Blocked based DCT and chaos Image Compression Encryption

[1]Neeraj Giri, [2]Kalpana Rai, [3]Sneha Soni

[1]MTech Scholar, [2]Professor and HOD, [3]Assistant Professor

[1,2,3]Department of Computer Science, Sagar Institute of Research Technology-Excellence, Bhopal, India

***Abstract*— A rise in data transmission rates and other security issues have resulted from the Internet's dramatic rise in popularity. Compressing and encrypting data at the same time is essential for the secure transfer of multimedia content, such as digital photographs. The development of compression methods in combination with strong encryption methods in hybrid combinations like chaotic mapping has helped alleviate this issue. In this work, blocked DCT and chaotic maps (Arnold and Logistic maps) are used to compress and encrypt the medical images respectively in hybrid combination for safe and lightweight transmission. We demonstrated how to reduce the size of the original medical image by employing the blocked discrete cosine transform. The compressed image is then encrypted using Arnold and a logistic map. We have shown experimentally that the hybrid system employed significantly improves the majority of the metrics used to evaluate a system's performance, including PSNR, SSIM, NPCR, UACI, and the correlation coefficient. Through cryptanalysis, it is proven that the proposed crypto system is secure against differential and statistical assaults. The proposed cryptographic system is suitable for use in telehealth applications.**

***Index Terms*—Medical Image, Encryption, Compression, Arnold map, Logistic map, and Blocked DCT.**

I. INTRODUCTION:

One of the most serious problems in today's evolving digital society is protecting one's privacy. Recent innovations and breakthroughs in computer-assisted diagnostics have boosted the acceptance of smart health care solutions. Artificial intelligence, big data analysis, and other cutting-edge technologies are frequently used in these approaches because they allow for more precise and timely results. Getting medical attention remotely through the internet is a real possibility currently, and it might be the key to curing a wide range of conditions without leaving your home [1]. These solutions often rely on cloud computing for data storage and processing, making it easy to collaborate with specialists from all over the world who may have expertise in different areas. And if that's not enough, the processing load can be split up across several machines.

The diagnostic process relies heavily on images produced during medical operations. Transporting pictures from one location to another can be a time-consuming and costly process, but it is sometimes necessary when sending images from a hospital, lab, or university for diagnosis. In order to convey information, people might employ a broad range of instruments. Portable devices like as scanners, handheld cameras, and portable x-ray machines can be used for this purpose since they can send data to a remote server instantly for additional processing [2]. The security of image data is an important consideration for telemedicine. The right to privacy must be safeguarded. The patients' right to privacy must be upheld as a matter of ethics.

The medical industry has made tremendous progress, leading to the gathering of a massive amount of data. This information must be processed and communicated efficiently to keep pace with the developing treatment modalities. It's certain that you'll run across issues during this process, the most prevalent of which are likely to be limited bandwidth and worries about the security of your data. Medical images are only one kind of data that has to be compressed in a way that meets all of the specified criteria and is secure from unauthorized access. The requirements for devices and sensors that sample medical signals are evaluated, and a one-step solution is provided to address the two issues of lightweight requirements, and privacy sensitive considerations [3].

Abdmouleh et al. [4] proposed an approach of partial encryption based on the Discrete Wavelet Transform (DWT) and compatible with the standard JPEG2000 to guarantee the best and safest transmission and storage of medical images. Ashwini et al. [1] proposed the idea of using chaotic-based compression-encryption to secure medical images in a way that is similar to how compressed sensing works with images. Mixing a sine map with an improved logistic map might result in a chaotic map. In the validation phase, the proposed map is compared to the logistic map using the Lyapunov exponent and the approximation entropy. The proposed method is tested on a number of different medical images, and its results are compared over a range of sample sizes.

One method for the compression and encryption of medical pictures was proposed by Chiranjeev et al. [5], and it relied on DNA and AES. Specifically designed for use with medical images, the DNA-based compression-encryption method presented in this research is a first of its kind. When split down into bit-planes, a large fraction of medical images are composed of uniform pixels. When photos are broken down, these pixels stand out even more. The proposed DNA-based Quad Tree Decomposition approach was created with the hope that redundancy might be eliminated concurrently with compression. In order to reduce the file size of the medical image files, Afandi et al. [6] propose an approach that combines the Discrete Cosine Transform (DCT) with Arithmetic Encoding.

The authors of this study offered a method for the transmission of medical images that included a block-based discrete cosine transform as a means of reducing the size of the data file while also being encrypted using a chaos-based algorithm that made use of Arnold and logistic map..

