Image Binary Matrix Processing to Encrypt-Decrypt Digital Images

Mohamad Al-Laham[1], Firas Omar[2], Ziad A. Alqadi[3]
MIS Department, Al-Balqa Applied University, Amman, Jordan[1]
Faculty of Information Technology, University of Petra, Amman, Jordan[2]
Faculty of Engineering Technology, Al-Balqa Applied University, Amman, Jordan[3]

***Abstract*—This research study presents a simple cryptographic solution for protecting grayscale and colored digital images, which are commonly used in computer applications. Due to their widespread use, protecting these photos is crucial to preventing unauthorized access. This article's methodology manipulates an image's binary matrix using basic operations. These specified actions include increasing the 8-column matrix to 64 columns, reorganizing it into 64 columns, separating it into four blocks, and shuffle the columns using secret index keys. These keys are produced using four sets of common chaotic logistic parameters. Each set executes a chaotic logistic map model to generate a chaotic key, which is then translated into an index key. This index key shuffles columns during encryption and reverses during decryption. The cryptographic approach promises a large key space that can withstand hacking. The encrypted image is secure since the decryption procedure is sensitive to the precise private key values. Private keys are frequently chaotic logistic parameters, making encryption resilient. This method is convenient since it supports images of any size and kind without modifying the encryption or decryption techniques. Shuffling replaces difficult logical procedures in typical data encryption methods, simplifying the cryptographic process. Experiments with several photos will evaluate the proposed strategy. The encrypted and decrypted photos will be examined to ensure the method meets cryptographic standards. Speed tests will also compare the proposed method to existing cryptographic methods to show its potential to speed up picture cryptography by lowering encryption and decryption times.**

***Keywords*—Image processing; binary matrix; encrypt-decrypt; digital image**

I. Introduction

This research presents a revolutionary picture cryptography system that protects digital images from unauthorized access with simplicity, versatility, and strong security characteristics. Cryptography, DCI, GI, IBM, shuffle, PK, CK, IKEY, CLMM, quality, throughput, MSE, PSNR.

Digital images, such as grey images (GI) [1] and digital color images (DCI) [2], are crucial for computer applications and may contain private, secret, or confidential data, making hack protection a crucial concern. Image cryptography is an effective approach to safeguard digital images. Image cryptography uses encryption and decryption functions (Fig. 1(a) and 1(b)) [3]. The encryption and decryption functions alter the source picture and private key (PK) to produce encrypted and decrypted images, respectively [4], [5].

Good crypto systems must match these criteria [2]:

- The peak signal noise ratio (PSNR) [6] measured between the two images must be low.
- The decrypted picture must match the source image, have zero MSE, and have infinite PSNR [7].
- For high security, the PK must offer a hack-resistant key space [8].
- Cryptography should be fast, with minimal encryption and decryption times and maximum throughput [9].
- To simplify encryption and decryption, use a short sequence of instructions [10].
- The crypto technique must be flexible enough to handle any picture type and size without affecting encryption or decryption operations [11].

Grey image (GI) is a group of pixels organised in 2D matrix [12]. Fig. 2 shows how a histogram, decimal matrix, and grey image binary matrix may portray the image. IBM is obtained by bending and transforming the picture decimal matrix to binary [13].

Digital color image (DCI) is a 3D decimal matrix of pixels [14] with 3 bytes each to store the colors (red, green, and blue). Histograms, 3D decimal matrix, and color image binary matrix (CIBM) (see Fig. 3) can describe DCI. The CIBM is created by bending the image 3D matrix to one row matrix and converting the row matrix to binary [15], [16].

Researchers and practitioners have intensively studied data encryption strategies, relying mainly on the Data Encryption Standard (DES) and Advanced Encryption Standard. This effort, detailed in several articles, has improved our understanding of encryption [2]. Contributions that adapt or invent non-chaotic and chaotic encryption methods have further varied the debate [17]. These methods strike a unique balance between high-quality results and fast processing [18].

Although established encryption algorithms and those based on DES/AES frameworks have advanced the industry, they have limits. Limitations can waste resources or slow performance, especially when encrypting digital voice data. This research's proposed solution aims to alleviate these drawbacks and maybe improve encryption efficiency. To support these statements, Table I summarises the main aspects of DES and AES and the attributes expected from the proposed encryption technique [19].

This programme shows a dedication to improving encryption technology by combining established standards with

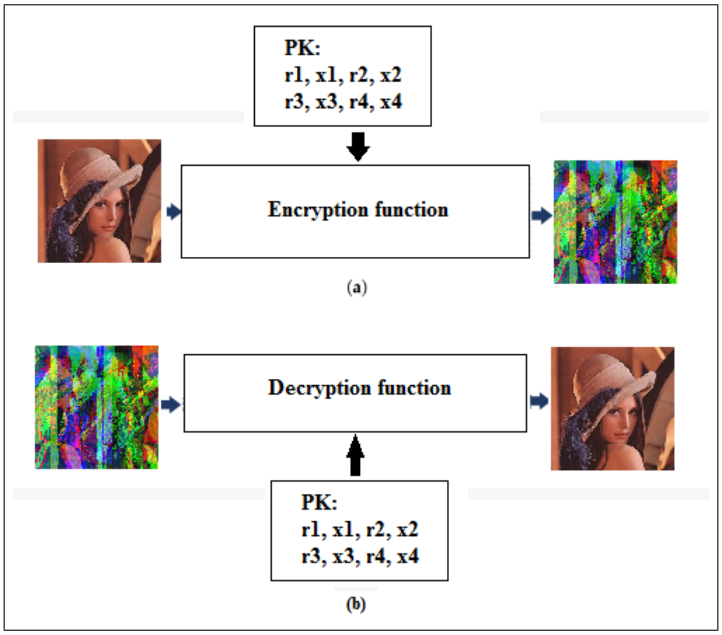
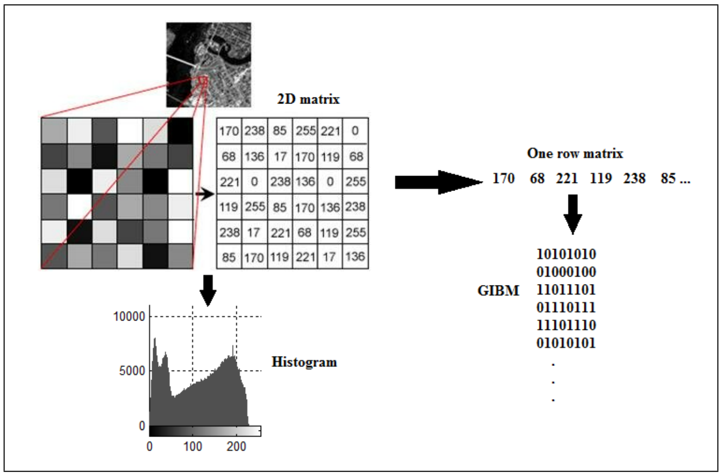


Fig. 1. Image crypto system diagram.



