An efficient framework for securing medical images using chaotic hash scrambling and logistic diffusion

Dr. N. Anithadevi
Assistant Professor, Dept of Information Technology Coimbatore Institute of Technology Coimbatore, India anithadevi@cit.edu.in

V. Roopa
Student, Dept of Information Technology, Coimbatore Institute of Technology Coimbatore, India, roopavelusamy@gmail.com

M. Najila
Student, Dept of Information Technology, Coimbatore Institute of Technology Coimbatore, India, najilabanu2002@gmail.com

J. Swethaa Shri
Student, Dept of Information Technology, Coimbatore Institute of Technology Coimbatore, India, swethaashri36@gmail.com

S. Priyanka
Student, Dept of Information Technology, Coimbatore Institute of Technology Coimbatore, India, priyankaselvaraj2409@gmail.com

Abstract

Recently, there has been a rapid growth in the utilization of medical images in telemedicine applications. Image encryption is an interesting research topic, especially in medical images. This is due to the importance of security when storing and transmitting digital images. Our main goal is to propose a framework which produces an image encryption and decryption procedure that combines several methods such as chaotic-hash scrambling to perform the confusion process, Henon Map and diffusion with logistic maps to obtain strong encryption against various attacks. The proposed encryption procedure is proven to have resistance to statistical and differential attacks which have been measured by several measuring tools such as histogram analysis, chi- square, entropy, correlation coefficient andavalanche effect. In addition, our proposed framework also generates an unique key for encryption and decryption process using Philox Pseudo Random Generator. Our proposed system can be efficiently applicable in telemedicine applications for securing medical images.

Keywords: *Chaotic-Hash Scrambling, Henon Map, Logistic Map Diffusion, Histogram Analysis, Correlation-coefficient, Avalanche Effect.*

I. INTRODUCTION

A. Cryptography

Recently, the internet has elevated to the status of a fundamental human need. Internet usage is becoming more andmore popular, especially during the COVID-19 pandemic. Internet usage and technological innovation are becoming increasingly important to communication, and safe data transfer is being replaced by online data storage. One approach of data security is cryptography. Making data unintelligible to outsiders is the science of data encoding, also known as cryptography. Image encryption is a hot topic right now since it can be challenging to manipulate some intrinsic properties to achieve effective encryption. A few of the image's innate qualities are great volume, huge redundancy, and high correlation between adjacent pixels. It uses some text-friendly encryption methods like AES and DES, which work well with text but are less successful when applied to images.

B. Medical Image Security

The use of image data to diagnose a variety of diseases has become widespread due to the rapid advancements in medical device technology. Since medical images are transmitted over various networks, safeguarding them has become a significant issue in recent years. Confidentiality, integrity, and authenticity are required for the safe transmission of medical images. Unauthorized use of these images may result in the loss of patient data privacy. However, if these images are subject to even the slightest modification, it could lead to a misinterpretation that risks thelives of the patients.

In general, image steganography, image watermarking, and image encryption can be used to secure digital images. The simplest and most effective way to secure medical image security is by encryption, which converts a plain image into an unreadable one using a secret key. No one can restore the plain image without the secret key. Confusion and diffusion are the two main methods used in image encryption. Variousmedical image security methods are presented, yet they could be attacked. Medical images have a substantial correlation between nearby pixels, so eliminating this correlation requires for a permutation (scrambling) technique with a greater securitylevel.

C. Chaotic System

One of the best and most efficient methods for image encryption is a chaotic system. To achieve encryption, this method employs a certain pixel randomization pattern. Among other intrinsic aspects, it benefits from ergodicity, aperiodicity, pseudorandom properties, vulnerability to initialconditions, and control parameters. Despite the fact that entropyandhistogram values are two of the properties used togauge how secure image encryption is against statistical attacks, they are not altered by this method. Instead, this technique effectively just shuffles the positions of the pixels. The chaos system is frequently combined with several procedures, such as XOR substitution, or numerous techniques, such as DNA coding, compressed sensing, El Gamal, Elliptic curve, and so forth, in order to strengthen thesecurity of image encryption.

