, even with eavesdropping 50% of data, no useful information was obtained from the image or data. In the symmetric systems, with eavesdropping 100% of data, no useful information was obtained by multiple attacking the encrypted data. Offered high security along with achievable high speeds and compact data packages classify sweeping computational ghost imaging among the best applicable methods for optical data encryption.

Introduction

Ghost-imaging (GI) is a recently developed technique of imaging. Basically, it is based on splitting the optical source into two arms. One arm, the reference, is directed to a charged coupled device (CCD) detector to record the spatial pattern. Other arm, the object, illuminates the object being reflected\transmitted to a bucket detector. The image is retrieved by second-order correlation of these two intensities[1–4]. GI has found many application such as in, 3D imaging[5], X-ray imaging[6,7], face recognition[8], imaging from turbulence medium[9], remote sensing[10], and also data encryption[11,12]. In 1995, Pittman et al[13] presented a realization of GI by a quantum source. They used BBO-crystal for splitting the source beam to the signal and idler beams. Later, Boyd et al[14] in 2002, proved that ghost imaging can be carried out by a pseudothermal source. Computational GI (CGI) was first introduced by Shapiro[15] through employing a spatial light modulator (SLM)[16] or digital micro-mirror device (DMD)[17] rather than CCD for measuring the intensity profile of the reference arm. Main problem in GI is its relatively lower speed or longer capturing time compared to those of other imaging techniques. To overcome these barriers, our group introduced sweeping CGI (SCGI) method in 2019[18]. There, random generated matrices in CGI were manipulated to have an all-bright row or column and in each shot the position of this set of cells were swept horizontally or vertically. Our method eas capable of enhancing the imaging speed for moving objects around 22[19] and 4000[20] folds compared to the previously reported data. Furthermore, since imaging of the still objects required a pre-defined number of shots, equal to the sum of row and column number of the random generated matrix, GI was instantly captured. Secure and impenetrable connection is among the essential needs for a reliable data communication. In the case of image encryption, approaches such as digital signature, authentication, data hiding and sharing have greatly progressed to limit unauthorized access. Data encryption was first introduced in 1980 by dividing encrypting into three main scenarios of raw data, compress data and detailed data encryption[21]. Also, data encryption can be performed asymmetrically or symmetrically. In symmetric case, encryption key is shared between the transmitter and receiver. However, in the asymmetric case, encryption key is available to public, while only the intended user has access to the decryption key[22]. So far, Different algorithms have been employed for data encryption, such as permutation, random modulation and confusion-diffusion techniques. The permutation method[21] is based on importing random pixels or lines to manipulate data placement. GI and optical encryption by GI[12] was shown to offer high security and also low-volume data packages sizes[23–25]. In recent years, researchers have proposed different optical encryption methods, such as GI encryption, chaotic encryption and dual random phase encryption[26]. Clemente et al[23] proposed first optical data encryption based on CGI.

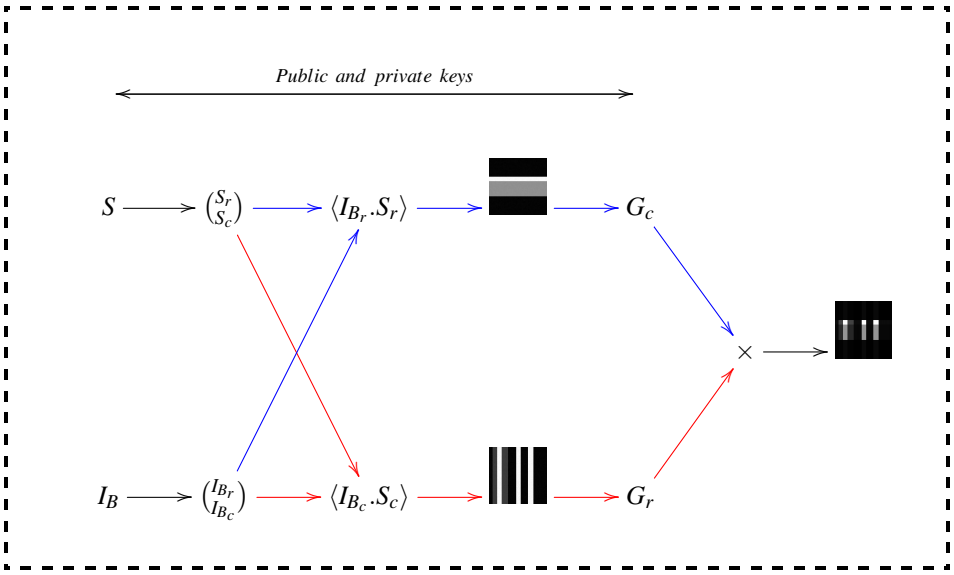


Figure 1. Encryption method based on SCGI

a	*b*	*c*	*d*	*e*	*f*	*g*
Original Image	*Reconstructed image by row sweep*	*Reconstructed image by column sweep*	*Plus (+)*	*Minus(−)*	*divided(÷)*	*cross(×)*
						
–	–	–	*0.9788**	*0.6494*	*0.9922*	*0.9924*
						
–	–	–	*1*	*0.9897*	*1*	*1*

Figure 2. The reconstructed images based on four main actions at the symmetric system, a. Original image, b. The reconstructed image by row sweep , c. The reconstructed image by column sweep, d. Image by plus e. Image by minus, f. Image by divide, g. Image by times.$* \equiv NPCR$

In 2012, our group[12] proposed gray-scale and color optical encryption based on CGI. Again, we verified optical encryption with selective CGI[11]. In 2014, Shengmei et al[27] proposed high-performance optical encryption based on CGI with QR codes and a compressive sensing technique. In 2018, Leihong et al[28] suggested GI public-key cryptography optical encryption and improved feasibility, security, and robustness of the proposed encryption scheme. In 2019, Dawei et.al.[26] followed research on double-layers GI optical information encryption and obtained improved security.
Here, we introduce optical image encryption by SCGI. Encryption is performed by both symmetric and asymmetric systems on the images. We show that encrypted images by the proposed method offer high security, high speed, and also compact data packages.

Theory and Methods

SCGI method and the encryption methods will explain obviously in this section.