170	238	85	255	221	0
68	136	17	170	119	68
221	0	238	136	0	255
119	255	85	170	136	238
238	17	221	68	119	255
85	170	119	221	17	136

Fig. 2. GI Presentation.

new methods. Thus, it seeks to build stronger, more efficient, and more adaptive encryption methods to suit digital security concerns, particularly in voice file encryption.

The suggested method preserves the image bit-by-bit using the image binary matrix. IBM would make it easy to rearrange the image binary matrix into any number of columns. Index keys make shuffling these columns easy. Shuffling will replace all the complex logical techniques used in existing image cryptography methods. Using image binary matrix for encryption-decryption is unique. This technology can simplify picture cryptography by using traditional, chaotic, non-chaotic, and hybrid techniques [20].

The rest of the paper contains the following: Section II provides a brief overview of the literature review. Section III provides a brief overview of the Proposed Method. Section IV introduces the implementation of the proposed method and obtained results discussion. Section V introduces the study conclusion.

II. Literature Review

For reliable and effective encryption, a number of studies have presented picture encryption techniques that make use of binary matrix operations and chaotic maps. To guarantee efficiency and security, Zhu et al. [21] presented an algorithm that combines binary matrix transformations with chaotic logistic maps. Similar to this, Zhang et al. [22] presented a method for strong encryption appropriate for digital photos that makes use of logistic chaotic maps and binary matrix operations. In order to achieve great security and computational efficiency, Khalil et al. [23] introduced an effective encryption system using binary matrix operations and logistic chaotic maps. To ensure secure encryption and resistance against attacks, Liu

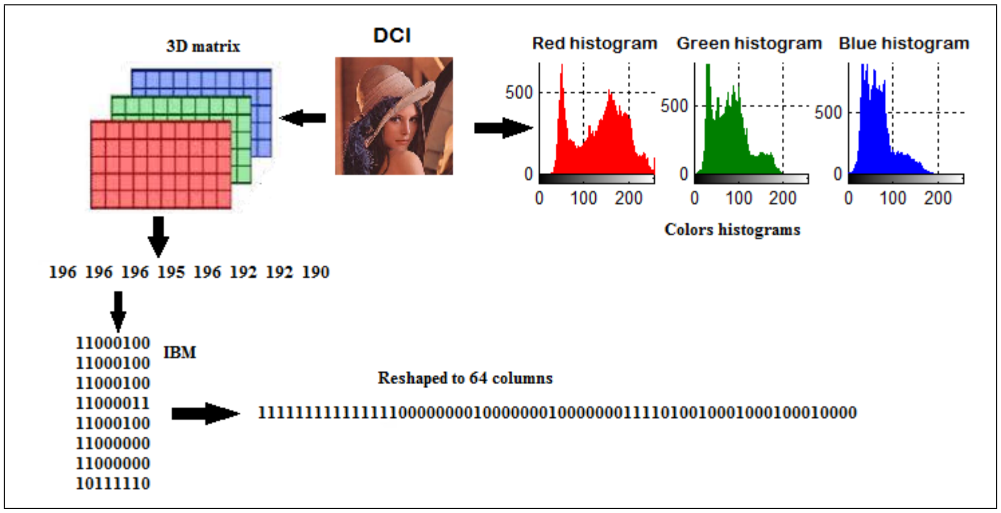


Fig. 3. DCI Presentation.

TABLE I. DES, AES, and Suggested Technique Characteristics [2]

Feature	Method		
	DES	AES	Proposed
Key length in bits	56	128 , 192 , & 256	512
Key space in combinations	1.84467E+19	3.40E+38	1.34E+154
Security	Can be broken easily as it has known vulnerabilities.	Secure	Highly secure
Sensitivity	Sensitive, the encryption & decryption functions must use the same PK	Sensitive, the encryption & decryption functions must use the same PK	Sensitive, the encryption & decryption functions must use the same PK
Number of rounds	16	depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)	4, one round for each block
Structure	Based on a Feistel network	Based on a substitution-permutation network	Based on shuffling & shuffling back
Round operations	Expansion, XOR operation with round key, Substitution & Permutation	Byte Substitution, Shift Row, Mix Column & Key Addition	Simple replacement operations
Block size	64 bits (8 bytes)	128 bits (16 bytes)	Image size in bytes divided by 4
Speed	Low	Fast	Faster
Number of secret keys	16, one key for each round	10, or 12 or 14, one key for each round	One key for each round
Quality	Excellent	Excellent	Excellent

et al. [24] presented an encryption approach merging binary matrix operations and chaotic maps.

By using logistic chaotic maps and advanced binary matrix transformations, Farah et al. [25] improved encryption, resulting in increased security and resistance against cryptanalysis. Pourjabbar et al. [26] presented a hybrid encryption technique that achieves improved security and robustness by fusing complex binary matrix operations with chaotic maps. A safe encryption technique that uses optimized binary matrix operations and logistic chaotic maps for robust encryption and attack resistance was presented by Ahmad et al. [27].

Xu et al. [28] and Luo et al. [29] both came up with image encryption methods that use logistic chaotic maps and binary matrix transformations to make the encryption work well and safely with the right parameters. The authors of the study [30] came up with a good way to encrypt pictures that is both secure and quick to compute. It uses logistic chaotic maps and optimized binary matrix transformations. Together, these studies show how secure and effective encryption for digital images can be achieved using binary matrix operations and chaotic maps.