Image encryption is frequently used for sending sensitive medical photos, especially in telemedicine. Medical photographs are essential for assisting medical teams in making diagnoses of patients. Medical photos provide delicate information about a patient's health. Due to the growing global interest in inpatient records, all of this crucial data, including

medical photographs, are stored on image and communication servers. In order to access the patients' medical history, various healthcare practitioners may need to exchange these records across real-world public networks. In order to protect and maintain patient privacy, it's crucial to use storage and communication technologies with a variety of application platforms. In actuality, security threats including unauthorized data access and manipulation can apply to medical imaging. Medical images differ from photos from common tests in several ways. In medical imaging, adjacent pixels are typically quite homogenous and associated. It seems reasonable that if medical image encryption is done using only pixel scrambling techniques, the outcomes will be mediocre.

In order to encrypt medical photos, this paper suggests a scrambling method based on a hash function as the primary encryption step. For creating strong resistance against differential attacks, the hash function is applied to the plain image and key [1]. The Philox random generator and hash function are used to process keys, making them more sensitive and resistant to brute-force attacks. The method of substitution is carried out using the processed key. Furthermore, the cypher image is made more resistant to statistical attacks by the dynamic bit-scrambling technique based on the Josephus sequence and diffusion. Limitations: While the suggested technique improves PSNR values for 24- bit medical images, it is still worse for SSIM [1].

A method using a joint compressive auto encoder framework is used to hide several images in a single cover image of the same size. In contrast to other deep learning-based full-image-to-image hiding techniques, the J-CAE method removes the trade-off between the imperceptibility of container images and the recovery performance of hidden images [2] while introducing a chaotic mapping system, resulting in smaller reconstruction errors for both container and hidden images. Additionally, the image hiding made possible by mapping feature representations reduces the ability of steganography tools to discover the J-CAE approach, improving security. As the hidden number is increased, the processing time for multiple images grows steadily [2].

The minimal quality loss of both the encrypted and decrypted images can be achieved by concealing a full- color image inside another one of the same size [3]. Deep neural networks are built specifically to work as a pair and are simultaneously trained to develop the hiding and displaying processes [3]. The system is tested on real-worldimages from a wide variety of sources and was trained on images chosen at random from the ImageNet collection. Beyond demonstrating how deep learning can be used to successfully hide images, this system also focuses at how the result is obtained and applies a number of changes to determine whether image quality in both the host and concealed image can be maintained. Simple picture alterations and sophisticated machine learning-based adversaries are both included in this transformation. Full Cryptographic schemes are not used to hide the images [3].

Steganography, cryptography, and neural networks can be used to conceal an image inside a larger or similar container image. Although the cryptographic method employed is very straightforward, it works well when combined with deep neural networks. Other steganography methods involve uniformly hiding data, which makes it less secure but hides it effectively. This approach addresses these issues and makes data concealment secure and uneven [4]. With CNNs, we can more effectively handle the images while

requiring less parameters to set up the model by encoding image-specific properties into the architecture. CNN performs effectively and provides more accurate results [4].

A hybrid data compression algorithm is employed to execute lossy and lossless compacting Steganography methods while increasing the input data's level of RSA (Rivest-Shamir- Adleman) cryptography encryption to increase security. The Huffman coding algorithm is used to compress the plaintext, while the discrete wavelet transform (DWT) based algorithm is used to compress the cover image [5]. Lossy compression is used to minimize the cover image's size. The encrypted data will then be inserted into the compressedcover image using the least significant bit, or LSB. This method is used to reduce the volume of each transmission to facilitate rapid transmission. The image quality declines when it is compressed [5].

II. SYSTEM ARCHITECTURE

A. Proposed System

a. Methodology

Encryption Process, Decryption Process, Resistance to Statistical and Differential Attacks, and Deployment are the four primary elements that make up our suggested solution. The user must first submit the image to be encrypted and provide the date of birth associated with their Aadhaar number in order for a unique key to be generated. With chaotic hash scrambling, the plaintext image is obscured. The input parameter for Philox Pseudorandom Generator is the key (PPG). Then, joint procedures are carried out on the SHA512 (PPG) and SHA512 results (Key). Then, using the Henon Map as a guide, all the bit pixels are scrambled. The cypher image is obtained by using Logistic Diffusion on the image pixels. The cypher image must be uploaded in order to begin the decryption process, and the user must enter thekey value that was created during the encryption process. Decryption is the opposite of encryption.

