Discrete Chaotic of Encryption and Decryption of Digital Images Security Using Color Signal

Name Kuldeep

Computer Lecturer, Department of Computer Science, Indira Gandhi Govt. Post Graduate College Tohana,

E-mail: kuldeep.mtech85@gmail.com

ABSTRACT

There is a wealth of data contained within a single picture. In humans, visual processing occupies over a third of the cortex. Images have a crucial role in conveying data. Images are used in many contexts, including medical records storage, aerial photography by satellite, astronomical observations of planetary motion via telescopes, personal identification via fingerprints or irises, etc. Millions of bits of information, primarily in the form of digital pictures, are produced every day as a byproduct of digital communication. Using cryptography to protect private data is a smart security measure. Cryptography is a system for encoding and decoding information for secure data transmission and storage. Encryption and decryption have an indefinite future because of technological progress. Schematic encryption can withstand many crypt analyst attacks, as shown in the security analysis. Information must be reliable and secure for it to be respected by the recipient.

Keywords:-Encryption, Decryption, Image, PSNR, MSEINTRODUCTION

DOI Number: 10.14704/nq.2022.20.9.NQ440062 **Neuro Quantology 2022; 20(9):661-669**

The purpose of image encryption is to ensure that no unauthorized party can view the image during transmission over a network. Internet communication, transmission, and medical imaging are just some of the numerous domains that can benefit from image encryption, video encryption, and chaos based encryption. Communication in the field of medical and the military, etc. There will be no limits to what can be achieved when encryption develops in the future. Unique characteristics of image data include high redundancy, low pixel-to-pixel variability, and great bulk capability. To safeguard sensitive data, encryption methods are important. The term "encryption" will refer to the process of transforming a plaintext message into an unreadable form known as cipher text [1]. The process of decryption is the reversal of encryption, or the transformation of encrypted text back into its original, plain form. [1].

Encryption [2] has evolved as a vital component in protecting data on public networks such as the internet, private networks such as intranets, and even extranets. To encrypt data, we employ mathematical procedures and keys to transform it into cipher text before sending it across a network, and to decrypt it, we use the same tools to convert cipher text back into original data. The primary focus of security management is user authentication, as well as the integrity, correctness, and security of data resources.

As networking technology advances and the internet's user base expands, the volume of information communicated in all aspects of human life grows exponentially. Financial transactions, online interactions, school instruction, medical care, military training, and other such activities are examples. The material submitted could be in any format, such as text, images, or videos. Information exchange on open, public networks facilitates the exploitation of sensitive data [1,2]. As a result, securing the transmission of private data through networks has arisen as a hot issue of research. To address this critical issue, cryptographic algorithms might be applied. You can hold confidential discussions even in hostile environments with the help of cryptography. Traditional cryptographic algorithms such as IDEA, DES, RSA, EL Gamal, and others fall under two major categories: key cryptosystems and double key cryptosystems. These cryptosystems' basis are

found in tough mathematics problems. These earlier cryptosystems are only intended for encrypting textual data. Images distinguish themselves from text by having huge, redundant data capacity, for example. Traditional encryption techniques are unable to deal with these anomalies. When developing an effective image cryptosystem, using typical encryption methods to disperse and jumble image data offers a considerable problem.

LITERATURE REVIEW

Zhang, Q., & Ding, Q. (2015) Digital image communication has grown in importance as network and communication technology have advanced. As a result, the advancement of digital image encryption technology has received a lot of focus. In this research, we offer a method for encrypting digital images using the Advanced Encryption Standard (AES) algorithm and demonstrate how to do so in MATLAB. We next integrate the two methods by means of digital picture processing and obtaining data suitable for the AES encryption algorithm. Encryption of the digital image follows, with the algorithm implemented using MATLAB simulation. The results demonstrated that the approach may more effectively realize the effect of encryption and decryption through a comparison of the histogram analysis and the analysis of the key.[1]

