

A Novel Rotation-Based Image Cryptography using Adaptive Block Sizes and Dynamic Matrix Keys

Sudeep S R, Deepa N P, Subramanya, Umashankar, Dhanwin H
Department of Electronics and Communication Engineering
Dayananda Sagar College of Engineering
Bengaluru, India

Abstract—With the widespread use of social media platforms, it is imperative to provide security for the information being transmitted. Normally confidential data are protected by Standard encryption and decryption methods. As these techniques often include extensive arithmetic and logical operations, performance reduction is inevitable. Additionally, their reliance on private keys of fixed lengths and fixed data-block sizes introduces vulnerabilities and security is potentially compromised. In this paper, a novel cryptography method for digital image is proposed, where a color image is used as image key to create a matrix private key (MPK) which is highly resistant to hacking. This method utilizes a preliminary state to configure essential parameters and secret information for generating the MPK. The variable data-block size and the selected rounds defines the complexity of the MPK, enhancing adaptability and security. The evaluation of the effectiveness of the proposed method is based on parameters such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Correlation Coefficient (CC), and throughput. The comparative analysis of the proposed method is done with other established methods of cryptography, such as Data Encryption Standard (DES), Blow Fish (BF), Triple-DES (3DES), Advanced Encryption Standard (AES). The method also maintains robustness while expediting the encryption–decryption process, making it an ideal for practical applications.

Keywords— Image_key, Matrix Private key(MPK),MSE, PSNR

I. INTRODUCTION

Digital color images, are one of the most important kinds of data being used by individuals and organizations. These color images play a crucial role in various applications including security and medical sectors where image protection is very important owing to the fact that the image is of private or personal nature. Thus, providing security will prevent unauthorized use of the digital image by intruders, data breachers, hackers. A digital color image which is in the form of a three-dimensional matrix as in Fig 1 contains a substantial amount of information, every one of the three primary colors: red, green and blue is denoted by a separate two-dimensional matrix.



Fig.1. Image Color Matrixes

The key technique normally used to secure digital photos is cryptography, which utilizes a private key and arithmetic and logical operations are performed on the data through this private key to get an encrypted data. At the destination decryption is performed using the same key to get back the data.

In this paper, symmetric cryptography is used, where image key is used to create a matrix private key (MPK) as shown in Fig 2 and data is encrypted by performing arithmetic and logical operations using this key and then the data is decrypted.

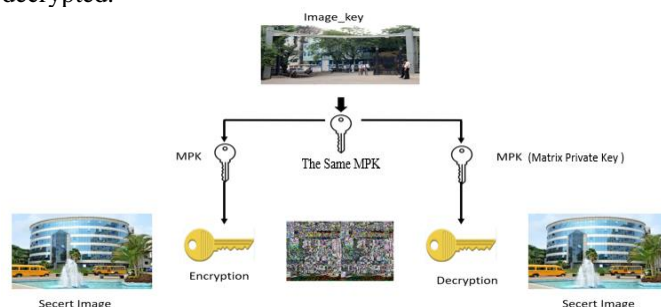


Fig.2 Cryptography process

According to the studies the encryption–decryption process must be. Easy and Simple to implement, optimizes for the best quality parameters during encryption and decryption, maximizes throughput (processed bytes per second) to minimize encryption–decryption time, and offers strong security against hacking of messages. The method chosen in this paper will achieve the following

- Modification of the digital image in such a way that it becomes blurred. the strength of encryption can be evaluated based on computed quality parameter, for

effective encryption the mean square error (MSE) value should be very large, while the peak signal-to-noise ratio (PSNR), should be very low.

- Very high encryption efficiency to minimize the encryption time along with decryption time, thereby improving the throughput by processing more bits per second.
- Flexibility and scalability, the ability of users to change the private key length, data block size or the number of encryption/decompression iterations.
- Simple and easy to apply due to the use of logical and arithmetic operations.
- Versatility of use, to support a range of information types, such as text messages, text files, and digital images

The paper aims to enhance the classical techniques performance by reducing the complex operations, reducing the time taken to produce private keys, and enhancing the security level of the encryption process.