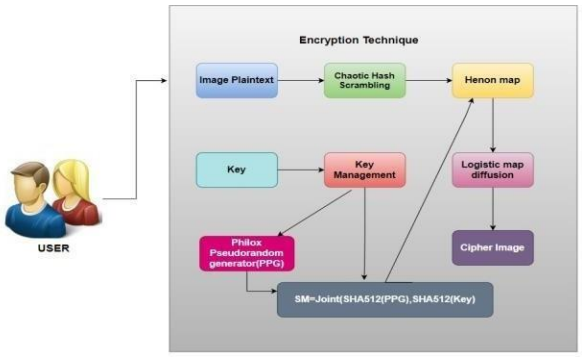
b. Encryption

Sensitive data is managed and kept in large amounts online, either on servers connected to the cloud or elsewhere. Cybersecurity is used by encryption to protect against cyberattacks like malware and ransomware as well as brute-force attacks. Data encryption secures transferred digital data on computer networks and the cloud. Digital data is divided into two categories: transmitted data (also known asdata in flight) and stored data (sometimes known as data at rest).

The outdated Data Encryption Standard has been replaced by more recent encryption techniques to secure data. These algorithms protect data and support security objectives including non-repudiation, integrity, and authentication. In order to verify the message's origin, the algorithms first authenticate it. The integrity of the data is then checked to ensure that the contents have not altered. The non-repudiation initiative also prevents senders from concealing legal activities. Data is encrypted and decrypted using two unique cryptographic asymmetric keys using using asymmetric encryption, sometimes referred to as public-key cryptography. A "public key" and a "private key" are the names of these two keys. Symmetric encryption is a type of encryption in which the plaintext and cipher text are encrypted using the same secret symmetric key. Concerns regarding public cloud security and securing data in complicated environments are growing as more enterprises migrate to hybrid and muti-cloud data can be protected with the

help of enterprise-wide data encryption and encryption key management.

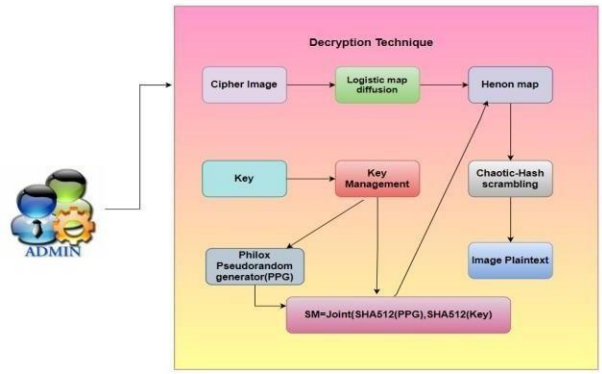
Fig 1 Flowchart of Encryption Process



c. Decryption

Data that has been encrypted can be decrypted and returned to their original form. Typically, encryption is done in reverse. It decodes the data such that only a trusted user with access to the secret key or password may decrypt the information. Privacy is one of the reasons for using an encryption-decryption system. It's important to carefully examine any access from unauthorized groups or people as information goes over the Internet. As a result, the data is encrypted to prevent theft and loss of data. Text files, photos, emails, user data, and directories are a few typical items that are encrypted. The person who receives decryption gets a prompt or window where they can input a password to access the encrypted data. In order to decrypt the data, the system extracts and turns it into words and visuals that may be easily understood by both a reader and a system. It is possible to decrypt data manually or automatically. A set of keys or a password might also be used to carry it out.

Fig 2 Flowchart of Decryption Process



d. Henon Map

Henon suggested the well-known Henon map in only two dimensions as a condensed method for examining the dynamics of the Lorenz system.

The equations that provide Henon Map are

$x_{n+1} = 1 - ax_n^2 + by_n$ (1)

$y_{n+1} = x_n$ (2)

It is also possible to write this nonlinear two-dimensional map as the two-step recurrence relation

$x_{n+1} = 1 - ax_n^2 + bx_{n-1}$. (3)

e. Chaotic System

Chaotic cryptology is the application of chaos theory to the practice of cryptography, the research or methods used to transfer information secretively and securely in the presence of a third party or adversary. The unsolvable issue of quick and highly secure image encryption has been solved in a novel and effective manner via chaos-based encryption [1].

A chaotic system is one of the best and most effective techniques for photo encryption. This approach uses a specific pixel randomization pattern to produce encryption. It benefits from ergodicity, aperiodicity, pseudorandom

characteristics, vulnerability to beginning circumstances, and control parameters, among other fundamental features. Entropy and histogram values, which are two characteristics used to assess how secure image encryption is against statistical attacks, are unaffected by this technique. Instead, this method essentially does is change the pixels' locations. Numerous crucial characteristics of chaotic systems include their high sensitivity to beginning conditions and system parameters, pseudo randomness, non-periodicity, topological transitivity, etc. The majority of features satisfy cryptographic requirements like diffusion and mixing. As a result, chaotic cryptosystems have more beneficial and real- world uses.

f. Logistic Map Analysis

The security of cryptosystems based on common one- dimensional discrete chaotic maps, such the logistic map, is poor.

