STM JOURNALS

Research & Reviews: Journal of
Physics

ISSN: 2278-2265 (Online)
ISSN: 2347-9973 (Print)
Volume 15, Issue 1, 2026
January–April
DOI (Journal): 10.37591/RRJoPHY

https://journals.stmjournals.com/rrjophy

Research RRJoPHY

Comparative Analysis of Encryption–Decryption Performance for Binary, Grayscale, and Color Images Using the Discrete Fractional Fourier Transform

Kawther H. Al-khafaji[1,*]

Abstract

The discrete fractional Fourier transform (DFRFT) provides an effective model of image encryption by further developing the classic Fourier transform by adding fractional orders, which increases the degrees of freedom. Owing to the omnipresence of digital media in many industries like education, healthcare, and entertainment, the mobility of visual data has become a significant issue to keep confidential. Images form one of the main ways of exchanging information and, therefore, huge encryption mechanisms should be used to maintain privacy. In this work, three different types of images, namely, binary, grayscale, and color (RGB) images, are encrypted with the DFRFT image encryption scheme. The suggested solution has a high level of improvement in security, where the two keys must be correct before successful decryption, and unauthorized access is highly unlikely. The scheme has proved to be effective under the set of image quality measures. Some common measures were made to objectively judge the quality of the decrypted images. These measurements give information about the quality of the preservation of the visual and structural integrity of each of the images following the encryption procedure. The Discrete Fractional Fourier Transform (DFRFT) based cryptosystem was found to be effective, scalable, and capable of supporting the various image modalities. Its capability of multidimensional data processing and computational stability connects it a promising source of transmission and storage of secure images in its real-life usage. The outcomes of the simulations reveal that the approach generates correct encryption and decryption of the system with all types of images and provides high visual fidelity and robustness, which is why it is appropriate to use it in transmitting and storing images safely.

Keywords: Discrete fractional Fourier transform, Fourier transform, fractional Fourier transform, image encryption, Discrete Fractional Fourier Transform (DFRFT) cryptosystem

INTRODUCTION

Mathematical transforms, such as the Fourier and cosine transforms, are useful in representing, processing, and analyzing signals. Discrete forms of these transforms have found extensive use in image processing, which is but one of the numerous fields in which such transformations have been applied. A time-domain signal can be converted into a frequency-domain signal using the discrete Fourier transform (DFT). Therefore, the inverse Fourier transform is a process of converting a signal in the frequency-domain to a time-domain signal. With the diversity of potential uses, these transforms have been expanded with additional parameters. One such generalization is the Fourier transform generalization, that is, the discrete fractional Fourier transform (DFRFT) [1]. Generalized Fourier transform, Fractional Fourier transform (FRFT) [2, 3]. The DFRFT is a time–frequency-domain rotation that represents a signal as existing between

***Author for Correspondence**
Kawther H. Al-khafaji
E-mail: rababmahdi49@gmail.com

[1]Assistant Professor, Faculty of Education for woman, Kufa University, Kufa, Iraq

Received Date: January 19, 2026
Accepted Date: January 28, 2026
Published Date: January 30, 2026

Citation: Kawther H. Al-khafaji. Comparative Analysis of Encryption–Decryption Performance for Binary, Grayscale, and Color Images Using the Discrete Fractional Fourier Transform (DFRFT). Research & Reviews: Journal of Physics. 2026; 15(1): 54–66p.

the frequency and time domains. Its uses include pattern recognition, filter construction, and signal analysis. Many variations of Fractional Fourier Transforms (multiple forms/variations) (FRFTs) have been developed as a result of extensive research efforts to develop the theory behind the DFRFT owing to its growing applicability [1]. One of the key areas of application of the Fractional Fourier Transform (FrFT) is data-wide applications, alongside the DFrFT, is signal and information security, namely, signal and picture encryption. Numerous researchers have recently proposed methods that incorporate different randomized variants of the DFrFT in addition to fractional transforms, thereby adding additional security characteristics to the encryption of signals [4–6].

DIGITAL IMAGE TYPE

For purpose-image encryption, it is useful to distinguish the following three types of images, as shown in Figure 1, listed below [7, 8]:

Fractional Fourier Transform (DFRFT)

Here, we provide a brief discussion of the mathematical foundations of the discrete fourier transform (DFT) and its variants. The DFT serves as the basis for the development of the discrete fractional fourier transform (DFRFT). The

N × N

N×N DFT matrix is given as:

$$F_{m.n} = \frac{1}{\sqrt{N}} e^{-j(\frac{2\pi}{N})(mn)}, 0 \le m, n \le N-1 \quad (1)$$

The DFT of a vector (x) is the discrete Fourier transform of a vector.

$$X = F \cdot x \quad (2)$$

where DFT $(2-D)$ of an N × N matrix x is given as follows:

$$X = F \cdot x \cdot F^T \quad (3)$$

Only four eigenvalues are present in the DFT matrix *F*. We assume an almost triangular matrix, N×N matrix S, with nonzero values.

$$S_{n,n} = 2\ cos\left(\frac{2\pi}{N} \cdot n\right), 0 \le n \le (N-1)$$

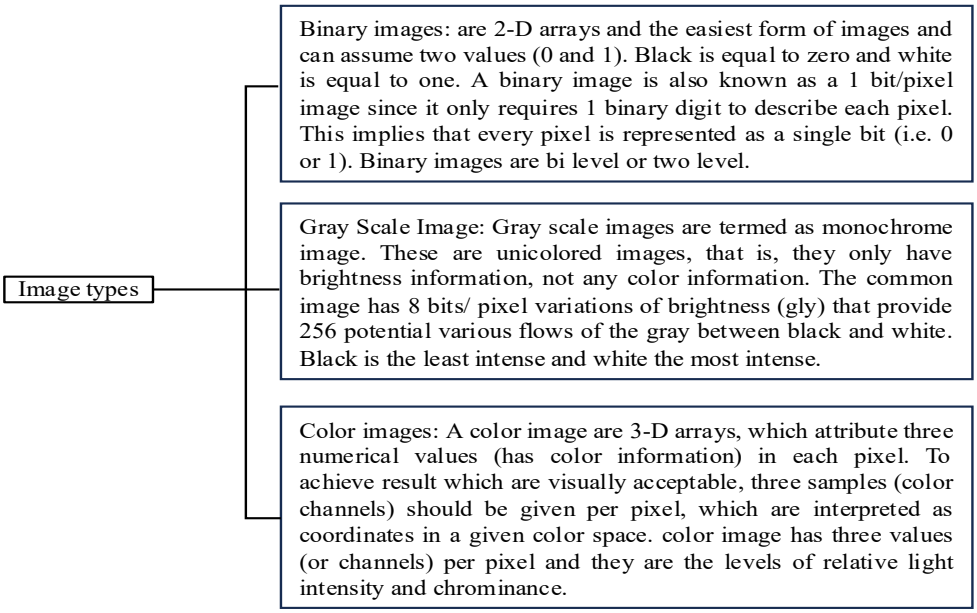

Figure 1. Digital image type.

$$S_{n,n+1} = S_{n+1,n} = 1, 0 \le n \le (N-2)$$
$$S_{N-1,0} = S_{0,N-1} = 1 \quad (4)$$