II. LITERATURE WORK

Encryption algorithms transform data into ciphertext, ensuring its confidentiality. These algorithms utilize encryption keys to alter the information in a specific, reversible manner, allowing it to be decrypted back into original text using the corresponding decryption key. Related works highlights a variety of encryption algorithms [1][2][3], each tailored to meet distinct requirements. Additionally, as older algorithms become vulnerable, new encryption techniques are developed to maintain data security.

To enhance efficiency without compromising data protection, it has been proposed to reduce the number of rounds in encryption algorithms [4], while still maintaining robust security. For instance, an innovative method to improve QR code security by integrating cryptography and visual cryptography techniques has been explored [5][6][7]. This multi-layered approach significantly strengthens the resilience of QR codes against various types of attacks, providing enhanced data protection.

Many techniques are being used to encrypt-decrypt private data, and standard methods are used as a basis [8][9][10], Data encryption standard (DES), advance encryption standard (AES), triples DES (3DES), and blowfish method (BF) are some of these. These methods have been extensively studied and implemented due to their reliability and adaptability in various applications.

III. RELATED WORK

In this research paper, the proposed method consists mainly of performing two operations MPK generation and Image encryption. The images used in this work is shown in Fig 3



Fig. 3. Set of source images

A. MPK Generation

color image serves as an image_key to produce a matrix private key (MPK) [11]. The parameters required are set as initial values, and secret image is chosen which is required to create the private key. The variable block size of the data, and the strength of the MPK is solely dependent on how many rounds is chosen

The generation of the Matrix Private Key (MPK) involves using specific information to construct a 2D matrix, where the rows represent rotation count and columns represent the block size. The parameters required includes

- selecting the color channel (1 for red, 2 for green, 3 for blue)
- determining the type of operation (1 for extraction, 2 for resizing the image)
- choosing the number of rounds (nr)
- specifying the block size (bs).

Additionally, the row and column from which the MPK to be extracted are defined, with the matrix size being equal to bs * nr. Finally, the MPK is saved for further use. For the Image_key the MPKs generated for different parameters are shown in Fig 4

Initialization includes generating a 2D MPK based on the image_key, operation_type, color_channel, num_rounds, and block_size.

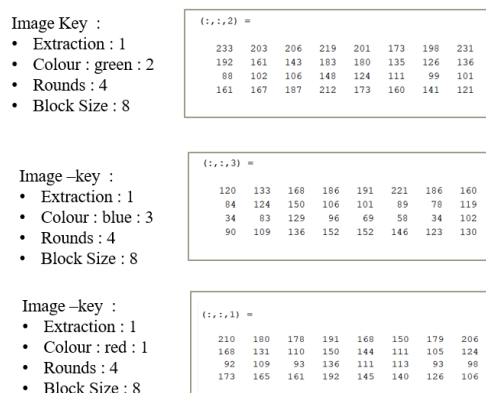


Fig. 4. MPKs for different parameters

size and values of the MPK are altered by changing the block length, substituting the image_key by a different image will modify the values of the MPK elements, as illustrated in the Fig 5 and Fig 6

B. Image Encryption

It is performed using the MPKs through a shifting operation. shifting value for the image blocks is decided by the element in the MPK, while the number of positions to be shifted is decided by the input image's pixel value. The image is then encrypted based on these shifting values, resulting in the encrypted image.



Rounds=4, Block Size=6

(:, :, 1) =					
118	144	181	197	201	157
89	135	108	89	72	104
43	105	86	52	32	84
100	132	158	162	146	139

Rounds=6, Block Size=7

(:, :, 3) =						
116	128	180	189	220	202	155
117	159	168	162	170	165	158
74	125	121	74	65	43	97
38	101	125	74	64	42	101
40	92	129	99	96	50	93
111	125	153	169	171	157	144

Fig. 5. Image key with corresponding MPK



Rounds=5, Block Size=8

(:, :, 1) =							
206	186	185	193	171	158	188	208
207	145	126	169	151	112	121	157
94	103	91	120	129	110	88	93
121	131	108	161	108	120	103	104
176	165	168	193	152	142	128	107

Rounds=2, Block Size=8

(:, :, 1) =							
183	154	143	169	154	131	143	167
138	138	128	165	130	126	108	100

Fig. 6. Image key with corresponding MPK

The operation process for one image_key and one secret image is denoted in Fig 7. The proposed algorithm for encryption phase is as follows