II. Related Work:

Blocked DCT:

DCT is a mathematical transformation for converting signals between the spatial domain and the frequency domain. Since that a block-based DCT reduces the amount of information needed to reconstruct a digitized image, it is widely used in digital image and video compression systems. Blocked DCT is carried out here, which not only results in superior compression in comparison to DCT in its standard form. In Blocked DCT, the image is divided into four sections; the DCT is then applied to each section individually; finally, the four blocks are combined into one; this technique significantly cuts down on compression time and aids in resolving the issues of data storage and transformation prior to encryption.

Logistic Map:

A chaotic system that uses a logistic map is one example. It is a non-linear map in discrete time that only has one dimension, and its non-linearity is quadratic. The equation of state for the logistic map is as follows [7]:

$$y_{n+1} = u * y_n * (1 - y_n) \qquad (1)$$

Arnold Map:

Arnold Map is commonly utilized in image stenography, authentication, and image cryptography. It is employed as a scrambling phase in all of these scenarios, with the number of iterations serving as a key.

III. Method:

In this section, we demonstrate the suggested approach for medical image encryption and decryption. To simplify the discussion of the suggested approach, we divide it into two stages: encryption and decryption.

Encryption:

The following is a description of the Encryption algorithm (refer **Fig. 1**):

Step 1: partition the plain picture A into four equal portions labelled A_1, A_2, A_3, and A_4.

Step 2: Using a discrete cosine transform, these sub-blocks A_1, A_2, A_3, and A_4 are compressed individually.

Step 3: Different compressed subblocks are then merged.

Step 4: Using the secret keys u and y_0, the logistic map is applied to the compressed picture in this step.

Step 5: Apply Arnold map to scramble the image and get compressed encrypted image.

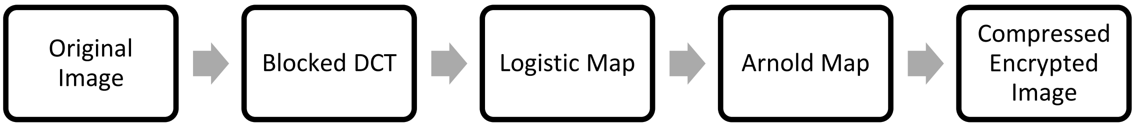

Fig. 1 Encryption Process

Decryption:

The following is a description of the Decryption algorithm (refer **Fig. 2**):

Step 1: Apply inverse Arnold map to unscramble the image.

Step 2: Using the secret keys u and y0, the logistic map is applied to the image in this step and get decrypted image B.

Step 3: Divide the image B into four equal portions labelled B_1, B_2, B_3, and B_4.

Step 4: These B_1, B_2, B_3 and B_4 sub blocks are decompressed separately using inverse discrete cosine transform.

Step 5: Finally separated decompressed sub blocks are combined together to get decrypted image.

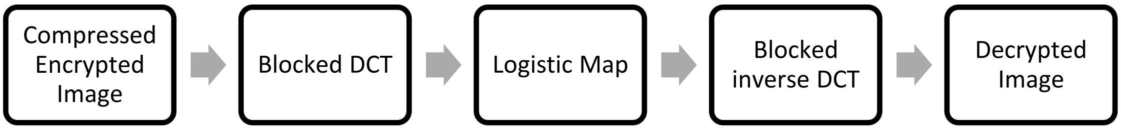

Fig. 2 Decryption Process

IV. Result Analysis:

The experiment is performed in Matlab R2016b on Intel Core i5. The data sets include imaging modalities such as MRI, and X-Ray. The experiment uses 50 randomly selected samples. In **Fig. 3**, we see the proposed algorithm being used to compress and encrypt the original 256×256 medical image and **Fig. 4** illustrated the histogram visualization of the original, compressed encrypted and decrypted 256×256 medical image.