As is common knowledge, a logistic map is defined as follows

xn+1 = xn (1 xn) (4)

where n = 0, 1, and (0, 4).

The key might be represented by the parameter andstarting value x0. Three segments of the parameter can be investigated by experiments under the following circumstances: x0 = 0.3. After multiple repetitions, the algorithm yields the same value when (0, 3). To obtain the cypher image, do the diffusion using the XOR operation on the picture pixels and K. Before conducting the XOR operation in this process, the decimal must be converted to binary [1].

g. SHA 512

Text of any length can be hashed using the Secure Hash Algorithm (SHA-512), which yields a fixed-size string. Each output generates a length of SHA-512 of 512 bits (64 bytes). The Bit Shares network is the mostsignificant application of SHA-512 in block chain technology. A hashing algorithm called SHA-512 operates on data that is supplied to it. Many things, like internet security, digital certificates, and even block chains, use hashing algorithms. It is a member of the SHA-2 family of hashing algorithms. This algorithm is used for hashing aadhaar number, date of birth, and key.

h. Pseudo Random Number Generator

A pseudo-random number generator (PRNG) is a technique that generates random number sequences using mathematical formulas. PRNGs generate a set of numbers that closely approximate the properties of random numbers. A seed state is used by a PRNG to start from an arbitrary starting state. If the beginning of the series is known, many numbers are created quickly and can also be repeated later. The numbers are therefore precise and deterministic. Using the previous random integer, the integer constants, and the integer modulus, we get the subsequent random integer. The algorithm needs an initial Seed to get going, which must be supplied in some way. By using modulo arithmetic, one can recreate the appearance of randomness [1]. Applications where several random numbers are needed and where it is advantageous to readily replay the same sequence are suited for PRNGs. Simulation and modelling applications are common instances of these applications. Applications requiring really unpredictable numbers, such as data encryption and gaming, arenot suited for PRNGs.

III. SYSTEM DESIGN AND IMPLEMENTATION

A. Encryption

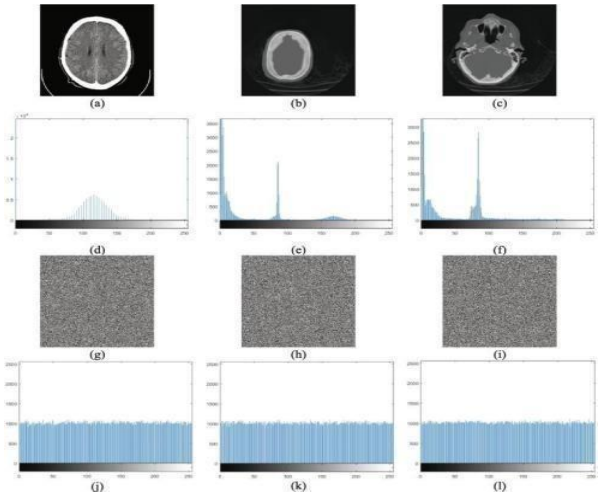
The encryption method is resistant to statistical and differential attacks since it employs the

diffusion and confusion process. It's crucial to use a powerful hash algorithm toanalyse plain images and keys in order to increase the security of keyspace analysis. The chaotic approach is still commonly employed in picture encryption due to its primary property, with a logistic map being one of the most popular methods. A unique key is generated using the user's date of birth and Aadhaar number. The produced key is then sent as an input parameter to the Philox Pseudorandom Generator (PPG). Following that, joint operations are performed on the SHA512 (PPG) and SHA512 results (Key).The plain text image is scrambled using the Arnold Chaotic Hash Scrambling technique. Then, all bit pixelsare scrambled using the Henon Map. On obtaining the encrypted image, Atlast Logistic Diffusion is applied to the image's pixel data.

B. Decryption

Thedecryption operation is fairly simple but requires input in the form of a cypher image and key. It reverses the encryption process. Use Logistic Diffusion to read the is a graph that shows the frequency distribution of pixel values in a grayscale (0 to 255). The resulting encrypting effect improves as the pixel value distribution appears more equal [1].