Input: Secret Image, Image_key

Output: encrypted Image

1. Extract the image_key to generate MPK
2. Divide the secret image into N blocks
3. Resize the image so that MPK is the same size as message block

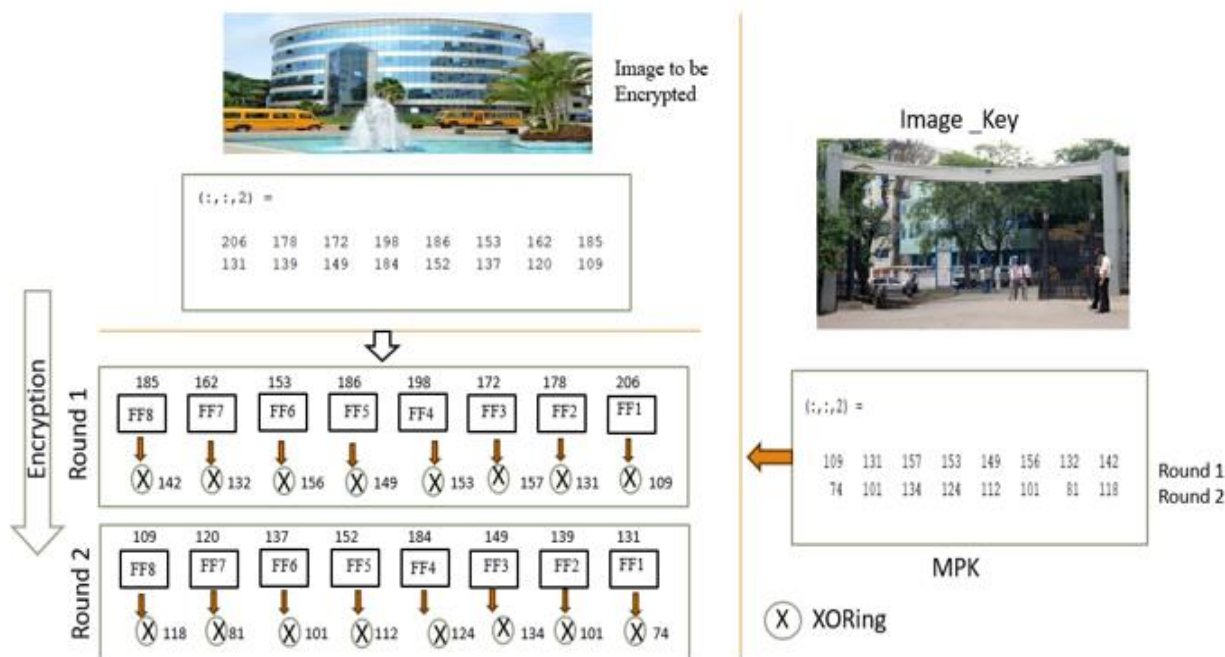


Fig.7. Operation Process

For all message block and MPKS, XOR and shifting operation is performed. each element's value will be used as a rotation parameter of the block. additionally, it will determine the number of left rotations required for the corresponding message block. Multiple messages and keys are utilized in the approach proposed. The encrypted images for different parameters are shown in Fig 8. Consider the block of image to be encrypted be

```
(:,:2) =
206 178 172 198 186 153 162 185
131 139 149 184 152 137 120 109
```

MPK generated from the image_key is
 (:,:2) =

```
109 131 157 153 149 156 132 142
74 101 134 124 112 101 81 118
```

Each pixel of the image undergoes multiple rounds of XOR operations with the MPK. The result is an encrypted image.

```
209 72 128 245 154 192 108 128
147 71 225 78 70 195 181 245
```

It is observed that as the rotation count and block size increase, the quality of the encrypted image improves. The block size can vary between 1 to 60. In our tests, due to the MATLAB specification there is a limitation on the block size of an image. The encryption time for the images that are large is satisfactory ensuring the methods efficiency. Therefore, selecting an image with any size is feasible while preserving a increased value of throughput. The recovered image after decryption is depicted in Fig 9 It is similar to encryption, here the encrypted pixel value Is Xored with the MPK. The MPKs, which are essential for decryption, are securely transmitted to the receiver along with the encrypted image. To ensure security, a randomly generated secret PIN is used as an additional layer of protection. During the Encryption Process:

