Content is available at: CRDEEP Journals
Journal homepage: http://www.crdeepjournal.org/category/journals/global-journal-of-current-reseach-gjcr/

Global Journal of Current Research

(ISSN: 2320-2920) (Scientific Journal Impact Factor: 6.122)

UGC Approved-A Peer Reviewed Quarterly Journal

Full Length Research Paper

Asymmetric Colour Image Encryption Techniques Based on Singular Value Decomposition

MD Eqbal Ahmad Shirazi[1]
Research Scholar in Computer Science Department, Magadh University, Bodhgaya Bihar, India.

ARTICLE DETAILS

Corresponding Author:
Md. Iqbal Ahmad Shirazi

Key words:
Asymmetric, Color Image, Encryption, Singular Value

ABSTRACT

A fresh method for encrypting color images, employing Singular Value Decomposition (SVD), is introduced. The initial color image undergoes encryption, transforming it into a ciphertext displayed as an indexed image through the new technique. The red, green, and blue elements of the image are encoded into a complex function, later separated into U, S, and V components using SVD. The ciphertext's data matrix is derived by multiplying orthogonal matrices U and V, incorporating phase-truncation. Consequently, the encrypted indexed image occupies a reduced space compared to the original image.

1. Introduction

In recent years, there has been a notable surge in internet usage, accompanied by widespread utilization of color images across communication platforms, sparking considerable security apprehensions. As usage grows, there is continuous development and refinement of security measures, yet nefarious individuals persistently seek vulnerabilities in cryptographic methods and protocols. Despite the inherent limitations of digital security systems, incorporating specific physical parameters can mitigate these shortcomings. Optical cryptosystems, boasting numerous degrees of freedom, provide swift and dependable security solutions. [1]. Within an asymmetric cryptosystem, decryption keys are distinct from encryption keys, as noted by Qin and Peng.

[2] Qin and Peng introduced a phase-truncated Fourier transform-based asymmetric cryptosystem. Chen and Chen[3] conducted the inaugural study on phase-truncated asymmetric cryptosystems in the Fresnel domain specifically for color images. Encryption methods for color images may vary between single-channel and multi-channel approaches. Researchers have enhanced security by employing chaotic maps to scramble input images. Dong[4] proposed an asymmetric color image encryption scheme utilizing hash values and discrete-time maps. Yao et al.[5] presented a robust color image asymmetric cryptosystem based on singular value decomposition, demonstrating its resilience against known-plaintext and chosen-plaintext attacks.

This study introduces a novel approach to color image encryption in a single channel, employing singular value decomposition within the fractional Fourier transform and gyrator domains. The encryption algorithm, asymmetric in nature, integrates chaotic maps such as affine transform or the Tinkerbell map to augment security. The subsequent section presents two encryption algorithms: one utilizing the gyrator domain and the other based on the fractional Fourier transform domain. The first algorithm incorporates chaotic affine transform as a pre-processing technique, while the latter employs the Tinkerbell map for the same purpose.

- Scheme A entails an asymmetric color image encryption method leveraging singular value decomposition and chaotic affine transform within the gyrator domain.

- Scheme B involves an asymmetric color image encryption technique employing singular value decomposition and chaotic Tinkerbell map within the fractional Fourier domain.

[1] Author can be contacted at: *Research Scholar in Computer Science Department, Magadh University, Bodhgaya Bihar, India.*
Received: 15-4-2024; Sent for Review on: 19-04-2024; Draft sent to Author for corrections: 12-05-2024; Accepted on: 21-05-2024; Online Available from 25-05- 2024

2. Singular Value Decomposition

Singular value decomposition (SVD) is a reliable and robust method for matrix decomposition. For a matrix A of size $r \times s$, A with dimensions r × s, there exist orthogonal matrices U and V, sized r × r and s × s respectively, such that A = USV^T, where V^T denotes the transpose of V, and S = diag(a1, a2, … ai … , at), where ai represents eigenvalues (with ai ≥ ai+1, where i = 1, 2, … r − 1, and t = min(m, n)) of A. The SVD method finds successful application in watermarking and digital image encryption.

During encryption, the input image is divided into three distinct components: U, S, and V, which can be stored separately at different locations to heighten security. Moreover, the sequence of multiplication of U, S, and V holds paramount importance for accurate decryption of the given image. Figure 1 illustrates the impact of Singular Value Decomposition on an input grayscale image of a man.