F and *S* share the same eigenvectors but differ in eigenvalues, which means that. According to the eigen decomposition that the authors used to represent the ath-order of the N × N DFrFT array in the following form:

$$F^a = V\Lambda^a V^T \quad (5)$$

$$\mathrm{F^a} = \begin{cases} \sum_{k=0}^{N-1} e^{-j(\frac{\pi}{2})ka} v_k v_k^T & for\ N\ odd \\ \sum_{k=0}^{N-2} e^{-j(\frac{\pi}{2})ka} v_k v_k^T + e^{-j(\frac{\pi}{2})Na} v_N v_N^T & for\ N\ even \end{cases} \quad (6)$$

V eigen vectors of matrix F (or Lambda) and Lambda diagonal matrix with its diagonal values equal to the eigenvalues of each column eigenvector v_k in V , and $v_k$is the normalized k th order discrete HermiteGaussian-like eigenvector of S. The α^{th} order $1-$ D Discrete Fourier Fractional Transform DFRFT of the one-dimensional 1-D vector x of order 1 -n is calculated as follows:

$$X = F^a \cdot x \quad (7)$$

The 2D DFrFT of a to an N×N matrix x is computed as follows:

$$X = F^a \cdot x \cdot (F^a)^T \quad (8)$$

IMAGE ENCRYPTION WITH DISCRETE FRACTIONAL FOURIER TRANSFORM (DFRFT)

The encryption method proposed in this section is a *round-based iterative cipher.* In each round, a random phase matrix and the Discrete Fractional Fourier Transform (DFRFT) are applied sequentially.

An original image $P$of size $N \times N$is first multiplied element-wise by a random phase matrix defined as

$$\exp(j\beta_{m,n})$$

where $\beta_{m,n}$represents a randomly generated phase distribution.

The resulting matrix is then transformed using the DFRFT of order a, producing an intermediate matrix C. This matrix is further multiplied element-wise by another random phase matrix

$$\exp(j\gamma_{m,n})$$

followed by the application of a DFRFT of order $(b-a)$to obtain the encrypted image Y.

The encryption process uses the two random phase matrices and the fractional orders $a$and $b$as keys.

Decryption is performed by applying the inverse operations in reverse order. Specifically, DFRFTs of orders $-(b-a)$and $-a$are applied along with the conjugate phase matrices $\exp(-j\gamma_{m,n})$and $\exp(-j\beta_{m,n})$, respectively.

The encryption and decryption processes can be mathematically summarized as follows [9].

Encryption Stage

During the procedure of DFRFT method, input image P is multiplied by the first exponential random matrix exp (j bm), after which the DFRFT (order a) is encrypted, and again, the resulting matrix is

multiplied by the second exponential random matrix exp (j 3n), and again, encrypting the image with DFRFT order b-a. To encrypt the image, the queer random matrices at the encryption and decryption locations should be orthogonal to each other [10]. The DFrFT of the image encryption method is illustrated in Figure 2.

$$C = F^{a} \cdot (P \otimes \exp(j\beta m)) \cdot (F^{a})^{T} \quad (9)$$

$$Y = F^{a-b} \cdot (C \otimes \exp(j\gamma n)) \cdot \left(F^{a-b}\right)^{T} \quad (10)$$

The operators are element-by-element multiplication operations of the two matrices, which are the operators in Figure 2, and T represents the transpose of the matrix [11].

Decryption Stage

The process of removing the initial message from an encrypted message is known as decryption. This is the retrogressive section of encryption. The input used herein is an encrypted picture. Input image Y is acquired, and the DFRFT of order '$a - b$' is then performed on it, which is then multiplied by a random matrix ($\exp(-j\beta m)$), which can overcome the effect of the random matrix ($\exp(j\beta m)$) as they are both orthogonal to the other. The resulting matrix DFrFT of order -a is then multiplied, and the result is multiplied by the random matrix ($\exp(-j\gamma n)$) to generate the decrypted image. [9, 10] The DFRFT decryption scheme is illustrated in Figure 3.

$$C = F^{a-b} \cdot (Y \otimes \exp(-j\gamma n)) \cdot \left(F^{a-b}\right)^{T} \quad (11)$$

$$P = F^{-a} \cdot (C \otimes \exp(-j\beta m)) \cdot (F^{-a})^{T} \quad (12)$$

SIMULATION PERFORMANCE ANALYSIS AND DISCUSSION

This subsection explains the dataset of images that are used for experimental purposes. Several standard (binary, grayscale, and color) pictures were downloaded from the USC-SIPI database, and a

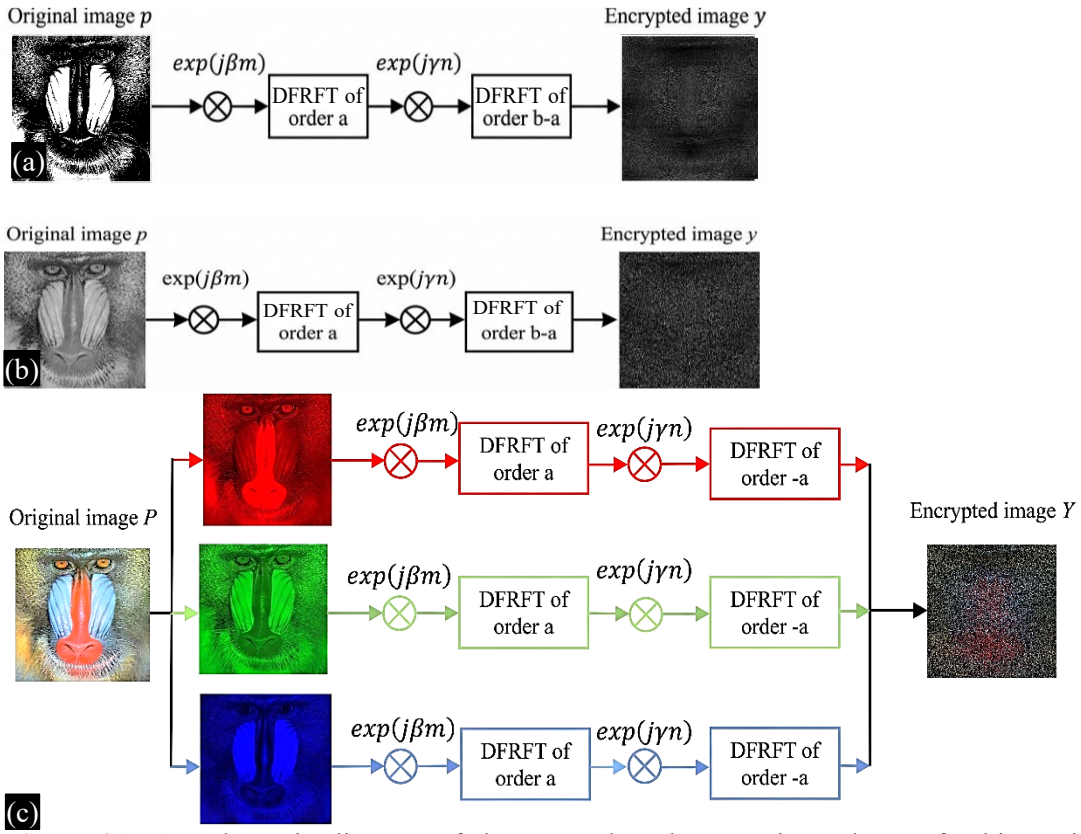

Figure 2(a-c). Schematic diagram of the DRPE-based encryption scheme, for binary images, for grayscale images, and for color images.

