International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Fusion - Scalable Key Space Image Encryption for Enhanced Brute-force Attack Resistance

Suresh N. Nakum(RS-GTU)[1], Mehul B. Shah[2]

[1]Department of Electronics and Communication Engineering,
Government Engineering College, Rajkot,
Gujarat Technological University, Ahmedabad-382424, India
e-mail: sureshgec7@gmail.com

[2]Department of Electronics and Communication Engineering,
G.H. Patel College of Engineering, V.V. Nagar,
Charutar Vidyamandal University, Anand-288001, India
e-mail: drmehul.iitb@gmail.com

Corresponding Author: *Mehul B. Shah*[2]

Abstract

This paper introduces a novel method that leverages multiple random fusion (RMF) based image encryption techniques to address the demands of high-security applications. In cloud-based privacy-preserving systems for gray-level medical images for health care combine the power of encryption and cloud storage capacity. Inspired by ancient practices of safeguarding wealth by burying it deeply and concealing the location as secret keys, this scheme is designed to be scalable. The number of keys required is decided by specific security needs, considering computational resource and encryption time constraints. The method begins by randomly shuffling image blocks or pixels using secure keys or nonlinear transformations such as chaotic maps. Following this, random fusion operations are performed, including shadowing using high-energy signals and adjusting variance to achieve a uniform probability density function. This approach ensures that information leakage is prevented. It is tested for a highest number of key values of 2^{80000} or approximately 10^{24000}, with comparable values of statistical performance parameters. This high key space enhances robustness against brute-force attacks and can be integrated with other encryption methods to provide a general, scalable, and highly secure solution for applications where security is paramount.

Math. Sub. Classification: 37N99, 60E05, 60F05, 65C05, 68Q25, 94A08, 94A60.

Key Words: Brute-force attack, Central limit theorem (CLT), Chaotic map, Random multiple fusion (RMF), Scalable key space (SKS), Shadowing and variance adjustment (SVA).

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1 Introduction

In cloud-based scenarios for storing medical image, encryption plays a pivotal role by effectively obscuring the signal to the extent that the recovery of the original content without the corresponding secret keys becomes a near-impossible endeavor. A substantial majority of image encryption methods predominantly rely on permutation and substitution operations [1]. Image signal encryption algorithms can be delineated into three distinct categories, the conventional approach [1], which primarily caters to textual data, lays the foundation for the first category. Second, the transform-based methods, which effectively grapple with the limitations imposed by a restricted key space [2] use only two keys for information hiding. The third category is characterized by chaos-based techniques, frequently harnessed for key generation and the imparting of permutation or substitution operations to image pixel values. Among these well-established chaotic maps such as Logistic [3, 4], Arnold [5, 6] and others are favored due to their heightened sensitivity to key variations, rendering them notably effective in the realm of image encryption. The utilization of chaotic maps extends across a spectrum of applications, as cited in [7–10]. Objective of the proposed method is to confront the challenge of a limited key space associated with conventional schemes by implementing a two-step process. Initially, we employ chaotic maps and other methods based on Block shuffling-M1 [11], Zig-zag scan-M2 [12], Arnold-M3 [13] and John S. and Murli P.'s (JSMP) chaotic map-M4 [14], which effectuate the permutation of blocks or pixels. This is subsequently followed by the application of random multiple fusion (RMF) to expand key space in conjunction with shadowing and variance adjustment (SVA) introduced to overcome challenge of getting flat histogram after encryption process.

2 Primary Cipher Image Generation Models

The proposed encryption technique incorporates a permutation operation that relies on the theoretical concepts expounded upon in methods M1 to M4 as discussed below then step-2 Algorithm 1is applied to all four pieces of work, validating generality property of this method.

M_1 The block shuffling method [11], owing to its compatibility with the JPEG compression standard, gained prominence. In this technique, the generation of the primary cipher image involves using a block size of 4 for an image with dimensions of 256x256. It commences with the sequential generation of row and column numbers, each being assigned an index. Subsequently, two permutation sequences, denoted as W and X, each with a length of 64, are created for the rows and columns of the block, respectively. The given image is then partitioned into blocks, with each block being placed at the position indicated by (W, X). This process of block transposition is repeated for each block to generate the cipher image.

M_2 This methodology adopts a zigzag scanning technique [12], to traverse the pixels within an image. The resulting image then undergoes a bit wise XOR operation with a randomly generated matrix. Finally, image blocks, each of size 4x4, are subjected to a 90-degree rotation, resulting in the production of an encrypted image. The zigzag scanning and 90-degree rotation operations effectively alter the pixel positions, while the XOR operation modifies their values.

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

M_3 The Arnold map is employed to transform the positions of pixels (i, j) using a transformation matrix $T = [1, 1; L, L + 1]$ [13]. Each position vector (i, j) is represented as P(i, j), and the process initiates with the initialization of z as 1. While z remains less than 8, a new position Pnew is computed using the modulo operation with respect to N1, i.e., $Pnew = Mod(T * P, N1)$. Consequently, Pnew yields a number that increases by 1, determining the new pixel position. This process is iterated for all pixels within the image, resulting in the generation of the cipher image.

M_4 The JSMP chaotic map [14], exhibits remarkable chaotic properties, as the random values it generates successfully pass all statistical tests provided by the national institute of standards and technology (NIST). In the case of the 1D JSMP chaotic map, the iterative equation is represented as $x(n + 1) = mod[r^2(x^2(n) - 5) - r^3(x^2(n) - 5)^2, 1]$. By generating random numbers within the range of 0 to 1 using this map and subsequently sorting them, random index values are obtained. These index values are then used to transpose the pixel values of an image, which is represented as a vector. The resulting cipher image is further enhanced by subjecting it to an additional layer of encryption process through scrambling.

The generated cipher image by any one method from M1 to M4 discussed above undergoes an additional layer of complexity by using an RMF accompanied by SVA as in Algorithm 1.