- The image is encrypted using the encryption algorithm, which utilizes a combination of keys, include the MPKs
- A random PIN is generated for securing the Decryption process
- The MPKs are transmitted securely, but they are protected by this randomly generated secret PIN

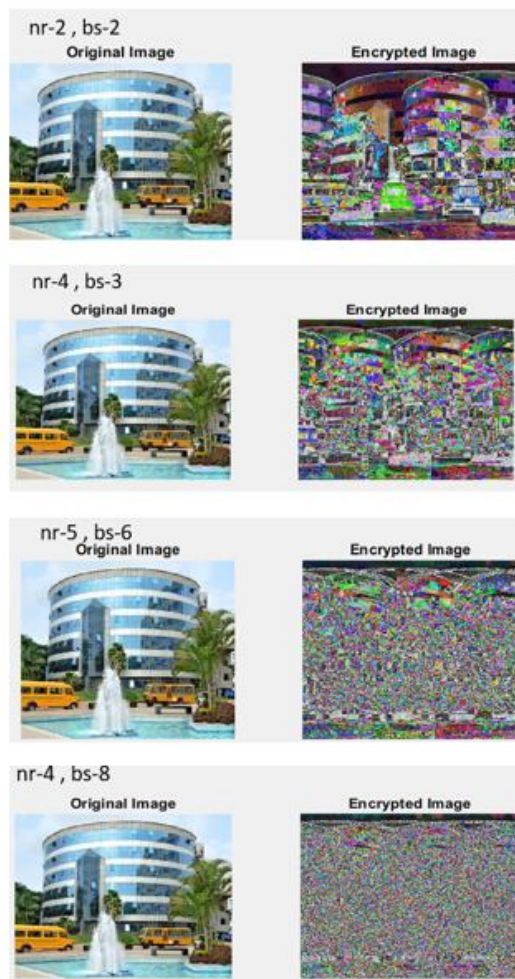


Fig. 8. Encrypted images for different block sizes

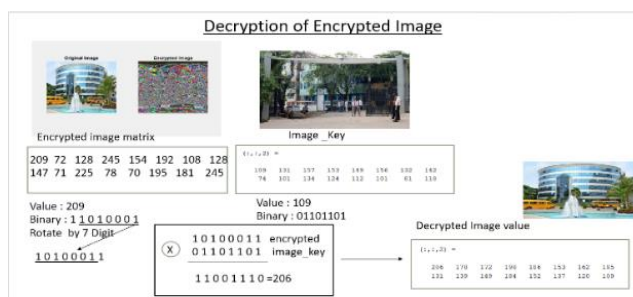


Fig. 9. Decryption process

While transmitting to the receiver:

- The encrypted image is sent to the receiver.
- In addition to the encrypted image, the secret PIN is also shared via a secure channel (e.g., SMS, email etc.,) as shown in Fig 10

During decryption

- The receiver receives the encrypted image and the secret PIN.
- The receiver enters the PIN into the decryption application

Key Retrieval and Decryption:

- Upon entering the correct PIN, the decryption application uses it to unlock the MPKs.
- The unlocked MPKs are then applied to decrypt the image, restoring it to its original form as in Fig 11