In their seminal work, Benaissi et al. [31] proposed a novel approach that utilizes chaotic maps, specifically the logistic chaotic map and two-dimensional chaotic maps, to generate secret keys. The algorithm achieves a trade-off between security and computing speed by utilizing binary matrix operations. The algorithm leverages the essential randomness of chaotic maps for encryption.

Wang et al. [32] employed the integration of Arnold transformation with chaotic systems to achieve diffusion and confusion in picture encryption. The encryption procedure utilizes binary matrix operations to enhance the strength of cryptography. This combination enhances the encryption process by providing an additional level of protection.

In their study, Yu et al. [33] employed DNA coding and chaotic scrambling techniques to generate encryption keys, thereby augmenting the level of security. The use of binary matrix operations enhances the security of the encryption method by complementing the chaotic scrambling and DNA coding techniques.

While Erkan et al. [34] were encrypting and decrypting, they used chaotic maps to make keys and combined bit-plane complexity segmentation with binary matrix operations. The present integration leverages the intricate nature of picture bit-planes, augmenting the encryption process with an extra layer of protection in conjunction with the resilience offered by chaotic maps.

Furthermore, Cun et al. [35] introduced an image encryption technique that incorporates chaotic maps and DNA encoding. This algorithm employs chaotic maps for key generation and DNA encoding, along with binary matrix operations for encryption and decryption.

Zheng et al. [36] propose an efficient picture encryption algorithm that integrates binary matrix operations with chaos, specifically logistic map chaos. The combination of chaotic maps and binary matrix operations in encryption algorithms demonstrates the efficacy of enhancing security measures for picture encryption.

III. Proposed Method

The proposed technique employs basic tasks to apply GI and DCI cryptography and will not alter while changing the picture to be encrypted-decrypted. Description of these tasks is as follows:

A. *Image preprocessing*

The source/encrypted picture preparation task will follow these steps:

1) Read the picture.
2) Determine image size.
3) Resize picture matrix to one row.
4) Convert picture row matrix to obtain IBM.
5) Adapt IBM to 64 columns.
6) Divide the binary matrix into 4 blocks with 16 columns each.

This task may be completed via mat lab operations:

```
C1=imread('st_images/4.2.07.tiff');
[nn1 nn2 nn3]=size(c1);
LL1=nn1*nn2*nn3;
cc2=reshape(c1, 1, LL1);
L1=fix(LL1/8) * 8;
c2 = cc2(1 : 1 : L1);
c31 = dec2bin(c2, 8);
c3 = reshape(c31, L1/8, 64);
block1=c3(:,1:16);
block2=c3(:,17:32);
block3=c3(:,33:48);
block4=c3(:,49:64);
b1=block1;b2=block2;
b3=block3;b4=block4;
```

B. *Secret Indices Keys Generation*

The private key (PK) contains the values of 4 sets of chaotic logistic parameters (r1, x1, r2, x2, r3, x3 and r4, x4), these parameters are used to run four chaotic logistic map models to get four chaotic keys, each of this key will be sorted to get the indices key.

The secret indices keys task is required to generate 4 secret indices keys (IKEY1 thru IKEY4), one key will be needed to process one block, the indices keys are obtained by sorting chaotic keys, which are generated by running four chaotic logistic map models (CLMM) **[35-40]**, this task can be implemented applying the following steps:

1) Generation of secret indices keys: Chaotic logistic map models (CLMM) behave chaotically, hence obtaining four secret indices keys (IKEY1–IKEY4) for processing one block requires an organised technique. The following methods sort chaotic keys generated by CLMMs to retrieve these indices keys:
2) Initiating Chaotic Logistic Map Models (CLMMs): Set up four CLMMs first. Each model will start with unique parameters. These factors usually include the seed (or beginning point) and the chaos-inducing logistic parameter (r). These factors greatly affect logistic map chaos, thus their choice is critical.
3) Create chaotic sequences for each of the four CLMMs: The logistic map equation is used iteratively to generate values. Chaos theory and cryptography employ the logistic map equation to produce unexpected, seemingly random sequences.
4) Use the resulting chaotic sequences from each CLMM to create a chaotic key: This technique usually entails picking a portion of the chaotic sequence and converting it into a binary or integer sequence for cryptography applications.
   To generate secret indices keys (IKEY1-IKEY4), sort each chaotic key. Sorting organises chaotic main pieces in ascending or declining order. The index keys are based on the element order. These keys will determine the sequence of blocks or components during encryption or decryption.
5) Application to Encryption / Decryption: Use generated indices keys (IKEY1–IKEY4) to encrypt or decrypt data blocks. Each key rearranges or transforms one block of data in its sequence. In this stage, indices keys directly contribute to the cryptographic process, ensuring data security and integrity.Get the private key (PK), which contains four pairs of chaotic logistic parameters r and x used to perform a CLMM to produce a chaotic key.
6) Execute CLMMs.
7) Convert CK to IKEY.

This task can be implemented by executing the following Matlab operations:

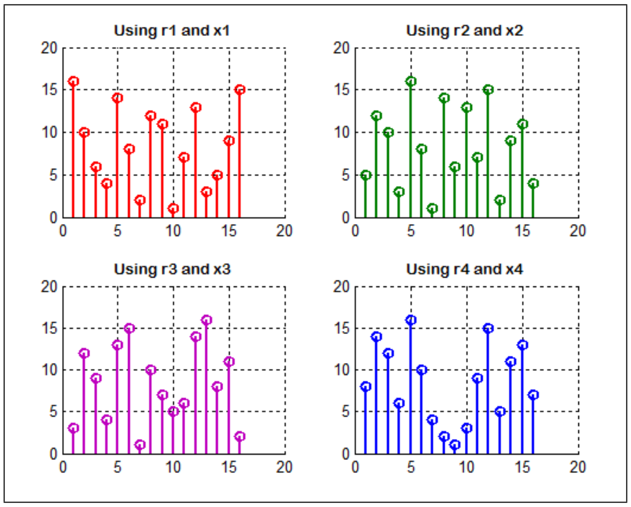


Fig. 4. IKEY Sensitivity.

```
r1 = 3.67; x1 = 0.31; r2 = 3.75; x2 = 0.22;
r3 = 3.95; x3 = 0.16; r4 = 3.61; x4 = 0.29;
for i=1:16 x1=r1*x1*(1-x1);
CK1(i)=x1;
end
[ff IKEY1]=sort(CK1);
for i = 1 : 16
x2 = r2 * x2 * (1 − x2);
CK2(i) = x2;
end
[ff IKEY2]=sort(CK2);
for i = 1 : 16
x3 = r3 * x3 * (1 − x3);
CK3(i) = x3;
end
[ff IKEY3]=sort(CK3);
for i = 1 : 16
x4 = r4 * x4 * (1 − x4);
CK4(i) = x4;
end
[ff IKEY4]=sort(CK4);
```

