Multiuser optical image authentication algorithm based on sparse constraint and polar decomposition in cascaded fractional Mellin domain

Kehar Singh*

keharsiitd@gmail.com

kehars@physics.iitd.ac.in

***Optics and Photonics Center IIT Delhi**

Co-workers: Sachin and P.Singh, CUH Mahendergarh (Haryana)
Sachin, P.Singh,and K.Singh (Manuscript under review)

ITNT-2022 (SAMARA), May26

Outline

- Polar Decomposition (Matrix Computations)
- Log-Polar Operator (Nonlinear Transform)
- Fractional Fourier Transform(FrFT)
- Fractional Mellin Transform (FrMT)
- Nonlinear Cryptosystem
- Known-plaintext attack (KPA) analysis on a single FrMT- based cryptosystem
- Multiuser Encryption and Authentication Algorithm
- Results and Discussion
- Nonlinear correlation, Probability parameters, Histograms, Data loss, Noise, Entropy,
- Summary and Conclusions

Polar Decomposition

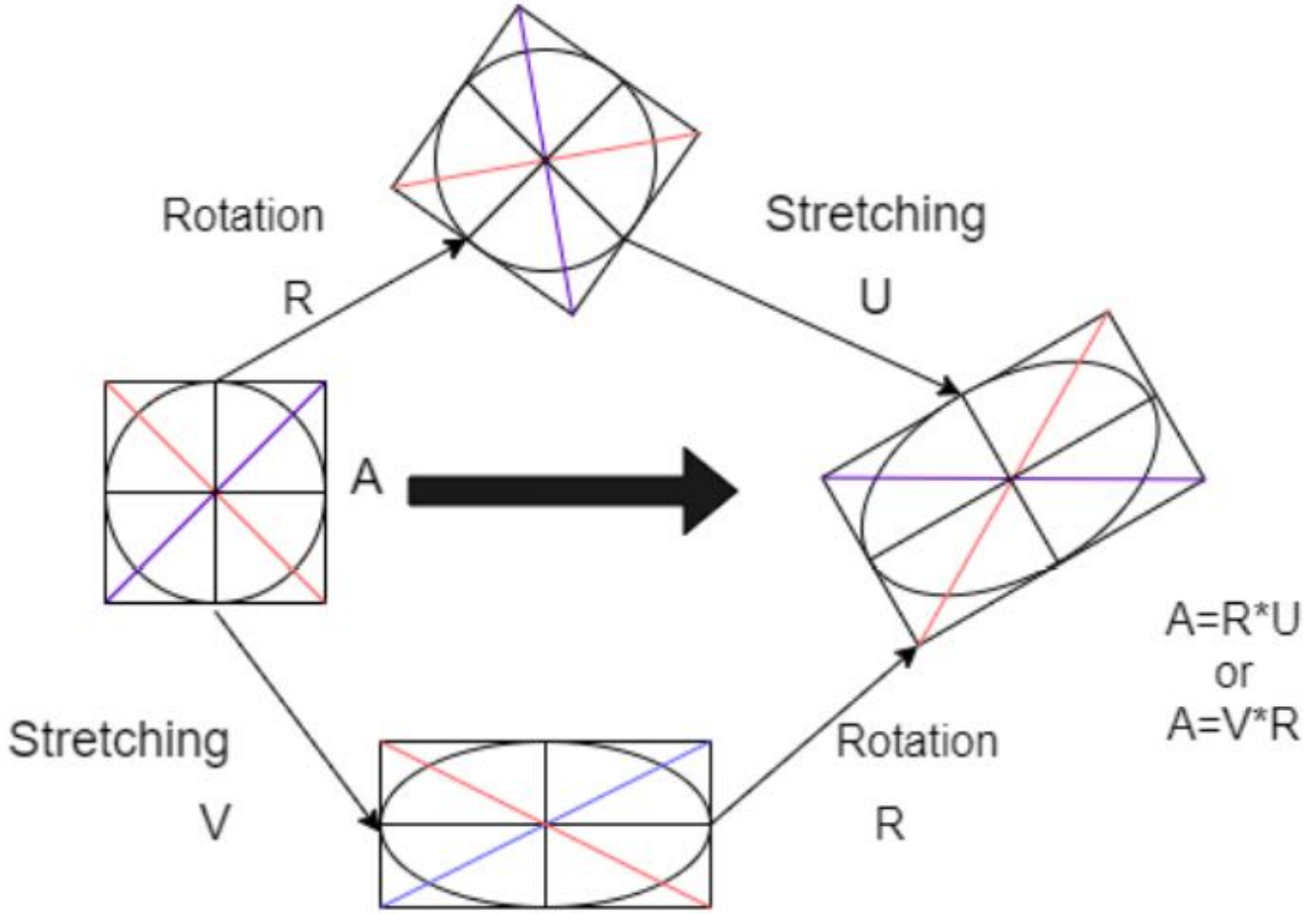
- **Process of decomposing a system into linearly independent factors. PD of an image $A(x, y)$ of size $M \times N$**

$$PD\big(A(x,y)\big) = [R \;\; U \;\; V] \qquad , \qquad A(x,y) = R * V \; or \; U * R$$

- **U and V are symmetric positive definite matrices of size $M \times N$ (Stretching matrices).**
- **R is a rotational matrix of the size $M \times N$.**
- **Symmetric positive definite matrix $(U \; or \; V)$ and the rotational matrix (R) can be used to reconstruct the input matrix $A(x, y)$.**

Golub and Van Loan, Matrix Computations (John Hopkins Univ.Press 1983)

R. Kumar and C. Quan, Asymmetric multi-user optical cryptosystem based on polar decomposition and Shearlet transform, Opt. Lasers Eng. 120 (2019) 118–126,



Polar Decomposition; Geometric representation

The calculation of polar decomposition can be illustrated by assuming a 3×3 matrix.

Consider a matrix $A = \begin{bmatrix} 1 & 3 & 9 \\ 2 & 4 & 7 \\ 5 & 6 & 8 \end{bmatrix}$

In order to perform polar decomposition, the first step is to find the matrix R. Therefore, we calculate a matrix A^*A where A^* is a transpose conjugate operator.

$$A^*A = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 4 & 6 \\ 9 & 7 & 8 \end{bmatrix} \begin{bmatrix} 1 & 3 & 9 \\ 2 & 4 & 7 \\ 5 & 6 & 8 \end{bmatrix} = \begin{bmatrix} 30 & 41 & 63 \\ 41 & 61 & 103 \\ 61 & 103 & 194 \end{bmatrix}$$

Find the change of basis matrix (S) from eigen space of A^*A in order to diagonalize A^*A. Matrix (S) contains the eigen vectors of A^*A. Matrix (B) contains the eigen values of the A^*A in its diagonal. Take the square root of Matrix (B) to get matrix C.

$$S = \begin{bmatrix} 0.6143 & 0.7320 & 0.2946 \\ -0.7619 & 0.4532 & 0.4628 \\ 0.2052 & -0.5087 & 0.8361 \end{bmatrix}$$

$$B = \begin{bmatrix} 0.1972 & 0 & 0 \\ 0 & 11.5988 & 0 \\ 0 & 0 & 273.2040 \end{bmatrix} \text{ and } C = \begin{bmatrix} 0.4441 & 0 & 0 \\ 0 & 3.4057 & 0 \\ 0 & 0 & 16.5289 \end{bmatrix}$$

To calculate U, find $U = SCS^{-1}$

$$U = \begin{bmatrix} \mathbf{0.6143} & \mathbf{0.7320} & \mathbf{0.2946} \\ \mathbf{-0.7619} & \mathbf{0.4532} & \mathbf{0.4628} \\ \mathbf{0.2052} & \mathbf{-0.5087} & \mathbf{0.8361} \end{bmatrix} \begin{bmatrix} \mathbf{0.4441} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{3.4057} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{16.5289} \end{bmatrix} \begin{bmatrix} \mathbf{0.6143} & \mathbf{-0.7619} & \mathbf{0.2052} \\ \mathbf{0.7320} & \mathbf{0.4532} & \mathbf{-0.5087} \\ \mathbf{0.2946} & \mathbf{0.4628} & \mathbf{0.8361} \end{bmatrix}$$

$$U = \begin{bmatrix} 3.4269 & 3.1752 & 2.8591 \\ 3.1752 & 4.4967 & 5.5405 \\ 2.8591 & 5.5405 & 12.4550 \end{bmatrix}$$

U is symmetric positive definite matrix.