2.1 Key Space Scalability

In compression scalability is employed to achieve a harmonious equilibrium between the quality and size of an image [15].

Definition 1 (Fusion of Random Variables)**.** *Let $\{X_i\}_{i=1}^N$ be a set of independent random variables. The fusion operator $\mathcal{F}$ is defined as a function that combines $\{X_i\}$ into a single output random variable $X = \mathcal{F}(X_1, \ldots, X_N)$.*

The output of level one processing is fused with multiple random images, generated using different pseudo random number generators (PRNG) seeds as secret keys, followed by normalization. This results in multiple keys that can be increased based on security needs. As the count of seed-based random images increases, the key space expands, bearing a resemblance to a deeper burial. Users have the option to choose optimal parameters for a larger key space while still ensuring reasonable processing time, due to the key space scalability (SKS) property.

2.2 Minimum number of Keys Needed

In order to ensure effective encryption, it is necessary to include a minimum number of random images that exceed the just noticeable difference (JND) [16].

Theorem 1 (Fusion Count and DNCHS Condition)**.** *Let N be the number of fused random variables. If*

$$N > \text{DNCHS},$$

then the fused output X necessarily deviates from original shape and enters a high–entropy regime.

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Algorithm 1 Key Space Scalable Image Encryption

Procedure ENC($Ie_1, N, DNCHS$)[1] ▷ Ie_1-image after permutation.

do
$Q \leftarrow NormConstant$
$LoopCount \leftarrow N + DNCHS$
while $LoopCount \neq 0$ **do**
$RS \leftarrow Seed$ ▷ RS is seed of $PRNG$
if $LoopCount \neq N + DNCHS$ **then**
$RI \leftarrow GeneratedRandomImage$
$Ie_1 \leftarrow Ie_1 + RI$ ▷ Fusion with Ie_1
else
$HRI \leftarrow HighEnergyRandomImage$ ▷ Shadowing by HRI
$Var \leftarrow HVariance$ ▷ Set variance of high energy image
$Ie_1 \leftarrow Ie_1 + HRI$ ▷ HRIused for histogram flattening
end if
$LoopCount \leftarrow LoopCount - 1$
end while
$Ie_2 \leftarrow Ie_1/Q$ ▷ Q-Normalization constant
Plot PDF
while $PDF \neq UniformPDF$ ▷ Set optimum HEVariance by trials
end Procedure ▷ Ie_2 -Encrypted image

Procedure DEC($Ie_2, N, DNCHS, RS$)[2] ▷ DEC opposite to that of ENC
$Ie \leftarrow Ie_2 * Q$ ▷ De-Normalization
$LoopCount \leftarrow N + DNCHS$
while $LoopCount \neq 0$ **do**
$RS \leftarrow Seed$
if $LoopCount \neq N + DNCHS$ **then**
$RI \leftarrow GeneratedRandomImage$
$Ie \leftarrow Ie - RI$ ▷ De-Fusion
else
$HRI \leftarrow HighEnergyRandomImage$ ▷ Ues same-HRI
$Var \leftarrow HVariance$
$Ie \leftarrow Ie - HRI$ ▷ De-Shadowing
end if
$LoopCount \leftarrow LoopCount - 1$
end while
$Ie_1 \leftarrow Ie$
end Procedure

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This ensures that observers cannot discern any visual clues about the image content to be on safer side though it is second level of an encryption. To enhance encryption, it's recommended to maintain a minimum value of approximately three times the JND, referred to as the desired number of cover to hide signal (DNCHS).

2.3 Histogram Flattening by Shadowing

A uniform PDF is needed in order to not reveal any information about encrypted images [11–14]. The technique described here in effectively functions,

Lemma 1 (Gaussian Behavior Under Standard Fusion)**.** *If each X_i has finite variance and zero correlation, then the fused output $X = \mathcal{F}(X_1, \ldots, X_N)$ tends toward a Gaussian distribution as N increases, by the Central Limit Theorem.*

but without SVA, its histogram exhibits non-uniformity, as per CLT [17].The issue of non-uniform histograms can be mitigated through a process known as shadowing. This procedure involves the fusion of a thousand (K) times high-energy random signal with a low-energy signal, followed by subsequent normalization. This technique has not been previously utilized in the literature.

Conjecture 1 (High–Energy Fusion Produces Flattening)**.** *If the fusion operator $\mathcal{F}$ is energized by a high–intensity uniform weighting function, then the resulting fused random variable Z departs from Gaussian behavior and approaches a nearly flat uniform–like distribution.*

This approach is based on the concept that if X and Y are random variables having PDF $f(X)$ and $f(Y)$ Eq. (1), PDF of their sum Z Eq. (2) can be obtained through the convolution of their respective pdfs $f(Z) = f(X + Y) = f(X) * f(Y)$. Where, f(X) is a Gaussian distribution and f(Y) is a uniform distribution with high energy.

$$f(X) = \frac{1}{n\sigma_i\sqrt{2\pi}} e^{-\left(\frac{x-n\mu i}{2(n\sigma_i)^2}\right)} \quad and \quad f(Y) = \frac{1}{255K} \tag{1}$$

$$f(Z) = \frac{1}{255K\sqrt{2\pi}n\sigma_i} \int_{n\mu_i}^{255K+n\mu_i} e^{-(\tau-z)^2/2(n\sigma_i)^2} d\tau \tag{2}$$

σ_i is variance and μ_i is mean of fused random variables respectively. For a numerical Example, the Gaussian PDF is approximated by the vector$-X = [1, 3, 1]$, while the high energy uniform PDF is approximated by the vector of length forty$-Y = 5 * [1, 1, 1, ...1]$.