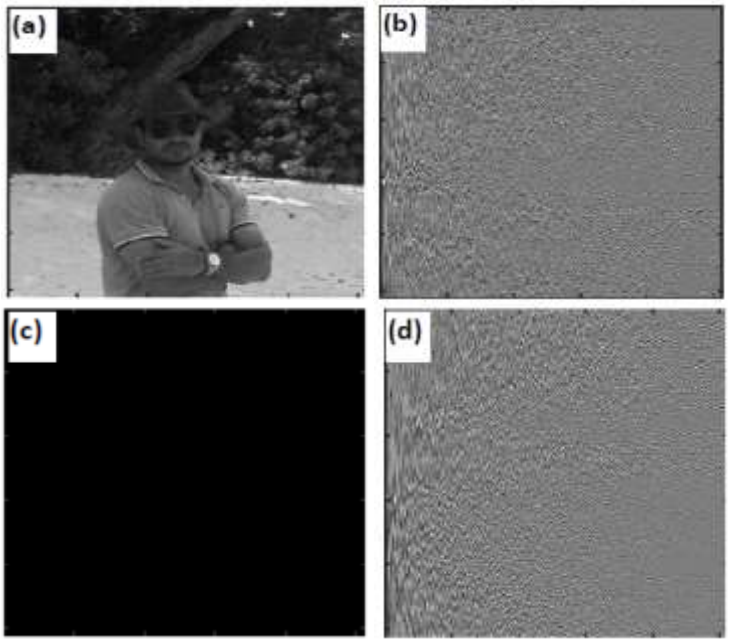


Fig 1 Singular value decomposition of input grayscale image of Man(a). (b-d) are respectively U, S and V components of singular value decomposition of input image.

3. Proposed Schemes

In This section delves into a comprehensive discussion of the proposed encryption schemes and their implementation.

Scheme A

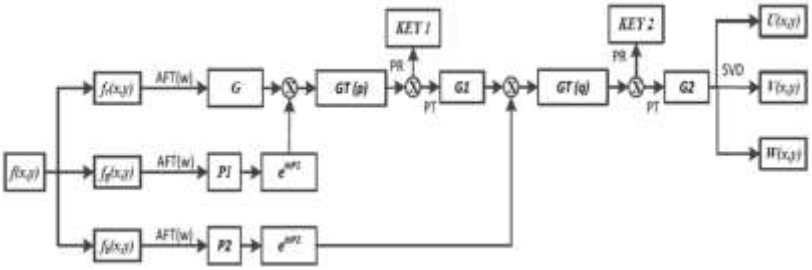


Fig 2: Flowchart of the proposed encryption scheme A.

The proposed encryption Scheme A is illustrated through a schematic diagram in Figure 2. The encryption process initiates with the decomposition of an input color image $f(x, y)$ into its constituent channels: red, green, and blue. Subsequently, these channels undergo an affine transform (AT) with w iterations. The transformed red channel image is designated as the amplitude image, while the green and blue channels are treated as phase masks.

The red channel image is then combined with the phase mask of the green channel and subjected to a gyrator transform (GT) of order p. The phase-reserved segment of the resulting image is designated as decryption key 1, whereas the phase-truncated segment is bonded with the phase mask of the blue channel and subjected to another gyrator transform of order q. The new phase-truncated segment of the resulting image is decomposed into three components (U, S, V) using singular value decomposition (SVD), while the new phase-reserved segment serves as decryption key 2.

Scheme B

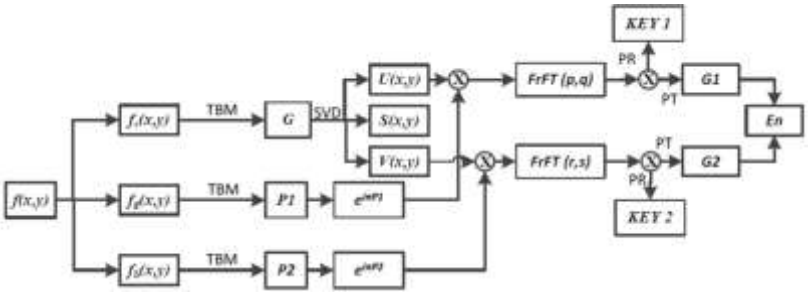


Fig 3. Flow chart of the proposed encryption scheme B

A schematic diagram of the proposed encryption scheme B is shown in Figure 3. Here, the input color image $f(x, y)$ is divided into indexed-red, green, and blue channels. Each indexed image undergoes transformation by the Tinkerbell map (TBM), using parameters a, b, c, and d. The resultant red channel image is considered the amplitude image, while the corresponding green and blue channels serve as phase masks.