$R = AU^{-1}$ and R is unitary matrix such that $RR^* = R^*R = I$. Here R^* is the matrix obtained after performing transpose and conjugate on matrix R.

$$\mathrm{R} = \begin{bmatrix} -0.1275 & -0.3745 & 0.9184 \\ -0.4423 & 0.8503 & 0.2853 \\ 0.8878 & 0.3698 & 0.2740 \end{bmatrix}$$

The second symmetric positive definite matrix V can calculated by using R such that $V = AR^{-1}$.

$$V = \begin{bmatrix} 7.0151 & 4.6763 & 4.4633 \\ 4.6763 & 4.5137 & 5.1729 \\ 4.4633 & 5.1729 & 8.8499 \end{bmatrix}$$

Log-Polar Operator (Nonlinear Transform)

Is a non-uniform and nonlinear sampling method for converting images from their Cartesian coordinates $I(x, y)$ to their Log-Polar coordinates $I(\rho, \theta)$.

$$\rho = log\sqrt{(x - x_0)^2 + (y - y_0)^2} \ , \quad \theta = \left(\frac{y - y_0}{x - x_0}\right)$$

- **Coordinate (x_0, y_0) denotes the center pixel and (x, y) denotes the sampling pixels of image $I(x, y)$ in Cartesian co-ordinates.**
- **ρ is radius and θ is angular position in the Log-Polar co-ordinates. Circumference of the circle is sampled with the same number of samples for each radius in angular direction.**
- **There exists no one-to-one correspondence between cartesian-, and log polar coordinates.**
- **Therefore, pixels closer to the center of the image are over-sampled, but pixels away from the center are either missed or under-sampled.**
- **Advantage of Log-Polar coordinates over Cartesian coordinates is that the rotation and scaling operation in Cartesian coordinates are represented as shifting operation in the Log-Polar coordinates system. The mathematical evidence of the above fact is illustrated below:**

Let an input image $f(x, y)$ be scaled and rotated about parameter a and angle α and that results in $g(x', y')$. In terms of the coordinates system, coordinates $[x\ y]$ change to $[x'\ y']$ by using

$$\begin{bmatrix} a\cos\alpha & -a\sin\alpha \\ a\sin\alpha & a\cos\alpha \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

where $\alpha = \left(\frac{y}{x}\right)$. Let $g(\rho', \theta')$ be the Log-Polar transformed image of $g(x', y')$ whose radius ρ' and angular position θ' are obtained as below:

$$\rho' = \log \sqrt{x'^2 + y'^2}$$

$$\rho' = \log \sqrt{(a\,x\cos\alpha - a\,y\sin\alpha)^2 + (a\,x\sin\alpha + a\,y\cos\alpha)^2}$$

$$\rho' = \log \sqrt{a^2(x^2 + y^2)} = \rho + \log a$$

$$\theta' = \tan^{-1}\left(\frac{y'}{x'}\right)$$

$$\theta' = \tan^{-1}\left(\frac{ax\sin\alpha + ay\cos\alpha}{ax\cos\alpha - ay\sin\alpha}\right)$$

In the polar coordinate system, by substituting the value of $x = \rho\cos\theta$, and $y = \rho\sin\theta$

$$\theta' = \tan^{-1}\left(\frac{a\,\rho\,\cos\theta\sin\alpha + a\,\rho\sin\theta\cos\alpha}{a\,\rho\,\cos\theta\cos\alpha - a\,\rho\,\sin\theta\sin\alpha}\right) = \tan^{-1}\left(\frac{\sin(\theta+\alpha)}{\cos(\theta+\alpha)}\right), \qquad \theta' = \theta + \alpha$$

L. Gong, X. Liu, F. Zheng, and N. Zhou, Flexible multi-image encryption algorithm based on log-polar transform and double random phase encoding technique, J. Mod. Opt. 60 (2013) 1074-1082.

Log-Polar operator can be applied to annular domain only. Therefore, some parameters are required to be fixed in advance to implement the Log-Polar operator. These parameters are: the center of annular domain (c_x, c_y), radii of the innermost (r_i) and outermost (r_o) rings, and number of sampling points along distance (n_r) and angle axes (n_w).

Sampling points (n_r) and $(n_{w)}$ are used to describe the number of rings and number of wedges in the Log-Polar operation There is a need for tradeoff between the quality of recovered image and computational time. Therefore, the sampling points n_r and n_w need to be selected wisely. The result of image encryption using the Log-Polar operation is depicted in Fig.

Log-Polar operation; (a) Plaintext, (b) Log transformed image, and (c) Recovered image of 'Building'.

Fractional Fourier Transform (Fr FT)

- **Generalization of the full Fourier transform, and is widely used in signal and image processing.**
- **It has an additional degree of freedom i.e., fractional parameter, say p.**
- **The FrFT for an input function $f(x)$ is given by,**

$$F^p\big(f(x)\big) = \int_{-\infty}^{\infty} f(x)\, K_p(x,u)dx$$

$K_p(x,u)$ is kernel of the transform

$$K_p(x,u) = \begin{cases} A\exp\big(i\pi(x^2\cot\phi - 2xu\csc\phi + u^2\cot\phi)\big) & \text{if } p = n\pi \\ \delta(x-u) & \text{if } p = 2n\pi \\ \delta(x+u) & \text{if } p = (2n+1)\pi \end{cases}$$

$A = \frac{exp(-i[\pi sgn(\phi)/u - \phi/2])}{\sqrt{|sin\phi|}}$ and $\phi = \frac{p\pi}{2}$. For $p = 1$, the FrFT is reduced to a full Fourier transform.

P.Kumar, J.Joseph, K.Singh, Double random phase encoding based optical encryption using some linear canonical transforms: weaknesses and countermeasures, In "Linear Canonical Transforms", Eds. J.J.Healy, M. Alper Kutay, H.Ozaktas, and J.Sheridan (Springer NY 2016) pp. 367-396.

Fractional Mellin Transform (Fr MT)

Log-polar operation and FrFT combine to give the FrMT. FrMT for an input signal $f(x, y)$ is,

$$M^p(u,v) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\; x^{((-2iu\pi/sin\beta)-1)} exp\left[\frac{i\pi}{tan\beta}(u^2 + ln^2x)\right] y^{((-2iv\pi/sin\beta)-1)}\; exp\left[\frac{i\pi}{tan\beta}(v^2 + ln^2y)\right] dx\, dy$$

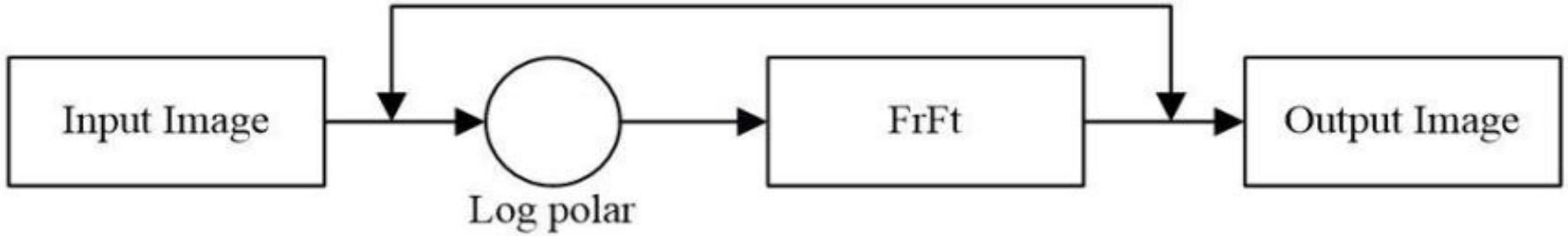
where $\beta = \frac{p\pi}{2}$, and p is fractional order of the transform.

The relationship between the FrFT (F^p) and FrMT (M^p) is

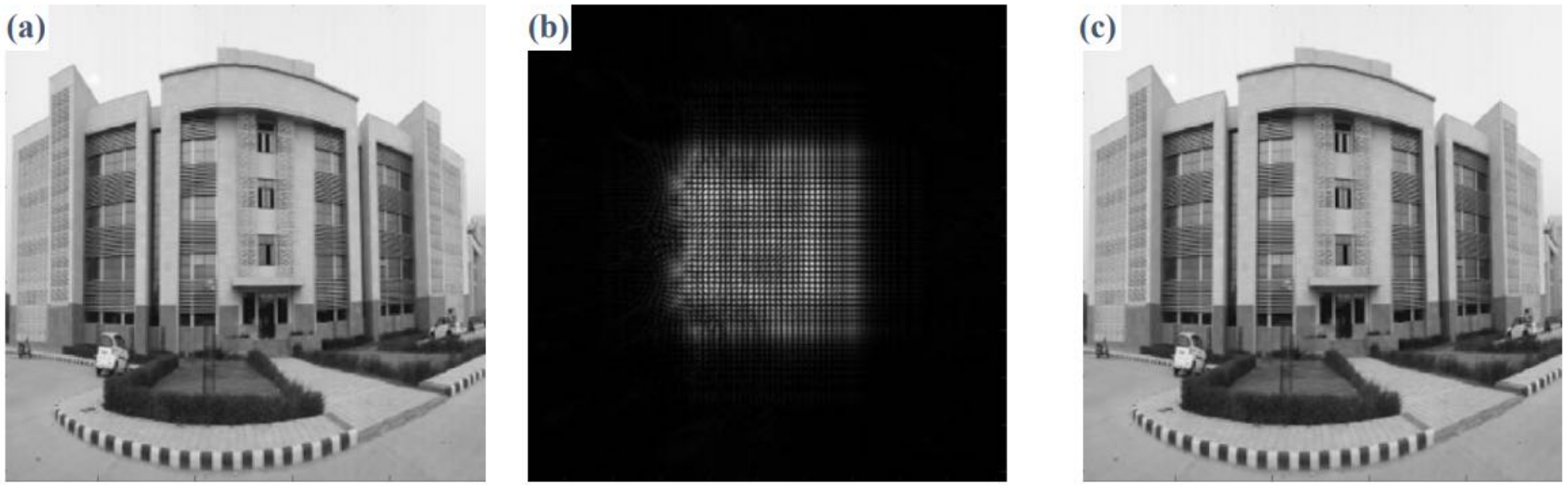
$$M^p(u,v) = CF^p\big(f(\rho,\theta)\big)$$

C is constant and $\rho = ln\left(\sqrt{x^2+y^2}\right)$ and $\theta = arctan\left(\frac{y}{x}\right)$. Figure illustrates the fractional Mellin transformation. The result of image encryption using the FrMT is depicted

(P. Singh, A.K Yadav, K. Singh, Security analysis of a non-linear-mask based cryptosystem in fractional Mellin domain , Asian J. Phys. 30 (2021) 1397-1406).