SCGI theory

In SCGI theory[18], the random patterns generated by an bright row or column pixels and a low background in each sampling .So, there were two kinds of random patterns that the intensity profile of the reference beam, are named S_r for row (vertical) and S_c for column (horizontal) scannings. In each shot, the place of this bright line is shifted to the next line until the whole reference matrix is swept. a $m \times n$ matrix would require $m+n$ sweeping shots to sweep the whole matrix. The horizontal and vertical

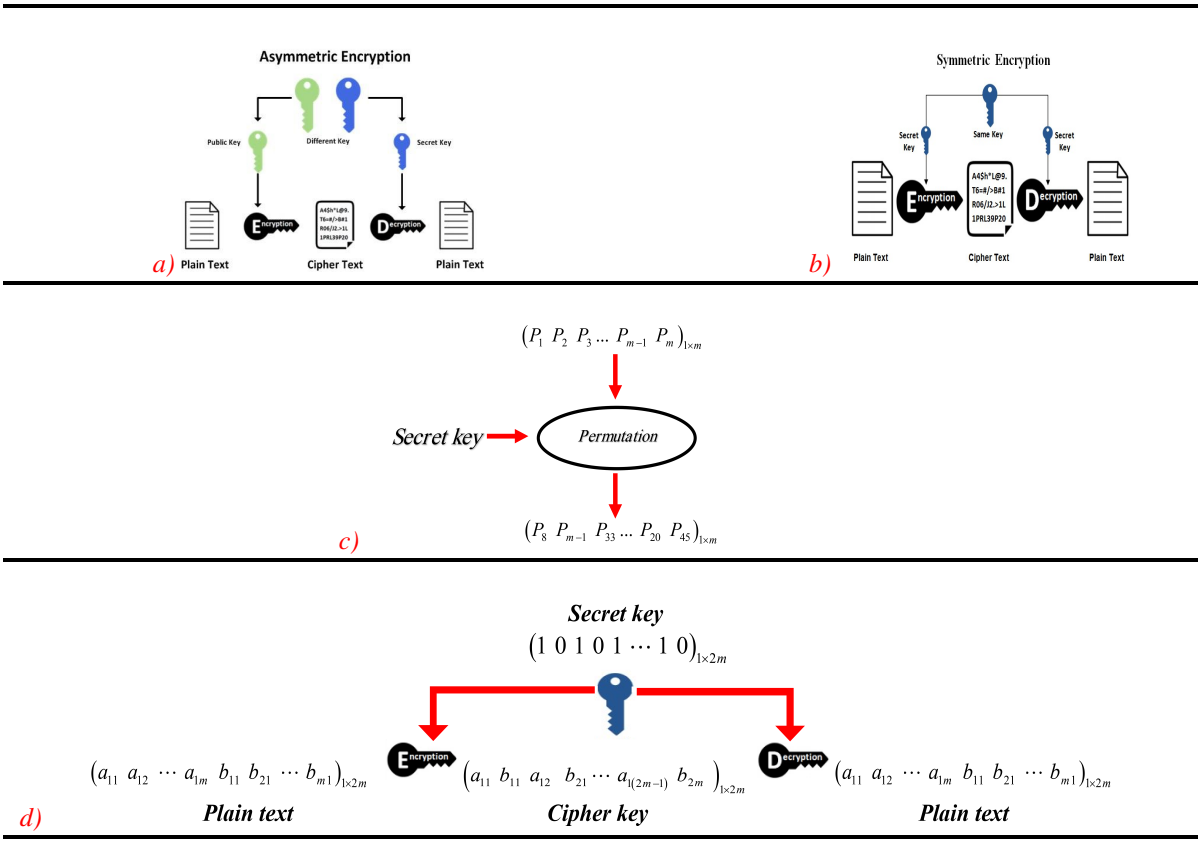


Figure 3. Encryption diagram, a) symmetric encryption, b) asymmetric encryption c, d) encryption diagram for SCGI base on the permutation algorithm.

sweepings are obtained individually as G_r and G_c matrices through the correlation relation between the bucket and the random pattern 1[15,29]:

$$G(x,y) \equiv \frac{1}{N}\sum_{n=1}^{N}(B_n - < B >)I(x,y) =< BI(x,y) > - < B > < I(x,y) \tag{1}$$

G_{c1} and G_{r1} are defined considering a row from G_c and a column from G_r, that calculated by[18]:

$$G_{r1}(1,j) = G_r(a,j), \quad a = arbitraryrowfrom1tom, \quad j = 1:n; \tag{2}$$

$$G_{c1}(i,1) = G_c(i,b), \quad b = arbitraryrowfrom1ton, \quad i = 1:m. \tag{3}$$

The final gray image $(G_(final))$ is reconstructed by cross product of $G_(c1)$ to $G_(r1)$:

$$G_{final}(m,n) = G_{c1}(m,1)G_{r1}(1,n). \tag{4}$$

Encryption

Encrypt has executed by SCGI and the permutation algorithm. So, the asymmetric and symmetric systems are used for encryption that is depicted in fig.1 and fig.3.

Also, to check the security level in encrypted image in above methods under different eavesdropping has been considered the number of pixel changing rate (NPCR) that first is mentioned in 2004 and is calculated as[30]:

$$D(i,j) = \begin{cases} 0, & if \quad C^1(i,j) = C^2(i,j) \\ 1, & if \quad C^1(i,j) \neq C^2(i,j) \end{cases} \tag{5}$$

$$NPCR : N(C^1, C^2) = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{D(i,j)}{T} \times 100 \tag{6}$$

Where C^1 and C^2 indicate ciphertext data before and after changing pixels of the original image, respectively, D is a 2D array is the number of pixels in the ciphertext. NPCR concentrates on the absolute values of a pixel that remains intact under different attacks and demonstrates number of changing pixels in a decrypted image. Its values are always between 0 and 1. $NPCR = 0$ and $NPCR = 1$ denote the lowest and highest security of the encryption system respectively[30]. In this work, $C^1(i,j)$ and $C^2(i,j)$ are encrypted image and non-encrypted image.

Symmetric system

In the symmetric system, cross-operator and row (G_r) and column(G_c) of reconstructed images (fig.2b,c) are selected as the secret key (private key). Therefore, four basic mathematical operators can be performed on the reconstructed images by SCGI. Steps followed for the symmetric encryption were:

1. Reconstructing the image by row and column sweeping, the SCGI method as in fig.2b,c.
2. Cross-operator and row/column matrix selection as the private keys to **encrypt** data.
3. Employing scrambled basic operator sequences to decrypt the data for mimicking an attacker as:
    - 3.1. Plus (fig.2d).
    - 3.2. Minus (fig.2e).
    - 3.3. Divided (fig.2f).
    - 3.4. Cross (fig.2g).
4. Employing pre-known basic operators on pre-selected row and column matrices for images reconstruction; data **decryption** by the receiver.
    - 4.1. Plus (undefined).
    - 4.2. Minus (undefined).
    - 4.3. Divided (undefined).
    - 4.4. Cross (fig.2a).