Singular value decomposition (SVD) splits the red channel image into three components (U, S, V). Unitary images U and V are combined with the green and blue channel phase masks, respectively, and then transformed by a fractional Fourier transform FrFT of orders (p, q) and (r, s), respectively. The phase-truncated segments of the resulting images are combined to form the encrypted image (En), while the phase-reserved segments serve as decryption keys. Additionally, the diagonal image S serves as a decryption key in the cryptosystem.

The decryption process, depicted in Figure 4, takes the ciphertext (En) as input and produces the recovered image as output. It involves the reverse process of encryption, where instead of singular value decomposition, the operation U × S × V^T is executed.

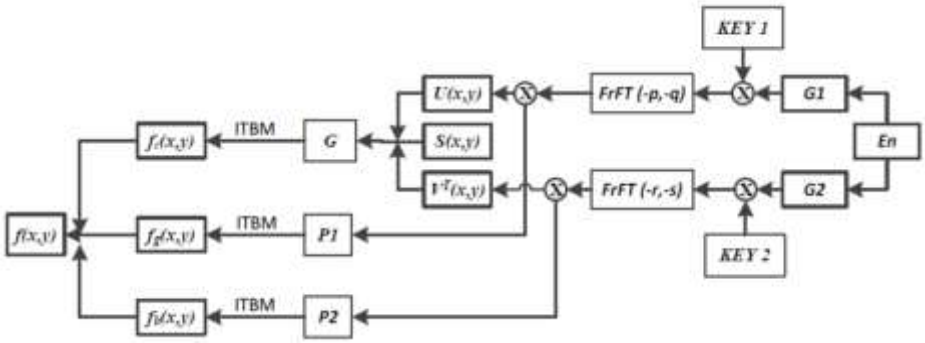
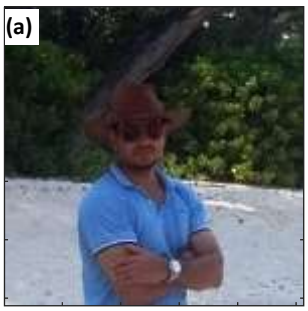


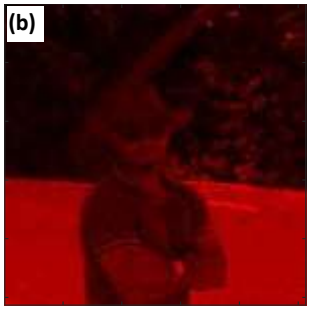
Figure 4: Flow chart of the proposed decryption scheme B.

4. Simulation Results and Discussion

4.1 Scheme Validation

In this section, the proposed schemes for color images have been validated through computer simulations. The results were obtained using MATLAB 7.14 on a system equipped with an Intel i7 processor, 16 GB RAM, and a CPU speed of 3.4 GHz, running on Windows 8 with a 64-bit operating system. The input color images used for validation were of a Man and Boy, as depicted in Figure 3 and Figure 4, respectively, with dimensions of 256 × 256 × 3 pixels each.





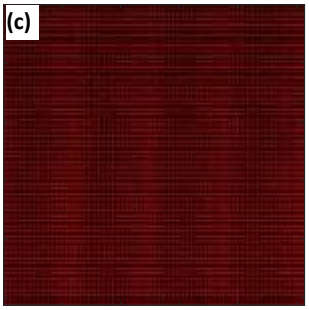


Fig 5: Results of validation of the Scheme A for (a) input color image (Man) 256×256×3 pixels; (b) is red channel of a; (c) is affine transformed image of b; (d-f) are encrypted images.

Figure 5 illustrates the validation results for Scheme A. The original input image is segmented into three channels: red, green, and blue (Figure 5 b showcases the red channel of the original image). Figure 5c displays the affine-transformed image of the red channel. and following the scheme A given in the Figure 2, It has been observed that the encrypted images U and V exhibit entirely random characteristics, resembling stationary white noise, except for the S component, which is diagonally dominant. The parameters used for the AT and GT in this investigation are w = 30, and p = 0.6, q = 0.4, respectively.