Flowchart diagram of the FrMT



Result of FrMT:(a) Plaintext,(b) FrM Transformed image,(c) Recovered image of 'Building'

Nonlinear Cryptosystem

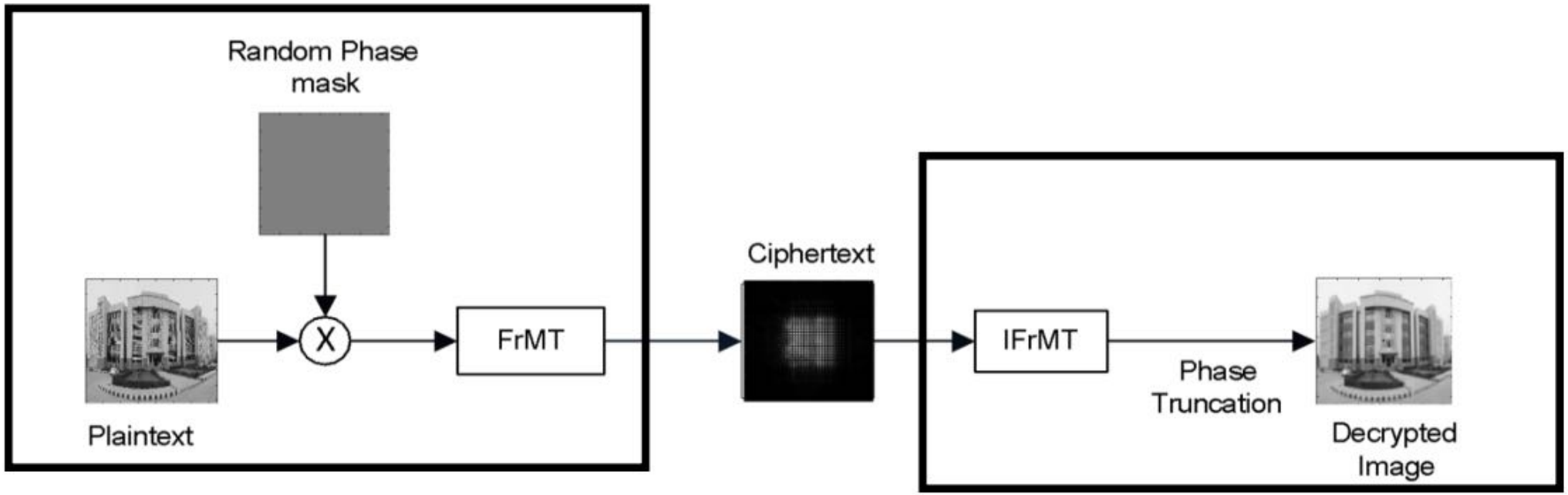
A random phase mask (RPM) is bonded to the plain-text and the resulting image is propagated through the FrMT to generate the ciphertext.

$$E = FrMT(I(x,y) * RPM)$$

$RPM = exp(2\pi i m(x,y))$; $m(x,y)$ **is a random matrix assuming values between 0 and 1.**

Decrypted image is obtained by applying inverse FrMT $(IFrMT)$ **on the ciphertext image.**

$$D = PhaseTruncation(IFrMT(E))$$



(a) Encryption process

(b) Decryption process

Known-plaintext attack (KPA) analysis on a single Fr MT- based cryptosystem

In the known-plaintext attack, an attacker has a pair of input and encrypted images, and also has all the information about the scheme, except the secret keys.

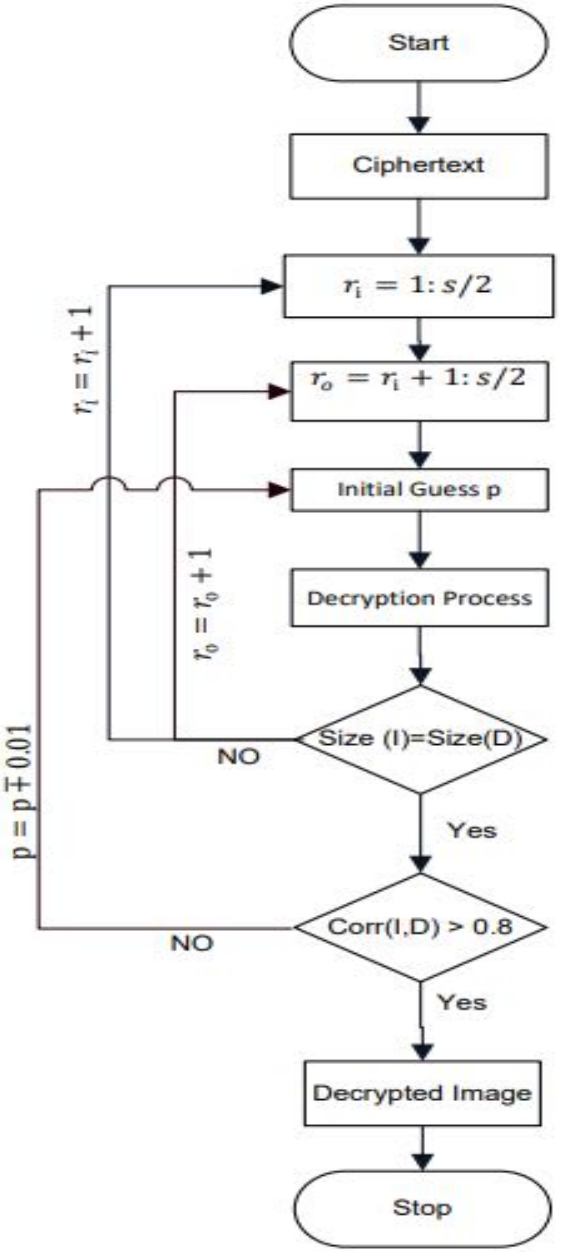
The cryptosystem discussed in the above subsection has FrMT parameters as secret keys. In fact, the attacker needs the radius of inner ring (r_i) and fractional order of the FrMT.

Decryption process starts by assuming an initial value of the radius of inner most ring, and the value of fractional parameter.

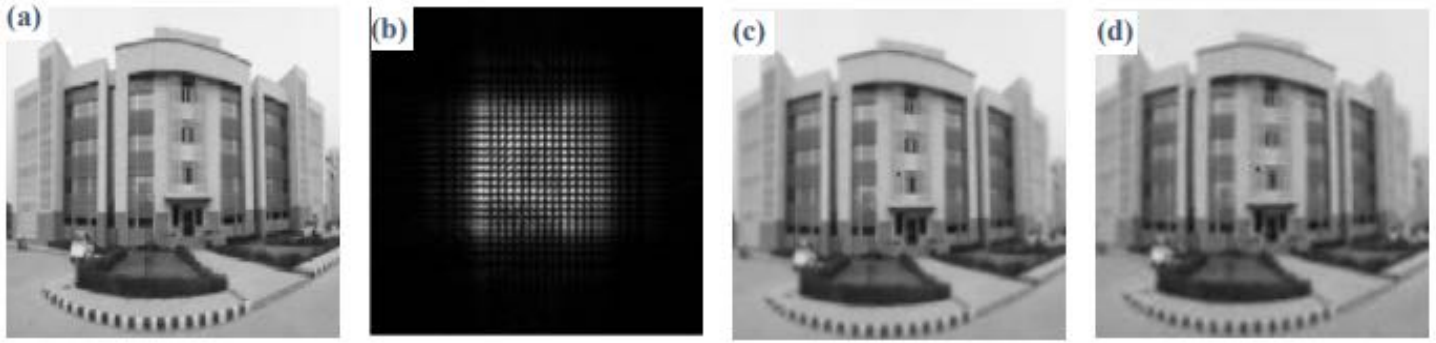
Ciphertext is decrypted using initial values as the secrete keys of the cryptosystem. Size of the decrypted image depends on r_i and r_o. If the size of the input image (I) and the retrieved image (D) are same, the attack algorithm is further continued otherwise the inner and the outer radii are updated .

Correlation coefficient (CC) between the plaintext and the retrieved image is calculated, and if it is more than 0.8, the attack algorithm terminates. If decrypted image is still not recognizable, the value of the fractional order p is updated and the process is repeated.

The convergence condition for the special KPA is the CC between plaintext and the recovered image. The decrypted image from the special KPA attack is shown in Fig. validating the proposed attack algorithm.



s=size of the cipher-text



(a) Plaintext image of 'Building'; (b-c) Corresponding ciphertext and recovered image y; (d) Retrieved image obtained by the iterative known-plaintext attack.

Multiuser Encryption and Authentication Algorithm

Encryption process

Step 1: Image $I(x, y)$ is bonded with an (RPM) and propagated through the $(FrMT)$ with center of the annular domain (c_x, c_y), radii of innermost ring r_i and the outermost ring r_o, and the number of sampling points along distance n_r and angle axes n_w. $E_1(u, v) = FrMT^p(I(x, y) * RPM1)$

p is order of the FrMT, $RPM1 = exp(2\pi i * R_1)$, and R_1 is a random matrix in the range of [0 1] having same size as that of the input image.

Step 2: A probability parameter k_1 is used to construct a binary amplitude random mask (BARM) of the size of signal E_1. The probabilities of ones in BARM are defined by k_1. Sparse from the signal E_1, is extracted by bonding the BARM with E_1 and output result is stored as E_2.