Asymmetric system

In the asymmetric system, cross-operator and pre-defined row and column matrices of the are considered as the public keys and the permutation algorithm (fig.3c,d) on bucket detector intensities or row and column matrices of the reconstructed images (G_r and G_c) are considered as the private key. Because data is made by two matrices, these matrices could be encrypted individually or together. Consequently, there are three different methods for data encryption in an asymmetric system. In the first method, row and column data of the reconstructed image are placed in a matrix of $G_k = (r_1 \dots r_m c_1 \dots c_m)_{1,2m}$. Then, encryption is performed on this matrix with random permutation algorithm. As seen in fig.3d, the G_r (row matrix) and G_c(column matrix) elements have placed in the odd and even places of G_k, called as the cipher key. The authorized user receives a cipher key to apply the PA on the data and decrypt it. Fig.4 and fig.5 depict simulation and experimental results by using this method. Also, NPCR values for these set of the studies are shown in fig6a and fig7a. As the second method, row/column data of the reconstructed images were separately encrypted or decrypted. This means that the permutation algorithm was separately applied on $G_r \equiv$ (row matrix) $= (r_1 r_2 r_3 \dots r_m)_{1,m}$ row matrix and $G_c \equiv$ (column matrix) $= (c_1 c_2 c_3 \dots c_m)_{m,1}$ column matrix of reconstructed images. This time, the unauthorised attacker has to decrypt two set of data, a row and a column matrix. Consequently, the security of data is doubled in this method. The NPCR values for the theoretical and experimental results of this method based on eavesdropping percentages are indicated in fig.6b and fig.7b, respectively. It can be seen that the security of data is increased more than two folds and the NPCR values did not decrease below 0.88 for the experimental results. As the third method, which is similar to the second, the encryption was performed only one the (G_r) or column matrix and (G_c) row matrix as well as the other column matrices were remained intact. This time, one of the matrices does not have any encryption. Simulation and experimental results of the NPCR based on eavesdropping percentages are depicted in fig.6c and fig.7c respectively.

Steps for asymmetric encryption were:

1. Reconstructing the image by row and column sweeping as described in the SCGI approach.
2. Selecting cross-operator and choosing a row and a column matrix for images reconstruction as the public keys.
3. Applying permutation algorithm as private key on the bucket detector intensities or the row/column data of reconstructed images ((G_r) and (G_c)) for data **encryption**.
    - 3.1. Apply step3 on the first method.
    - 3.2. Apply step3 on the second method.

3.3. Apply step3 on the third method.

4. **Decryption** with employing the corresponding permutation algorithms on the matrices.

The permutation algorithm for the first, second, and third methods are depicted in following equation:

$$\mathrm{PA}=\begin{cases}1)\text{First method}, & G_k=(r_1c_1r_2c_2\dots r_mc_m)_{1,2m}\\ 2)\text{Second method}, & G_r=(r_1r_2\dots r_3)_{1,m}\quad \textbf{and}\quad G_c=(c_1c_2\dots c_3)_{m,1}\\ 3)\text{Third method}, & G_r=(r_1r_2\dots r_3)_{1,m}\quad \textbf{or}\quad G_c=(c_1c_2\dots c_3)_{m,1}\end{cases} \tag{7}$$

Results

Symmetric system

First, image encryption based on symmetric SCGI system is explained in the methods section and results depicted in fig.2. In the symmetric method, after imaging via SCGI, cross-operator and row/column choosing are considered as private keys. Therefore, attacker applies four basic actions for reconstructing images via SCGI. Fig.2 depicts images by applying plus (d), minus (e),divided (f) and cross (g) actions on (b) and (c) images. *NPCR* For simulations $(d-g)$ were 0.9788, 0.6494, 0.9922 and 0.9924,respectively. Also, *NPCR* for experimental images $(d-g)$ were 1, 0.9897, 1 and 1, respectively. The NPCR results show that symmetric method has a very high security.

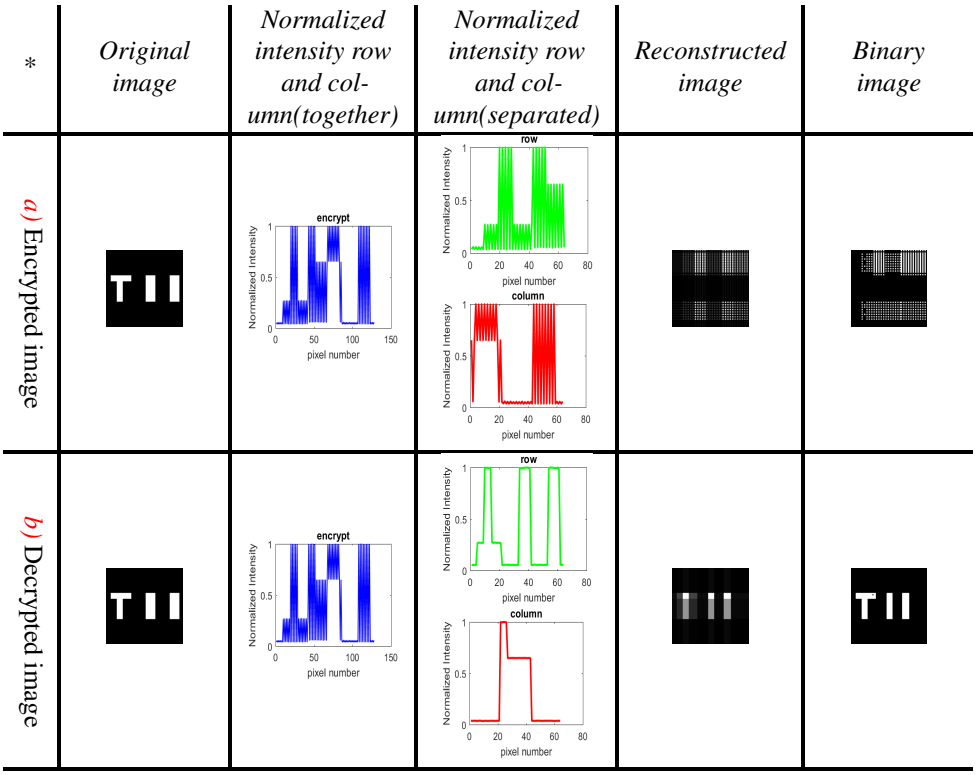


Figure 4. The simulation results at the asymmetric system (first method): the reconstructed images by, a) Encrypted image, b) Decrypted image

Asymmetric system

Second, the encryption was performed based on asymmetric SCGI as explained in the method section. Fig.3 illustrates the encryption diagram by using the permutation algorithm. Fig.4 and fig.5 are simulation and experimental results based on the permutation algorithm. For example, in the fig.4, the second column shows normalized intensities for the row and column values based on the permutation algorithm, the third column shows normalized intensities of the previous column that was separated into two row and column matrices for image reconstruction. The fourth and fifth are reconstructed images and their binary equivalent. In the first method, row and column data of the reconstructed image are placed a matrix of