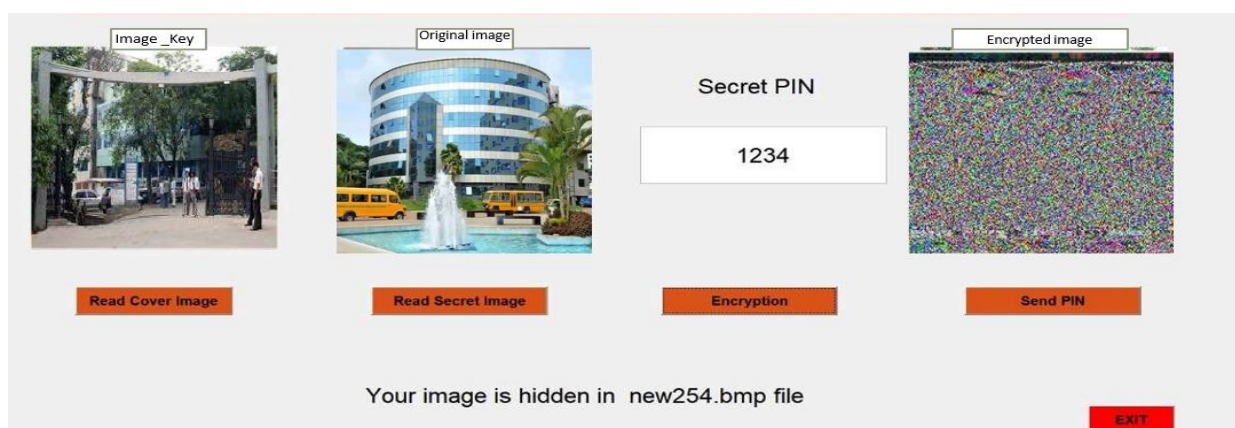


Fig. 10. Transmission with secret pin

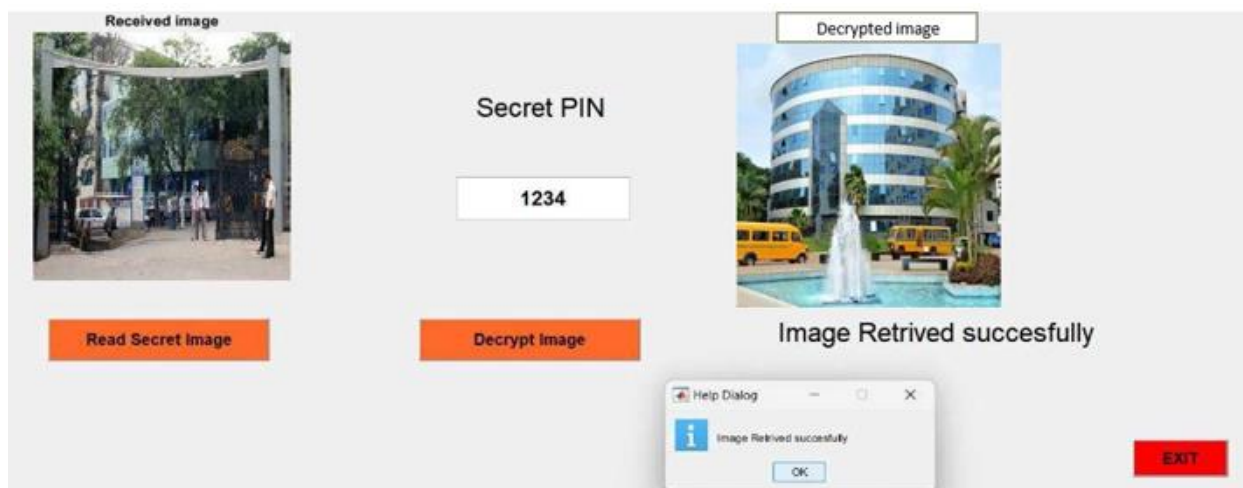


Fig. 11. Reception with secret pin

IV. EXPERIMENTAL RESULTS

The method proposed is realized using MATLAB on a Core i5 2.5 GHz processor with 8 GB of RAM. The increase in security level is based on two parameters. (1) secrecy about the image_key (2) the generated MPK relies on block size, number of rounds and color channel chosen. for the block size of 60 the number of combinations to break the key is $(2^8)^{60} = 2^{480}$ this gives a good security. The implementation of the method was done by using sequence of images wherby experimental results were compared with conventional techniques as in Table1 to demonstrate an improvement in efficiency, which was achieved by decreasing the encoding time and decoding time without retaining the quality parameter values such as MSE and PSNR. A novel approach for color image cryptography was developed, tested, and successfully executed. Achieved results confirmed that proposed method fulfills the image quality requirement by achieving good and acceptable values of MSE and PSNR during the encryption and decryption process. The proposed method imposes no constraints on the chosen image key, letting it to be of any type, size, or format as in Fig 12. While increasing the image size may result in longer encryption times, the method remains efficient even for large images.