Elgendy, F., Sarhan, A. M. et al,(2016) This work presents a new, safe chaos-based model for the encrypted and decrypted transfer of digital images. The proposed method involves several phases of increasing confusion and spreading the information around. This "confusion" phase is repeated n times with a new "key" each time. In order to further disperse the output of the confusion stage, the diffusion stage is repeated m times with a new key each time. The proposed image cryptosystem is more secure since the key space is expanded through nested iterations in the confusion and diffusion phases using a different key for each round. In order to determine the most secure 2D chaotic confusion map to utilize with the proposed image cryptosystem, a comprehensive security analysis is performed on the entire family of maps in question. Based on the findings, the Standard map has the highest security level among the 2D chaotic confusion maps analyzed. This is because the Standard map is more complex and has a larger key space.[2]

Pakshwar, R., Trivedi, V. K et al,(2013) Many distinct methods of image encryption and decryption are discussed in this study. Additionally emphasizes the need of image encryption methods, With more and more people turning to digital methods for sending and storing photos, safeguarding their privacy, reliability, and provenance is becoming an increasingly pressing concern. Images can be made more secure through the use of encryption, and new methods of doing so are always being developed. This paper includes a literature review of over 25 studies that explore various methods of encrypting images by randomly shuffling their pixels and reducing their association with one another. This study provides a comprehensive overview of the various image encryption methods currently in use. Further, the practicality of image encryption and decryption methods is analyzed.[3].

Shankar, K., Lakshmanaprabu, S. K. et al,(2020) The shared communication Model has a critical and onerous task to secure the safety of digital photographs. Data is encrypted and decoded in a highly secure office using a combination of private and public keys. In this paper, we present the unique Multiple key-based Homomorphic Encryption (MHE) algorithm for image protection. The most secure key for encryption and decryption procedures can be chosen using the AdaptiveWhale Optimization (AWO) technique. As the fitness function, we optimized for PSNR using both the original and encrypted images. Our solution outperforms existing encryption methods by splitting the original image down into chunks and then reorganizing them in a secure manner. When compared to various encryption algorithms, the findings reveal that the proposed model has superior quality, with the best PSNR and the lowest MSE.[4].

Chowdhary, C. L., Patel, P. V. et al,(2020) Many imaging technologies use symmetric and asymmetric cryptography algorithms to encrypt digital information. The majority of the research efforts contributed in the literature are focused on the Advanced Encryption Standard (AES) algorithm. The hybrid technique combines the convenience and simplicity of symmetric algorithms with the increased security of

asymmetric algorithms. The symmetric key algorithms of HC, AES, and DPC are more secure than the asymmetric key cryptography given by the ECC and ElGamal cryptosystems. ECC and AES are appropriate for remote or private chats with smaller image files because to the time required for encryption and decoding. Using test cases and measurements, we discover that ECC and HC give a robust overall solution for image encryption.[5]

Qaid, G. R., &Talbar, S. N. (2012) The goal of this study is to improve the privacy and security provided by picture encryption based on digital color signals. An encryption and decryption technique has been designed and deployed to provide privacy and security during the transmission and storage of image-based data. A novel encryption algorithm has been developed in order to deliver images without quality loss. An image-encryption algorithm was devised and successfully tested on a limited sample of images in this study. Increased speed and security are critical in today's pervasive digital environment, which is powered by increasingly powerful computers. Real-time picture security is problematic due to the compute demand and processing time necessary to encrypt and decrypt an image. Cutting-edge picture compression and encryption technologies are required to address these difficulties.[6]

Pan, H., Lei, Y., & Jian, C. (2018) Image data currently accounts for the majority of data carried via networks as a result of technological improvements. Picture encryption solutions have evolved in tandem with the advent of image stealing methods. We need a more robust image encryption solution as ways of stealing sensitive data get more complex. When a photograph is encrypted using chaotic technology, the ciphertext exhibits an unpredictability that significantly reduces the possibility of decipherment when compared to other techniques. As a result, modern digital image encryption mainly relies on the study of algorithms based on chaotic technology. The dual logistic chaotic map is used in this work to investigate the state of the art in digital photo encryption research.[7]

Pourasad, Y., Ranjbarzadeh, R et al,(2021) Since the early 2000s, various information security specialists have focused their attention on image encryption. Several studies, however, have been conducted utilizing diverse methodologies, and novel and helpful algorithms have been provided to improve secure image encryption solutions. Modern chaotic approaches can be found in a variety of contexts, including the construction of cryptographic protocols and the encryption of visual content. Digital image encryptions based on chaotic algorithms are a novel approach to digital image security. This method encrypts images using random chaotic sequences and is both extremely safe and extremely fast. One disadvantage of this procedure is its poor degree of precision. To that end, this paper investigates the link between the chaos sequence and the wavelet transform value. As a result, a novel approach for digital image encryption was given, which is superior to the existing algorithms.[8]