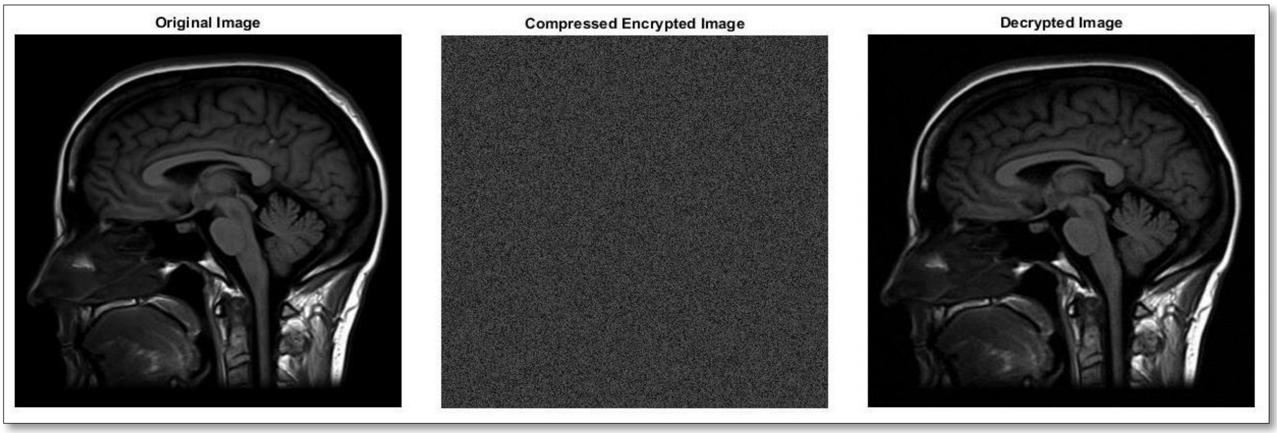

Fig. 3 Simulation result of original, encrypted and decrypted image

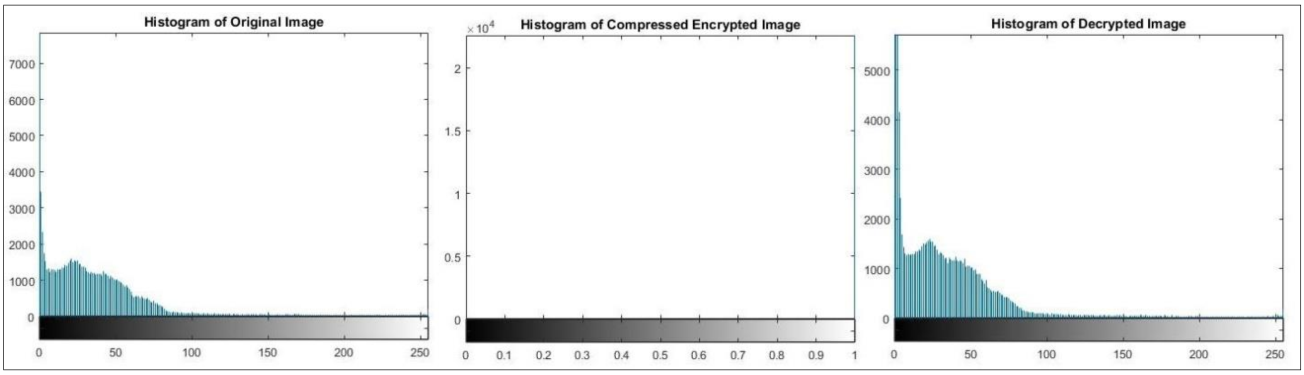

Fig. 4 Histogram of original, encrypted and decrypted image

Correlation Coefficient:

In order to prevent statistical attacks, it is essential that the encrypted data have a very low correlation to the original data. You can see the correlation between the encrypted and original image data in **Table 1**. With encrypted information, the correlation in all three directions is near to zero. The Correlation Coefficient graphical representation of the original and encrypted image is shown in **Fig. 5**.

Table 1 Correlation coefficient of the test images

Images	*Horizontal Correlation of Encrypted Image*	*Vertical Correlation of Encrypted Image*	*Diagonal Correlation of Encrypted Image*
MRI 1	-0.0043	-0.0009	0.0147
MRI 2	-0.0072	-0.0247	0.0006
X-Ray	-0.0063	-0.0003	0.0081

Image Quality Analysis:

Common metrics used to evaluate picture quality include the peak signal-to-noise ratio (PSNR) and the structural similarity index (SSIM). **Table 2** shows the results of image quality analysis.