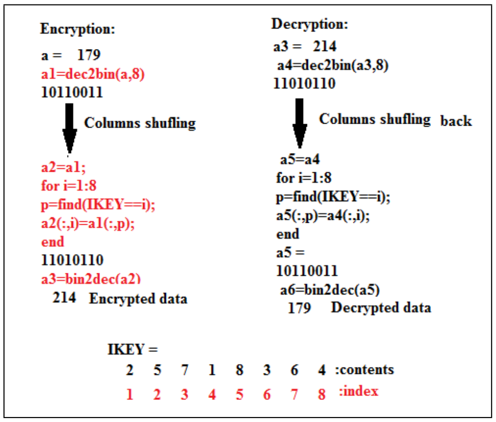
Fig. 4 demonstrates how altering the values of r and x using the following pairs of values alters the resulting IKEY:

$r1 = 3.67; x1 = 0.31;$
$r2 = 3.75; x2 = 0.22;$
$r3 = 3.95; x3 = 0.16;$
$r4 = 3.61; x4 = 0.29;$

C. Encryption / Decryption

There's a creative way to keep each piece of an image's digital jigsaw a secret using an IKEY. Like a digital patchwork, imagine an image in blocks. Before being sent online, each block is jumbled in a unique fashion, making it difficult for prying eyes to interpret without the secret key.

Every picture block has a unique IKEY. IKEY is like a secret recipe that shuffles the block's columns in a way only someone with the identical recipe can unshuffle, as seen in Fig. 5. The IKEY instructs us to jumble up the block's columns during encryption, which hides the picture. Taking a legible book and rearranging the letters renders it gibberish to anyone who doesn't know how to fix it.



```
Encryption:
a =   179
a1=dec2bin(a,8)
10110011
```

```
a2=a1;
for i=1:8
p=find(IKEY==i);
a2(:,i)=a1(:,p);
end
11010110
a3=bin2dec(a2)
  214   Encrypted data
```

```
Decryption:
a3 =   214
 a4=dec2bin(a3,8)
11010110
```

```
 a5=a4
for i=1:8
p=find(IKEY==i);
a5(:,p)=a4(:,i);
end
a5 =
10110011
 a6=bin2dec(a5)
  179    Decrypted data
```

```
IKEY =
    2    5    7    1    8    3    6    4  :contents
    1    2    3    4    5    6    7    8  :index
```

Fig. 5. Shuffling and shuffling back operations example.

The IKEY is used again when the image's rightful owner wishes to decode and reassemble it. This time, it's used to unmix the columns and place them back in order, like completing a puzzle or rearranging our book's jumbled letters into phrases.

To simplify, we'll use 8-column blocks. This approach efficiently shuffles and unshuffles image blocks (encrypts and decrypts), as seen in Fig. 5. Like a magic wand, it scrambles and unscrambles the image so only the correct person can see it.

The encryption task can be implemented by executing the following mat lab operations:

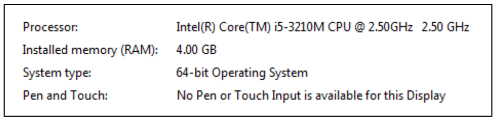
```
for i=1:16
p=find(IKEY1==i);
b1(:,i)=block1(:,p)
end
for i=1:16
p=find(IKEY2==i)
b2(:,i)=block2(:,p)
end
for i=1:16
p=find(IKEY1==i) b3(:,i)=block3(:,p)
end
for i=1:16
p=find(IKEY1==i)
b4(:,i)=block4(:,p)
end
c3=[b1 b2 b3 b4]
cc3=reshape(c3,L1,8)
c5=bin2dec(cc3)’
cc2(1,1:L1)=c5
c6=reshape(cc2,nnl,nn2,nn3)
```

The decryption task can be implemented by executing the following matlab operations:

```
for i=1:16
p=find(IKEY1==i);
 b1(:,p)=block1(:,i);
end
for i=1:16
p=find(IKEY2==i);
b2(:,p)=block2(:,i);
end
for i=1:16
p=find(IKEY1==i);
b3(:,p)=block3(:,i);
end
for i=1:16
p=find(IKEY1==i);
 b4(:,p)=block4(:,i);
end
c9=[b1 b2 b3 b4];
c99=reshape(c9,L1,8);
c10=bin2dec(c99)’;
c77(1,1:L1)=c10
cll=reshape(c77,nn1,nn2,nn3);
```

IV. Implementation and Results Discussion

The proposed method was implemented using MATLAB version 7, the program was executed using a PC with the following specification:



Processor:	Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz 2.50 GHz
Installed memory (RAM):	4.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

The proposed method was implemented using various gray and color images, the images were taken from [https://sipi.usc.edu/database], and Table II shows the basic information of these images:

TABLE II. Selected Images Basic Information

Image #	Image	Type	Size
1	4.2.03.tiff	Color	786432
2	4.2.05.tiff	Color	786432
3	4.2.07.tiff	Color	786432
4	5.1.14	Gray	065536
5	5.2.08	Gray	262144
6	5.2.09	Gray	262144
7	5.2.10	Gray	262144
8	7.1.07.tiff	Gray	262144

To evaluate the efficiency of the proposed method the quality, speed and sensitivity analyses were conducted:

A. Quality Analysis

Image cryptography research must meet theoretical criteria for robust cryptosystems and show practical usefulness in preserving original pictures. The suggested method was carefully tested to a selected collection of photos to test its ability to precisely replicate the source images after decryption.