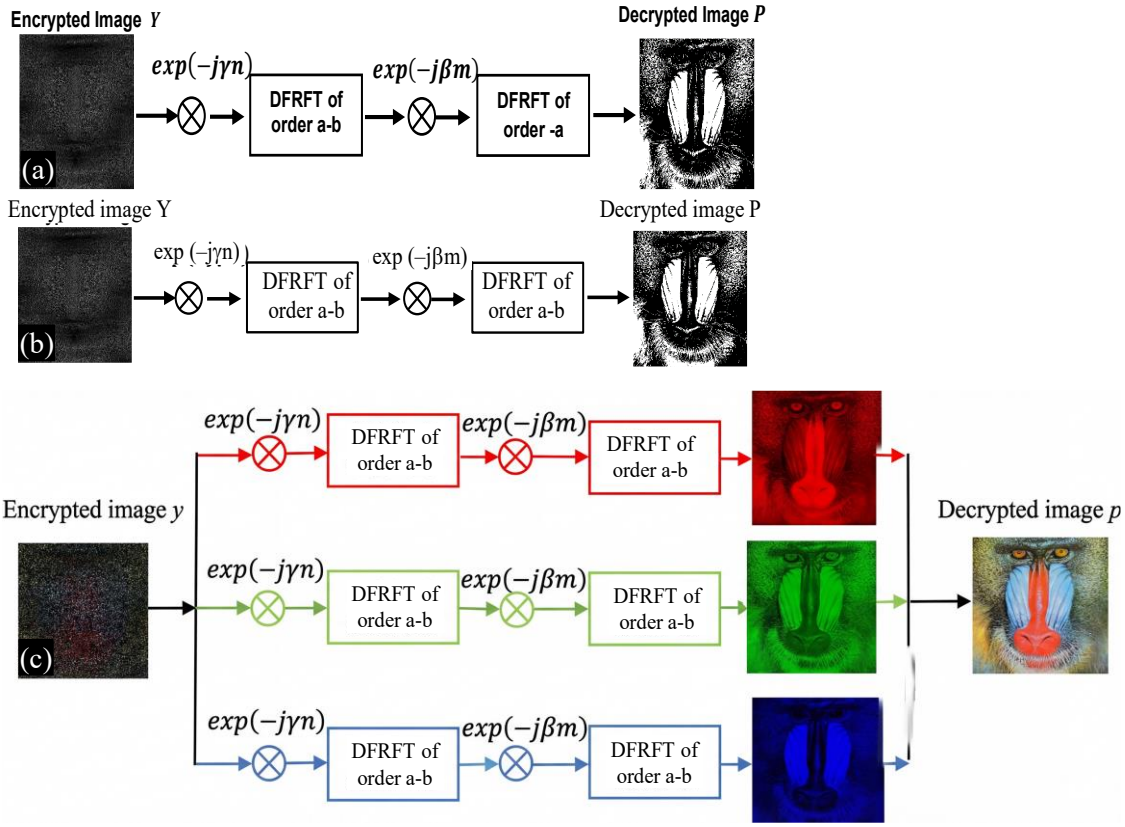

Figure 3(a–c). Schematic diagram of decryption for color image.

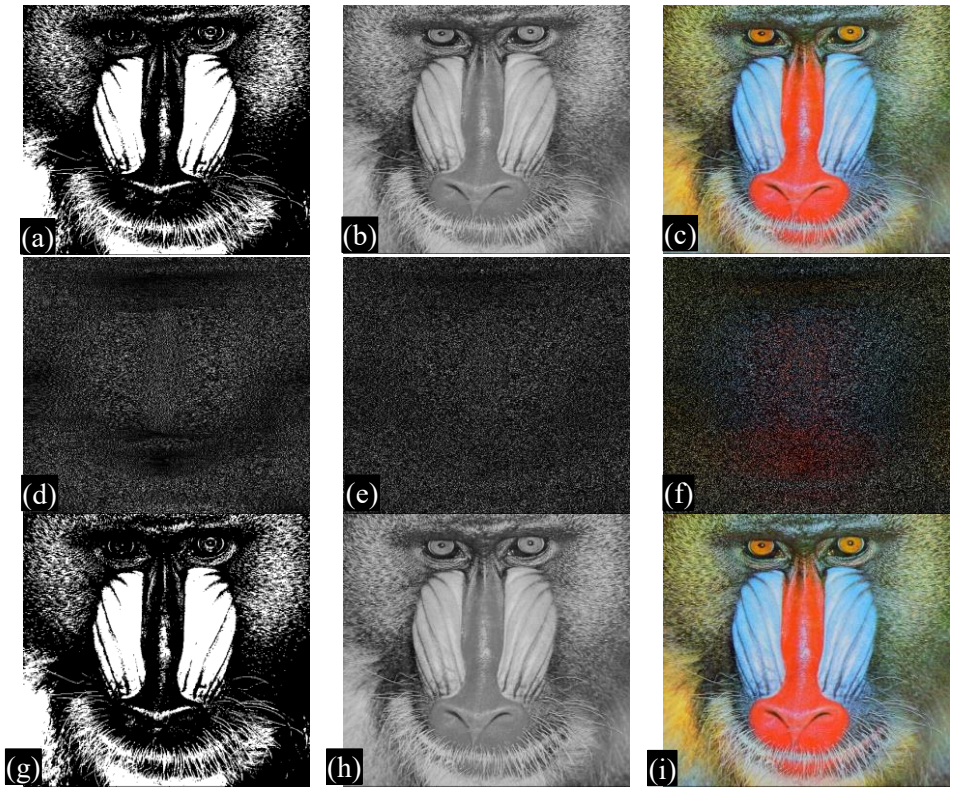

Figure 4(a–i). (a) Original binary image, (b) encrypted binary image, (c) decrypted binary image, (d) original gray image, (e) encrypted gray image, (f) decrypted gray image, (g) original color image, (h) encrypted color image, and (i) decrypted color image.

Table 1. Full-reference (FR) and No-reference (NR) encryption performance parameters for evaluating the efficiency of algorithms for the three images (binary, grayscale, and color).