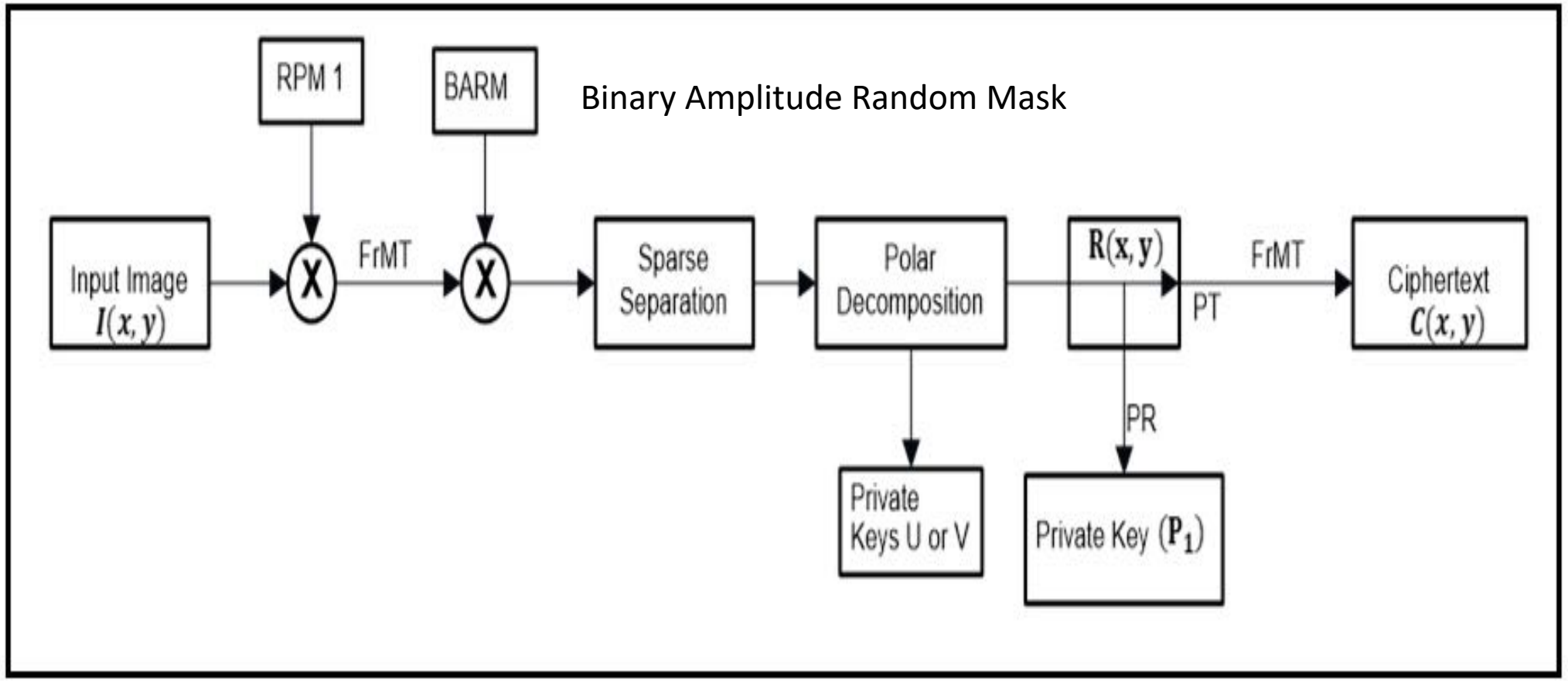
$$E_2(u, v) = E_1(u, v) * BARM$$

Step 3: PD is used to decompose the sparse separated signal (E_2) into three signals R, U, and V. Signals U and V are used as the private keys in the cryptosystem, and signal R is further processed.

$$[R\ U\ V] = PD(E_2(u, v))$$

Step 4: Using principle of phase-truncation and phase-reservation, the phase part i.e. (R) is reserved which acts as private key. Phase-truncated part i.e. $abs(R)$ is further propagated through the $(FrMT)$.

$P_1 = angle(R)$, $E_3 = abs(R)$, $C = FrMT^p(E_3(x, y))$ Ciphertext of encryption algorithm



Schematic diagram of the encryption process of the proposed scheme.

Sparsity also used by: H. Wei and X. Wang, Optical multiple-image authentication and encryption based on phase retrieval and interference with sparsity constraints, Opt. Laser Technol. 142(2021) p. 107257, Art ID107257.

Decryption and authentication process

Step1: The ciphertext obtained in the encryption process is back-propagated through the FrMT, and the output image is bonded with a private key P_1 to obtain D_1 as: $D_1 = FrMT^{-p}(C) * exp(i * P_1)$

Step 2: D_1 is bonded with one of the private keys, i.e., either U or V obtained by PD operation during the encryption process. $D_2 = D_1 * U \; or \; V * D_1$

Step 3: D_2 is propagated through the FrMT and the amplitude of the resultant output gives the partial decrypted image. $D_3 = |FrMT^{-p}(D_2)|$

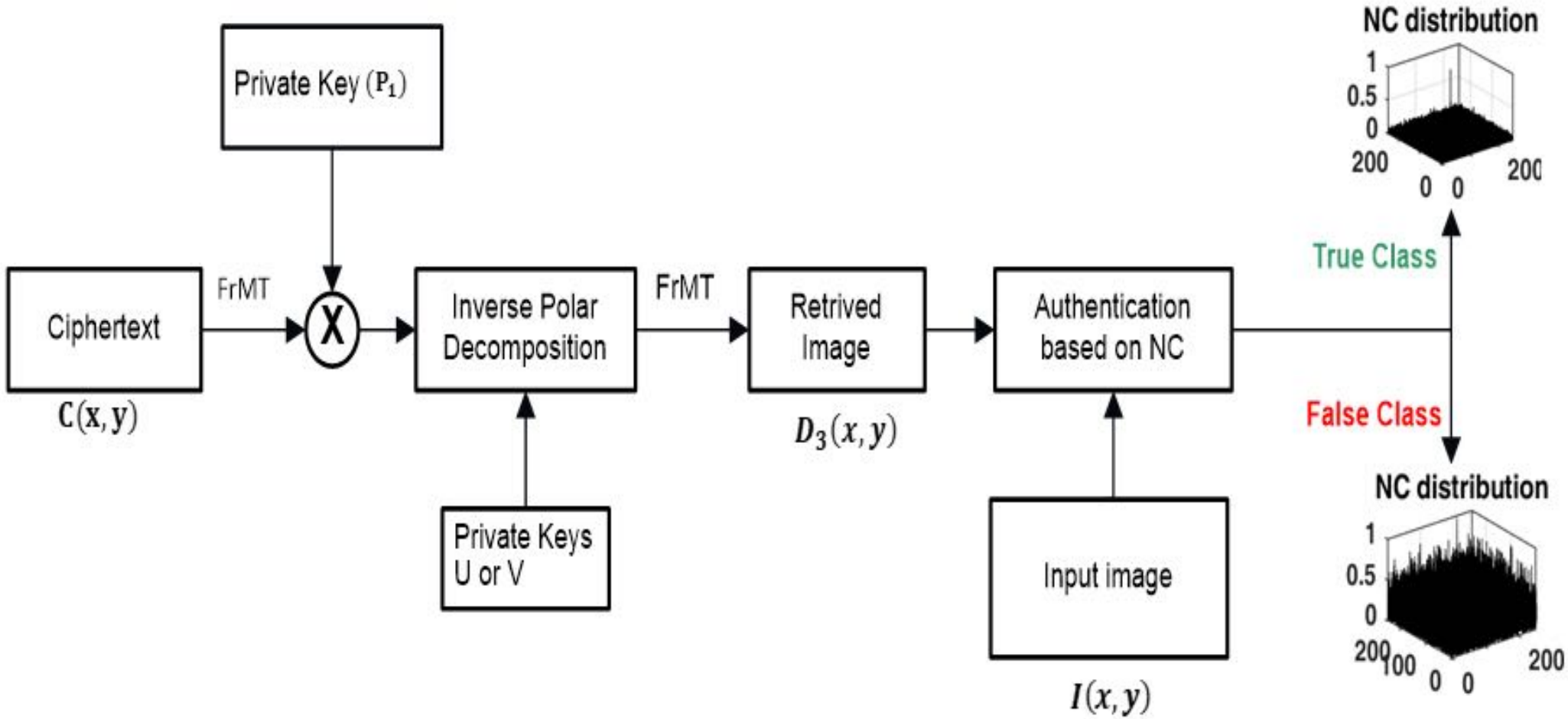
It is not always possible to recognize the recovered data (D_3) obtained from partial decryption. Therefore, similarity between the plaintext and recovered image is identified by using a correlation function. There are various correlators e.g.nonlinear correlation (NC) function, joint-correlation transformations, and joint-fractional correlation transformations]. The NC function provides the best true classification results. The decrypted image can be considered a true class image if it exhibits a significant correlation peak in the NC function. When the NC function's distribution is noisy, the image is classified as a false class image, indicating fake authentication attempt Mathematically, the NC function is expressed by

$$NC(x,y) = IFT|I'(u,v).* D_3'(u,v)|^k \times e^{i*\theta(u,v)}$$

$$I'(u,v) = FT\big(I(x,y)\big), D_3'(x,y) = FT\big(D_3(x,y)\big)$$

$$\theta(u,v) = angle\big(I'(u,v)\big) - angle\big(D_3'(u,v)\big)$$

$NC(x,y)$ denotes the nonlinear correlation function, FT denotes the Fourier transform, IFT denotes the inverse Fourier transform, $I(x,y)$ is input image, $D_3(x,y)$ is recovered image, and k denotes the nonlinearity index.



Decryption-cum-authentication process of proposed algorithm.