Despite the scientific rigour and unique approach of the suggested technology, all decrypted photos showed corruption and degradation. This behaviour casts doubt on the technique’s cryptographic integrity and capacity to preserve picture quality and fidelity during the encryption-decryption cycle.

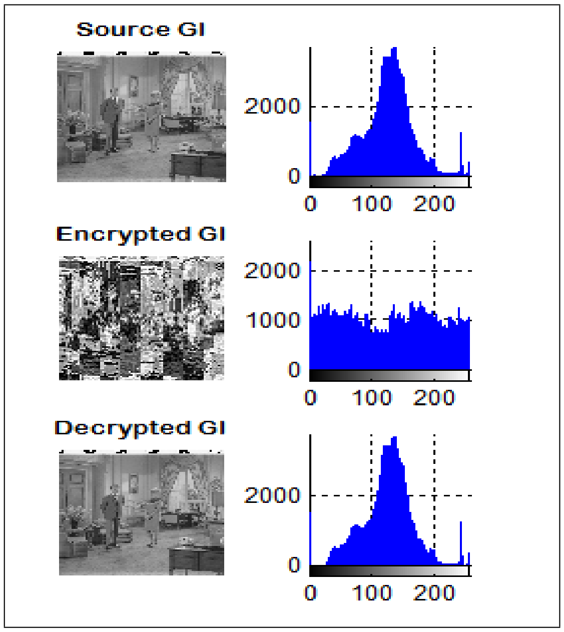


Fig. 6. GIs sample outputs.

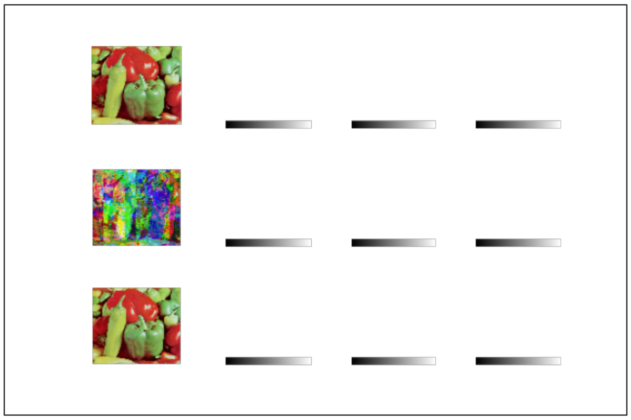


Fig. 7. DCIs sample outputs.

Fig. 6 and 7 show the differences between decrypted and original photos. This data is crucial for scholarly discourse and offers a pragmatic assessment of the proposed methodology. Visual documentation helps researchers understand technique constraints and shortcomings by allowing them to examine results.

This shows that image cryptography requires constant invention and testing. It encourages a thorough method evaluation to improve its strength and dependability. A cryptosystem that retains image resolution and prevents unauthorized entrance is theoretically and practically possible in digital cryptography. practical.

The quality of the encrypted photographs was carefully assessed to prove the picture encryption technology worked. MSE and PSNR were calculated in this assessment. These traditional picture quality measurements show how accurate encrypted images are compared to unencrypted ones.

The MSE is the arithmetic mean of the squared discrepancies between pixels in the original and encrypted pictures. Encryption drastically alters data, increasing Mean Squared Error (MSE). PSNR measures the relationship between a signal's highest amplitude (the original image) and the intervening noise (encryption) that degrades it. A lower PSNR indicates more distortion, lowering image quality after encryption.

Table III shows that all photos had higher MSE values and lower PSNR values. The pattern shows that the proposed encryption method meets excellence standards. A powerful encryption system expects high Mean Squared Error (MSE) values since the encryption process considerably alters the data. The low PSNR values show how these adjustments affect image quality, demonstrating the encryption's influence.

Quantitative evaluations of original and encrypted photos show that the recommended encryption method meets cryptographic system quality standards. The method's high Mean Squared Error (MSE) and low Peak Signal-to-Noise Ratio (PSNR) figures show its ability to change image data for security while maintaining image quality. This precise balance is crucial to digital picture encryption. Encrypting photographs while maintaining quality is the goal of this balance. proving the method's academic and practical feasibility. The source and encrypted photos' quality criteria are in Table III.

TABLE III. SOURCE AND ENCRYPTED PHOTOS' QUALITY CRITERIA

Image #	MSE	PSNR
1	8268.8	20.6228
2	5098.5	25.4582
3	9276.1	19.4734
4	6507.9	23.0175
5	6921.7	22.4010
6	6269.8	23.3903
7	7908.0	21.0690
8	7631.7	21.4246
Remarks	High	Low

B. Speed Analysis

Academic assessments of picture encryption methods extend beyond image quality to encompass processing efficiency. This comprehensive method entails the reprocessing of selected photographs using recommended encryption and decryption. The duration of the encryption and decryption phases, measured in seconds (ET/DT), and the rates, recorded in kilobytes per second, are crucial to this research.

The speed parameter data give an empirical foundation for evaluating the operational efficiency of the suggested methodology. The assessment is crucial for comprehending the tangible ramifications of employing the approach in real-life scenarios, as the speed of processing frequently dictates the usability and acceptance of encryption technology.

Table IV presents a summary of the encryption and decryption timings of this investigation, as well as the computed speeds for each processed photo. These indicators assist academics in analysing the strengths and weaknesses of the method's processing efficiency.

Analysis of encryption and decryption timings and speeds helps determine the method's practicality and efficacy. This study contributes to the theoretical knowledge of picture encryption algorithms and provides suggestions for optimizing encryption techniques to boost the speed and efficiency of handling digital photos.