Proof. From Lemma 1, fusion under standard energy conditions tends to produce a Gaussian distribution. However, when the number of fused RVs satisfies $N >$ DNCHS, the fusion operates in an enhanced–energy regime. This regime pushes the distribution away from the Gaussian form and drives it toward a flatter shape due to increased dispersion and equalization of probability mass. Increased flattening directly implies higher entropy, yielding $H(Z) \geq H(X)$. Thus, the theorem follows. The convolution of these two distributions is depicted in Fig. 1, where zero values are observed at the beginning and end cause corner cutting. However, this issue can be resolved by variance adjustment. □

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

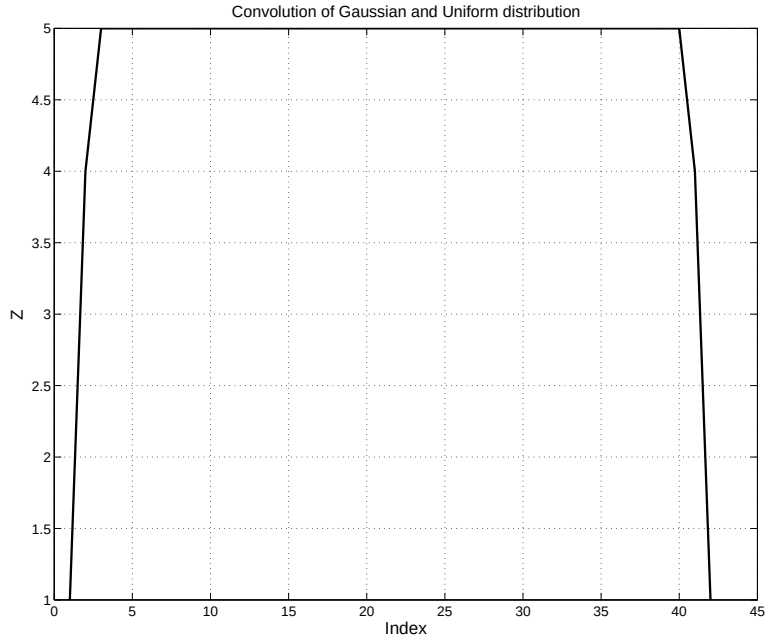

Figure 1. Distribution of Z=X+Y having corner cutting

Algorithm Explanation: The algorithm begins with the permuted image Ie_1 and initializes parameters using N and $DNCHS$. A normalization constant Q and loop counter are set to control the iterative process. In each iteration, either a random image (RI) or a high-energy random image (HRI) is added to Ie_1 for fusion and histogram flattening. The loop continues, enhancing randomness and equalizing the image distribution. Finally, the image is normalized by Q, and the variance is adjusted until the PDF becomes uniform, ensuring strong encryption. The decryption process is exactly opposite to that of encryption. The decryption procedure exactly reverses every operation performed during encryption. It begins with the encrypted image and restores its original scale by multiplying with the same normalization constant used earlier. The algorithm then iteratively removes the randomness added during encryption, for each iteration, the corresponding value from the chaotic sequence determines whether a Random Image RI or a High-Energy Random Image HRI was used, and the same component is now subtracted in reverse order of application. This step-by-step removal of RI/HRI gradually eliminates the injected energy and restores the image's pre-fusion structure. The algorithm retrieves the permuted intermediate image. Finally, the inverse of the initial permutation map is applied to this image to reconstruct the original pixel arrangement. The result is the perfectly recovered plain image, demonstrating the reversibility and lossless nature of the proposed encryption scheme.

3 Experimental Setup and Performance Parameters

The application of RMF follows, various types of transposition in the given setup, and its performance is evaluated based on the discussed parameters.

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3.1 Experimental Setup

This simulation was conducted on an HP workstation equipped with an Intel(R) Core(TM) i7-6700HQ CPU operating at 2.60GHz, with a 64-bit Windows platform using MATLAB 2019b. To compare the results with other schemes, medical test images of MRI and CT scans were utilized for experimentation from [18, 19], The original image exhibits a non-uniform histogram, indicating that its pixel intensities are unevenly distributed across the dynamic range as shown in 2. The values of the variables are as follows: $N = 100$ and for key space analysis, the values $N = 1000$ and $N = 10000$ are used; $DNCHS = 60$, and $Q = 1060$ for $N = 1000$ in Algorithm 1.

3.2 Performance Parameters

The performance evaluation primarily employs parameters mathematically defined below.

1. The term key space refers to the collection of all conceivable binary key combinations as used in[20].

2. The concept of key sensitivity refers to the minute alteration in the key value that renders decryption impracticable.

3. Peak signal-to-noise ratio (PSNR) Eq. (3) is a metric that quantifies the quality of a signal as compared to noise. Average noise power is represented by mean square error (MSE) Eq. (4) for general image of size $s = MN$.

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right)(\mathrm{dB}) \tag{3}$$

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}}\sum_{\mathrm{i}=1}^{\mathrm{M}}\sum_{\mathrm{j}=1}^{\mathrm{N}}\left|\mathrm{O}\left(\mathrm{i},\mathrm{j}\right) - \mathrm{Ie}(\mathrm{i},\mathrm{j})\right|^2 \tag{4}$$

$Ie(i, j)$ represents the encrypted image pixel value, while $O(i, j)$ corresponds to the original image pixel value.

4. Number of pixel change rate (NPCR) Eq. (5) calculates the percentage of pixel values that have changed, taking into account the size of the image.

$$\mathrm{NPCR} = \frac{1}{\mathrm{MN}}\sum_{\mathrm{i}=1}^{\mathrm{M}}\sum_{\mathrm{j}=1}^{\mathrm{N}}\mathrm{L}\left(\mathrm{i},\mathrm{j}\right) \times 100\,(\%)$$

$$\mathrm{L}\left(\mathrm{i},\mathrm{j}\right) = \begin{cases} 0 & \text{if } \mathrm{O}\left(\mathrm{i},\mathrm{j}\right) = \mathrm{Ie}\left(\mathrm{i},\mathrm{j}\right), \\ 1 & \text{if } \mathrm{O}\left(\mathrm{i},\mathrm{j}\right) \neq \mathrm{Ie}\left(\mathrm{i},\mathrm{j}\right), \end{cases} \tag{5}$$