Results and Discussion

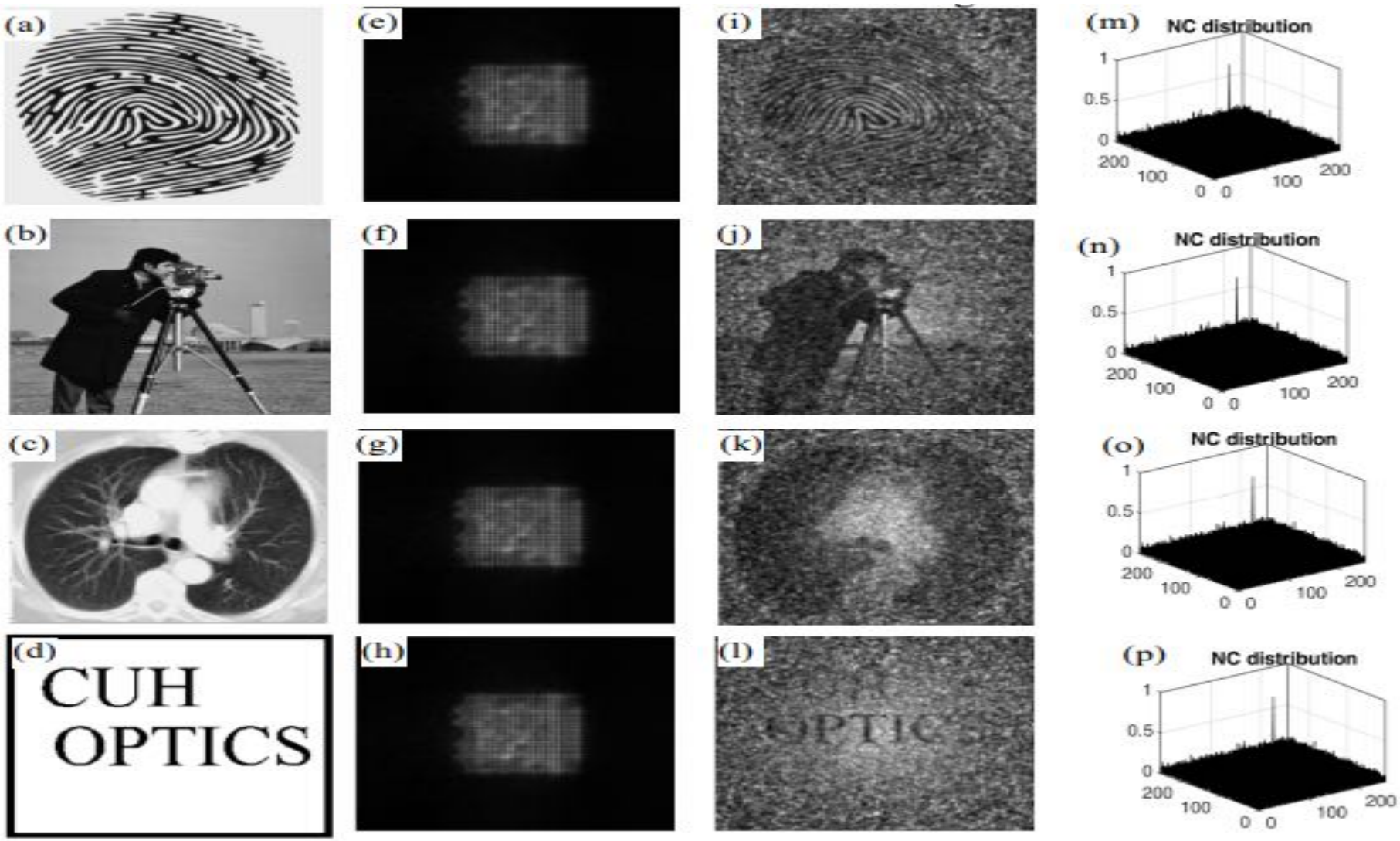
- **Simulation using MATLAB™ 2020a**

- **Images having 255×255 pixels.**
- **Center of the annular domain $(c_x = 128, c_y = 128)$, the radius of innermost $(r_i = 1)$ and outermost $(r_o = 90)$ rings,**

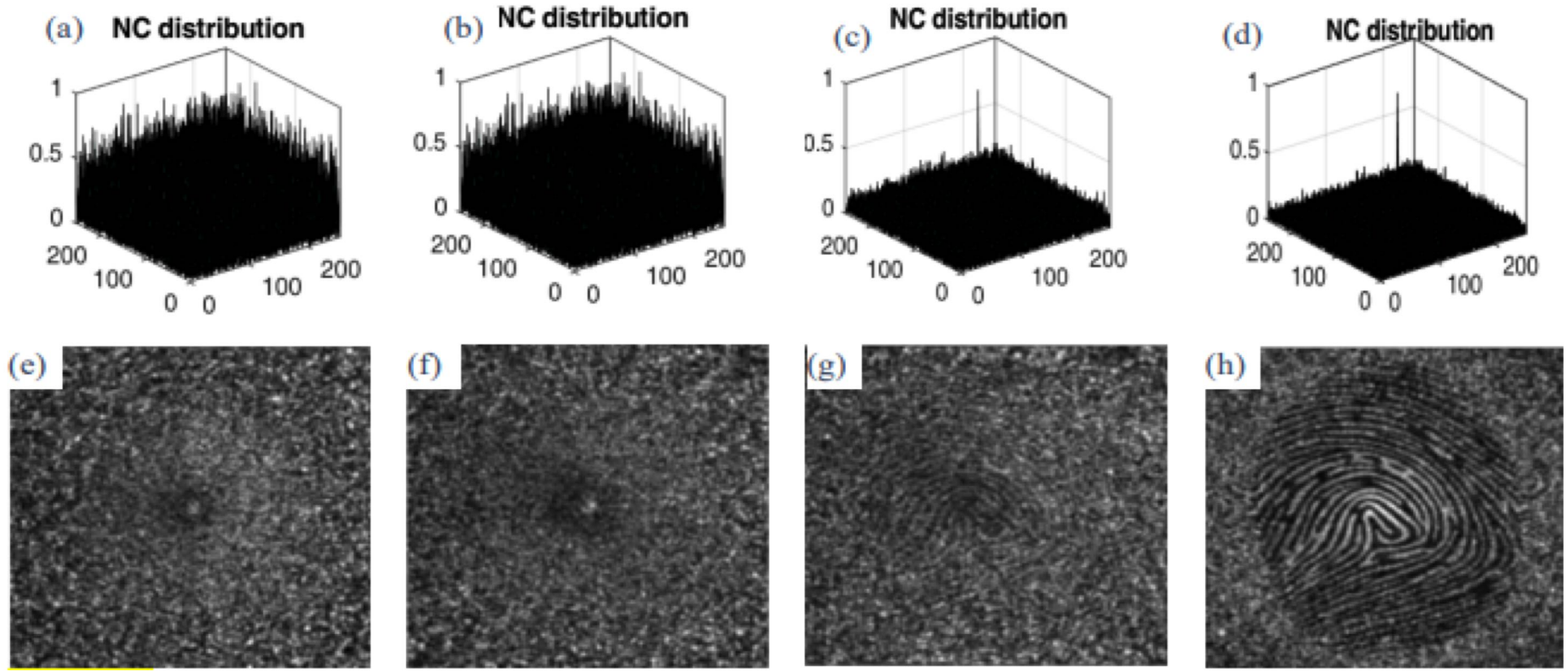
- **Number of sampling points along distance $(n_r = 511)$, and angle axes $(n_w = 511)$.**

- **Probability parameter k_1 and the nonlinearity index k were set at 0.6 and 0.5 .**

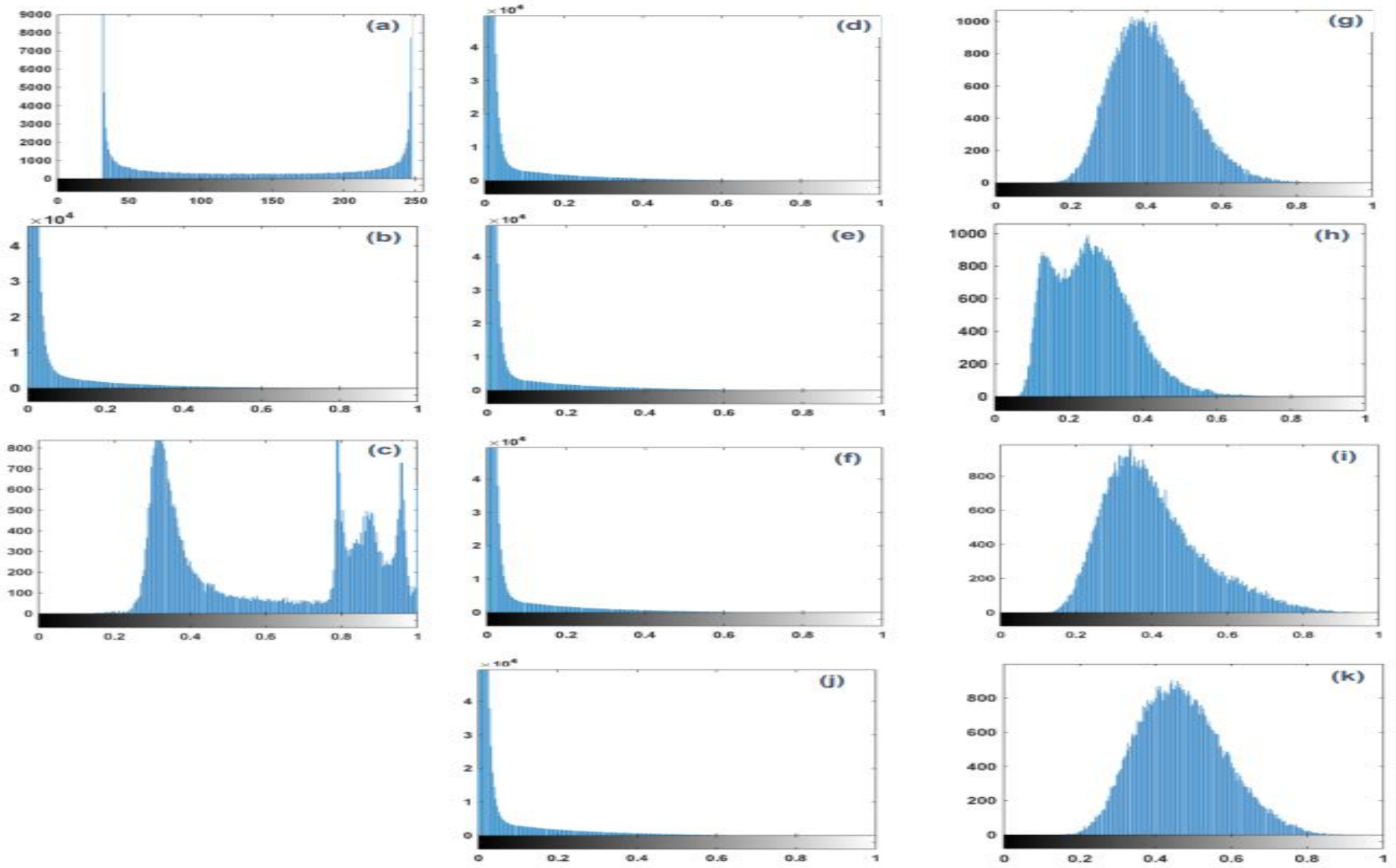
- **The parameters $k_1 and\ k$ can be varied between 0 and 1.**