Figure 6 displays the validation outcomes for Scheme B. For the sake of simplicity, the same values of FrFT orders in the spatial domain (i.e., p = q and r = s) have been employed in the simulations. The FrFT parameters used are p = 0.8 and r = 0.5.

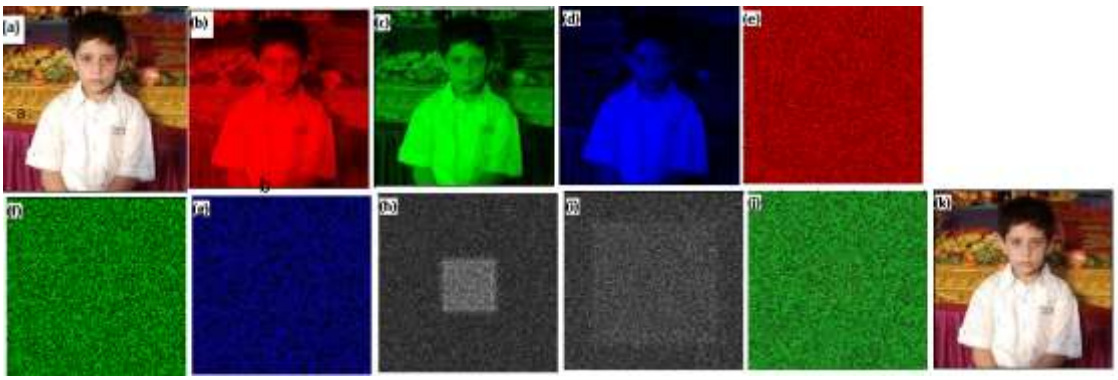


Fig 6: Validation of the scheme. (a) Original image (Boy); (b-d) are its RGB channels; (e-g) are their corresponding Tinkerbell map transformed images; (h-j) are components G1, G2 and encrypted image respectively, and (k) is the recovered color image.

The Tinkerbell Map's parameters are as follows: a = 0.9, b = -0.6013, c = 2, and d = 0.5. Additionally, initial values for $x0$ and $y0$ are given as $x0$ = 0.178 and $y0$ = 0.158. The original image (depicted in Figure 6a) is decomposed into its red, green, and blue channels (illustrated in Figures 6 b, c, d). Figures 6 e, f, g exhibit the Tinkerbell map-transformed images of the RGB channels, which are then encrypted according to Scheme B outlined in Figure 3. The encrypted image, along with its components $G1$ and $G2$, is depicted in Figures 6 j, h, i, respectively. The decrypted image, shown in Figure 6 k, faithfully represents the original image, validating the proposed scheme. It is noteworthy that the encrypted image components closely resemble stationary white noise and exhibit complete randomness.

5. **Key sensitivity**

In the context of the proposed cryptosystems, a scheme is deemed secure if it exhibits high sensitivity to its parameters, including both decryption and encryption keys. These parameters encompass the orders of the gyrator transform, fractional Fourier transform, as well as the parameters of the affine transform and Tinkerbell map. A sensitivity analysis has been conducted for these parameters, and the outcomes are illustrated in plots of mean-squared error (MSE), as indicated by the expression:

$$MSE = \frac{1}{N \times N} \sum_{x=1}^{N} \sum_{y=1}^{N} |I_o(x,y) - I_r(x,y)|^2 \quad (1.1)$$

In the expression, Ir(x, y) and Io(x, y) represent the pixel values of the decrypted image and the input image, respectively, while N denotes the size of the image. Figure 7 displays the plots of MSE versus affine parameter and orders of gyrator transform for the indexed channel-red of the Man image. These plots reveal that Scheme A is highly sensitive to even minute changes in the values of these parameters.