5. Entropy Eq. (6) represents, the average number of bits required to encode each intensity $\theta k = Ie(i, j)$ or$Io(i, j)$ value present in an image vector.

$$\mathrm{H}\left(\theta\right) = \sum_{\mathrm{k}=1}^{\mathrm{s}}\mathrm{P}(\theta_{\mathrm{k}})\log_2\frac{1}{P\left(\theta_{\mathrm{k}}\right)} \tag{6}$$

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6. Unified average change in intensity (UACI) Eq. (7) represents the mean difference between an original image and an encrypted image, normalized by the maximum intensity value.

$$\mathrm{UACI} = \frac{1}{\mathrm{MN}} \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} \frac{|\mathrm{O}(\mathrm{i},\mathrm{j}) - \mathrm{I}_e(\mathrm{i},\mathrm{j})|}{255} \times 100\,(\%) \tag{7}$$

7. Correlation Eq. (8) is the degree of similarity between two images, in different directions. Here E-represents expectation, D-represents standard deviation and s-represents length of an image vector Eq. (9, 10).

$$\mathrm{R}_{\mathrm{o,Ie}} = \frac{\mathrm{E}[\,(\mathrm{O} - \mathrm{E}\,(\mathrm{O}))\,(\mathrm{Ie} - \mathrm{E}\,(\mathrm{Ie}))]}{\sqrt{\mathrm{D(O)D(Ie)}}} \tag{8}$$

$$\mathrm{E}\,(\mathrm{O}) = \frac{1}{\mathrm{S}} \sum_{\mathrm{k}=1}^{\mathrm{s}} \mathrm{O_k} \tag{9}$$

$$\mathrm{D}\,(\mathrm{O}) = \frac{1}{\mathrm{S}} \sum_{\mathrm{k}=1}^{\mathrm{s}} (\mathrm{O_k} - \mathrm{E(O)})^2 \tag{10}$$

8. Absolute mean shift (AMS) represents the shift in the mean value of an original image towards the 128-mean of a uniform PDF.

9. The chi-square value Eq. (11) is calculated by summing the squared differences between the observed and expected frequencies of intensity, divided by the expected frequency of intensity.

$$\chi^2 = \sum_{\mathrm{l}=0}^{255} \frac{(f\theta_l - E(f\theta_l))^2}{E(f\theta_l)} \tag{11}$$

4 Results and Discussion

As shown in Fig. 3 the slight differences observed in the encrypted images and their corresponding histograms arise from the fact that each encryption instance employs distinct secret keys for the RI and HRI stages. Since a minimal variation generates entirely different encryption dynamics. As a result, the encrypted outputs though visually noise-like, exhibit subtle variations in their statistical distributions. This sensitivity to key changes is a desirable security property, ensuring that each encryption run produces a uniquely randomized cipher image and histogram, thereby enhancing resistance against statistical attacks and brute force key–recovery attempts. It has been observed that simply by viewing encrypted images does not provide any clues about the original image as shown in figure. 3. The histograms of all the encrypted images appear flat, Corner cutting removed. The critical Chi-square value of 259, meets the quantitative criteria for a uniform PDF. The AMS falls near to its ideal value 0, within a narrow range from 0.2216 to 0.9501, ensuring uniformity.

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

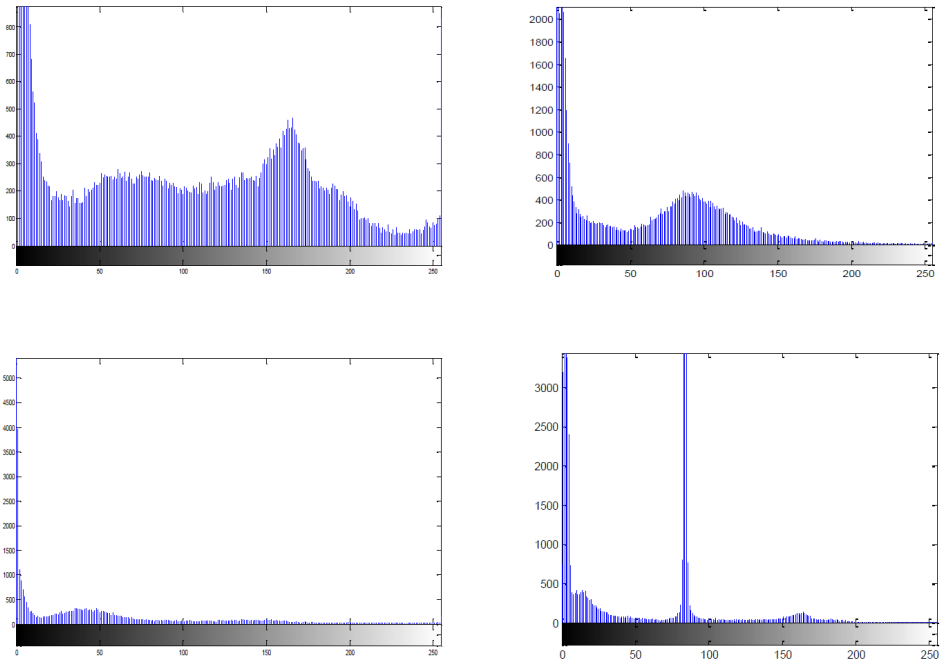

Figure 2. From left to right: Input original images MRI1, MRI2, CT1 and CT2's non uniform histograms having X- axies labels represent pixel intensity values and that of Y axies used for pixel count values, for each MRI and CT scan medical images from [18, 19]