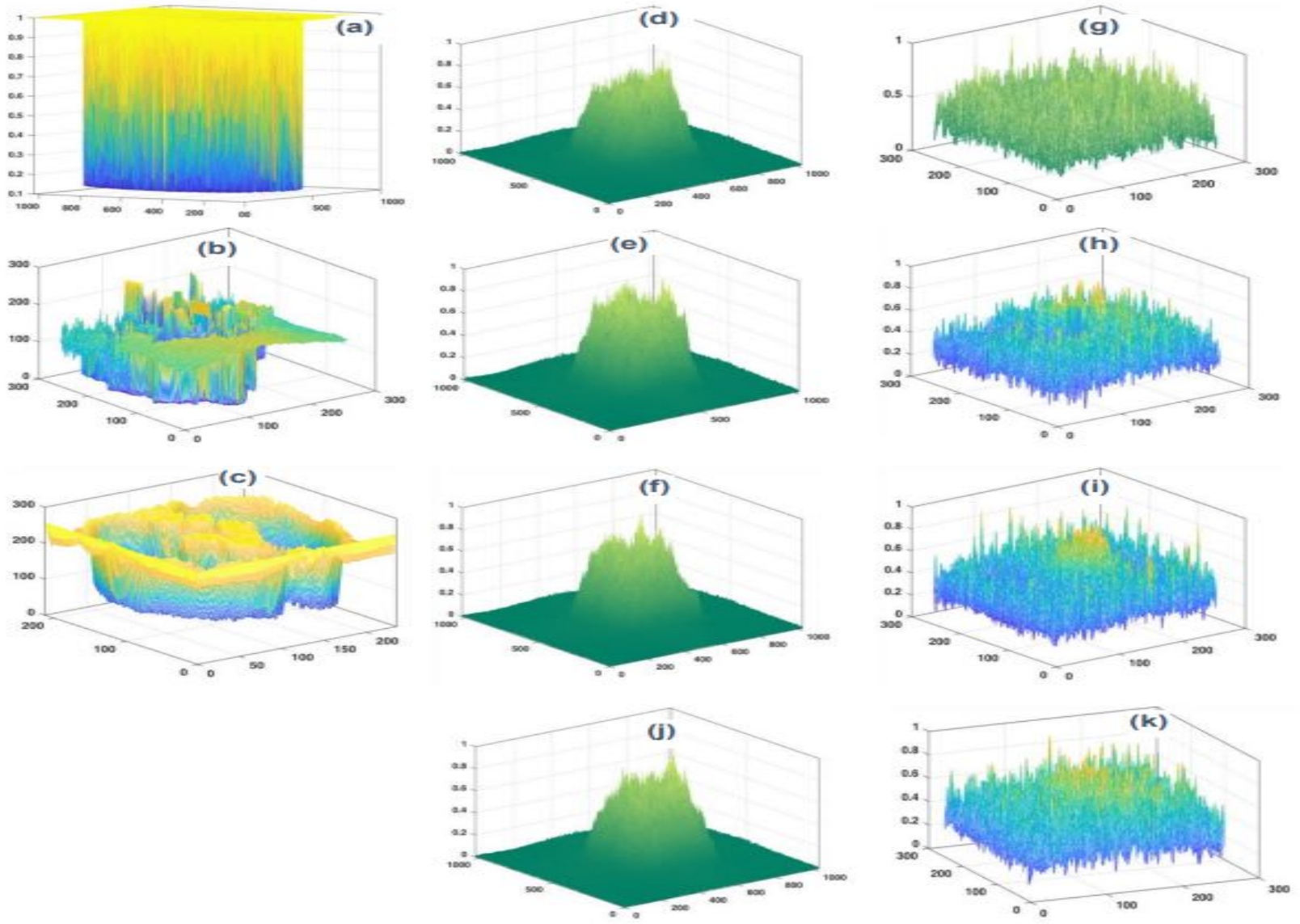
(a-d) Plaintext image of 'Fingerprint', 'Cameraman', 'Medical' and 'Binary object' , (e-h) Corresponding ciphertexts, (i-l) Decrypted images, and (m-p) Nonlinear correlation distribution plots between decrypted-, and original images.



NC distribution plot of 'Fingerprint' image for authentication corresponding to probability parameter (a-d) $k_1 = 0.1, 0.3, 0.5, and\ 0.9$; (e-h) Corresponding decrypted images.



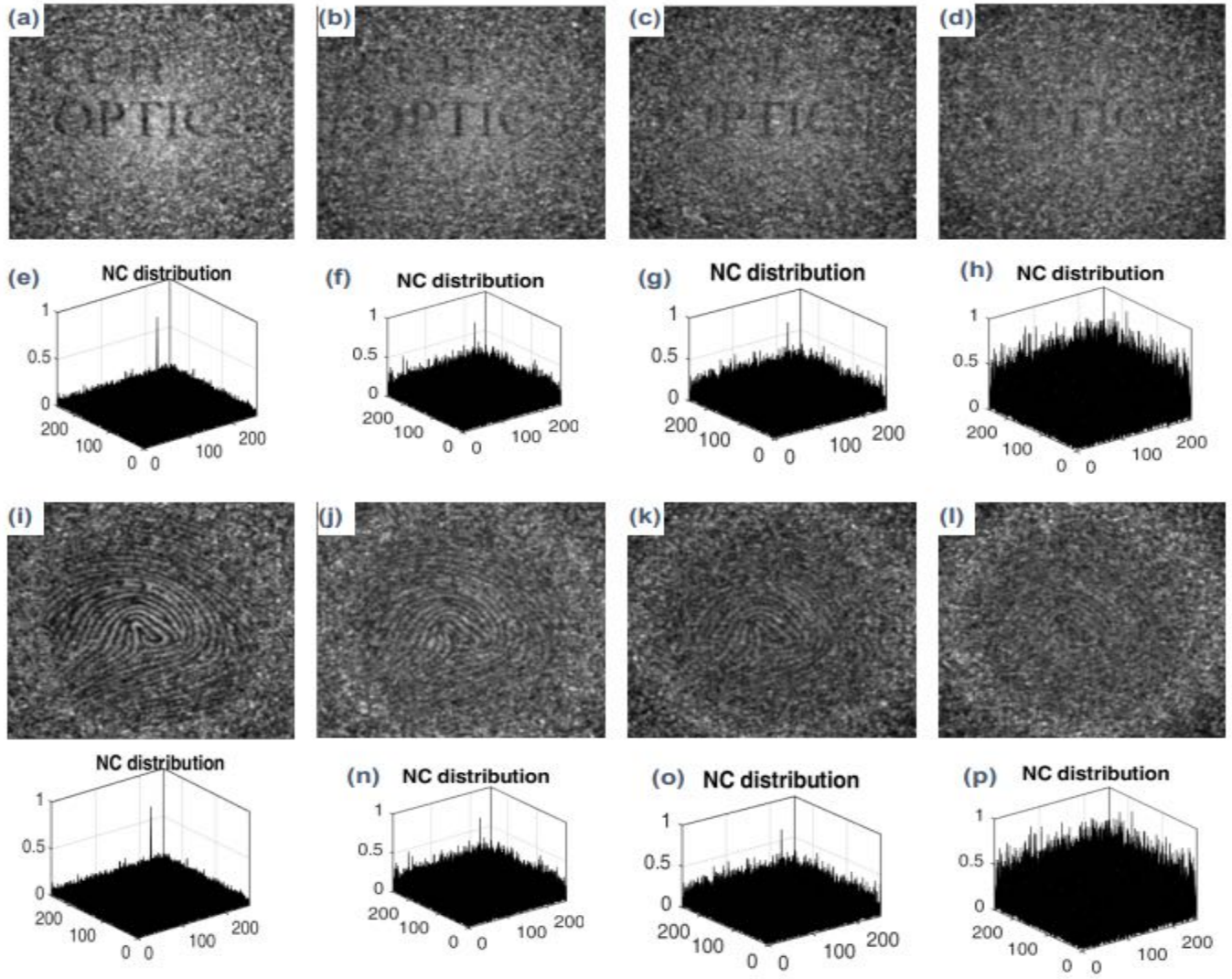
Histogram plots: (a-c) plaintext image of Fingerprint, Cameraman, Medical image, corresponding (d-f) ciphertext, and (g-i) decrypted image respectively. (j-k) Histogram plot for ciphertext and decrypted image of 'Binary image'.