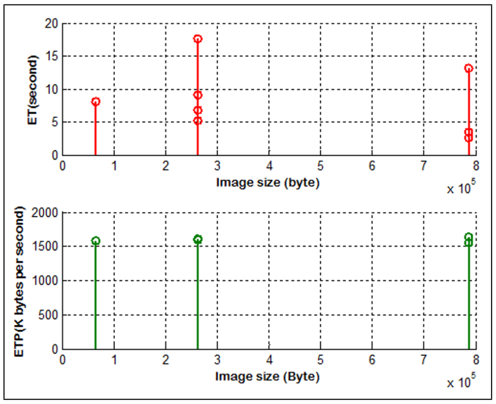


Fig. 8. ET and ETP vs image size.

TABLE IV. SPEED RESULTS

Image #	MSE	PSNR
1	8268.8	20.6228
2	5098.5	25.4582
3	9276.1	19.4734
4	6507.9	23.0175
5	6921.7	22.4010
6	6269.8	23.3903
7	7908.0	21.0690
8	7631.7	21.4246
Remarks	High	Low

From Table IV we can see the following facts:

- Average encryption time for the suggested approach is 2.1072 seconds.
- The proposed picture cryptography approach transferred 1607.6 kilobytes per second.
- Fig. 8 shows that the effective temperature/distance threshold increases with picture size.
- Image size, around 1600 K bytes per second (Fig. 8), does not effect performance.

To improve photo encryption, [37] compare the recommended encryption method to common methods. This analytical approach compared the suggested technique's operational velocity and data processing capability to chaotic and non-chaotic encryption [38]. The recommended technique improved speed and processing capacity, as shown in this comparison.

This comparative research shows that the proposed method speeds up data encryption and decryption. The investigation showed that the suggested method outperforms current methods in throughput and performance. Table V shows how fast the suggested solution is compared to traditional encryption.

This technique again increased speed by adding chaotic and non-chaotic procedures [17] into the comparison study. The extensive Table VI evaluation showed that the suggested encryption system had superior throughput and speed. The speed increase is significant, making the proposed procedure more efficient than field methods.

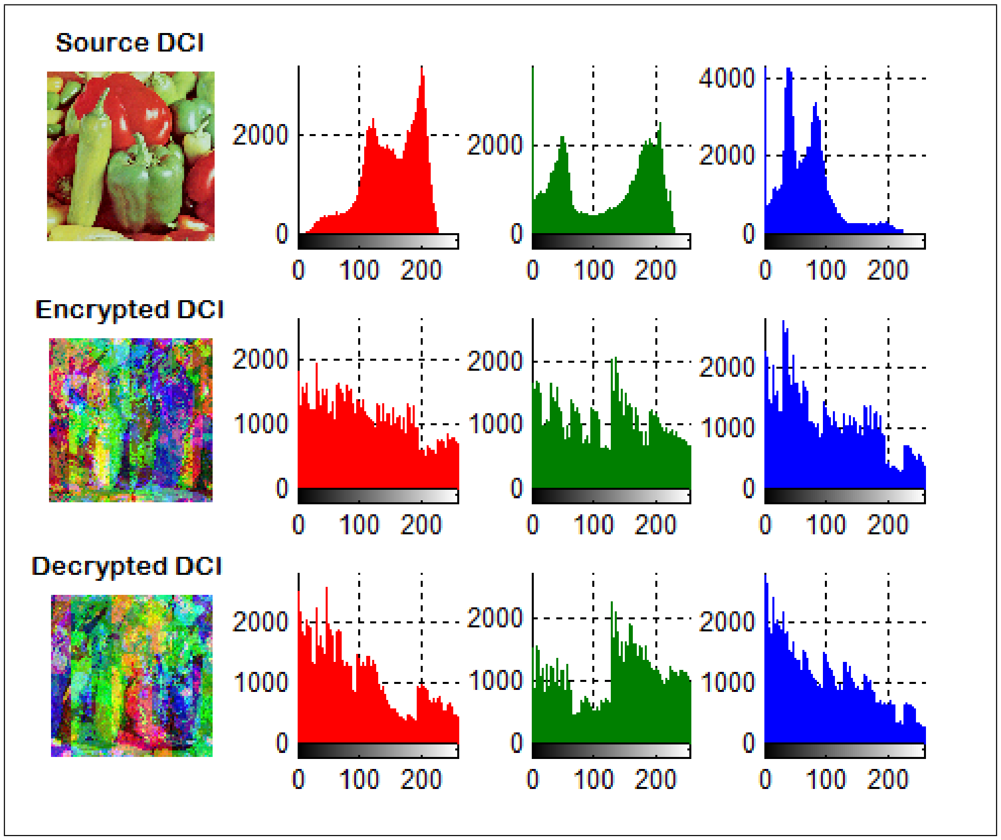


Fig. 9. Sensitivity analysis outputs.

TABLE V. Proposed Method Speed up Comparing with Standard Methods

Method	ETP *(K-bytes/second)*	Speed up of the proposed method
Proposed	1607.60	01.0000
DES	86.7881	18.5233
3DES	74.6363	21.5391
AES	90.3135	17.8002
RC2	61.8961	25.9726
RC6	155.5953	10.3319
Speed up of the proposed method equal proposed method throughput divided by other method throughput		

TABLE VI. Proposed Method Speed up Comparing with Introduced by Different Authors Methods [17]

Method	Ref.	Average throughput *(K-bytes/second)*	Speed up of the proposed method
Proposed		1607.600	1.00000
Non-chaotic	[17]	170.3906	9.43480
Chaotic	[17]	141.2305	11.3828
Hyper chaotic	[17]	636.3379	2.52630
Introduced in	[39]	888.8867	1.80860
Introduced in	[38]	911.0352	1.76460
Introduced in	[37]	638.4082	2.51810
Introduced in	[40]	360.4102	4.46050
Introduced in	[2]	384.9609	4.17600

These findings show that the proposed method could change cryptography's speed and efficiency, contributing to picture encryption research. The proposed method increases throughput and performance, showing that sophisticated cryptographic algorithms can speed up processing and improve encryption technologies for digital communication and data protection.

Tables V and VI show that the suggested technique accelerated picture cryptography. The suggested approach has lower encrypting and decryption times than conventional and other chaotic and hyper chaotic methods, increasing image cryptography throughput.