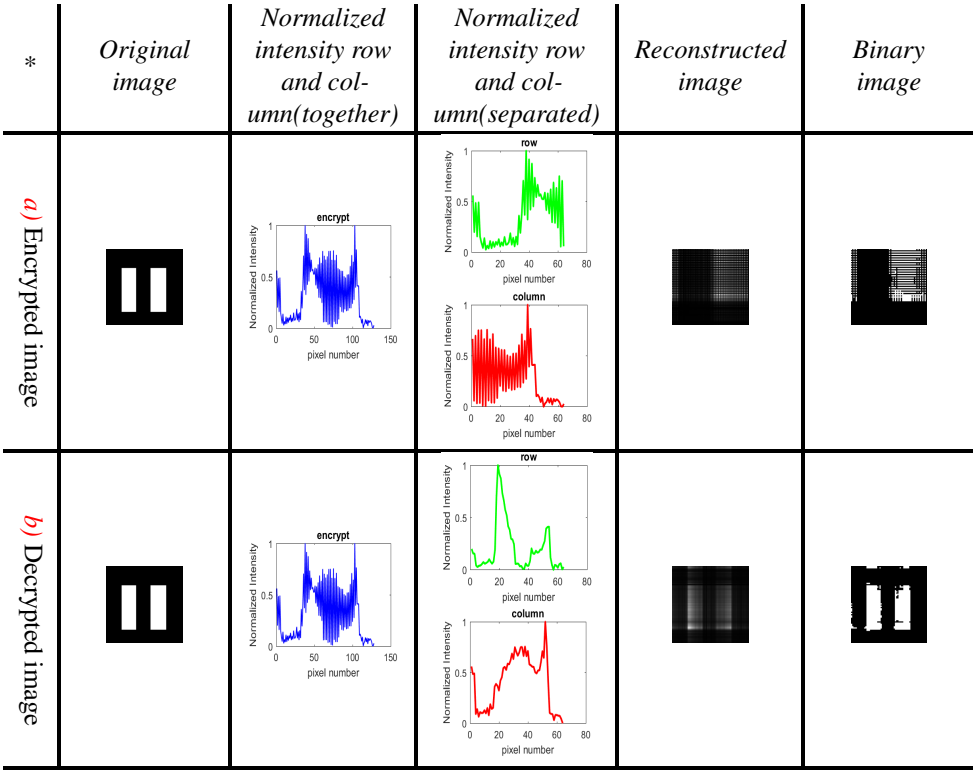


Figure 5. The experimental results at the asymmetric system (first method): the reconstructed images by, a) Encrypted image, b) Decrypted image

$G_k = (r_1 \dots r_m c_1 \dots c_m)_{1,2m}$. Then, encryption is performed on this matrix with random permutation algorithm. Also, *NPCR* results for encrypted image versus eavesdropping percentage are depicted in the fig.6 and fig.7. The graphs of fig.6b and fig.7b have high encryption where G_r and G_c had encrypted. For decrypting the data, attacker needs to understand two permutation algorithms.

NPCR values for simulations and experimental results in the asymmetric case are depicted in fig.6 and fig.7 versus eavesdropping percentage. Results are compared to previous data in the literature[11,12,23] to verify obtained higher security, higher speed, and smaller data packing under the same eavesdropping percentages. Our results have almost the equal securities compared to our previous results in[11] with the exception of their realization with lower shot numbers. In conclusion, NPCR values of the symmetric and the second method of asymmetric encryption, where row/column data of the reconstructed images were separately encrypted, have the highest security.

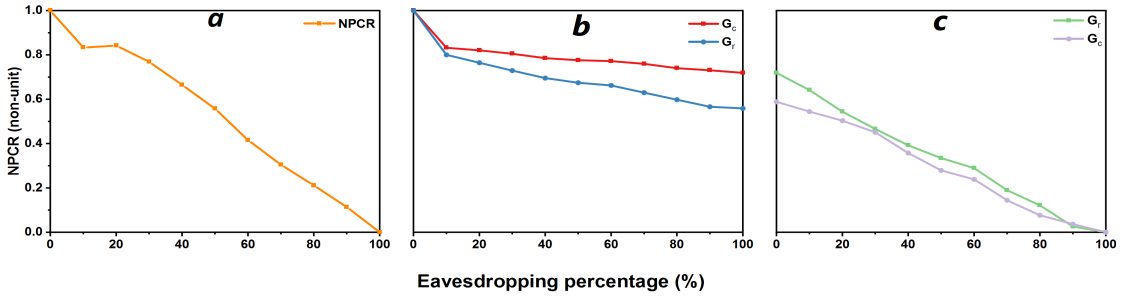


Figure 6. The *NPCR* of the simulation results by encryption variables a) G_k, b) G_r and G_c, and c) G_r or G_c

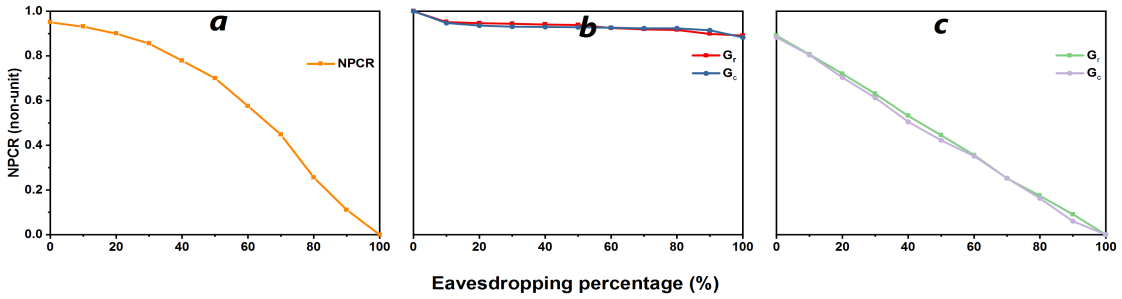


Figure 7. The *NPCR* of experimental results by encryption variables a) G_k,b) G_r and G_c, and c) G_r or G_c

Conclusion

Optical encryption was performed based on SCGI, which offers lower number of shots, shorter image capturing, encryption and description times. This enables high speed and compact data encryption. Encryption had two systems as the symmetric and asymmetric. Also, NPCR as a parameter that displays security level of the decrypted images by an attacker was measured in each case. In the symmetric system, cross operator and selected row and column matrices are private keys. So, we suppose that an attacker implies four basic mathematical operators for decrypting the data. Result for the symmetric system reveal NPCR values close to unity and imply very high security. In the asymmetric case, cross operator and row and column matrices selection are the public keys. We performed a permutation algorithm on row and column matrices, which is assumed as the private key. The asymmetric approach was divided into three sub-systems. This is based on encrypting row and column matrices after their combination as a single matrix, individually or separately. Obviously, separate encryption of the row and column matrices doubles the security. Through the introduced technique, pixel changing rates as high as previously reported values were obtained. However, since our method requires very low shot numbers for image reconstruction, imaging and data processing was quite faster. This also enables smaller data packages and faster communication and promisees widespread application of sweeping ghost-imaging encryption in high security data transfering.