4.1 Key Space and Brute Force Attack Resistance

Encryption keys are determined by the number of seeds used to generate 2-D random signals. If each seed is an eight-bit number, the key space is 2^8. In general, for N seeds, it's calculated as 2^{8N}. For N=100, N=1000, and N=10000, the key spaces are 2^{800}, 2^{8000}, and 2^{80000}, respectively, with execution times of approximately 4.59s, 39.06s, and 341.21s. Key space practically$\leq$ 4096 bits in most of practical schems. This encryption scheme offers scalable key spaces, making it adaptable to different higher security levels and resistant to brute force attacks as depicted in figure. 5 is also increases. Tradeoff between key space and execution time is observed. The robustness of the proposed encryption algorithm against brute-force attacks can be analytically demonstrated by evaluating the exhaustive key-search time for various key lengths. The total key space for an n-bit key is 2^n, and the expected average time to recover the key by exhaustive search is given by $T_{\text{avg}} = \frac{2^n}{2r}$, where r denotes the rate of key trials per second. Considering a high-performance HP workstation equipped with an Intel(R) Core(TM) i7-6700HQ CPU operating at 2.60 GHz on a 64-bit Windows platform using MATLAB 2019b, a realistic key-testing rate of $r = 10^9$ keys s^{-1} is assumed. Converting seconds to years by 1 year $= 3.15576 \times 10^7$ s, the logarithmic relation for the average search time becomes

$$\log_{10}(3.15576 \times 10^7) = \log_{10}(3.15576) + \log_{10}(10^7) = 0.499105 + 7 = 7.499105.$$

$$\log_{10}(T_{\text{avg,yr}}) = n \log_{10}(2) - 1 - \log_{10}(r) - 7.499105.$$

Accordingly, for key lengths of 800, 8000, and 80000 bits, the computed average brute-force decryption times are approximately $10^{222.32}$, $10^{2390.32}$, and $10^{24080.32}$ years, respectively. Given that the age of the universe is about 1.38×10^{10} years ($\log_{10} \approx 10.14$), these values exceed it by factors of $10^{212.18}$, $10^{2380.18}$, and $10^{24070.18}$ times, respectively. Such magnitudes

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

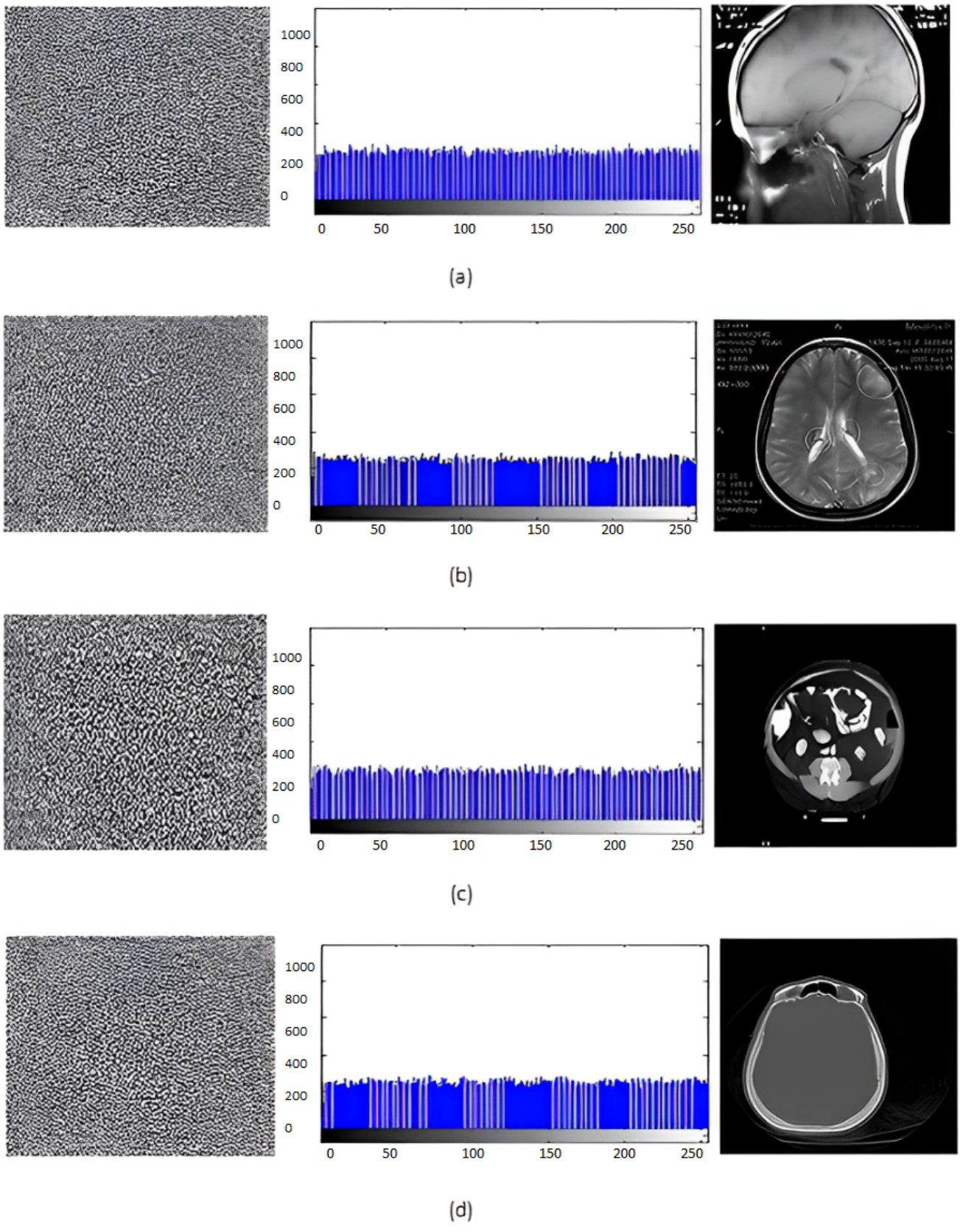

Figure 3. From left to right: a) Encrypted images, b) Image's histograms having X- axes labels pixel intensity values and Y- axes labels pixel count values, c) Decrypted images same as original. Two of each MRI and CT scan medical images from [18, 19]