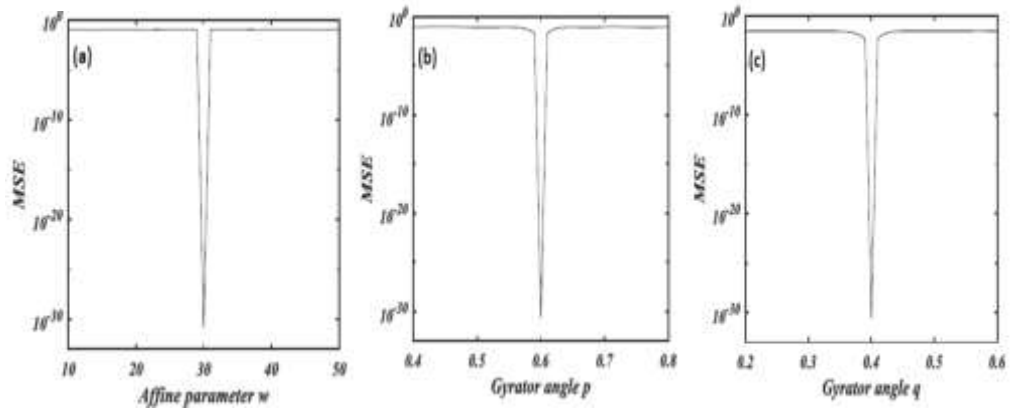


Fig 7: Plots of sensitivity (MSE) relative to (a) parameter *w* of affine transform (AT); (b,c) parameters p and q of gyrator transform (GT) respectively for Scheme A.

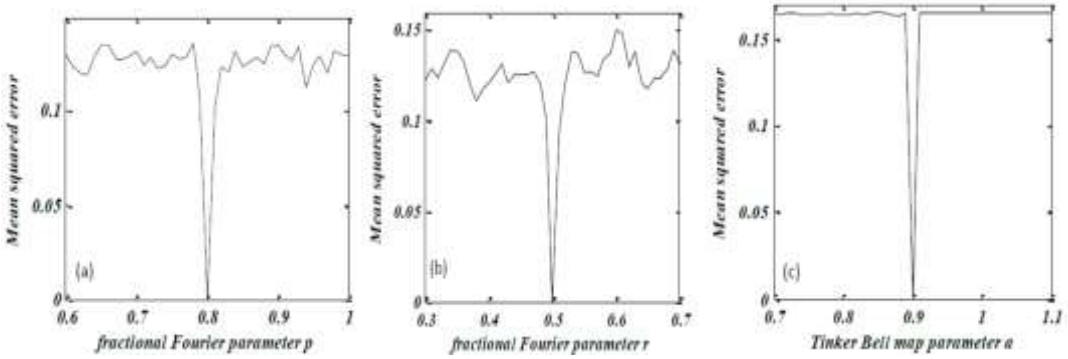


Fig 8: Sensitivity (MSE) plots relative to (a,b) fractional Fourier transform (FrFT) order p and r respectively, (c) Tinkerbell map parameter *a*.

Figure 8 depicts the plots of MSE versus Tinkerbell map parameters and orders of fractional Fourier transform for the red channel of the Boy image. These plots reveal a high degree of sensitivity to even minor variations in the values of these parameters. The scheme's sensitivity has been validated through the sensitivity results of encryption parameters, particularly those of the Tinkerbell map. Notably, the analysis of key space in the case of the optical implementation of fractional Fourier transform (FrFT) has been conducted by Unnikrishnan et al. [6]. They have described that the key space of the FrFT parameters is approximately on the order of 10^{12}. In their computations, each Tinkerbell map parameter exhibits sensitivity on the order of 10^{15}. Additionally, the use of Singular Value Decomposition (SVD) allows for 6 possible combinations for combining three encrypted images. Consequently, the overall size of the key space amounts to roughly 6×10^{62}, a magnitude sufficiently large to withstand brute-force attacks for a considerable duration. Therefore, the sensitivity plots for both Scheme A and Scheme B establish that the encryption schemes are indeed sensitive to their encryption keys.

6.Noise attack analysis

The robustness of a cryptosystem can be assessed by evaluating its performance against various attacks, including occlusion attacks, noise attacks, chosen plaintext attacks, known plaintext attacks, and more. To test the resilience of the proposed cryptosystem against noise attacks, the encrypted data (E) is intentionally corrupted with noise of strength (δ), resulting in a

noisy image (Eo). This can be expressed as: of a cryptosystem can be tested by evaluating its performance against various attacks such as occlusion attack, noise attack, chosen plaintext attack, known plaintext attack, etc. The endurance of the proposed cryptosystem against noise attack has been tested, when the encrypted data (E) is corrupted with noise of strength (δ) resulting in a noisy image (E_o). This is expressed as