IQM	The value of the images			IQM	The value of the images		
	Binary	***Grayscale***	***Color***		***Binary***	***Grayscale***	***Color***
ET (sec)	7.106012	7.989197	21.236692	MDSI	0.775913	0.716810	0.715038
DT (sec)	6.885329	8.147813	23.466814	FSIM	0.334103	0.310022	0.300973
UACI	0.34875061	0.5082419	0.5381532	SSIM	0.173941	0.002320	0.001983
NPCR	0.460220	0.999866	0.999619	MS-SSIM	0.115509	0.181886	0.172317
CC	0.511486	0.681878	0.815001	SR-SIM	1.000000	1.000000	1.000000
UIQI	0.075027	-0.000005	-0.000005	SC	164.972487	472.898858	472.531638
SNR	1.000000	1.000000	1.000000	NK	0.887296	0.330693	0.379836
PSNR	4.608349	5.472894	4.748057	GSMD	0.491005	0.287532	0.282446
MSNR	1.000000	1.000000	1.000000	DSI	0.014568	0.754808	0.728101
WSNR	1.494943	0.328635	0.307267	Eo	0.932710	7.357875	7.752819
MSE	88.864403	254.732624	254.534817	Ed	0.995683	0.995683	0.995683
RMSE	9.426792	15.960345	15.954147	VIF	6.944751	6.149647	7.459844
LMSE	0.997574	0.986512	0.982886	BER	709923.	1063326.	1086080.
MAE	88.864403	254.732624	254.534817	Computer Vision and Scene Understanding System Integration (CVSSI)	0.395930	0.279053	0.269733
NAE	0.996520	0.995847	0.996078	Decision Support System (DSS)	0.006192	0.038591	0.039695
AD	88.555191	129.153530	136.795193	ESSIM	0.972874	0.988596	0.988508
MD	255.000000	230.000000	254.000000	FFS	0.747862	0.679033	0.681823

baboon picture with a size of 512 × 512 pixels was employed in our database, which is of the BMP type. To authenticate and confirm the functionality and safety of the intended image encryption system, numerical simulations were conducted in MATLAB 2021a. Encryption and decryption results using discrete fractional transforms (DFRFT) are shown in Figure 4. The effects of the encryption performance parameters were calculated, and their values are listed in Table 1.

Image Quality Assessment (IQA)

In encryption performance measures, the quality of the decrypted image is assessed based on the original images as the reference images. The assessment techniques used in this subsection are as follows: number of pixel change rate ($NPCR$), unified average changed intensity ($UACI$), correlation coefficient analysis (CC), universal image quality index (UQI), signal-to-noise ratio index (SNR), peak signal-to-noise ratio index (PSNR), mean signal-to-noise ratio index (MSNR), weighted signal-to-noise ratio (WSNR), mean square error index (MSE), root mean square error index ($RMSE$), Laplacian mean square error index ($LMSE$), mean absolute error index (MAE), normalized absolute error index (NAE), average difference index (AD), maximum difference index (MD), structural content index (SC), normalized cross-correlation (NK), gradient similarity metric ($GSMD$), mean deviation similarity index ($MDSI$), feature similarity index ($FSIM$), structural similarity index ($SSIM$), multiscale structural similarity index ($MS-SSIM$), spectral residual-based similarity index ($SR-SIM$), visual information

fidelity measure (VIF), number of bit error rate (BER), contrast and visual saliency similarity-induced index ($CVSSI$), discrete cosine transform Discrete Cosine Transform (DCT) subband similarity index (DSS), edge-strength-similarity-based image quality metric ($ESSIM$), features fusion similarity index (FFS), dissimilarity index based on order pattern analysis (DSI).

Simulation Results and Dataset Description

The safety of the encryption algorithm was studied according to the proposed scheme, and a series of experiments were conducted using 512 × 512-pixel baboon images. The actual performance of the algorithm was measured using various conventional measures and tests, such as the correlation of pixels, histogram, and information entropy, sensitivity to keys, and space.

The Effect of Encryption Process table

MATLAB 2021 was used to execute the simulation experiment under a Windows system. When the plaintext was encrypted and decrypted simultaneously, we could hardly notice any data of the plaintext image that played the role of providing information confidentiality. The plaintext image was compared with the decrypted image, and the decrypted image was absolutely identical to the original image. The coded and decomposed images of the baboon are shown in Figures 5–31.

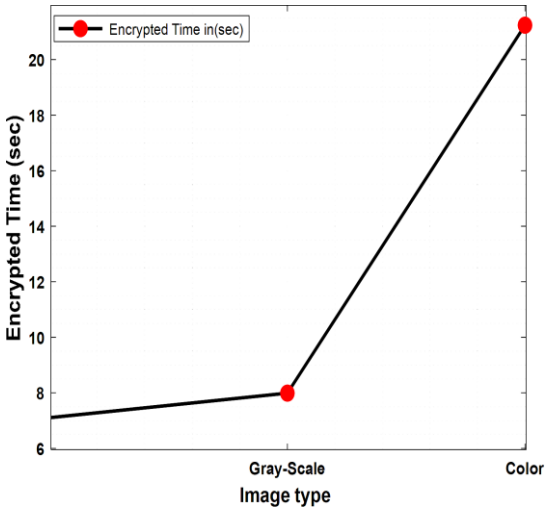

Figure 5. Effect of image type on encoding time.

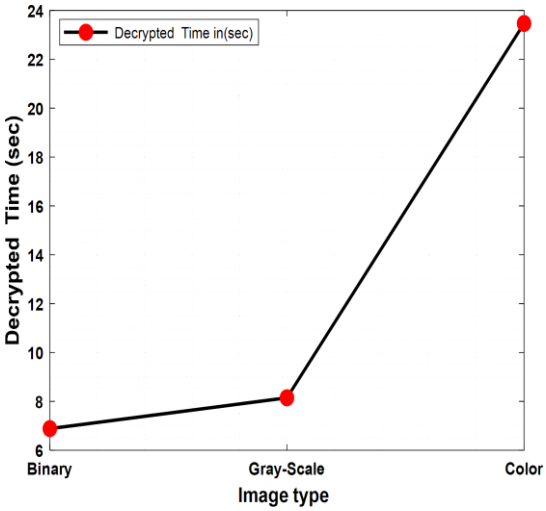

Figure 6. Effect of image type on decoding time.

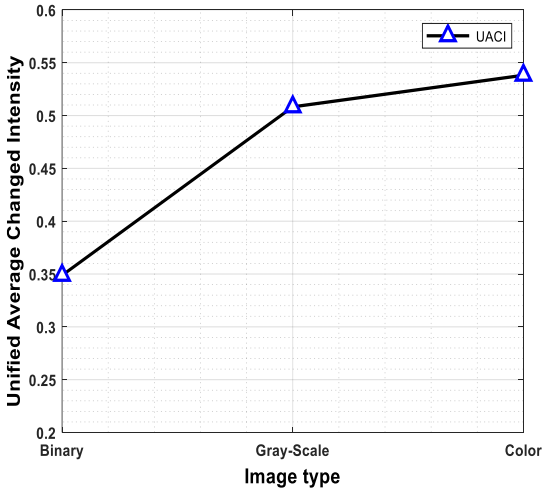

Figure 7. Effect of image type on UACI.

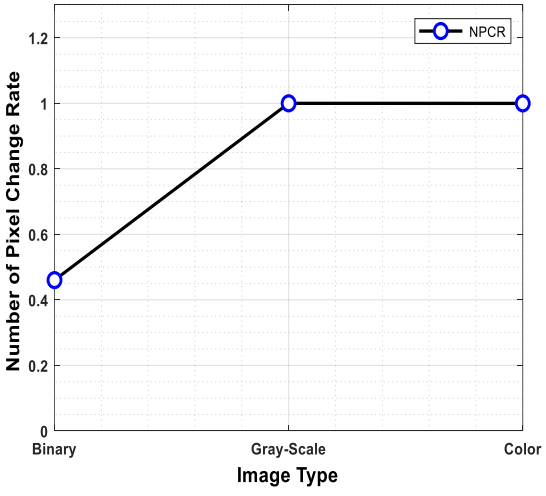

Figure 8. Effect of image type on NPCR.