Zhang, D., & Zhang, F. (2014) In this paper, we compare and analyze the corresponding relations between the effects of encryption and decryption and the security of two different encrypting schemes of the JPEG image chaotic encryption based on the encrypting principles of digital images, integrating the characteristic of JPEG image, and using discrete chaotic sequence. Both the encrypting and decrypting of images are quick when working with an 8 by 8 bit block, and they are compatible with the JPEG file format. The JPEG picture encryption is an efficient and practical method of protecting JPEG files during storage and transmission, satisfying a common security requirement in many contexts.[9]

Kumar, M., Aggarwal, A. et al,(2014) Visuals are becoming increasingly significant in our regular talks as we live in a multi-media age. Maintaining the privacy of photos when a user transfers them through an insecure communication network is a difficult task. Encryption can be used to keep images private. This study, in addition to offering a basic explanation of cryptography, describes the critical security properties of several common photo encryption algorithms. This study includes a complete discussion of many image encryption algorithms, a detailed comparison of several discrete image encoding schemes, and, finally, a conclusion and recommendations for further research.[10]

Ismail, I. A., Amin, M et al,(2010) High security, speed, reasonable computational overheads, and

computational power are only a few of the benefits suggested by the chaos based cryptographic methods over the more conventional encryption algorithms. Using two chaotic logistic maps and a sufficiently big external secret key, the authors of this study provide a stream cipher that is both efficient and robust, making it ideal for use in the encryption of images. The two chaotic maps are used in conjunction with the external secret key to muddle the connection between the cipher picture and the plain image. The beginning conditions for the chaotic maps are derived from the secret key. [11]

Deng, Z., &Zhong, S. (2019) Here, we presented an algorithm for encrypting digital images using a technique inspired by the chaotic mapping developed by Xiong et al. The authors theoretically analyzed the algorithm, highlighting how it did not require any prior knowledge of the orbital distribution and how any chaotic model could be used. Consequently, the approach considerably increased the size of the cryptographic space and drastically decreased the number of mapping rounds.[12]

METHODOLOGY

Picture encryption technologies may become an integral part of the image distribution process in the future to boost efficiency while maintaining the highest level of security. The rapid development of the web in the modern digital world has enhanced the need of digital photo protection. First, our proposed method divides the ROI of the original pictures into a random number of blocks, which are subsequently shuffled inside the image. An picture contains information that can be interpreted because of the relationship between its constituent pieces in a specific configuration. Figure 1 depicts the Multiple Key Holomorphic Encryption (MHE) procedure for image security. A unique approach to safeguarding one's privacy and the integrity of one's image.

We can compute the encrypted data without decrypting it and get the same answer as the "ascertained one" from the first image. The AWO method is mostly used to optimize the keys used in the encryption and decryption procedures, employing both private and public keys for MHE. The system's speed and efficacy are increased by improving the sender-receiver encryption's private and open keys. The yield image is then designated as the primary image for evaluating the success of the decryption approach using the PSNR Entropy. The purpose of this method is to increase the safety of encoded images by reducing the links between image elements and boosting the image's entropy value.

SYMMETRIC KEY CRYPTOSYSTEM

Using the same symmetric key for both encryption and decryption is a hallmark of symmetric key cryptography. Before any communication takes place, two sides exchange this symmetric key across an encrypted channel [10]. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are two examples of symmetric encryption algorithms that have seen widespread use and are well-known and respected (AES).

Advanced encryption standard algorithm

The National Institute of Standards and Technology (NIST) [11] suggests using the block symmetric key cryptosystem Advanced Encryption Standard. The AES method can handle plaintext blocks of 128 bits in size, and it can work with keys of 128 bits, 192 bits, or 256 bits in size, all while producing ciphertext of 128 bits. Key sizes for 10 rounds mode are 128 bits, 12 rounds mode is 192 bits, and 14 rounds mode is 256 bits; the rounds themselves are almost identical in all three modes. A key expansion module receives the input key and uses it to produce the subkeys for each iteration of the algorithm. Each round operation consists of four smaller operations: byte swapping, row shifting, row mixing, and round key adding.