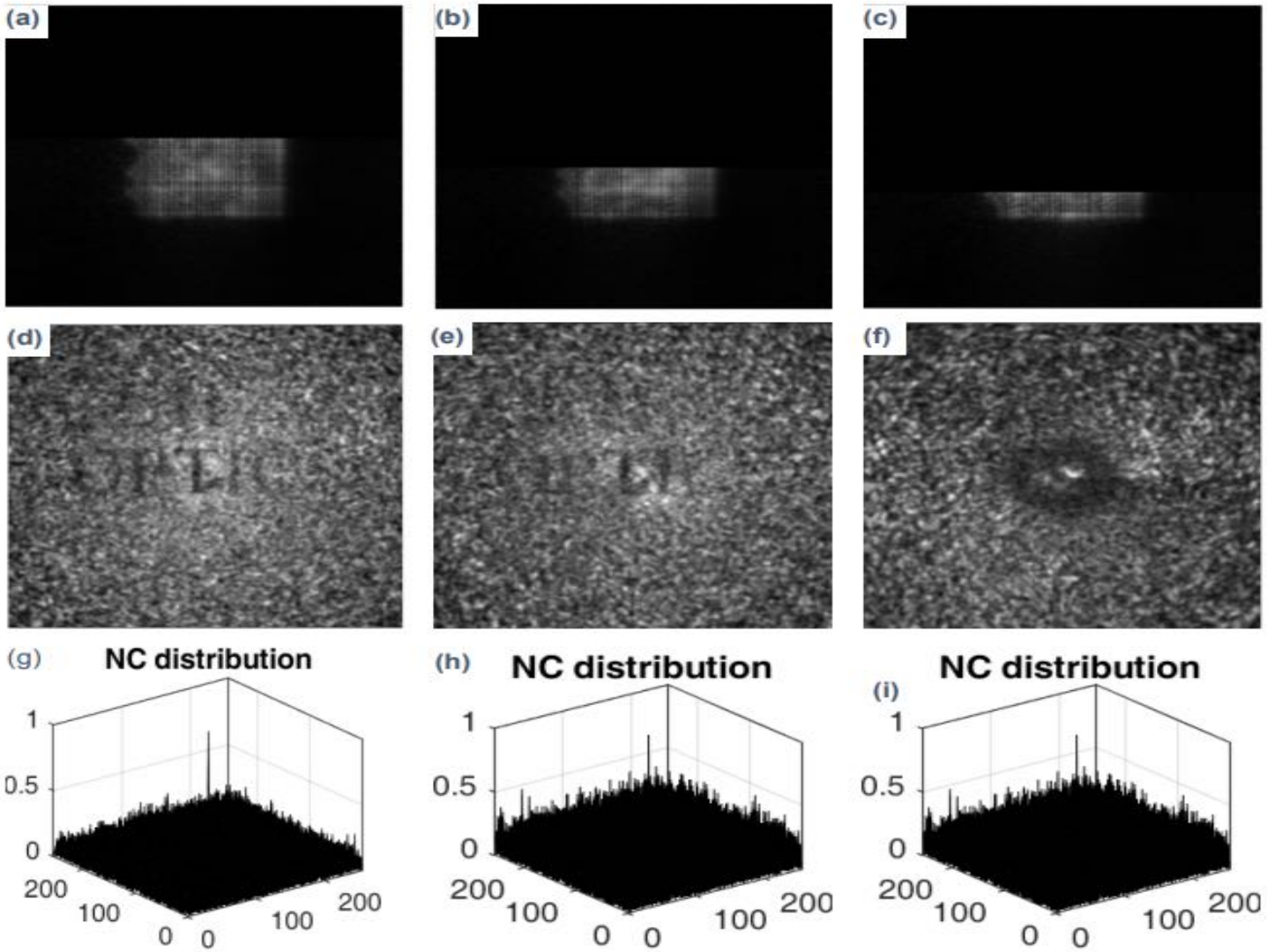
(a-c) Plaintext image of Fingerprint, Cameraman, Medical image, (d-f) corresponding cipher-text, and (g-i) decrypted image respectively. (j-k) 3-D plot for ciphertext and decrypted image of 'Binary image'

Image type	Information Entropy			Correlation coefficient between Plaintext and Decrypted image	MSE between Ciphertext and Plaintext
	Plaintext	Ciphertext	Decrypted	CC	MSE
Fingerprint Image	2.126	7.149	7.019	0.293	1.27×10^{54}
Cameraman Image	7.0097	7.247	7.107	0.535	4.96×10^{54}
Medical Image	6.996	7.128	7.076	0.535	4.45×10^{53}
Binary Image	0.269	7.169	7.024	0.186	3.07×10^{54}

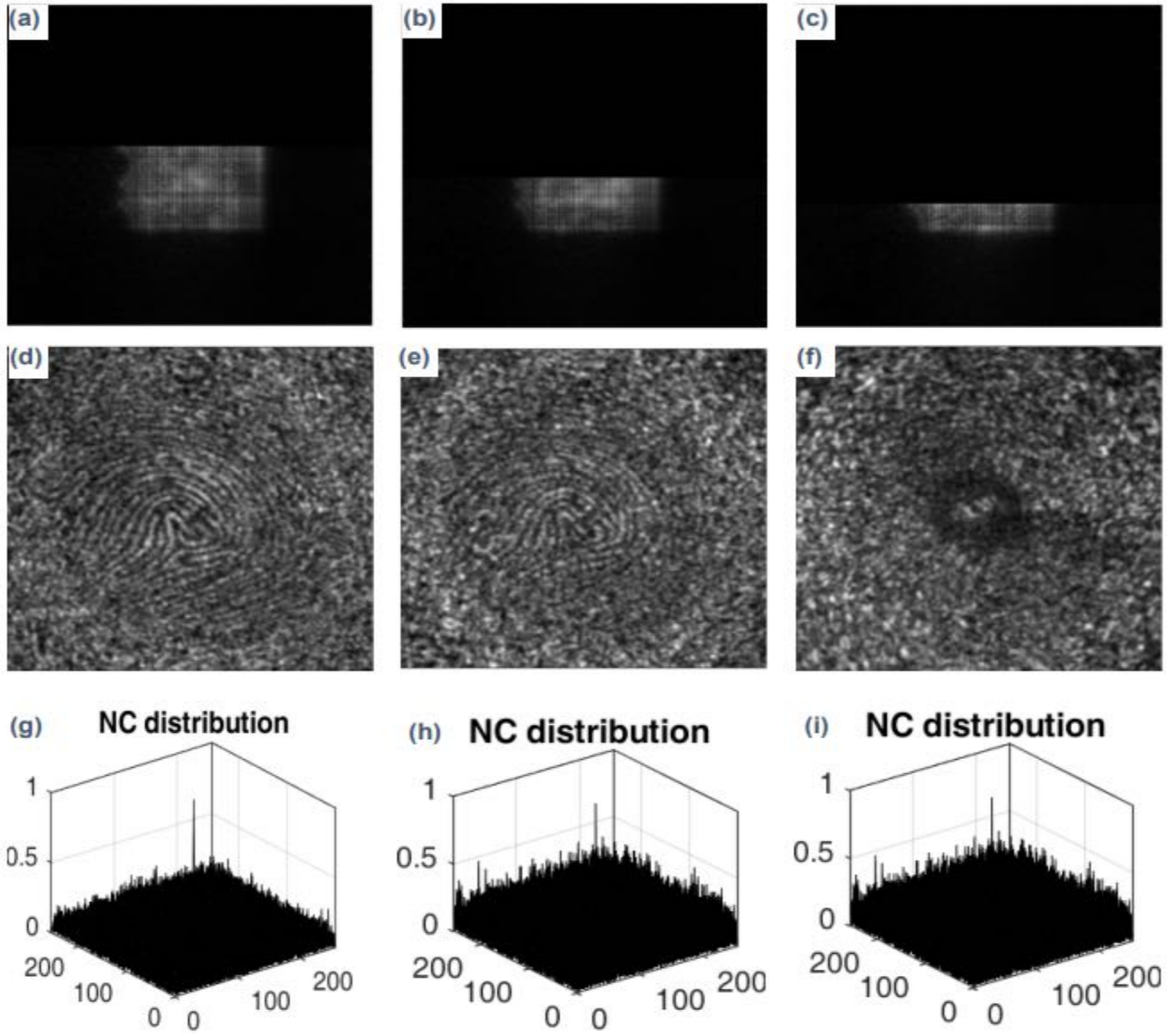
Calculated values of information entropy, CC values and MSE values.