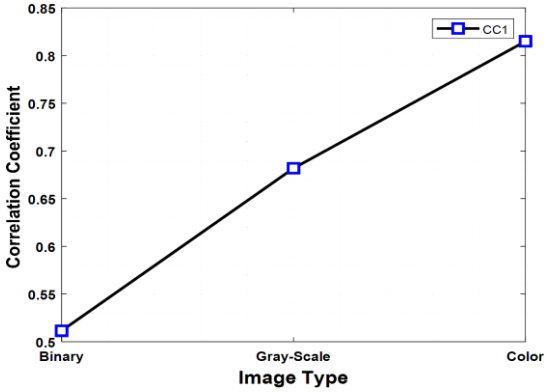

Figure 9. Effect of image type on CC.

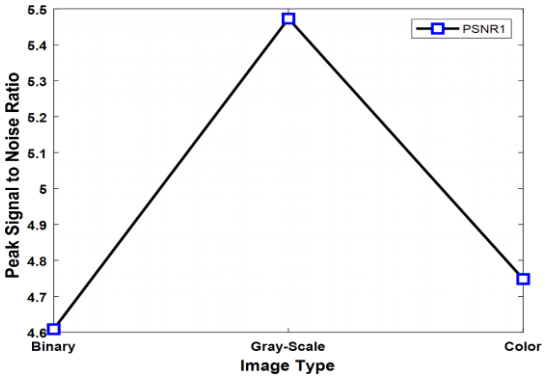

Figure 10. Effect of image type on PSNR.

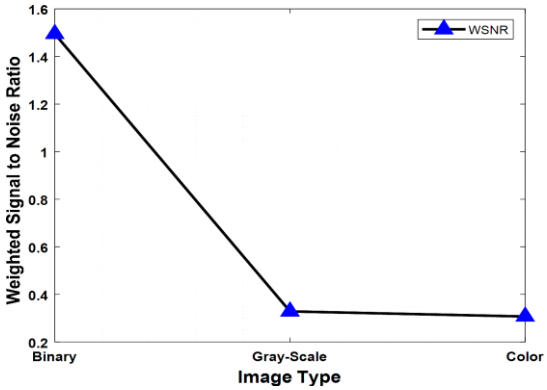

Figure 11. Effect of image type on WSNR.

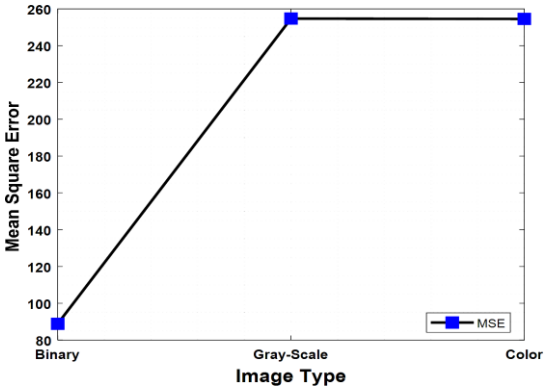

Figure 12. Effect of image type on MSE.

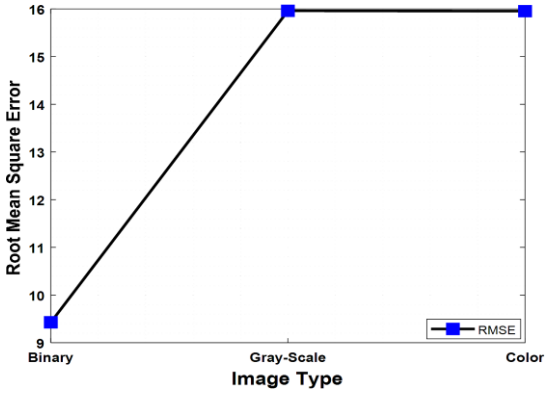

Figure 13. Effect of image type on RMSE.

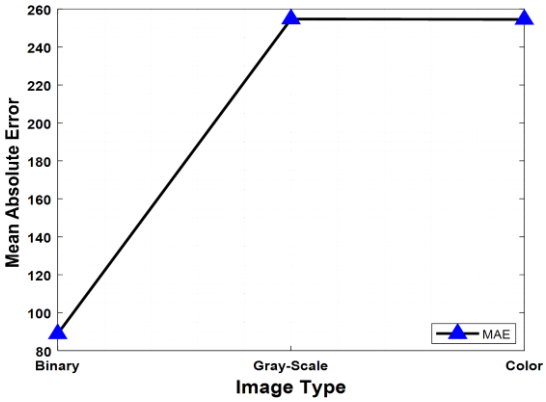

Figure 14. Effect of image type on MAE.

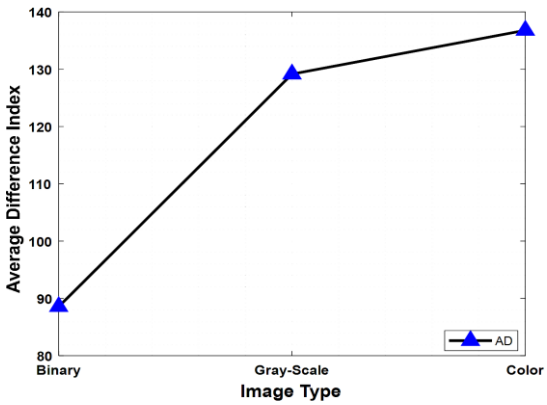

Figure 15. Effect of image type on AD.

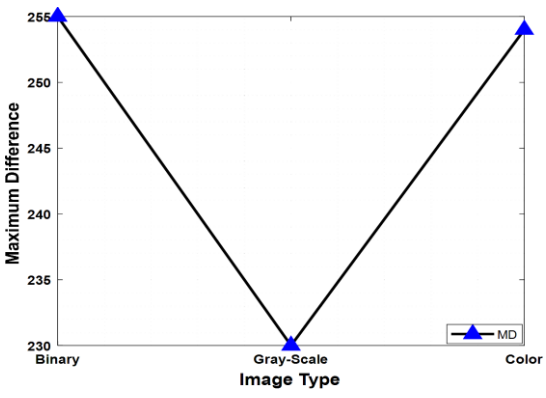

Figure 16. Effect of image type on MD.

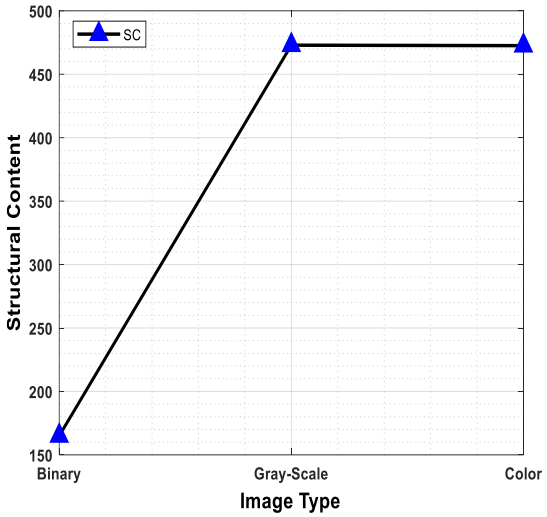

Figure 17. Effect of image type on SC.