Fig 3 Histogram Analysis



It is clear from the data displayed in the above picture that all of the histogram samples for encrypted photos have a comparable degree of consistency. Based on the histogram, this shows that encryption was successful.

b. Correlation Coefficient Analysis

Finding the correlation between adjacent pixels can be done via correlation coefficient analysis. A basic image should logically display redundant information due to the close values between pixels. The correlation coefficient value will be closer to 1 the more redundancy there is; otherwise,it will be closer to 0. Therefore, the plain image will typicallyresult in a plain image correlation coefficient valuethat will be close to 1. A more effective encryption schemeis one in which the correlation coefficient value of the cypher image is near to 0. Calculating the correlation coefficient analysis byusing

$$CC_{x,y} = \frac{cov(x,y)}{\sqrt{Dx}\sqrt{Dy}} \quad (5)$$

$$cov(x,y) = \frac{1}{n}\Sigma_{i=1}^{n}[x_i - E(x)][y_i - E(y)] \quad (6)$$

$$D(x) = \frac{1}{n}\Sigma_{i=1}^{n}[x_i - E(x)]^2 \quad (7)$$

$$D(y) = \frac{1}{n}\Sigma_{i=1}^{n}[y_i - E(y)]^2 \quad (8)$$

E(x) and E(y) stand for the expectations of x and y, and CCis the correlation coefficient. N is the number of pixels, x and y are the grey levels of two neighbouring pixel values, and n is the number of pixels [1]. For each plain and cypher image, 2000 pairs of pixels are employed in each direction (diagonal, vertical, and horizontal).

c. Avalanche Effect Analysis

To determine how much a little change to the plain image affects the cypher image bit, avalanche effect analysis is used. A 0.5 avalanche effect is ideal. This value is

calculated by comparing the bits in the plaintext-modified (C2) and plaintext-unmodified (C1) cypher images. If there are around 50% different bits between C1 and C2, the avalanche effect value is considered to be perfect. The key can also be changed in order to obtain C1 and C2. The avalanche effect can be used to test an encryption method's resistance to differential attacks and measure how sensitiveits keys are. The two cipher images can be converted to binary form in order to calculate the avalanche effect, which is then transformed into an array. It can then be calculated using

$$AE = \frac{\sum_{I=1}^{n} bC1_I \; V \; bC2_I}{n} \times 100\% \qquad (9)$$

Where AE stands for the avalanche effect, n is the number of bits, I is the index, and bC1 and bC2 are binary cypher image forms [1]. AE was put to the test twice in this investigation. The first included changing the 1-bit plain, while the second involved changing the key's 1-bit value.

D. Deployment

Flask Framework is used for deploying our suggested model. A web framework called Flask offers libraries for creating simple web applications in Python. Flask is built on top of the Jinja2 template engine and the Werkzeg WSGI toolkit. For the creation of Python web applications, the Web Server Gateway Interface (WSGI) has been the de facto standard. A well-liked Python template engine is jinja2. A web template system renders a dynamic web page byfusing a template with a particular data source. A webpage will be created after our model has been deployed in a flask. Two options for the encryption and decryption procedure are available on the main page. The user must upload the plain-text image that needs to be encrypted together with their Aadhaar number and date of birth on the encryption page after selecting the encryption button. By combining the user's aadhaar number and birthdate, a special key will be created. By selecting the download option, the user can download the encrypted image. Then, by selecting the decryption button, the user can begin the decryption procedure. The user will then be forwarded to the decryption page, where they must enter the key value created during the encryption process and upload the cypher image. By selecting the download option, the user can finally download the decrypted image.