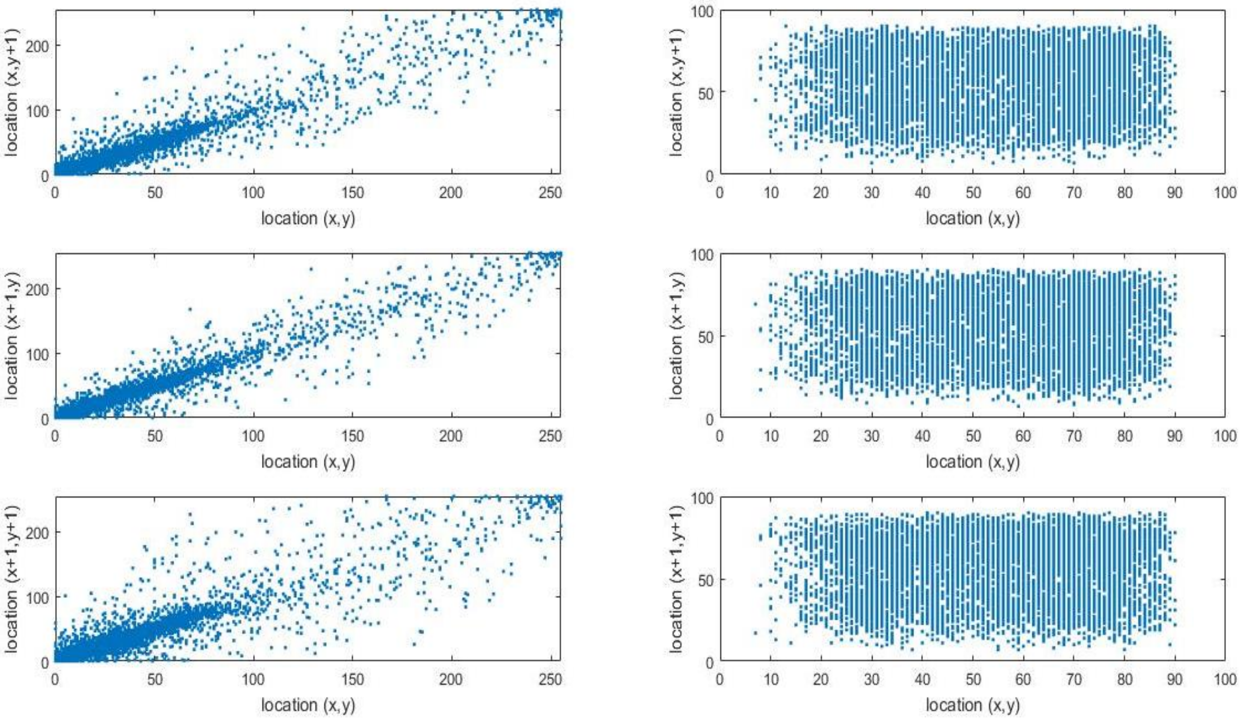

Fig. 5 Correlation coefficient diagram of the image

Table 2 PSNR and SSIM values of the test images

Images	*PSNR*	*SSIM*
MRI 1	40.0308	0.9542
MRI 2	37.7312	0.9409
X-Ray	42.7821	0.9623

NPCR and UACI:

Analysis of the original medical picture's sensitivity in relation to the encrypted image is what a differential attack is all about. Modifying even a single pixel of the original medical picture might a new and unique cypher picture. The "Number of Pixels Change Rate" (NPCR) and the "Unified Average Change Intensity" (UACI) are used to confirm these changes. **Table 3** illustrates the values of NPCR and UACI.

Table 3 NPCR and UACI values of the test images

Images	*NPCR*	*UACI*
MRI 1	99.63	33.44
MRI 2	99.64	33.42
X-Ray	99.62	33.41

V. CONCLUSION:

This paper uses blocked discrete cosine transform to compress the original medical picture. Afterward, Arnold and logistic map are used to encrypt the compressed picture. Through experimental research, we have demonstrated that the hybrid system used yields significant improvements across a wide range of performance analysis measures, including PSNR, SSIM, NPCR, UACI, and correlation coefficient, among others. The suggested crypto system is shown to be safe in the face of differential and statistical attacks by means of the cryptanalysis. The suggested cryptosystem is appropriate for telemedicine systems.

REFERENCES:

[1] K. Ashwini, R. Amutha, R. R. Immaculate, and P. Anusha, “Compressive sensing based medical image compression and encryption using proposed 1-D chaotic map,” in *2019 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2019*, 2019, doi: 10.1109/WiSPNET45539.2019.9032844.

[2] A. Sahay, C. Pradhan, and A. Sinha, “Medical signal security enhancement using chaotic map and watermarking

technique," in *Handbook of Research on Information Security in Biomedical Signal Processing*, 2018.

[3] J. Li *et al.*, "A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology," *BMC Med. Inform. Decis. Mak.*, vol. 20, 2020, doi: 10.1186/s12911-020-01328-2.

[4] M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhlel, "A novel selective encryption DWT-based algorithm for medical images," in *Proceedings - 2017 14th International Conference on Computer Graphics, Imaging and Visualization, CGiV 2017*, 2018, doi: 10.1109/CGiV.2017.10.

[5] C. Bhaya, M. S. Obaidat, A. K. Pal, and S. H. Islam, "Encrypted Medical Image Storage in DNA Domain," in *IEEE International Conference on Communications*, 2021, doi: 10.1109/ICC42927.2021.9500718.

[6] T. M. K. Afandi, D. H. Fandiantoro, Endroyono, and I. Ketut Eddy Purnama, "Medical Images Compression and Encryption using DCT, Arithmetic Encoding and Chaos-Based Encryption," in *Proceedings - 2021 International Seminar on Intelligent Technology and Its Application: Intelligent Systems for the New Normal Era, ISITIA 2021*, 2021, doi: 10.1109/ISITIA52817.2021.9502246.

[7] B. Ahuja and R. Doriya, "Bifold-crypto-chaotic steganography for visual data security," *Int. J. Inf. Technol.*, vol. 14, no. 2, 2022, doi: 10.1007/s41870-022-00861-9.