Author contributions statement

All authors Conceptualized and developed the idea and methodology. S.R.G. performed the experiments and developed the codes. B.O. revised codes and experimental setup. S.A. and R.K. discussed and interpreted results. Original draft was prepared by S.R.G. and B.O and revised by S.A and R.K.

Competing interests

The authors declare no competing interests.

References

1. Erkmen, B. I. & Shapiro, J. H. Ghost imaging: from quantum to classical to computational. *Adv. Opt. Photonics* **2**, 405–450 (2010).
2. Ghaleh, S. R., Ahmadi-Kandjani, S., Kheradmand, R. & Olyaeefar, B. Improved edge detection in computational ghost imaging by introducing orbital angular momentum. *Appl. optics* **57**, 9609–9614 (2018).
3. Ryczkowski, P., Barbier, M., Friberg, A. T., Dudley, J. M. & Genty, G. Ghost imaging in the time domain. *Nat. Photonics* **10**, 167–170 (2016).
4. Khakimov, R. I. *et al.* Ghost imaging with atoms. *Nature* **540**, 100–103 (2016).
5. Sun, B. *et al.* 3d computational ghost imaging. In *2014 IEEE Photonics Conference*, 174–175 (IEEE, 2014).
6. Klein, Y., Schori, A., Dolbnya, I., Sawhney, K. & Shwartz, S. X-ray computational ghost imaging with single-pixel detector. *Opt. express* **27**, 3284–3293 (2019).
7. Pelliccia, D. *et al.* Towards a practical implementation of x-ray ghost imaging with synchrotron light. *IUCrJ* **5**, 428–438 (2018).

8. Qiu, X., Zhang, D., Zhang, W. & Chen, L. Structured-pump-enabled quantum pattern recognition. *Phys. review letters* **122**, 123901 (2019).
9. Zhao, S. *et al.* The influence of atmospheric turbulence on holographic ghost imaging using orbital angular momentum entanglement: Simulation and experimental studies. *Opt. Commun.* **294**, 223–228 (2013).
10. Erkmen, B. I. Computational ghost imaging for remote sensing. *JOSA A* **29**, 782–789 (2012).
11. Zafari, M., Ahmadi-Kandjani, S. *et al.* Optical encryption with selective computational ghost imaging. *J. Opt.* **16**, 105405 (2014).
12. Tanha, M., Kheradmand, R. & Ahmadi-Kandjani, S. Gray-scale and color optical encryption based on computational ghost imaging. *Appl. Phys. Lett.* **101**, 101108 (2012).
13. Pittman, T., Shih, Y., Strekalov, D. & Sergienko, A. V. Optical imaging by means of two-photon quantum entanglement. *Phys. Rev. A* **52**, R3429 (1995).
14. Bennink, R. S., Bentley, S. J. & Boyd, R. W. "two-photon" coincidence imaging with a classical source. *Phys. review letters* **89**, 113601 (2002).
15. Shapiro, J. H. Computational ghost imaging. *Phys. Rev. A* **78**, 061802 (2008).
16. Frumker, E. & Silberberg, Y. Femtosecond pulse shaping using a two-dimensional liquid-crystal spatial light modulator. *Opt. letters* **32**, 1384–1386 (2007).
17. Wang, Y. *et al.* High speed computational ghost imaging via spatial sweeping. *Sci. reports* **7**, 45325 (2017).
18. Rajabi-ghaleh, S., Olyaeefar, B., Kheradmand, R. & Kandjani, S. A. Ultra-fast vivid computational ghost imaging of still and moving objects by sweeping random patterns. *J. Opt.* (2020).
19. Li, X., Deng, C., Chen, M., Gong, W. & Han, S. Ghost imaging for an axially moving target with an unknown constant speed. *Photonics Res.* **3**, 153–157 (2015).
20. Gholami-milani, S., Olyaeefar, B., Ahmadi-kandjani, S. & Kheradmand, R. Grayscale and color ghost-imaging of moving objects by memory-enabled, memoryless and compressive sensing algorithms. *J. Opt.* **21**, 085709 (2019).
21. Lian, S. *Multimedia content encryption: techniques and applications* (CRC press, 2008).
22. Goldreich, O. *Foundations of cryptography: volume 2, basic applications* (Cambridge university press, 2009).
23. Clemente, P., Durán, V., Tajahuerce, E., Lancis, J. *et al.* Optical encryption based on computational ghost imaging. *Opt. letters* **35**, 2391–2393 (2010).
24. Kong, L.-J. *et al.* Encryption of ghost imaging. *Phys. Rev. A* **88**, 013852 (2013).
25. Sun, M., Shi, J., Li, H. & Zeng, G. A simple optical encryption based on shape merging technique in periodic diffraction correlation imaging. *Opt. Express* **21**, 19395–19400 (2013).
26. Leihong, Z. *et al.* Research on double-layers optical information encryption based on ghost imaging. *Opt. Commun.* **455**, 124585 (2020).
27. Zhao, S., Wang, L., Liang, W., Cheng, W. & Gong, L. High performance optical encryption based on computational ghost imaging with qr code and compressive sensing technique. *Opt. Commun.* **353**, 90–95 (2015).
28. Yi, K., Leihong, Z. & Dawei, Z. Optical encryption based on ghost imaging and public key cryptography. *Opt. Lasers Eng.* **111**, 58–64 (2018).
29. Bromberg, Y., Katz, O. & Silberberg, Y. Ghost imaging with a single detector. *Phys. Rev. A* **79**, 053840 (2009).
30. Wu, Y., Noonan, J. P., Agaian, S. *et al.* Npcr and uaci randomness tests for image encryption. *Cyber journals: multidisciplinary journals science technology, J. Sel. Areas Telecommun. (JSAT)* **1**, 31–38 (2011).