The message is divided into blocks, with block sizes varying from 1 to 60 bytes. Each block size has been tested in our experiments, and all the results were found to be satisfactory. Figure 13 depicts graphs showing different parameters values compared with different image keys

The proposed method achieves excellent quality parameters values, i.e., MSE, PSNR, and CC. Additionally, it ensures high and acceptable throughput improving overall performance. The obtained results of PSNR, MSE and CC listed in the Table 1 Table 2 shows the computational analysis encrypted and decrypted images. The Average estimated time is 0.0060 seconds, while the average throughput is 5833.3 byte per second.

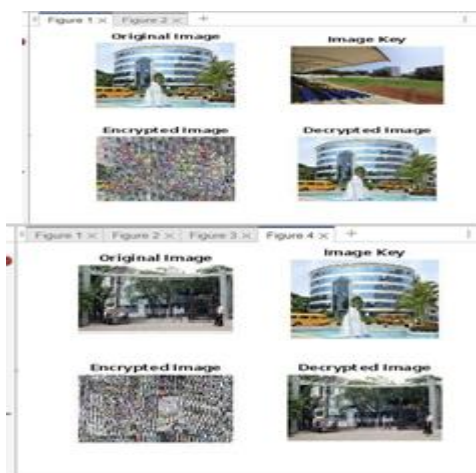


Fig.12. Encryption for different secret image with different keys

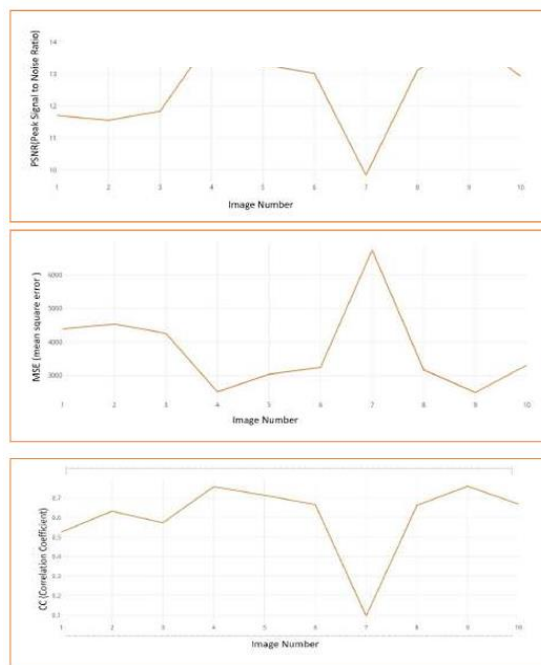


Fig. 13. graphical analysis

Table 1. Evaluation parameters




Image Number	MSE (mean square error)	PSNR(Peak Signal to Noise	CC (Correlation Coefficient)	Encryption Throughput	Decryption Throughput
2	4537.7369	11.5624	0.6328	1682622.9175	1738104.0298
3	4262.147	11.8345	0.57308	1689851.4283	1732520.4091
4	2511.3103	14.1318	0.75829	1675626.6145	1730388.9255
5	3036.9333	13.3065	0.71416	1706783.7572	1714377.2698
6	3244.123	13.0198	0.66638	1735164.3309	1769915.8064
7	6744.8325	9.8411	0.096618	1705258.1351	175900.1602
8	3169.9346	13.1203	0.66259	1734729.2557	1752373.705
9	2492.4228	14.1646	0.76091	1688674.1414	1738021.5227
10	3311.5166	12.9305	0.66861	1754753.6765	1765791.14599

Table 2. Computational analysis

Method Parameter	DES	3DES	AES	Blowfish	Rotation
PK length (bit)	56 (fixed)	112, 168 (fixed)	128, 192, 256 (fixed)	32-448 (fixed)	Not Fixed
Block size(bit)	64 (fixed)	64 (fixed)	128 (fixed)	64 (fixed)	701 (Variable)
Ability to deal with images	Difficult	Difficult	Difficult	Difficult	Easy
Encryption quality	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR
Efficiency	Slow	Slow	Slow	Moderate	Moderate
Structure	Feistel	Feistel	Substitution-Permutation	Feistel	Cireshift , Feistel
Security level	Adequate	Adequate	Excellent	Excellent	Excellent
Flexibility to modification	No	Yes	Yes	Yes	Yes
Simplicity	No	No	No	No	yes