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

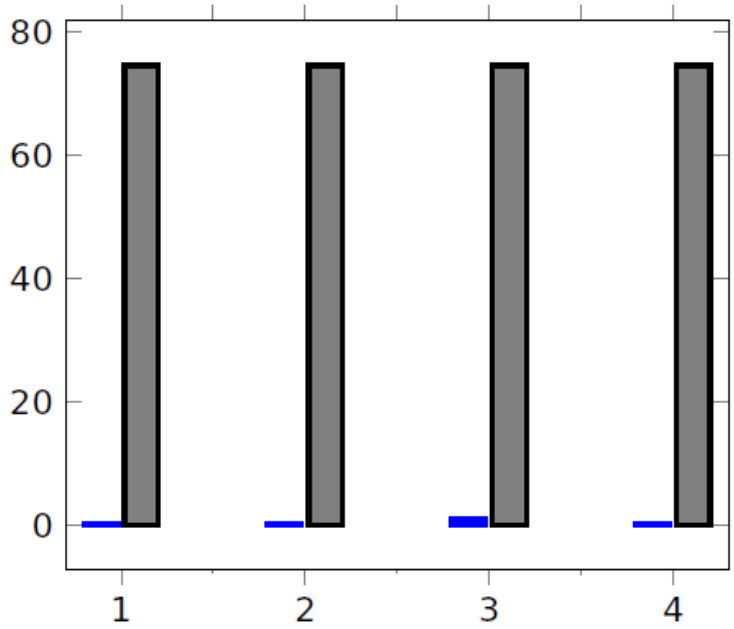

Figure 4. Average AMS on Y- axis of encrypted images in blue and original images in gray color, X- axis labels 1 for CT1, 2 for CT2, 3 for MRI1, and 4 for MRI2

conclusively establish that even the smallest 800-bit configuration provides incomparably high computational security, while the 8000 and 80000-bit key spaces extend the resistance to brute-force attacks to levels far beyond any conceivable physical or technological limits. Consequently, the proposed cryptosystem can be regarded as possessing an exceptionally strong defense against exhaustive key-search brute force attack attempts.

4.2 Key Sensitivity for Brute Force Attack Resistance

Many chaotic maps exhibit strong key sensitivity. Our scheme can be integrated with systems utilizing chaotic maps, thereby becoming sensitive to key value changes as minute

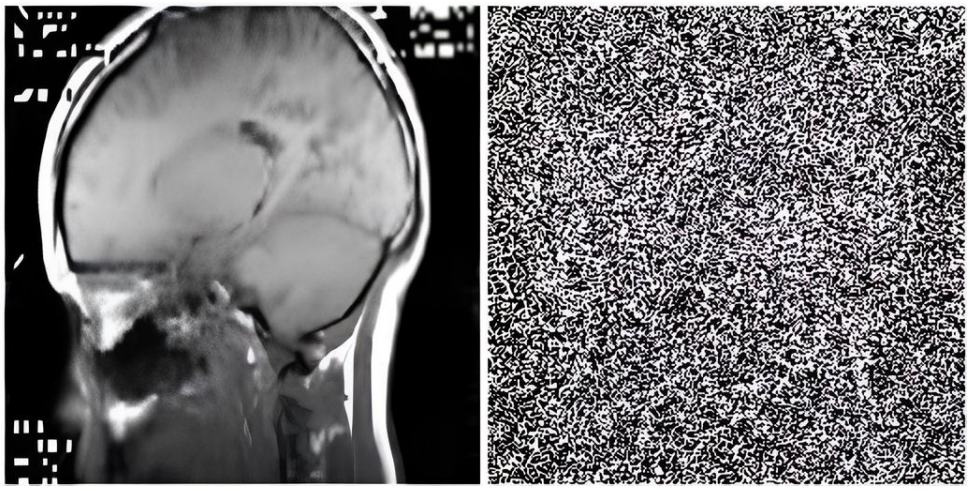

Figure 5. From Left to Right: a) Original and b) Brute force attacked image

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

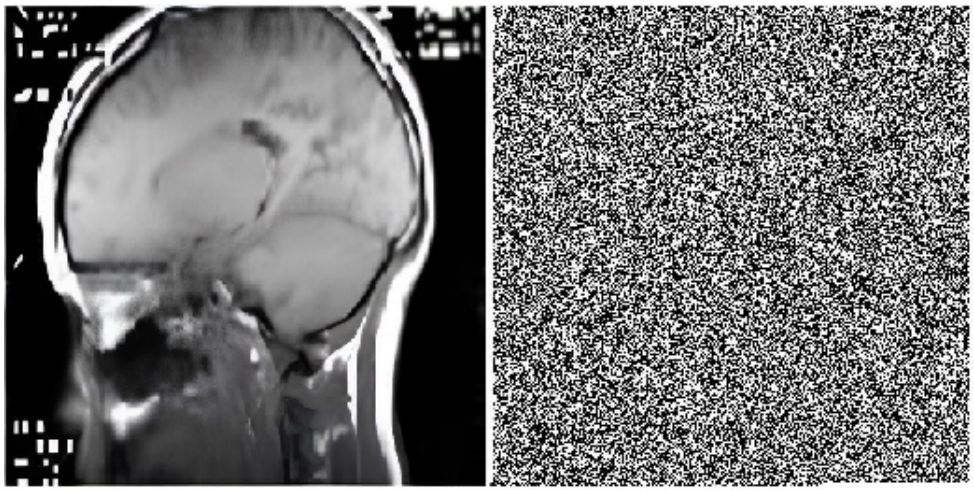

Figure 6. From left to Right: a) Image decrypted by the correct key. b) Brute force attacked image or image decrypted by correct key+δ for checking key sensitivity

Table 1. The parameter values obtained using proposed methods.