Figures

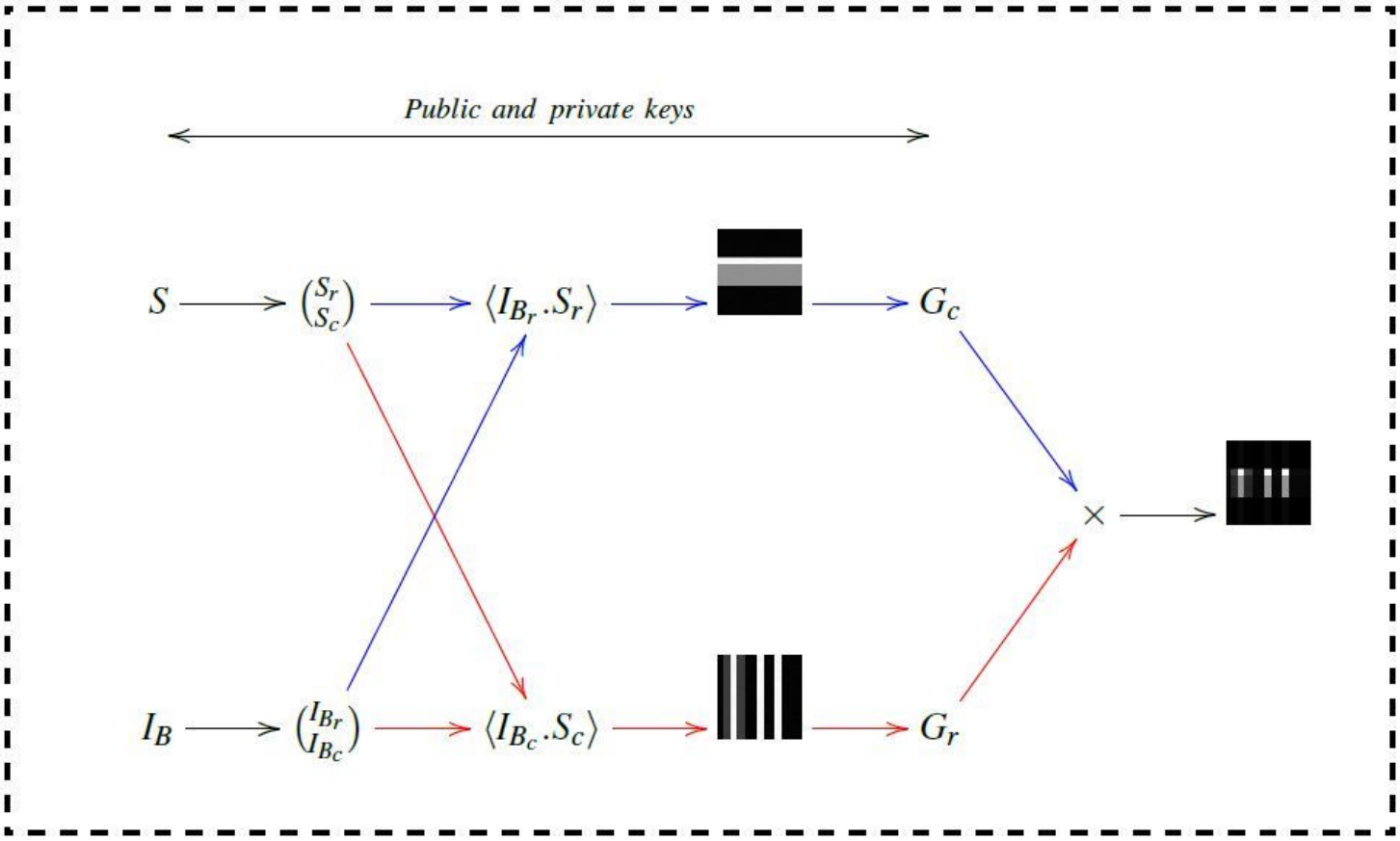


Figure 1

Encryption method based on SCGI

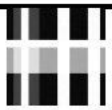
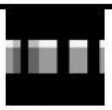
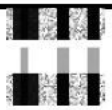
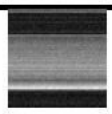
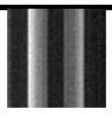
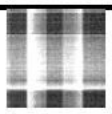
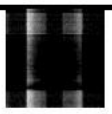
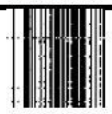
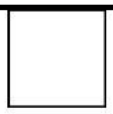
a	*b*	*c*	*d*	*e*	*f*	*g*
Original Image	*Reconstructed image by row sweep*	*Reconstructed image by column sweep*	*Plus (+)*	*Minus(−)*	*divided(÷)*	*cross(×)*
						
–	–	–	*0.9788**	*0.6494*	*0.9922*	*0.9924*
						
–	–	–	*1*	*0.9897*	*1*	*1*

Figure 2

The reconstructed images based on four main actions at the symmetric system, a. Original image, b. The reconstructed image by row sweep , c. The reconstructed image by column sweep, d. Image by plus e.