Fig 4 Home page

Fig 5 Encryption page

Fig 6 Encrypted image page

Fig 7 Encrypted image

Fig 8 Decryption page

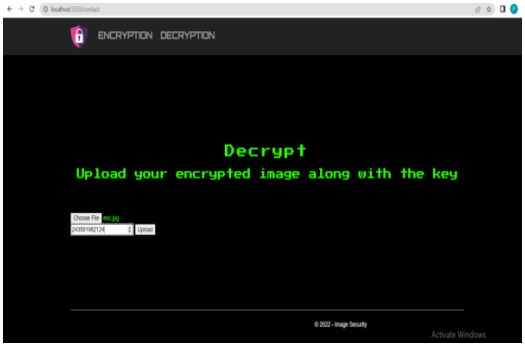


Fig 9 Decrypted image page

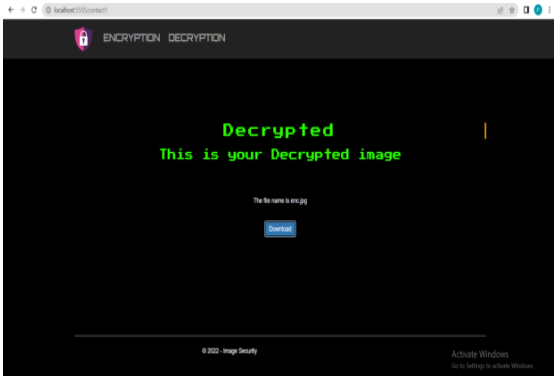
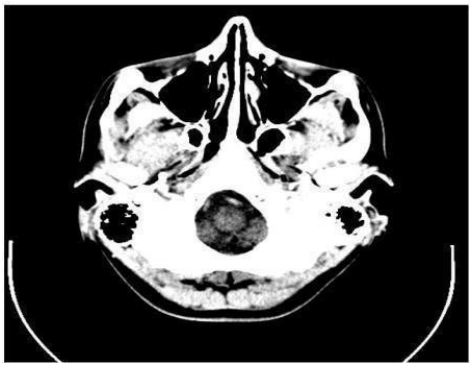


Fig 10 Decrypted image



IV. COMPARISON AND RESULTS

The effectiveness of the suggested encryption and decryption techniques is examined in this section. This technique is more suited to medical imaging, as was previously stated. To learn more about how well the suggested approach performs in comparison to earlier research, certain standard images are also tested.

It is evident from the results shown in Fig. 15 that all of the encrypted images histogram samples exhibit a comparable degree of consistency. Based on the histogram, this shows that encryption was successful. Chi-square analysis, which showed that the histogram had good consistency because all the generated values were smaller than 293, was also used to confirm this conclusion. Additionally, it has been proven thatthis research's average chi-square value is better to earlier related approaches. It is necessary to note that the chaotic hash scrambling and diffusion using a logistic map have a more significant impact on getting good results on this measurement.

The performance of the proposed approach performs exceptionally well on medical photos. The outcomes shown in Fig 17 demonstrate that the proposed method continues to havea higher correlation value than the earlier way. The correlation coefficient is not completely superior to the current approaches, though.

However, the majority of the measurement findings suggest that the proposed technique performs better, particularly for special and medical photos. This successful performance is strongly influenced chaotic hash scrambling, and diffusion stage using logistic map.

It is clear that Avalanche effect value in Fig 18 look to be extremely optimal based on the

avalanche effect statistics supplied because this is so near to the 50% value. However, it is clear that changes to the key seem to result 50.75%. The hashing operation on the key and key processing, which controls the encryption process's domino effect, greatly influences this.