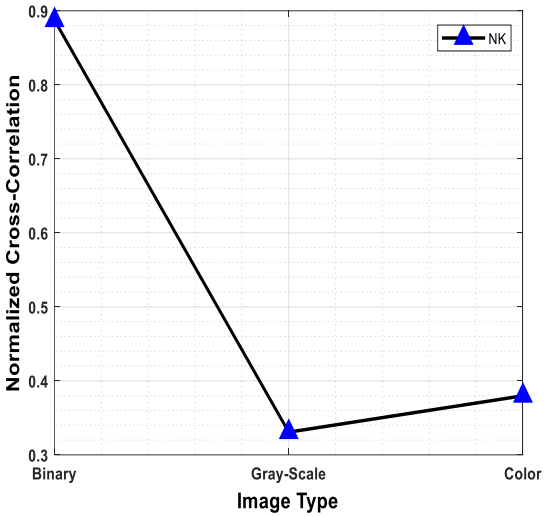

Figure 18. Effect of image type on NK.

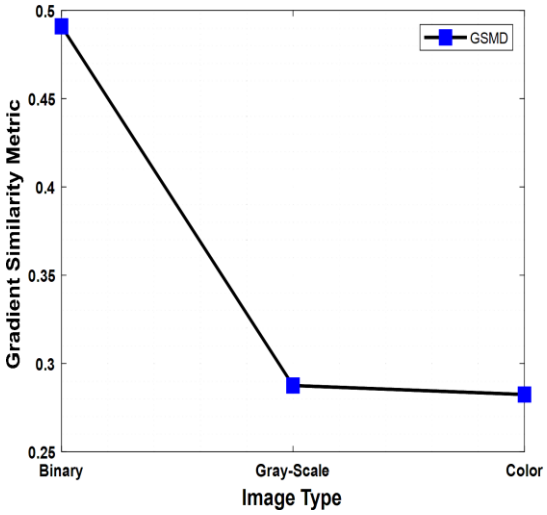

Figure 19. Effect of image type on GSMD.

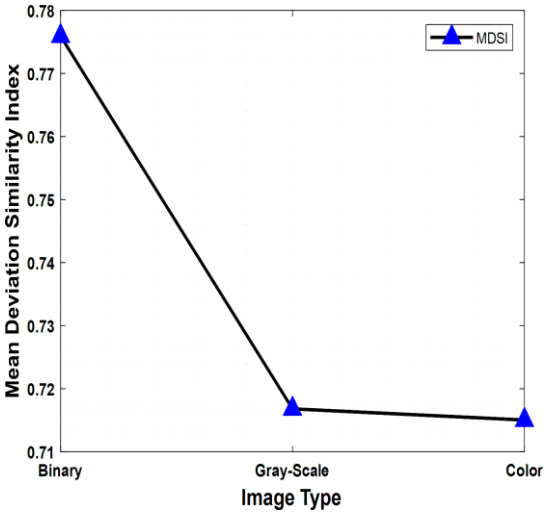

Figure 20. Effect of image type on MDSI.

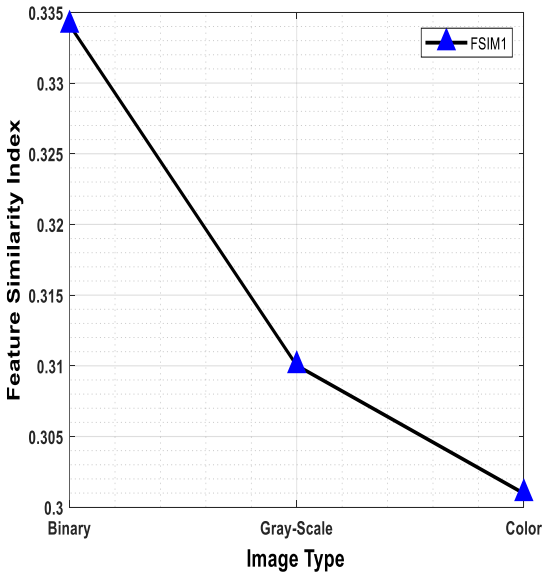

Figure 21. Effect of image type on FSMI.

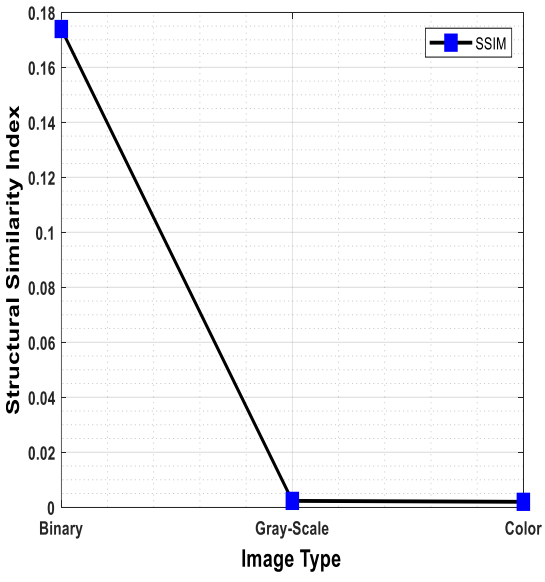

Figure 22. Effect of image type on SSIM.

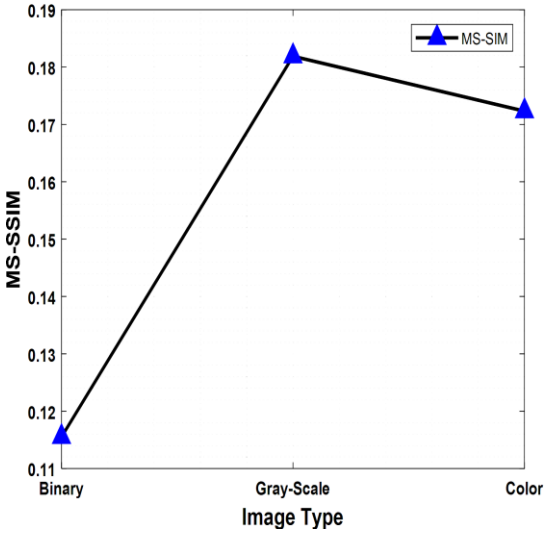

Figure 23. Effect of image type on MS-SSIM.

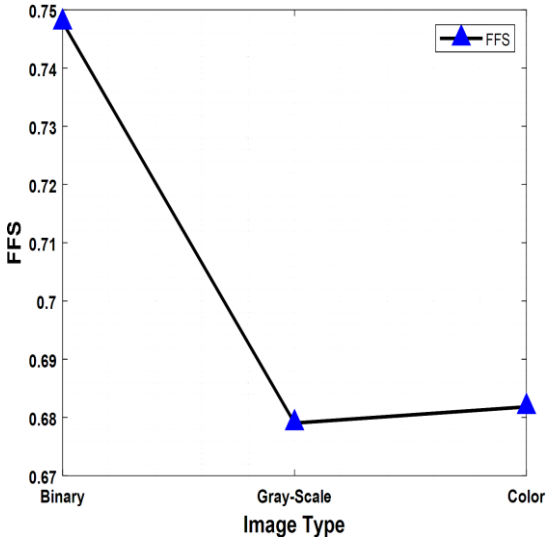

Figure 24. Effect of image type on FFS.