Asymmetric Key Cryptosystem

In an asymmetric key cryptosystem, both the public and private keys are employed. The idea is that learning one key does not betray the location of the others. For encrypting data, public-key cryptosystems are typically employed, while private-key cryptosystems are used when decrypting the data. The RSA algorithm is the most popular method of asymmetric encryption. [12].

RSA Algorithm

Based on prime numbers, the RSA Algorithm was invented by three scientists: Rivest, Shamir, and Adleman. This public key cryptosystem relies on the fact that each user must independently produce their own set of keys (public and private). Two huge, distinct prime numbers [13]

are used in a key generation process. Once the keys are created, encryption and decryption are computationally trivial processes. The RSA algorithm's security is based on how hard it is to factor really big integers computationally.

Attacks on Cryptographic Algorithms

Attackers frequently try to decipher messages by deciphering their encryption keys or by deciphering the ciphertext. To retrieve the plaintext from the ciphertext that is sent over the Internet, for instance, an attacker may use many techniques. On the other hand, the attacker could try to figure out the encryption key in order to decode anything that was encrypted with that key. This article details the most frequent methods of attack against cryptographic systems.

RESULTS AND DISCUSSION

Experimental results

The suggested image security model was run on an i5 processor with 4GB RAM in MATLAB2016a. The effectiveness of the suggested image security solution was measured using a variety of test images. Lena, a home, a pepper, and a baboon are the four standard images used in the simulation model. All these pictures came from the USC-SIPI Image Database. Experimental results for the Lena, pepper, monkey, and house images are shown in Table 1 for the original image, encrypted image, and decrypted image.

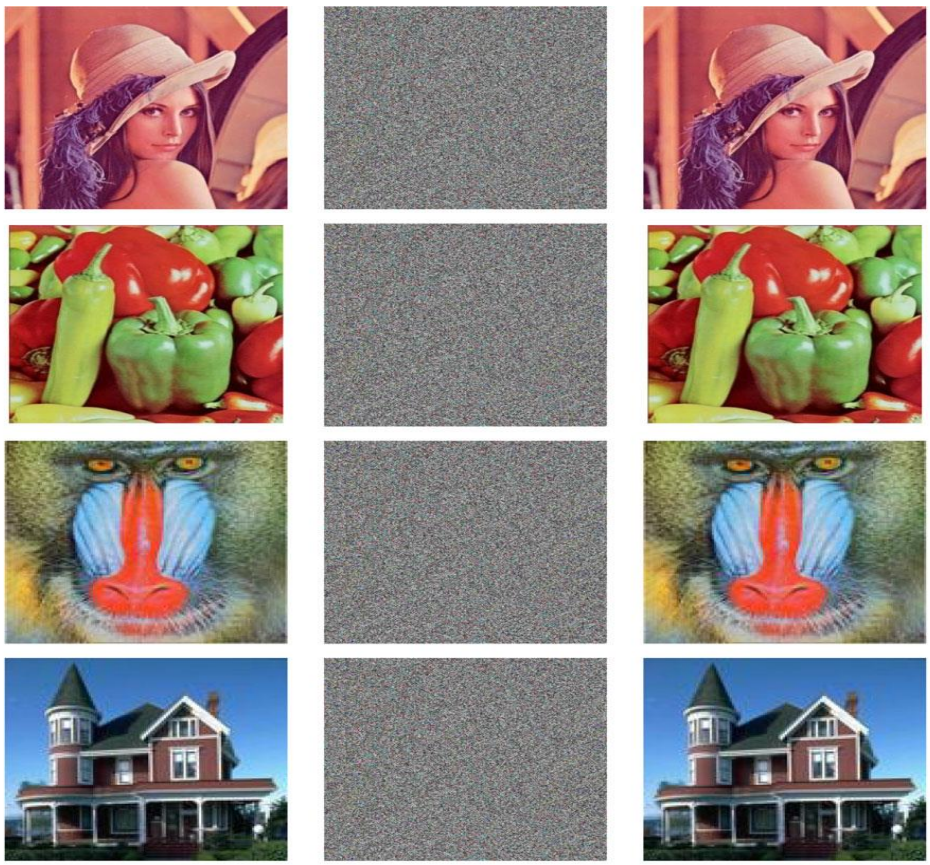
Performance analysis

Several measures, including PSNR, MSE, CC, and entropy, were used to evaluate the proposed technique and compare it to standard encryption and optimization practices.