The comparative analysis with standard methods is tabulated in table 3

Table 3. Comparative Analysis

Image_Key						
Secret image	Encryption Time(s)	Decryption Time(s)		Encryption Time(s)	Decryption Time(s)	
1 	0.80069	0.67347	6 	0.45323	0.44433	
2 	0.66574	0.64726	7 	2.9865	2.9508	
3 	0.6686	0.64934	8 	0.43957	0.43515	
4 	0.30078	0.29126	9 	0.089424	0.086885	
5 	0.39496	0.3932	10 	0.41031	0.40725	

V CONCLUSION

This paper introduces an innovative method for cryptography of secret Images. The proposed approach establishes a high level of security, providing robust protection and making it extremely challenging to hack the encrypted messages. The technique utilizes a secret image_key to create MPK required for extracting the secret pin. A key feature of this method is its flexible key, which dynamically adapts based on the data block size and the chosen image key.

The image key should remain confidential, known only to the sender and receiver. Additionally, it may be traded at any given time with other image without requiring modifications to the encryption method.

The proposed method places no restrictions on the choice of the image key, meaning any image can be chosen, regardless of type or size, thereby enhancing its versatility and practical applicability. The experiment results of the proposed method have shown that quality parameters have excellent values (MSE, PSNR, and CC, which meets the

requirements of robust cryptography. The experimental results demonstrate that the method proposed shows notable rise in speed as well as efficiency.

REFERENCES

- [1] A Gandhimathinathan K, Tejashree A, Tamilmani, "Standard Image Encryption Strategies:A Comprehensive Overview,2024 8th International Conference on Electronics, Communication and Aerospace technology (ICECA), 0.1109/ICECA 63461. 2024. 10800947,Coimbatore, India
- [2] Donagani Ramakrishna;Mohammed Ali Shaik, "A Comprehensive analysis of Cryptographic Algorithms: Evaluating Security, Efficiency, and Future Challenges", IEEE Access, 16 December 2024
- [3] Pradhumn Porwal, Adarsh Kumar Panda, Himanshu Sarad, Hritambh Hritvij, Dr. Sapna P J, "Security System Based On Image Encryption Using Fractal Matrix Method", International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), Vol :04/Issue:07/July-2022 Impact Factor- 6.752 e-ISSN:2582-5208
- [4] Mua'ad M.Abu-Faraj ,Ziad A. Alqadi," Rounds Reduction and Blocks Controlling to enhance the performance of standard method of data cryptography", IJCSNS International Journal of Computer science and Network Security, VOL.21 No.12, December 2021
- [5] Sapna P J, S.S. Rajanandan Rao, Abhishek A.B, Prajwal B P, Karan Deshmukh, " Visual Cryptography using Quadri Directional Search Algorithm with Remote Accessibility" International Journal of Engineering Research and Technology (IJERT), ISSN: 2278-0181, Vol 9 Issue 7, July 2020
- [6] Shreyanka Chougule, Sapna P J, "Randomized Visual Cryptography to Enhance security" 3rd IEEE International Conference on recent trends in Electronics, Information and Communication Technology, RTEICT-18th 19th May,2018
- [7] Cheshtaa Bhardwaj, Hitendra Garg, Shashi Shekhar, "A QR code-based user-friendly visual cryptography scheme" , 22 international conference on computational intelligence and sustainable engineering solutions CISES, 20-21 May 2022
- [8] Patel, K."Performance analysis of AES, DES and Blowfish Cryptographic algorithms on small and large data files.International Journal of information technology11, 81--819 (2019).
- [9] Gergana Spasova, Milena Karnova, "A New Secure Image Encryption Model Based on Symmetric Key", 2021 International Conference on Biomedical Innovations and applications (BIA), 02-04 June 2022
- [10] Meghana N, Sapna P J, "Multimedia Encryption For Enhancing data Security Using AES and Logistic Mapping",International Journal of Creative Research Thoughts (IJCRT), Volume 10, Issue 2, February 2022 |ISSN: 2320-2882
- [11] C.-C. Chang, J.-H. Horng, C.-S. Shih and C.-C. Chang, "A maze matrix-based secret image sharing scheme with cheater detection", Sensors, vol. 20, no. 13, pp. 3802, Jul. 2020.