Image by minus, f. Image by divide, g. Image by times.* □ NPCR

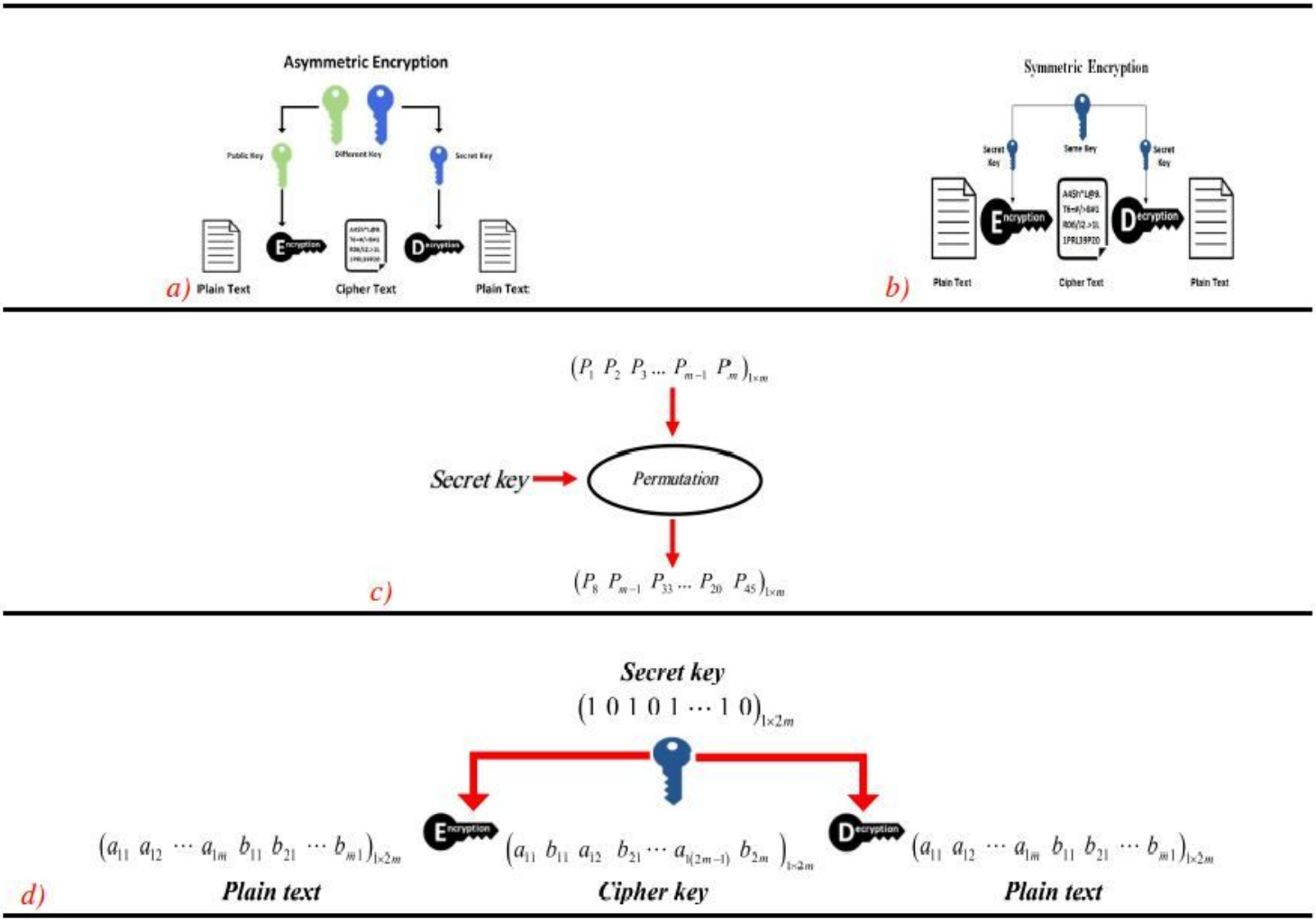


Figure 3

Encryption diagram, a) symmetric encryption, b) asymmetric encryption c, d) encryption diagram for SCGI base on the permutation algorithm.

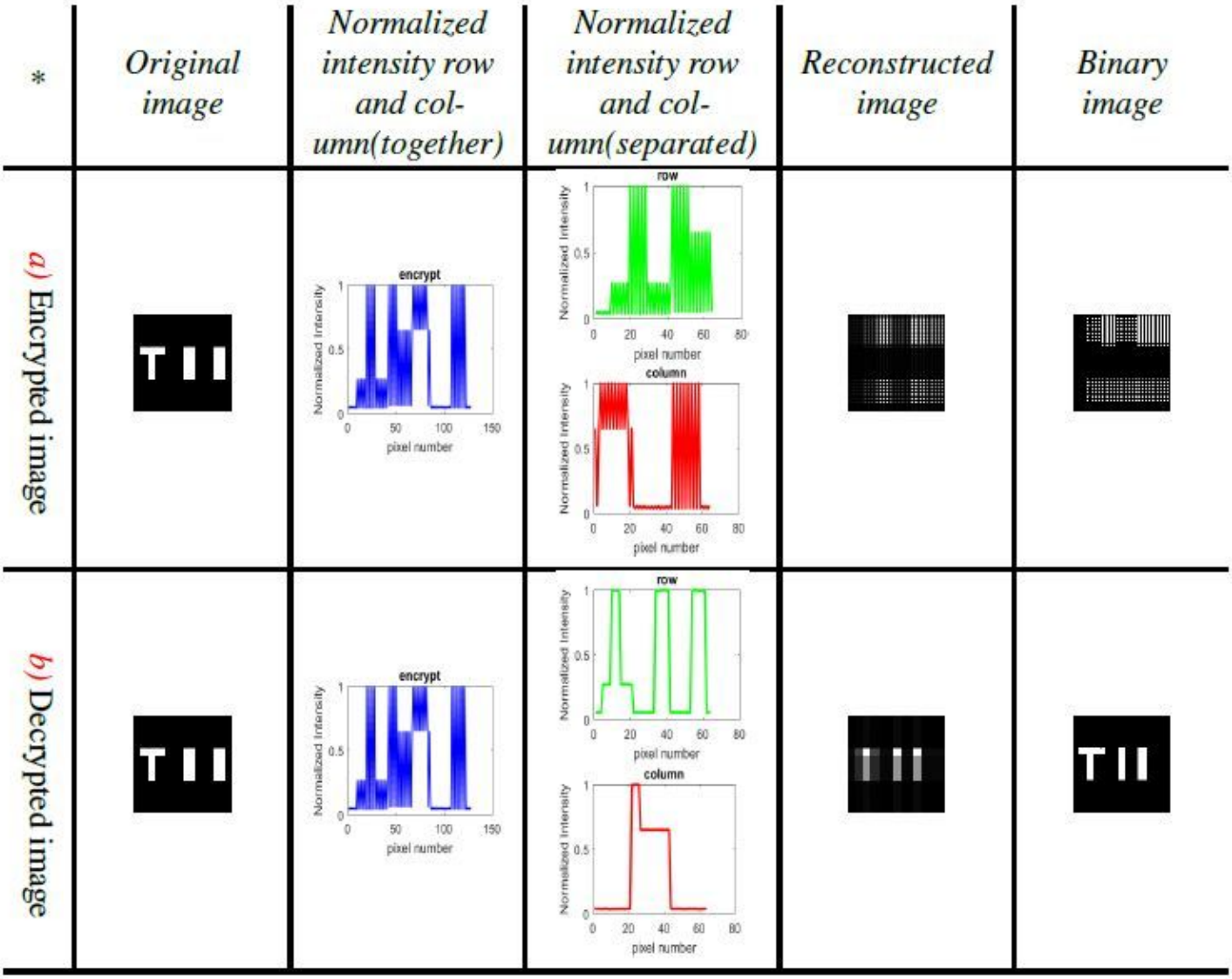


Figure 4

The simulation results at the asymmetric system (first method): the reconstructed images by, a) Encrypted image, b) Decrypted image