Fig 11 Histogram Analysis of existing mode

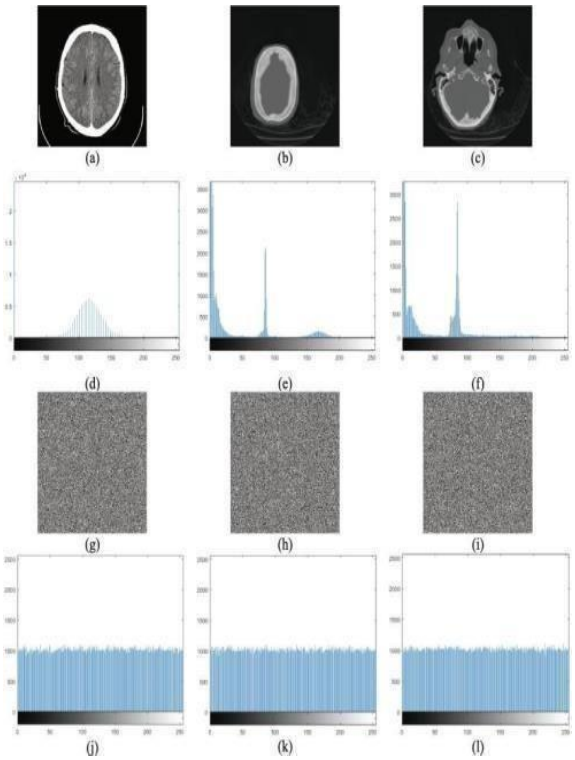


Fig 12 Histogram-original image of proposed model

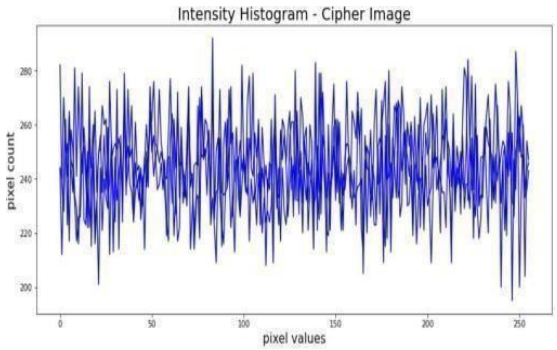


Fig 13 Histogram-cipher image of proposed model

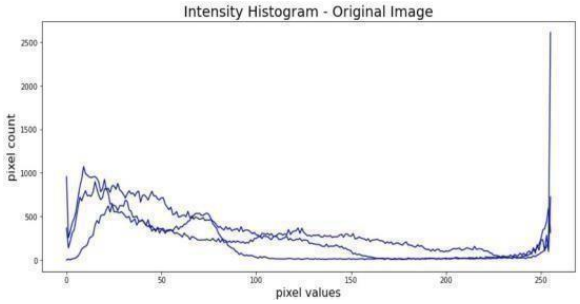


Fig 14 Correlation Coefficient-original image of proposed model

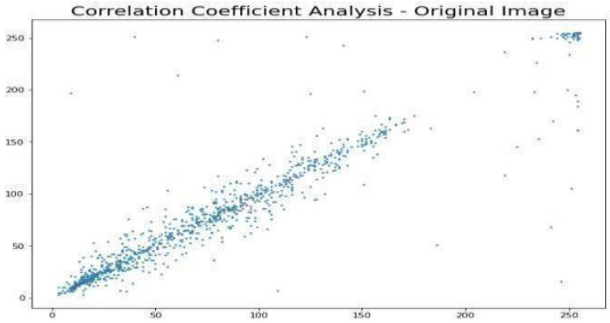


Fig 15 Correlation Coefficient-Encrypted image of proposed model

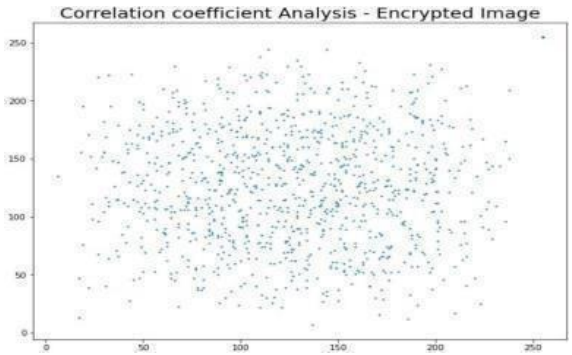
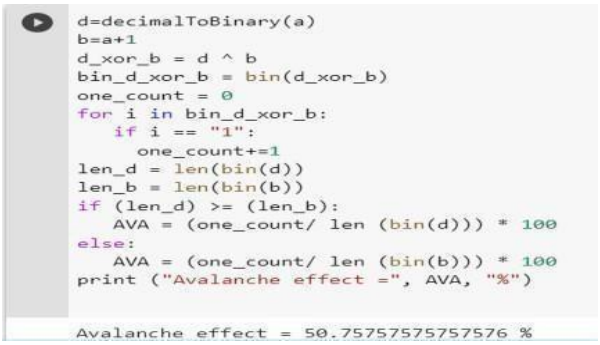


Fig 16 Avalanche effect of proposed model



```
d=decimalToBinary(a)
b=a+1
d_xor_b = d ^ b
bin_d_xor_b = bin(d_xor_b)
one_count = 0
for i in bin_d_xor_b:
    if i == "1":
      one_count+=1
len_d = len(bin(d))
len_b = len(bin(b))
if (len_d) >= (len_b):
    AVA = (one_count/ len (bin(d))) * 100
else:
    AVA = (one_count/ len (bin(b))) * 100
print ("Avalanche effect =", AVA, "%")

Avalanche effect = 50.75757575757576 %
```

Table 1 Comparison of Avalanche Effect

MODEL	EXISTING MODEL	PROPOSED MODEL
AVALANCHE EFFECT	50.037%	50.75

V. CONCLUSION AND FUTURE WORK

This study proposes an encryption method on medical imagesby performing a scrambling technique based on a hash function as the initial encryption step. The hash function is performed on the plain image and key to produce good resistance to differential attacks. The purpose of key processing is based on Philox pseudo random generator and hash function, making keys more sensitive and designed to be strong against brute-force attacks. The processed key is used for the substitution process. Furthermore, henon map and logistic diffusion strengthens the cipher image against statistical attacks and Differential attacks. This method has proven to have an excellent performance which has been tested with various measuring tools such as histogram analysis, correlation coefficient, avalanche effect. The complexity of the time required is also relatively fast. This method can later be adopted in applications such as telemedicine or applications to transmit medical images that require reliable security.