PSNR				
Methods	CT1	CT2	MRI1	MRI2
M1	6.0202	6.7487	7.1668	8.1974
M2	6.0348	6.7675	7.1867	8.1818
M3	5.4808	6.1115	6.4772	7.3785
M4	5.5348	6.1684	6.5500	7.44 01
NPCR				
Methods	CT1	CT2	MRI1	MRI2
M1	98.00	98.10	97.50	99.30
M2	99.59	99.58	99.57	99.60
M3	99.60	99.59	99.60	99.61
M4	99.9996	99.9901	99.9985	99.9997
Entropy				
Methods	CT1	CT2	MRI1	MRI2
M1	7.8640	7.8860	7.8645	7.8637
M2	7.8652	7.8863	7.8707	7.8682
M3	7.9840	7.9836	7.9848	7.9843
M4	7.9937	7.9938	7.9936	7.9932
UACI				
Methods	CT1	CT2	MRI1	MRI2
M1	33.33	33.03	33.20	33.38
M2	33.44	33.46	33.481	33.47
M3	33.46	33.46	33.44	33.45
M4	33.30	33.40	33.49	33.32

as $\delta = 0.001$ with such a small alteration, decryption becomes practically impossible, as illustrated in figure. 6.

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 2. The Correlation values obtained using proposed method.

	Correlation			
Methods	CT1	CT2	MRI1	MRI2
M1 HC	0.1546	0.1534	0.1518	0.1598
M1 VC	0.1609	0.1571	0.1645	0.1528
M1 DC	0.0300	0.0294	0.0279	0.0214
M2 HC	0.1520	0.1566	0.1518	0.1589
M2 VC	0.1543	0.1510	0.1587	0.1570
M2 DC	0.0254	0.0194	0.0326	0.0259
M3 HC	0.0061	0.0022	0.0020	0.0052
M3 VC	0.0030	0.0041	0.0018	0.0011
M3 DC	0.0061	0.0011	0.0086	0.0034
M4 HC	- 0.0066	0.0018	0.0065	-0.0038
M4 VC	0.0002	0.0010	0.0028	-0.0030
M4 DC	- 0.0125	0.0041	0.0024	0.0029

Table 3. Comparison of average results obtained except Chi-Sq. and Key Space with the values reported in literature.

Methods	Entropy	NPCR	UACI	HC	VC	DC	Chi-Sq.	Key Space
[12]	7.9973	99.6040	33.4654	0.0057	-0.0008	0.0037	243.52	10^{35}
[21]	7.9717	99.8714	-	-0.0032	0.0032	0.0008	-	10^{188}
[22]	4.7453	99.1432	32.5373	0.0057	0.0944	0.0067	-	10^{60}
[23]	7.9990	99.6114	33.4371	-0.0139	0.0177	0.0007	262.83	10^{98}
[24]	-	99.6600	33.3500	-0.0002	0.0053	0.0007	-	10^{77}
[25]	7.9991	99.9900	26.0350	-0.0226	0.0127	0.0057	-	10^{77}
Proposed	7.9936	99.9970	33.38	-0.0005	0.0003	-0.0008	259.02	10^{24000}

4.3 PSNR

Observed from Table 1 PSNR ranges from 5.5348 decibel to 8.1974 decibel, compared to the PSNR of the original image, which ranges from 40 to 45 decibel. This is because the encrypted image looks like a noise signal.

4.4 NPCR

The Table 1 shows NPCR obtained for encrypted images. Higher values indicate higher resistance to differential attacks. In a differential attack, the user attempts to change a single pixel and observes the resulting difference to estimate information. NPCR ranges from 99.57 to 99.9996, indicating that all pixel values are changed from their original values. JSMP based method has NPCR of about 99.99 to 99.9996%

4.5 Entropy

The proposed method has an entropy ranging from 7.8637 to 7.9936 Table 1, indicating that the image has almost zero redundancy.

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4.6 UACI

Its values for the implemented methods are shown in Table 1. This parameter also indicates the strength of the cipher against a differential attack. For high-security requirements, the UACI value should be greater than 25 , while the proposed method achieves a UACI of 33.46.

4.7 Correlation

The original image exhibits a high correlation value close to 1. Correlation values Horizontal (HC), Vertical (VC) and Diagonal (DC) are calculated and listed for encrypted images in Table 2. The JSMP-based method shows low average correlations of -0.0005 in the horizontal direction, 0.0003 in the vertical direction, and -0.0008 in the diagonal direction, as a result of correlation disruption by encryption.

So far paper structure identify and addresses the gap of small key-space in medical image encryption by proposing a fusion-based framework that achieves a uniform probability distribution rather than the conventional Gaussian profile, defined and found the DNCHS value, defined the AMS metric related to histogram uniformity, and observe the execution-time versus key-space trade-off, followed by a comparative analysis against state-of-the-art literature as below before concluding the study.

5 Comparison

From Table 3 the proposed encryption method exhibits very good performance overall when compared to other methods. It achieves an entropy of 7.9936, which is very close to the ideal value of 8 for gray scale images, indicating a high level of randomness and unpredictability in the encrypted image. This suggests that the method effectively obscures the original image data. The NPCR is 99.9970. The average UACI of the proposed method is 33.38, which is comparable to other method like [25] reports a UACI value of 26.035. Higher UACI indicates that the average intensity of differences between the original and encrypted images is substantial, contributing to the encryption effectiveness by making differential attacks more difficult. The average PSNR value is 6.4233. In terms of pixel average correlation coefficients, the proposed method achieves values very close to zero. HC is -0.0005, the VC is 0.0003, and DC is -0.0008. These near-zero values indicate that there is almost no correlation between adjacent pixels in the encrypted image, effectively eliminating patterns that could be exploited by attackers. This is a significant improvement over other methods like [23], this has a VC of 0.0944, indicating higher pixel correlation and thus potentially less secure encryption. The Chi-Square test value for the proposed method is 259.02, which falls within an acceptable range for a uniform distribution of pixel values, suggesting that the encrypted image's pixel values are evenly distributed. This uniformity is crucial for resisting statistical analysis attacks. Finally, the key space of the proposed method is scalable tested up to 10^{24000}, which is larger than the key spaces of other methods [12] and [21–24]. A larger key space enhances security by making brute-force attacks computationally infeasible. The combination of the proposed method tested with four other methods to ensure an integrability that enhance security.