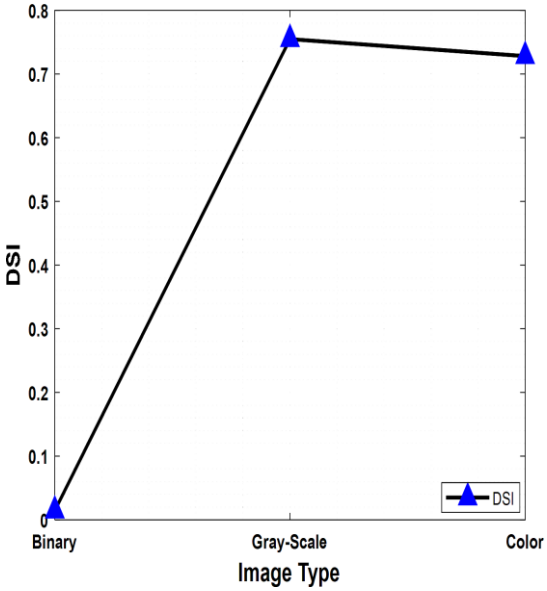

Figure 25. Effect of image type on DSI.

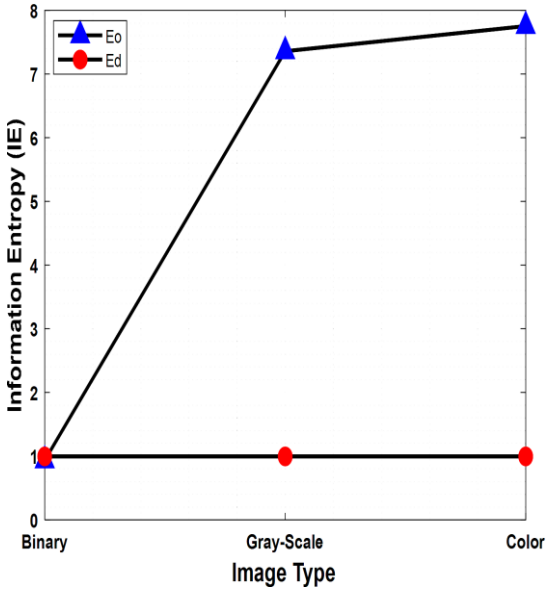

Figure 26. Effect of image type on IE.

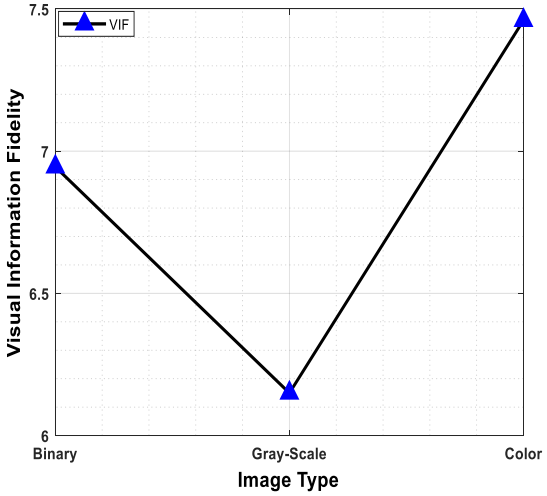

Figure 27. Effect of image type on VIF.

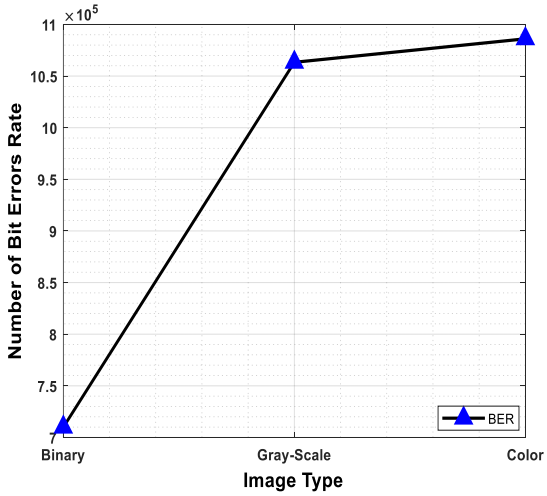

Figure 28. Effect of image type on BER.

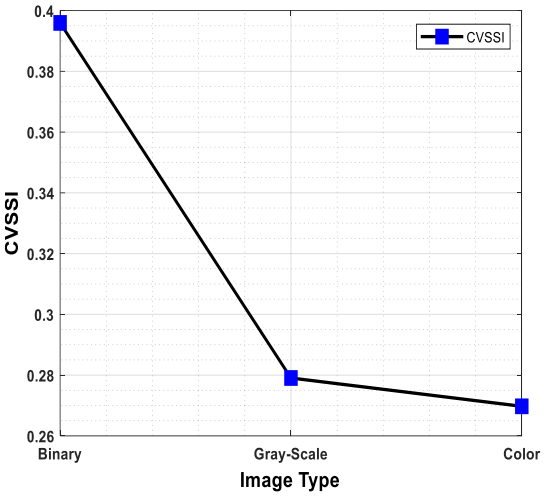

Figure 29. Effect of image type on CVSSI.

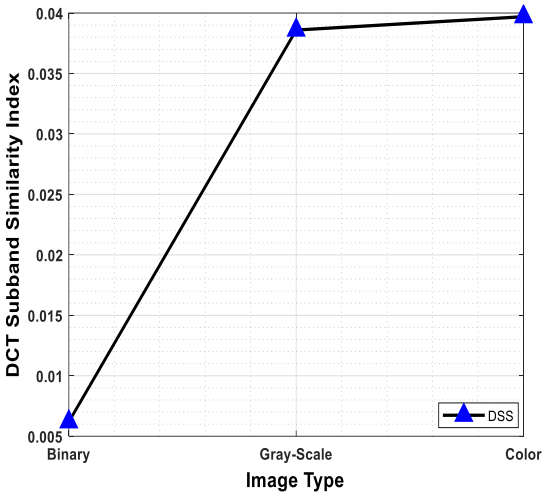

Figure 30. Effect of image type on DSS.

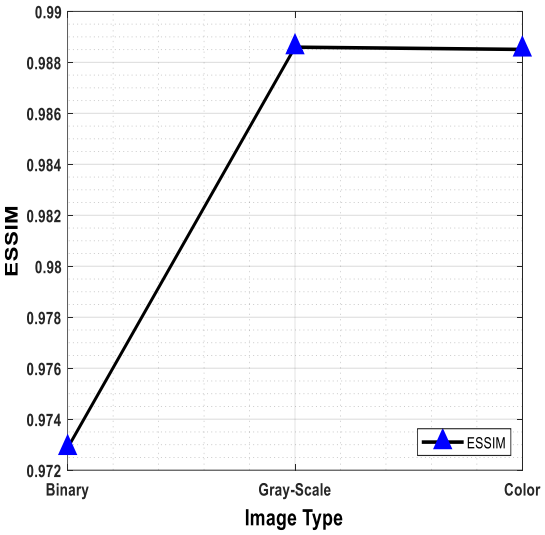

Figure 31. Effect of image type on ESSIM.