REFERENCES

Setiadi, D. R. I. M., Rachmawanto, E. H., & Zulfiningrum, R. (2022). Medical imagecryptosystem using dynamic Josephus sequence and chaotic-hash scrambling. Journal of King Saud University - Computerand Information Sciences, 34(9), 6818–6828.https://doi.org/10.1016/j.jksuci.2022.04.002

Chen, L., & Heipke, C. (2022). Deep learning feature representation for image matching under large viewpoint and viewing direction change. ISPRS Journal of Photogrammetry and Remote Sensing: Official Publication of the International Society for Photogrammetry and Remote Sensing (ISPRS), 190, 94–112. https://doi.org/10.1016/j.isprsjprs.2022.06.003

Desai, S. D., Patil, N., Nirmala, S. R., Kulkarni, S., Desai, P. D., & Shinde, D. (2022). Deep neural network based medical image steganography. 2022 International Conferenceon Smart Technologies and Systems for Next Generation Computing (ICSTSN), 1–5.

Z. Guan et al., "DeepMIH: Deep Invertible Network for Multiple Image Hiding," in IEEE Transactions on Pattern Analysis and Machine Intelligence, doi: 10.1109/TPAMI.2022.3141725.

Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji, B. N. (2022). Digital image steganography: A literature survey. Information Sciences, 609, 1451–1488. https://doi.org/10.1016/j.ins.2022.07.120

N. Subramanian, O. Elharrouss, S. Al-Maadeed and A. Bouridane, "Image Steganography: A Review of the Recent Advances," in IEEE Access, vol. 9, pp. 23409- 23423,

2021, doi: 10.1109/ACCESS.2021.3053998.

Liu, X., Ma, Z., Chen, Z., Li, F., Jiang, M., Schaefer, G., & Fang, H.(2022). Hiding multiple images into a single image via joint compressive autoencoders. Pattern Recognition, 131(108842),108842.https://doi.org/10.1016/j.patcog.2022.108 842

W. Tang, B. Li, M. Barni, J. Li and J. Huang, "An Automatic Cost Learning Framework for Image Steganography Using Deep Reinforcement Learning," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 952-967, 2021, doi: 10.1109/TIFS.2020.3025438.

S. Ghamizi, M. Cordy, M. Papadakis and Y. L. Traon, "Evasion Attack STeganography: Turning Vulnerability Of Machine Learning To Adversarial Attacks IntoA Real-world Application," 2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW), 2021, pp. 31-40, doi: 10.1109/ICCVW54120.2021.00010.

Das, A., Wahi, J. S., Anand, M., & Rana, Y. (2021). Multi- image steganography using deep neural networks.https://doi.org/10.48550/ARXIV.2101.00350

O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, andCompression Steganography Techniques," in IEEE Access, vol. 9, pp. 31805-31815, 2021, doi: 10.1109/ACCESS.2021.3060317.

S. Baluja, "Hiding Images within Images," in IEEE Transactions on Pattern Analysisand Machine Intelligence, vol. 42, no. 7, pp. 1685- 1697, 1 July 2020, doi:10.1109/TPAMI.2019.2901877.

Y. Ding et al., "DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things," in IEEE Internet of Things Journal,vol. 8, no. 3, pp. 1504-1518, 1 Feb.1, 2021, doi: 10.1109/JIOT.2020.3012452.

Sharma, K., Aggarwal, A., Singhania, T., Gupta, D., & Khanna,

(2019). Hiding data in images using cryptography and deep neural network. Journal of Artificial Intelligence and Systems, 1(1), 143 –162. https://doi.org/10.33969/ais.2019.11009

Van, T. P., Dinh, T. H., & Thanh, T. M. (2019). Simultaneous convolutional neural network for highly efficient image steganography. 2019 19th International Symposium on Communications and Information Technologies (ISCIT).