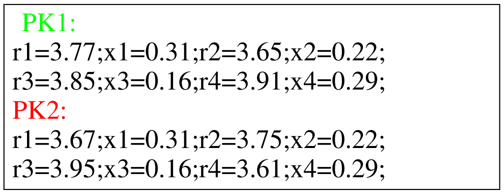
C. Sensitivity Analysis

Key consistency is crucial in academic research on cryptographic protocols, especially public key (PK) cryptography. To protect data, this method uses the same public key for encryption and decryption. Any change to the public key used during decryption indicates an illegal intrusion, resulting in data corruption and distortion.

An experiment tested the encryption mechanism's sensitivity to public key changes. This experiment encrypted a photo using PK1. Deciphering the encrypted image required modest modifications to the PK2 approach. This purposeful decryption key alteration simulates unauthorized entrance or manipulation.

Fig. 9 shows experiment results as histograms of the original and decrypted photos. The histograms' pixel value distribution shows image brightness and contrast. The histogram difference between the original and decoded photos shows the limitations of a revised public key. The distorted decrypted image shows how vulnerable the suggested technique is to encryption key changes and emphasises the need of key consistency throughout the encryption-decryption process.

This experiment emphasises the need of thorough key management in cryptographic system security research. It also highlights the consequences of major changes, showing how a data breach might lower image quality. Academic research helps the cryptography community build stronger encryption methods that can withstand unauthorized attacks and protect data.



PK1:
r1=3.77;x1=0.31;r2=3.65;x2=0.22;
r3=3.85;x3=0.16;r4=3.91;x4=0.29;
PK2:
r1=3.67;x1=0.31;r2=3.75;x2=0.22;
r3=3.95;x3=0.16;r4=3.61;x4=0.29;

V. Conclusion

A new image encryption method boosts digital security. This novel method uses a 512-bit public key for security. This method protects encrypted data from hackers with its large key space.

This method works because it responds to public key values. This sensitivity is needed for encryption, which safely obfuscates images, and decryption, which carefully restores them. It was shown that the technique recreates decrypted photographs precisely due to its high-quality standards.

While the suggested encryption method dramatically improves picture cryptography by reducing encryption time, the Efficiency boosts the method's supremacy over chaotic cryptography and classical encryption. This method is more efficient by using streamlined procedures to generate a secret key, split the image into blocks, strategically rearrange columns, then reverse these changes during decryption.

This method also offers versatility. It can process different-sized photos without changing encryption or decryption protocols. Encryption is efficient and effective regardless of data quality due to its versatility.

The approach was carefully tested on a variety of photos to determine its efficacy, efficiency, and responsiveness. After careful analysis, these tests showed that the technique meets and exceeds cryptographic system reliability standards. The suggested encryption approach offers a safe, efficient, and customisable solution for securing digital photos by combining powerful security features, increased speed, and operational simplicity.

References

[1] Md Rashedul Islam, TR Tanni, S Parvin, MJ Sultana, and Ayasha Siddiqa. A modified lsb image steganography method using filtering algorithm and stream of password. *Information Security Journal: A Global Perspective*, 30(6):359–370, 2021.

[2] Nan-Run Zhou, Long-Long Hu, Zhi-Wen Huang, Meng-Meng Wang, and Guang-Sheng Luo. Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm. *Expert Systems with Applications*, 238:122052, 2024.

[3] Chao Yuan, Hongxia Wang, Peisong He, Jie Luo, and Bin Li. Gan-based image steganography for enhancing security via adversarial attack and pixel-wise deep fusion. *Multimedia Tools and Applications*, 81(5):6681–6701, 2022.

[4] Chenxin Li, Brandon Y Feng, Zhiwen Fan, Panwang Pan, and Zhangyang Wang. Steganerf: Embedding invisible information within neural radiance fields. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pages 441–453, 2023.

[5] Mohammed Alweshah, Yasmeen Aldabbas, Bilal Abu-Salih, Saleh Oqeil, Hazem S Hasan, Saleh Alkhalaileh, and Sofian Kassaymeh. Hybrid black widow optimization with iterated greedy algorithm for gene selection problems. *Heliyon*, 9(9), 2023.

[6] Ahmad Zulfakar Abd Aziz, Muhammad Fitri Mohd Sultan, and Nurul Liyana Mohamad Zulkufli. Image steganography:: Comparative analysis of their techniques, complexity and enhancements. *International Journal on Perceptive and Cognitive Computing*, 10(1):59–70, 2024.

[7] Janaki Raman Palaniappan. Highly secure cryptography algorithm method to safeguard audios and visuals. *International Journal on Cryptography and Information Security (IJCIS)*, 12(3), 2022.

[8] AR Roddy and JD Stosz. Fingerprint feature processing techniques and poroscopy. In *Intelligent Biometric Techniques in Fingerprint and Face Recognition*, pages 35–105. Routledge, 2022.

[9] Zeyu Dong, Xin Wang, Xian Zhang, Mengjie Hu, and Thach Ngoc Dinh. Global exponential synchronization of discrete-time high-order switched neural networks and its application to multi-channel audio encryption. *Nonlinear Analysis: Hybrid Systems*, 47:101291, 2023.

[10] Keshav Sinha, Annu Priya, and Partha Paul. K-rsa: Secure data storage technique for multimedia in cloud data server. *Journal of Intelligent & Fuzzy Systems*, 39(3):3297–3314, 2020.

[11] Naihao Liu, Youbo Lei, Yang Yang, Zhiguo Wang, Rongchang Liu, Jinghuai Gao, and Tao Wei. Sparse time-frequency analysis of seismic data via convolutional neural network. *Interpretation*, 12(1):T47–T62, 2024.

[12] Kriti Taneja, Vinay Arora, and Karun Verma. Classifying the heart sound signals using textural-based features for an efficient decision support system. *Expert Systems*, page e13246, 2023.

[13] Yosra Annabi. Mathematical and electronic perception of electromagnetism. *International Journal of Innovation in Science and Mathematics*, 11(2), 2023.

[14] Snehashish Bhattacharjee, Mousumi Gupta, and Biswajoy Chatterjee. Time efficient image encryption-decryption for visible and covid-19 x-ray images using modified chaos-based logistic map. *Applied Biochemistry and Biotechnology*, 195(4):2395–2413, 2023.