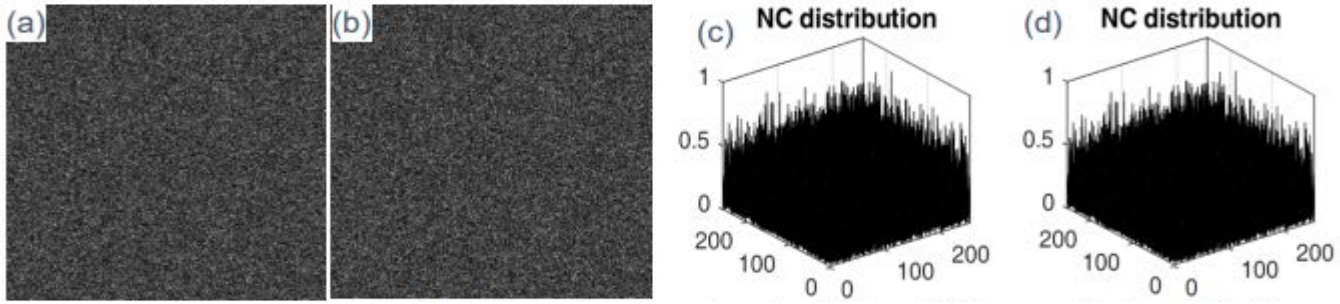
Decrypted images: (a-d) 'Binary'; (i-l) 'Fingerprint' corresponding to ciphertext with noise strengths $\phi = 1\times10^4, 3\times10^4, 5\times10^4, 7\times10^4$; (e-h) and (m-p) are corresponding NC plots for authentication.



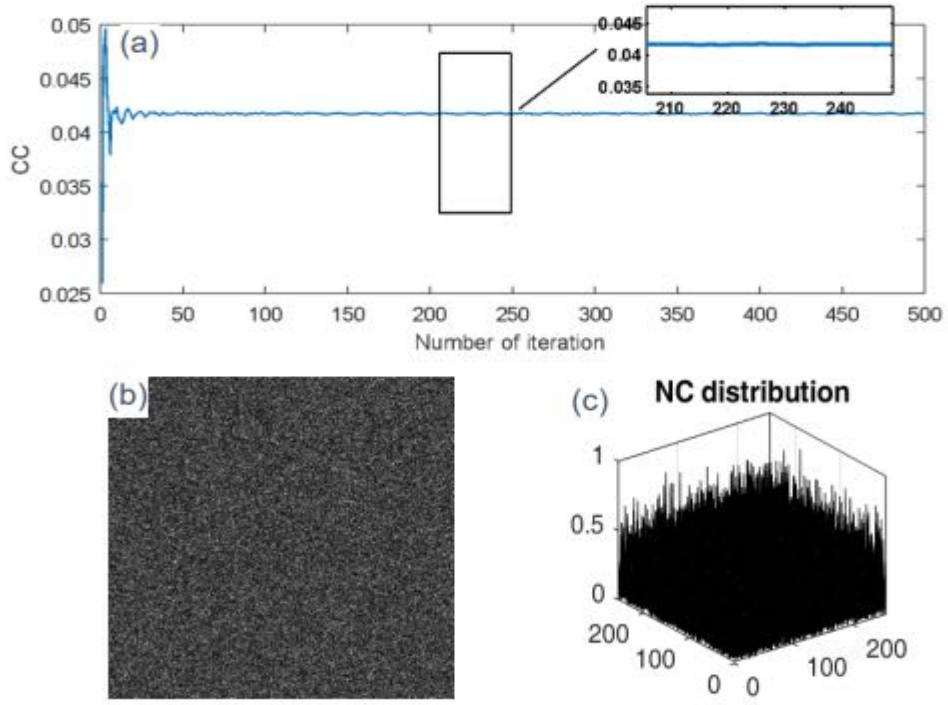
(a-c) Ciphertexts of 'Binary' image with data loss of 45%, 55%, and 65%; (d-f) Recovered images corresponding to (a-c) ; (g-i) NC distribution plots the authentication.



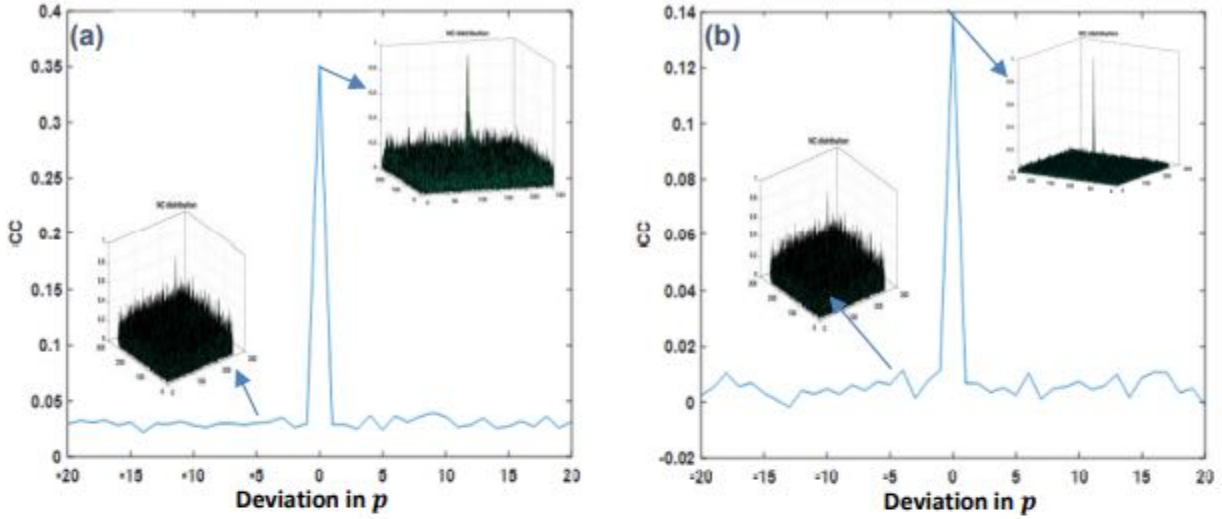
(a-c) Ciphertexts of 'Fingerprint' with data loss of 45%, 55%, and 65% respectively, (d-f) Recovered images corresponding to (a-c) ; (g-i) NC distribution plots for authentication.



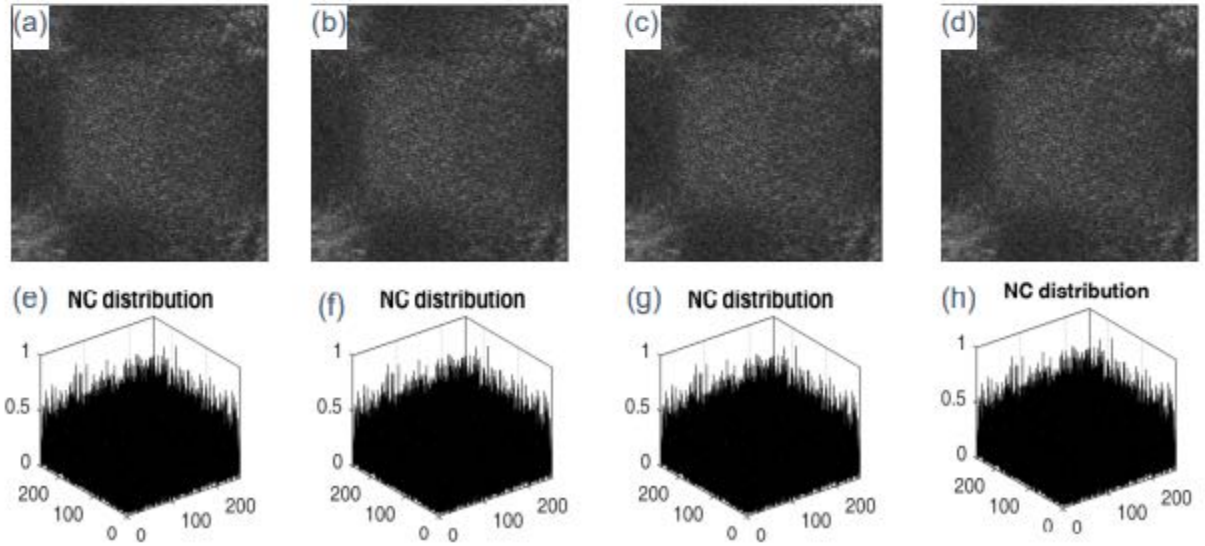
(a, b) Decrypted image of 'Fingerprint' by using CPA and KPA; (c-d) are NC distribution between decrypted image (a,b) and reference image.



Special iterative attack on the proposed algorithm: (a) CC versus number of iterations for 'Fingerprint' image, (b) Decrypted image of 'Fingerprint' after 500 iterations, (c) Corresponding NC distribution .



Plots of deviation: (a,b) fractional order parameter p, for 'Fingerprint' and 'Binary' images.



Decrypted images by using wrong private key, (a,b) P_1, (c,d) U *or* V for 'Fingerprint' and 'Binary' image, (e,h) NC between decrypted-, and reference plaintext image for 'Fingerprint' and 'Binary' image.

Summary and Conclusions

- **An iterative attack algorithm is proposed for the Fr MT-based cryptosystem.**
- **A novel multiuser image encryption and authentication algorithm is proposed with enhanced security.**
- **Sparse separation and polar decomposition are employed in the FrMT obtain the ciphertext.**
- **Since the sparse phases allow a partial decryption, the authentication step is required for validating the retrieved images.**
- **Polar decomposition provides an additional security to the encryption process and results into two private keys (P_1 *and* U *or* V).**
- **In the decryption, one private key (P_1) would be shared by both the users. Private key (U *or* V) can be used by a separate user which enables the multiuser capability of the proposed method.**
- **The multiuser capability along with the strong security features of the scheme makes it a potential authentication platform which can be used at the places where the same information/documents are accessed securely by several users.**
- **The results demonstrate the robustness and validity of the proposed algorithm for the security applications, and may be extended to the color images, audio, and video in future.**
- **Currently working on the application of AI tools to cryptography**

The End

Thank you for your attention

Questions if any?