Peak Signal to Noise Ratio : PSNR = $10 \log(\frac{255^2}{MSE})$ dB

Mean Square Error : MSE = $\frac{1}{N}\sum P_{act(i,j)} - P_{encry(i,j)}{}^2$

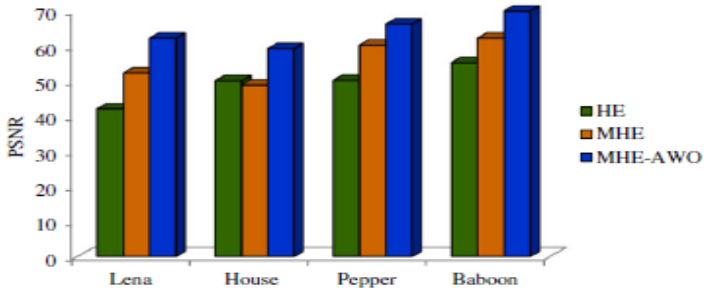
TABLE 1 Results for the proposed model



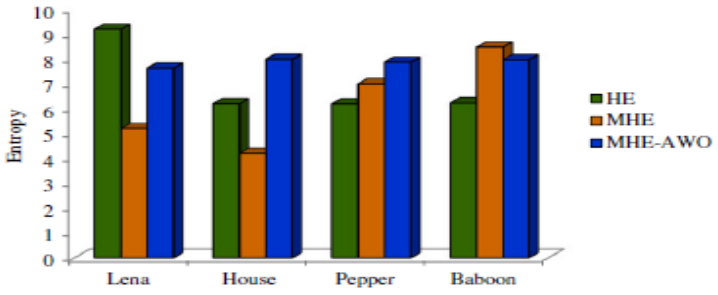
Proposed (MHE-AWO) image security results are shown in Table 2. The Entropy, PSNR, CC, MSE, entropy, and key sensitivity of each entity are broken down for four individual standards images. Also, the primary images were initially displayed in the first line, in the supplementary segment plots, the upgraded image obtained by the MWO method. By that time, the presentations had been analyzed in search of more secure visuals. The maximum sensitivity level was calculated to be 82.33% after the results of sensitivity analyses using keys of varying sizes were compared. The PSNR, CC, MSE, and entropy for Lena pictures, for example, are 64.93, 0.9983, 0.020, and 7.6554, respectively; other images were also used to generate the above table.

TABLE 2 Image security analysis for the proposed model

Image	PSNR	CC	MSE	Entropy	Key-Sensitivity
Lena	64.93	0.9983	0.020	7.6554	83.22
Pepper	65.75	0.9988	0.017	7.5256	84.08
Baboon	67.194	0.9998	0.031	7.7719	79.5
House	58.14	0.9965	0.099	7.7751	76.22



(A)



(B)