[15] S Divya, Swati Panda, Sugato Hajra, Rathinaraja Jeyaraj, Anand Paul, Sang Hyun Park, Hoe Joon Kim, and Tae Hwan Oh. Smart data processing for energy harvesting systems using artificial intelligence. *Nano Energy*, 106:108084, 2023.

[16] Mohamad Al-Laham, Sofian Kassaymeh, Mohammed Azmi Al-Betar, Sharif Naser Makhadmeh, Dheeb Albashish, and Mohammed Alweshah. An efficient convergence-boosted salp swarm optimizer-based artificial neural network for the development of software fault prediction models. *Computers and Electrical Engineering*, 111:108923, 2023.

[17] Youcef Bentoutou, El-Habib Bensikaddour, Nasreddine Taleb, and Nacer Bounoua. An improved image encryption algorithm for satellite applications. *Advances in Space Research*, 66(1):176–192, 2020.

[18] Mohammed Alweshah, Muder Almiani, Saleh Alkhalaileh, Sofian Kassaymeh, Essa Abdullah Hezzam, and Waleed Alomoush. Parallel metaheuristic algorithms for solving imbalanced data classification problems. *IEEE Access*, 2023.

[19] Sofian Kassaymeh, Salwani Abdullah, Mohammed Azmi Al-Betar, Mohammed Alweshah, Amer Abu Salem, Sharif Naser Makhadmeh, and Mohammad Atwah Al-Ma'aitah. An enhanced salp swarm optimizer boosted by local search algorithm for modelling prediction problems in software engineering. *Artificial Intelligence Review*, 56(Suppl 3):3877–3925, 2023.

[20] Mohammed Alweshah, Sofian Kassaymeh, Saleh Alkhalaileh, Mohammad Almseidin, and Ibrahim Altarawni. An efficient hybrid mine blast algorithm for tackling software fault prediction problem. *Neural Processing Letters*, pages 1–26, 2023.

[21] Shuqin Zhu, Congxu Zhu, and Wenhong Wang. A novel image compression-encryption scheme based on chaos and compression sensing. *IEEE Access*, 6:67095–67107, 2018.

[22] Jian Zhang and Da Huo. Image encryption algorithm based on quantum chaotic map and dna coding. *Multimedia Tools and Applications*, 78:15605–15621, 2019.

[23] Noura Khalil, Amany Sarhan, and Mahmoud AM Alshewimy. An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. *Optics & Laser Technology*, 143:107326, 2021.

[24] Lingfeng Liu and Suoxia Miao. A new image encryption algorithm based on logistic chaotic map with varying parameter. *SpringerPlus*, 5:1–12, 2016.

[25] MA Ben Farah, A Farah, and T Farah. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dynamics*, 99(4):3041–3064, 2020.

[26] Ahmad Pourjabbar Kari, Ahmad Habibizad Navin, Amir Massoud Bidgoli, and Mirkamal Mirnia. A new image encryption scheme based on hybrid chaotic maps. *Multimedia Tools and applications*, 80:2753–2772, 2021.

[27] Jawad Ahmad and Seong Oun Hwang. A secure image encryption scheme based on chaotic maps and affine transformation. *Multimedia Tools and Applications*, 75:13951–13976, 2016.

[28] Lu Xu, Zhi Li, Jian Li, and Wei Hua. A novel bit-level image encryption algorithm based on chaotic maps. *Optics and Lasers in Engineering*, 78:17–25, 2016.

[29] Yuqin Luo, Jin Yu, Wenrui Lai, and Lingfeng Liu. A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia tools and applications*, 78:22023–22043, 2019.

[30] Qing Lu, Congxu Zhu, and Xiaoheng Deng. An efficient image encryption scheme based on the lss chaotic map and single s-box. *Ieee Access*, 8:25664–25678, 2020.

[31] Sellami Benaissi, Noureddine Chikouche, and Rafik Hamza. A novel image encryption algorithm based on hybrid chaotic maps using a key image. *Optik*, 272:170316, 2023.

[32] Xingyuan Wang, Shengnan Chen, and Yingqian Zhang. A chaotic image encryption algorithm based on random dynamic mixing. *Optics & Laser Technology*, 138:106837, 2021.

[33] Jinwei Yu, Wei Xie, Zhenyu Zhong, and Huan Wang. Image encryption algorithm based on hyperchaotic system and a new dna sequence operation. *Chaos, Solitons & Fractals*, 162:112456, 2022.

[34] Uğur Erkan, Abdurrahim Toktas, Serdar Enginoğlu, Enver Akbacak, and Dang NH Thanh. An image encryption scheme based on chaotic logarithmic map and key generation using deep cnn. *Multimedia Tools and Applications*, 81(5):7365–7391, 2022.

[35] Qiqi Cun, Xiaojun Tong, Zhu Wang, and Miao Zhang. Selective image encryption method based on dynamic dna coding and new chaotic map. *Optik*, 243:167286, 2021.

[36] Jiming Zheng, Zheng Luo, and Qingxia Zeng. An efficient image encryption algorithm based on multi chaotic system and random dan coding. *Multimedia Tools and Applications*, 79(39):29901–29921, 2020.

[37] Abdurrahim Toktas, Uğur Erkan, Suo Gao, and Chanil Pak. A robust bit-level image encryption based on bessel map. *Applied Mathematics and Computation*, 462:128340, 2024.

[38] Dong Wen, Wenlong Jiao, Xiaoling Li, Xianglong Wan, Yanhong Zhou, Xianling Dong, Xifa Lan, and Wei Han. The eeg signals encryption algorithm with k-sine-transform-based coupling chaotic system. *Information Sciences*, 622:962–984, 2023.

[39] Zhenlong Man, Jinqing Li, Xiaoqiang Di, Yaohui Sheng, and Zefei Liu. Double image encryption algorithm based on neural network and chaos. *Chaos, solitons & fractals*, 152:111318, 2021.

[40] Xiaoqiang Zhang and Xuesong Wang. Multiple-image encryption algorithm based on dna encoding and chaotic system. *Multimedia Tools and Applications*, 78:7841–7869, 2019.