$$E_o = E(1 + \delta G) \quad (1.2)$$

In the provided expression, G represents Gaussian noise with a standard deviation of 1 and zero mean, while E denotes the encrypted image. Figures 9(a-c) display the recovered images for the red channel when encrypted images from Scheme A are subjected to inverse singular value decomposition and affected by noise with increasing strength δ = 0.3, 0.6, and 0.9, respectively. Similarly, Figures 10(a-d) depict the recovered images when encrypted images from Scheme B are infected with noise strengths δ = 0.2, 0.8, 1.4, and 2, respectively. It is noteworthy that even in the presence of significant noise in the ciphertext, the decrypted image remains of fairly good quality. Thus, the schemes have effectively endured the noise attack, as demonstrated by these results.

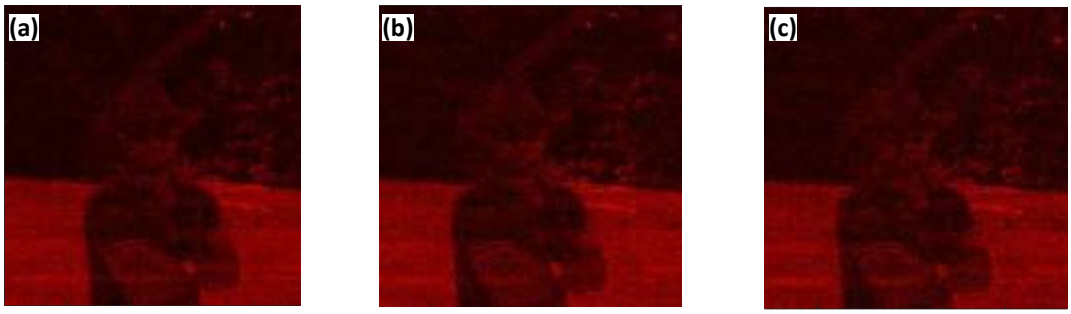


Figure 9Recovered images when the encrypted image (scheme A) has salt and pepper noise of varying strength (a–c) δ = 0.3, 0.6, and 0.9 respectively.

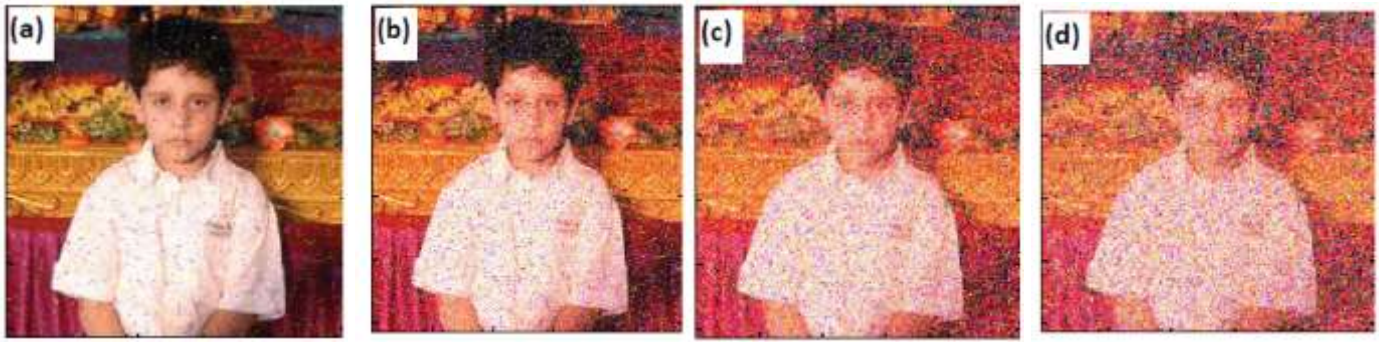


Figure 10 Results of decryption (scheme B) in presence of Gaussian noise with standard deviation 1 and zero mean, (a–d) with noise factor δ = 0.2, 0.8,1.4 and0. 2 and respectively.

7.Occlusion attack analysis

The resilience of the current systems in the event that encrypted data is lost was also assessed. Figures 11(a, c) show the encrypted photos of the Man for Scheme A with 40% and 60% loss of data, respectively, whereas Figures 11b and 11d show the corresponding recovered images. With a correlation value of 0.8695 and 0.7783, respectively, the original pictures may be retrieved when 40% and 60% of the data in encrypted photos is absent or blocked. By distributing the original input picture's pixels over the whole encrypted image, the suggested techniques provide protection against occlusion attacks.