Received on August 6, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6 Conclusion

The proposed method represents a significant departure from conventional approaches, as it results in a distinctive flat distribution, in contrast to the commonly encountered CLT outcomes of RMF. This departure is primarily attributed to the incorporation of shadowing effects and meticulous variance adjustments within the methodology. By integrating these elements, our approach seeks to mitigate the inherent limitations associated with only RMF, which often assume a normal distribution. The inclusion of shadowing factors acknowledges real-world complexities, ensuring a more flat representation of the encrypted data distribution. Moreover, the variance adjustments serve to enhance shape of distribution. This departure from normal distribution and the attainment of a flat distribution. Approach promising a more nuanced and adaptable framework for statistic of this application. It is observed that using the JSMP chaotic map method works really well. Obtained performance parameters of encryption algorithms like Average Entropy=7.9936, PSNR=5.5348, UACI=33.38, NPCR=33.38, Correlations are comparable and having SKS. To keep things secure, a parameter N can set to 10000, making the key space huge at 2^{80000} or approximately 10^{24000}. Practical impact is that the system can also integrated with other ways of image encryption to enhance its key space by large number to guard against potential brute force attacks. Future work focus on finding optimum solution for observed tradeoff between key space and execution time.

References

[1] C. E. Shannon, "Communication theory of secrecy system," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.

[2] N. Suresh and K. Karthik, "Secure fingerprint embedding based on modified gdft based parametric transform," in *IEEE International Conference on Image Information Processing*, 2011, pp. 1–6.

[3] L. Liu and S. Miao, "A new image encryption algorithm based on logistic chaotic map with varying parameter," *SpringerPlus*, vol. 5-289, pp. 1–12, 2016.

[4] L. Dragan, "S-box design method based on improved one-dimensionaldiscrete chaotic map," *Journal of Information and Telecommunication*, vol. 2, no. 2, pp. 181–191, 2018.

[5] K. T. Lin, "Image encryption using arnold transform technique and hartley transform domain," in *Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2013, pp. 84–87.

[6] D. Elmacı and N. B. Catak, "An efficient image encryption algorithm for the period of arnold's cat map," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 6, pp. 80–84, 2018.

[7] M. Dua and R. Bhogal, "Medical image encryption using novel sine-tangent chaotic map," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 9, p. 100642, 2024.

Received on August 6, 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[8] M. Gschwandtner, A. Uhl, and P. Wild, "Transmission error and compression robustness of 2d chaotic map image encryption schemes," *EURASIP Journal on Information Security*, pp. 1–16, 2007.

[9] M. Jain, A. Kumar, and R. C. Choudhary, "Improved diagonal queue medical image steganography using chaos theory, lfsr, and rabin cryptosystem," *Brain Informatics*, vol. 4, pp. 95–106, 2017.

[10] Z. Ma, W. Huang, and H. Gao, "A new block chain-based trusted drm scheme for built-in content protection," *EURASIP Journal on Image and Video Processing*, vol. 91, pp. 1–12, 2018.

[11] S. Rakesh, A. A. Kaller, B. C. Shadakshari, and B. Annappa, "Image encryption using block based uniform scrambling and chaotic logistic mapping," *International Journal on Cryptography and Information Security*, vol. 2, no. 1, pp. 49–57, 2012.

[12] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37 855–37 865, 2021.

[13] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[14] J. S. Muthu and P. Murali, "A novel dicom image encryption with jsmp map," *Optik - International Journal for Light and Electron Optics*, vol. 251, pp. 1–18, 2022.

[15] A. Jain and S. Panchanathan, "Scalable compression for image browsing," *IEEE Transactions on Consumer Electronics*, vol. 40, no. 3, pp. 394–404, 1994.

[16] W. Wan, J. Wu, X. Xie, and G. Shi, "A novel just noticeable difference model via orientation regularity in dct domain," *IEEE Access*, vol. 5, pp. 22 953–22 964, 2017.

[17] S. M. Ross, in *Introductory Statistics (Fourth Edition)*, fourth edition ed. Oxford: Academic Press, 2017, pp. 297–328.

[18] M. Levoy, "Medical images-the stanford volume data archive," 2021. [Online]. Available: https://graphics.stanford.edu/data/voldata/

[19] L. H. National Center for Biomedical Communications, "Medpix- a free open-access online database of medical images," 2009. [Online]. Available: https://medpix.nlm.nih.gov/home

[20] V. Dhairya, M. Ramchandra, B. Chetashri, B. Kiran, and C. Pallavi, "Modified caesar cipher and card deck shuffle rearrangement algorithm for image encryption," *Journal of Information and Telecommunication*, vol. 8, no. 2, pp. 280–300, 2024.

[21] S. Guhan, S. Arumugham, S. Janakiraman, A. Rengarajan, and R. Sundararaman, "A trio approach satisfying cia triad for medical image security," in *Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering*. Cham: Springer International Publishing, 2019, pp. 1109–1121.

Received on August 6, 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[22] S. Kumar, B. Panna, and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Med Biol Eng Comput*, vol. 57, p. 2517–2533, 2019.

[23] X. Chai, Z. Gan, and K. Yuan, "A novel image encryption scheme based on dna sequence operations and chaotic systems," *Neural Comput. and Applic.*, vol. 31, pp. 219–237, 2019.

[24] S. Bhattacharjee, M. Gupta, and B. Chatterjee, "Time efficient image encryption-decryption for visible and covid-19 x-ray images using modified chaos-based logistic map," *Springer Natur Appl Biochem Biotechno*, vol. 195, p. 2395–2413, 2023.

[25] J. Siju and S. N. Kumar, "Iot based medical image encryption using linear feedback shift register – towards ensuring security for teleradiology applications," *Elsevier Journal of Measurement: Sensors*, vol. 25, p. 100676, 2023.

Received on August 6, 2025