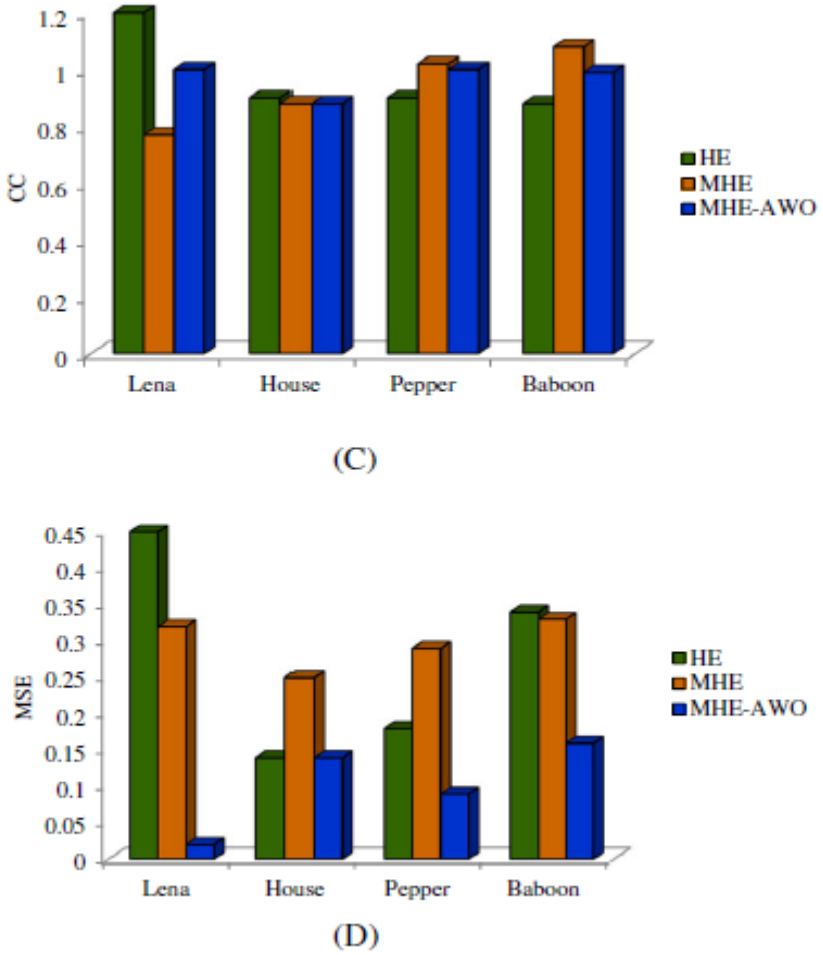


FIGURE 1 Comparative analysis for Image Security

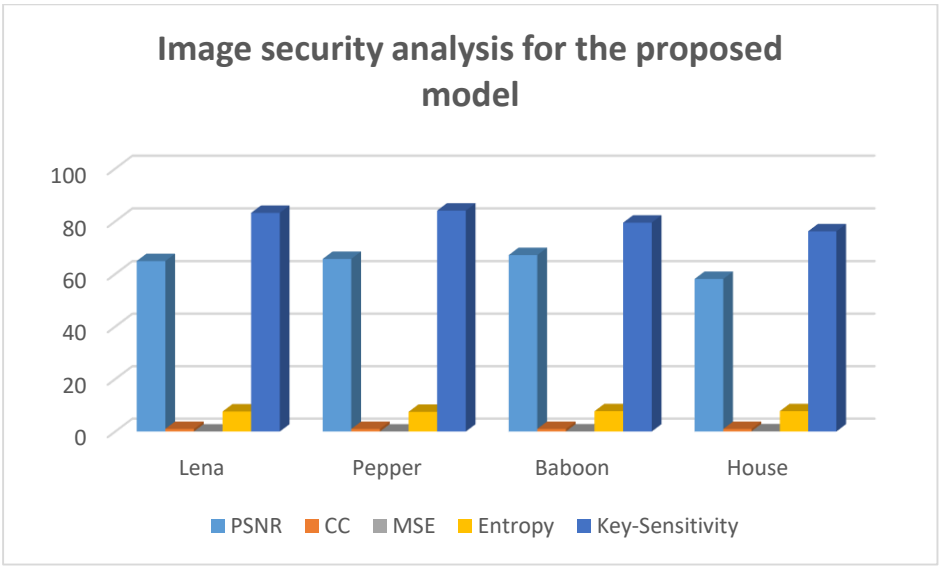


FIGURE 2 Fitness for optimization

Figure 2 depicts a comparison of various approaches to image protection, includingHE, MHE, and MHE-AWO. Figure 2 depicts the PSNR of various pictures, with the greatest value being 67.194 dB for MHE-AWO. In the secret image-based approach, the encrypted and decrypted versions of a photograph are used to reconstruct the original. Figures show the entropy, MSE, and CC values in further detail. The MSE number can be used to calculate the degree of difference between the encrypted and original images; ideally, it should be as small as possible. This operation would benefit greatly from the addition of the ability to encrypt multimedia files, as well as any other data that must be provided securely.