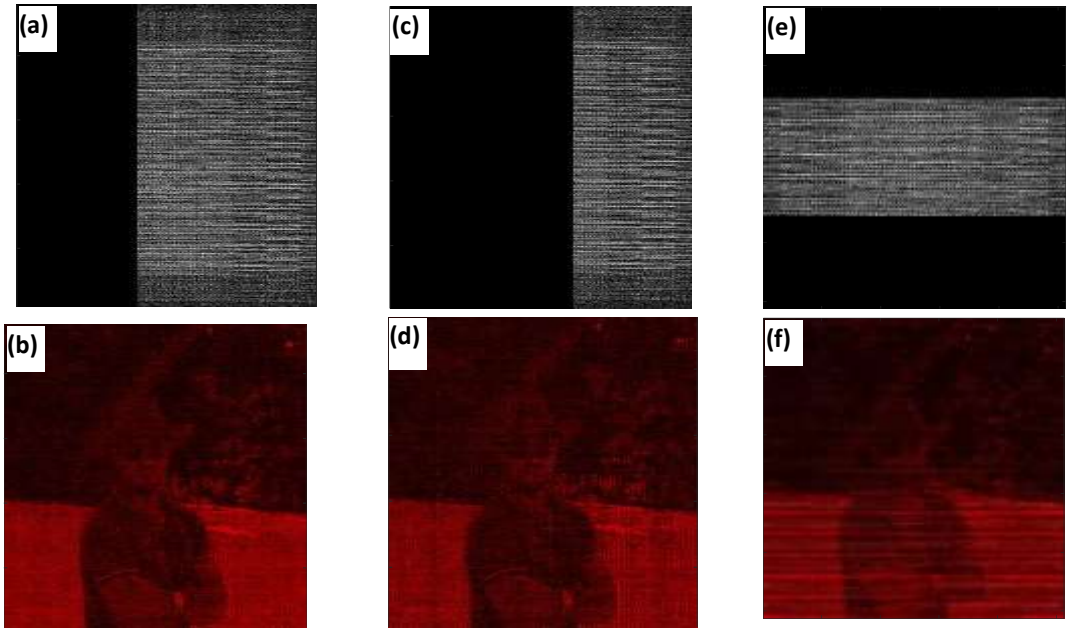


Fig 11 Occlusion results for the encrypted images of scheme A (after applying inverse singular value decomposition) for (a, c and e) respectively with 40%, 60% and 60% loss; figure (b, d and f) show the corresponding decrypted image of Man.

8. Conclusion

Two asymmetric encryption methods based on phase and amplitude truncation procedures have been suggested in this paper for single-channel colour pictures. These methods involve pixel scrambling of each channel of the original colour image using the Tinkerbell map and the affine transform. Through MATLAB 9.3 simulations, the schemes have been confirmed using colour pictures with size of 256×256×3. Using statistical analysis, which includes 3D plots and correlation distribution, their performance has been evaluated. Furthermore, the resilience of the schemes has been illustrated by means of widely employed occlusion and noise assaults. Sensitivity analysis research indicates that the transform orders, affine map parameters, and Tinkerbell map parameters have a significant impact on the novel schemes.

9. References

1.Refregier, P., Javidi, B. (1995). Optical image encryption based on input plane and Fourier plane random encoding. Optics Letters. 20 (7), pp 767–769.
2.Qin, W., Peng, X. (2010). Asymmetric cryptosystem based on phase-truncated Fourier transforms. Optics Letters. 35 (2), pp 118–120.
3.Chen, W., Chen, X. (2011). Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain. Optics Communications. 284 (16–17), pp 3913–3917.
4.Dong, C. (2015). Asymmetric color image encryption scheme using discrete-time map and hash value. Optik - International Journal for Light and Electron Optics. 126 (20), pp 2571–2575.
5.Yao, L., Yuan, C., Qiang, J., Feng, S., Nie, S. (2017). Asymmetric color image encryption based on singular value decomposition. Optics and Lasers in Engineering. 89 (Supplement C), pp 80–87.
6.Unnikrishnan, G., Joseph, J., Singh, K. (2000). Optical encryption by double-random phase encoding in the fractional Fourier domain. Optics Letters. 25 (12), pp 887–889.