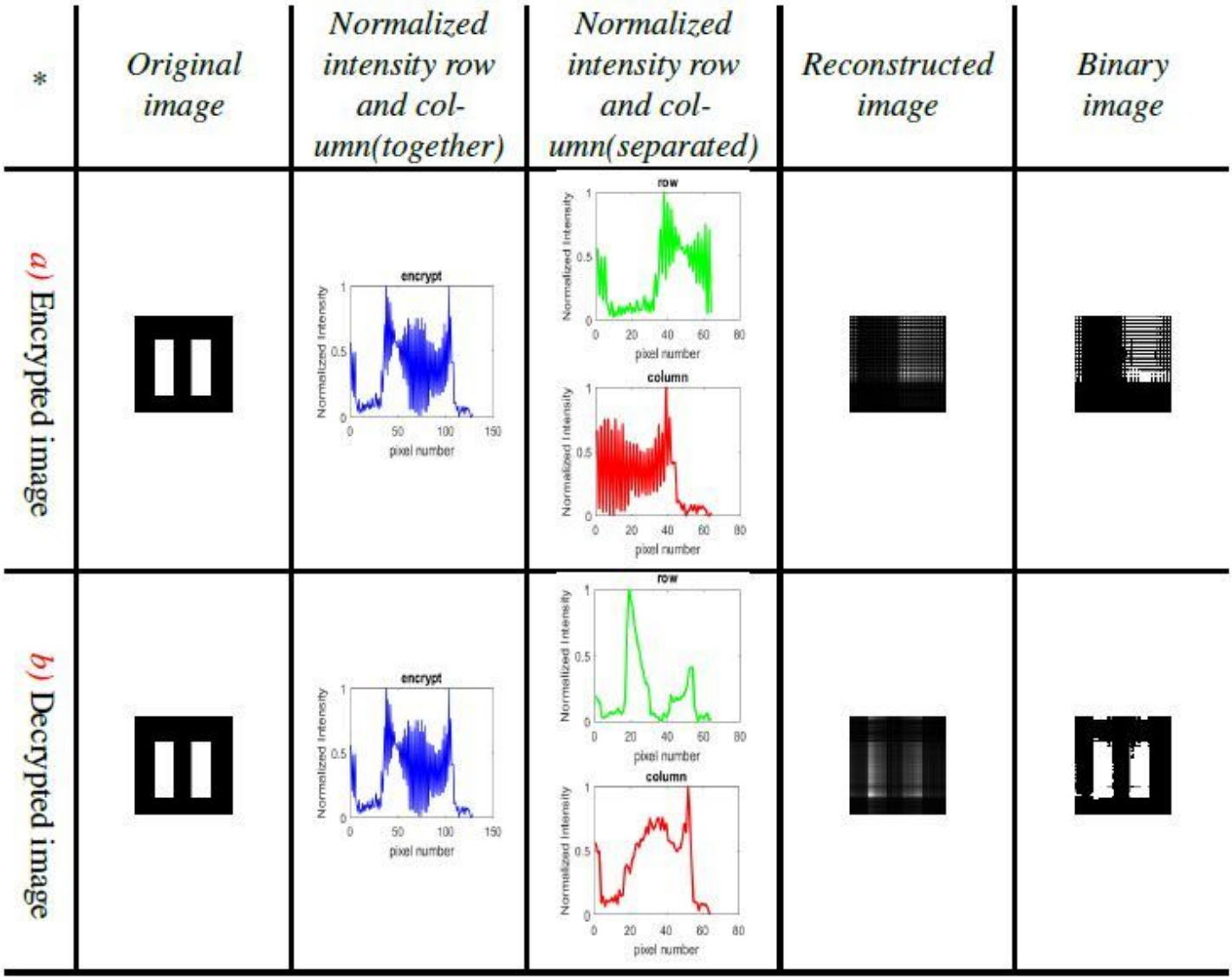


Figure 5

The experimental results at the asymmetric system (first method): the reconstructed images by, a) Encrypted image, b) Decrypted image

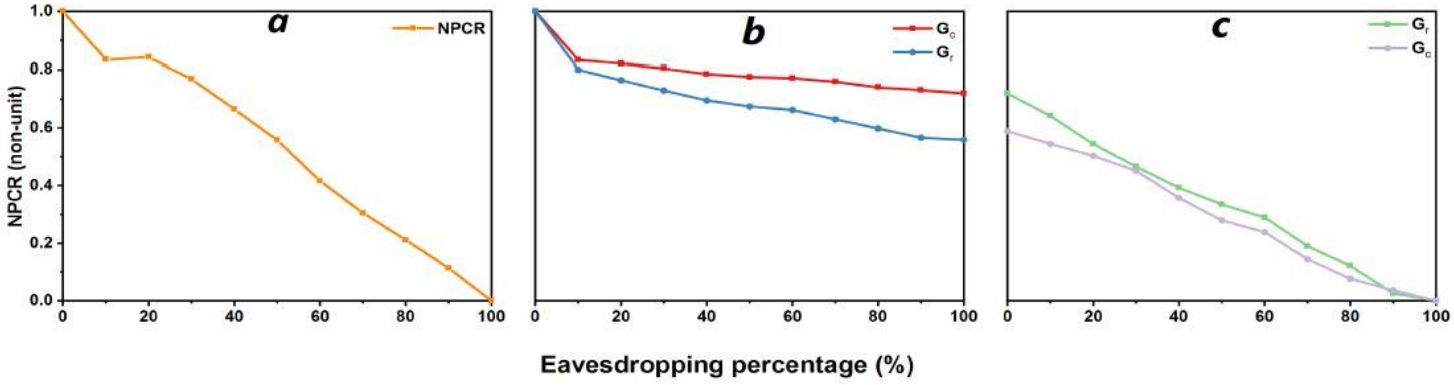


Figure 6

The NPCR of the simulation results by encryption variables a) Gk, b) Gr and Gc, and c) Gr or Gc

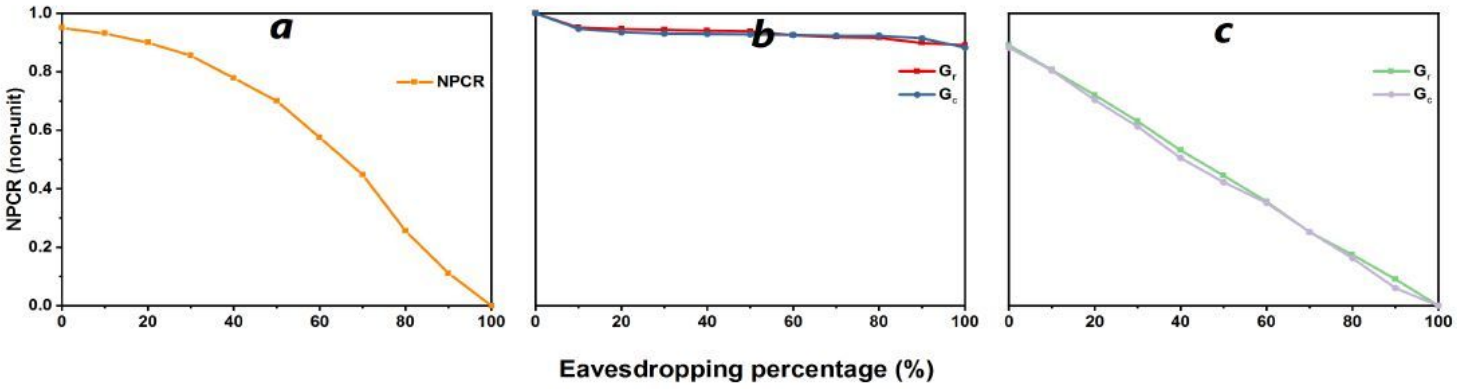


Figure 7

The NPCR of experimental results by encryption variables a) Gk,b) Gr and Gc, and c) Gr or Gc