Fitness evaluations of several different kinds of optimization strategies, including the GA, WO, and AWO, are shown in Figure 2. The highest level of physical fitness in AWO is attained after several repetitions of pepper imagery. In this case, PSNR on four photos is compared to the GA estimate of 45.28. The suggested model and the existing method are compared to one another based on the amount of time it takes to execute each with a variety of photos. Finally, the minimum time necessary to complete the encryption and decryption processes of this security procedure is depicted in Figure 6's comparison with execution time. Numerous estimation studies have attempted the aforementioned strategies for image encoding and decoding.

In Table 3, we can see the recommended model compared to the assault that was used; in this case, we may think of the attack as modifying the value of each individual pixel in the image.

47 The proposed strategy picture had a higher PSNR estimation when the attacks were linked to the various images. Contrasting the proposed technique with an estimate of the PSNR of the attack connections in a number of photos, we find that 85.65% of the original image was recovered. Whenever the CC.

TABLE 3 Attack applied results

Original Images	Attacked	PSNR	CC	MSE	Entropy
		48.22	0.9912	0.078	6.7851
		52.75	0.9898	0.087	7.1387
		56.89	0.9900	0.061	6.9719
		45.57	0.98725	0.147	6.5946

CONCLUSION

Using optimal key-based MHE, the research provided a model for analyzing digital image security operations involving encrypted images. Using a block-based transformation method prior to employing an encryption technique yielded positive results, demonstrating the image's security. Methods for analyzing runtime and investigating security are used to assess the effectiveness of the suggested approach. The results of applying the recommended technique show that it requires the fewest number of operations to encrypt and decrypt data. In the best case, the suggested method analyzes the fitness function as PSNR for all baseline photos. There is some investigation into how the proposed system will work in practice with respect to listening based on the duration of the exchange of information. The suggested security approach has a number of limitations, the most notable being that the selection model for public and secret keys requires a great deal of computational effort. Therefore, moving forward, we intend to primarily devote our time and energy to the study and exploration of increased security with a focus on new inspired algorithms to enhance the MHE's implementation.

REFERENCES

1. Zhang, Q., & Ding, Q. (2015, September). Digital image encryption based on advanced encryption standard (AES). In *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)* (pp. 1218-1221). IEEE.
2. Elgendy, F., Sarhan, A. M., Eltobely, T. E., El-Zoghdy, S. F., El-Sayed, H. S., &Faragallah, O. S. (2016). Chaos-based model for encryption and decryption of digital images. *Multimedia tools and applications*, *75*(18), 11529-11553.
3. Pakshwar, R., Trivedi, V. K., &Richhariya, V. (2013). A survey on different image encryption and decryption techniques. *International journal of computer science and information technologies*, *4*(1), 113-116.
4. Shankar, K., Lakshmanaprabu, S. K., Gupta, D., Khanna, A., & de Albuquerque, V. H. C. (2020). Adaptive optimal multi key based encryption for digital image security. *Concurrency and Computation: Practice and Experience*, *32*(4), e5122.
5. Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., &Ijaz, M. F. (2020). Analytical study of hybrid techniques for image encryption and decryption. *Sensors*, *20*(18), 5162.
6. Qaid, G. R., &Talbar, S. N. (2012). Encryption and Decryption of Digital Image Using Color Signal. *IJCSI International Journal of Computer Science Issues*, *9*(2-2), 588-592.
7. Pan, H., Lei, Y., & Jian, C. (2018). Research on digital image encryption algorithm based on double logistic chaotic map. *EURASIP Journal on Image and Video Processing*, *2018*(1), 1-10.
8. Pourasad, Y., Ranjbarzadeh, R., &Mardani, A. (2021). A new algorithm for digital image encryption based on chaos theory. *Entropy*, *23*(3), 341.
9. Zhang, D., & Zhang, F. (2014). Chaotic encryption and decryption of JPEG image. *Optik*, *125*(2), 717-720.
10. Kumar, M., Aggarwal, A., &Garg, A. (2014). A review on various digital image encryption techniques and security criteria. *International Journal of Computer Applications*, *96*(13).
11. Ismail, I. A., Amin, M., &Diab, H. (2010). A digital image encryption algorithm based a composition of two chaotic logistic maps. *Int. J. Netw. Secur.*, *11*(1), 1-10.
12. Deng, Z., &Zhong, S. (2019). A digital image encryption algorithm based on chaotic mapping. *Journal of Algorithms & Computational Technology*, *13*, 1748302619853470.

eISSN 1303-5150