DISCUSSION

In this study, image encryption and decryption techniques were applied to three versions of the same image: binary, grayscale, and colored (RGB). Common measures were adopted to objectively evaluate the quality of the decrypted images. These measurements provide information about the quality of the preservation of the visual and structural integrity of each image following the encryption procedure [12,13]. The results, as shown in Table 1 and the graphical charts, can be summarized as follows:

1. *Parameters of the encryption performance:* Encoding time (ET), decoding time (DT), UACI, CC, AD, IE, BER, and DSS are directly proportional to the development of the type of image. As the simplest type of binary image has only two values, and the grayscale becomes finer, values are the most common, culminating in color images.
2. *Visual quality metrics:* The values of WSNR, NK, GSMD, MDSI, FSIM, SSIM, FFS, and CVSSI showed a slight decrease in the grayscale images but further decreased to the lowest levels with colored images.
3. *Objective fidelity measures:* It can be concluded that a similar pattern is present based on the results of the applied objective measures (NPSR, MSE, RMSE, MAE, SC, and ESSIM): the quality scores increase with the variation of the image type between the binary and grayscale modes. However, when an image is converted to grayscale, the measures are likely to become steady with slight fluctuations when compared with the color version of the image. This implies

that the processes of encryption and decryption do not affect the quality of an image in grayscale or in color; however, binary images have low fidelity because they have less tonal information.

4. *Practical implications and algorithm strength:* The trends revealed demonstrate the strength and flexibility of the proposed encryption scheme. Although binary images were transformed into color images, which caused more complexities, the algorithm performed well in all measurements. Some minor impairments in the visual quality of the color images are anticipated because the data dimensionality is higher; however, the structural integrity is not compromised. Based on these findings, the proposed method can not only process simple types of images but is also scalable and effective with high-resolution, multi-channel images; hence, it can be deployed in real-life to ensure secure image transmission and storage.

Comparative Analysis of Encryption Efficiency in Binary, Grayscale, and Color Images

To evaluate the flexibility and efficiency of the proposed encryption scheme, a comparative analysis of its effectiveness on three image formats–binary, grayscale, and color images–is presented in the following section.

- *Efficiency of DFrFT algorithms in encrypting and decrypting a finished image:* Simulation precision indicated that the DFrFT algorithm is efficient in encrypting and decrypting a completed image with high accuracy in all three modes: monochrome, grayscale, and color. This indicates that the algorithm is flexible to use with various types of images without retrieval efficiency issues.
- *Visual Characteristics Match After Decryption:* The decoded images were tested using a variety of image quality parameters. The results indicated a high degree of correspondence between the original and decrypted images, which indicates the algorithm's accuracy in maintaining the image's visual features.
- *Algorithms:* Despite having three channels (RGB) in color images, the algorithm had no impact on performance. It is shown to have a high ability to process multidimensional data, which is the strength of the proposed system in the real world.
- *Strength to Withstand Attacks:* Various tests were conducted to determine the willingness of the proposed system to withstand possible attacks (statistical analysis, noise attacks, and modification attacks). The findings established that the system has a high level of security and robustness.
- *Computational and time stability:* The algorithm was found to be stable in its performance regarding the time of computational time to execute encryption and decryption of the image, and particularly when we compared the image with a varied composition to demonstrate the applicability of the algorithm to real-life applications.

CONCLUSION

The present study compares image encryption using the DFrFT on three versions of the same image: a binary, grayscale, and color image. The simulation results under ideal conditions (encryption and decryption with correct keys) demonstrate that the proposed scheme is efficient and workable for all types of images under ideal circumstances. Various objective image quality metrics are used to determine the fidelity of the decrypted images. The findings indicate that an image and its decryption produced a high percentage of similarity, proving that the algorithm is capable of maintaining visual and structural features. It is worth noting that in binary images, the fidelity was lower as they were recreated in grayscales and in color because of their limited tonal range, whereas in grayscale and color images, the fidelity was steady and of high quality. ET, DT, and statistical measures (UACI, CC, BER, and DSS) increased proportionally with the complexity of the image but remained within reasonable limits. The system was proven to be resilient to different attacks, such as statistical, noise-based, and modification attacks, confirming the resilience of the system as well as its strength and security. Overall, the DFrFT-based cryptosystem was found to be effective, scalable, and capable of supporting various image modalities. Its capability of multidimensional data processing and computational stability connects it to being a promising source of transmission and storage of secure images in real-life applications. This procedure was effective in the encryption and decryption of all three categories of images, as evidenced by the outcomes.

REFERENCES

1. Zhu B, Liu S, Ran Q. Optical image encryption based on multifractional Fourier transforms. Opt Lett. 2000;25:1159–61. doi:10.1364/OL.25.001159.
2. Luchko Y. Fractional Fourier transform. In: Kochubei A, Luchko Y, editors. Basic Theory. Berlin: De Gruyter; 2019. p. 225–40. doi:10.1515/9783110571622-009.
3. Zhao T, Yuan L, Li M, Chi Y. A reformulation of weighted fractional Fourier transform. Digit Signal Process. 2020;104:102807. doi:10.1016/j.dsp.2020.102807.
4. Ahuja B, Lodhi RS. Image encryption with discrete fractional Fourier transform and chaos. In: Kaliammal N, Mukherjee S, editors. Advances in Engineering and Technology. Fifth International Joint Conferences on CNC & CCPE 2014; 2014 Feb 21–22; Chennai, India. Red Hook (NY): Curran Associates Inc.; 2014. p. 247–54.
5. Annaby MH, Rushdi MA, Nehary EA. Image encryption via discrete fractional Fourier-type transforms generated by random matrices. Signal Process. 2016;49:25–46. doi:10.1016/j.image.2016.09.006.
6. Ashutosh D, Sharma D. Robust technique for image encryption and decryption using discrete fractional Fourier transform with random phase masking. Procedia Technol. 2013;10:707–14. doi:10.1016/j.protcy.2013.12.413.
7. Al-Khafaji KH. Using medical imaging to differentiate live and dead sperm cells: A technical and analytical study. Kuw Sci Res J Med Sci. 2026;3(1):1–8. doi:10.61705/ksrjms.3.1.2026.1.8.
8. Annadurai S. Fundamentals of Digital Image Processing. Delhi: Pearson; 2007. p. 211–27.
9. Rosenfeld A. Computer vision: Basic principles. Proc IEEE. 1988;76:863–8. doi:10.1109/5.5961.
10. Al-Khafaji KH. Regarding the security of discrete fractional Fourier transform in color image encryption and decryption. Al-Harf J. 2026;1(25):23–39.
11. Esam E, Elbendago S, Omer M. On the security of image encryption using discrete Fourier transform and fractional Fourier transform. Int J Eng Adv Technol. 2015;:27–38.
12. Ashutosh D, Sharma D. Image encryption using discrete Fourier transform and fractional Fourier transform. Int J Eng Adv Technol. 2013;2(4):886–90.
13. Sharma P. Efficient image encryption and decryption using discrete wavelet transform and fractional Fourier transform. [Preprint]. 2014. arXiv:1401.6087. doi:10.48550/arXiv.1401.6087.

