2023 3rd International Conference on Intelligent Technologies (CONIT)
Karnataka, India. June 23-25, 2023

Securing Medical Images using Compression techniques with encryption and Image Steganography

Pooranakala K.
PG Student,
Department of Computer Applications
Hindustan Institute of Technology and Science
Chennai, Tamil Nadu, India
brinthakarikalank@gmail.com

Dr.Vanita Jaitly
Associate Professor
Department of Computer Applications
Hindustan Institute of Technology and Science
Chennai, India
vanitaj@hindustanuniv.ac.in

2023 3rd International Conference on Intelligent Technologies (CONIT) | 979-8-3503-3860-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/CONIT59222.2023.10205855

Abstract- **Medical imaging is an essential component of the healthcare sector, enabling the transfer of medical images between widely separated locations to improve healthcare business practices. However, the transmission of medical images across public networks can result in several security concerns, including those related to authentication, integrity, and confidentiality. Therefore, the major goal of this research is to ensure the security and accuracy of medical images by maintaining their confidentiality and integrity. This proposed method aims to enhance the security of medical images during their transmission across public networks. The method involves three main steps: compression, encryption, and embedding To achieve the goal of maintaining the integrity and confidentiality of medical images, this research utilizes a multi-step process. First, the medical image undergoes compression using the Singular Value Decomposition (SVD) technique to reduce its size and eliminate any noise. Following this, the compressed image is encrypted using the Advanced Encryption Standard (AES) algorithm to ensure confidentiality. Finally, the encrypted image is securely enclosed within a cover image using the Least Significant Bit (LSB) steganographic technique to create a stego image. This technique ensures that the encrypted image is seamlessly incorporated within the cover image, without any visible or perceptible changes. This method ensures that the medical image remains confidential and maintains its integrity throughout the transmission process. Furthermore, this study developed the aforementioned technique, and the experimental outcomes were compared using MATLAB to hide medical images without encryption using LSB steganography as an additional layer of security. This study analyzed multiple medical image formats, including DICOM, TIFF, BMP, and JPEG. The findings indicate that combining encryption and steganography techniques provides improved results in terms of PSNR and MSE values, as contrasted to utilizing steganography alone.**

Keywords— Encryption, Steganography, LSB, SVD, Medical images,Security

I. INTRODUCTION

Medical images, such as X-rays, MRI scans, and CT scans, contain sensitive and personal information that must be protected from unauthorized access. The proposed approach provides a secure and efficient solution for storing and transmitting medical images. Medical imaging is an integral part of healthcare that enables healthcare professionals to share medical images between geographically separated locations. However, the transfer of medical images over public networks can pose various security risks, including issues related to confidentiality, integrity, and authentication. Therefore, safeguarding the confidentiality and integrity of medical images during their transmission is crucial and must be given the highest priority. This study proposes a novel method for securing medical images during their transmission over public networks. The proposed method comprises three steps: compression, encryption, and embedding. In the first step, the image undergoes compression using the SVD technique, resulting in a smaller image size and noise elimination. The second step implies encrypting the compressed image using the AES algorithm, providing robust encryption to maintain confidentiality. Finally, the encrypted image is securely embedded within a cover image using the LSB steganographic technique, creating a stego image. The SVD technique enables the compression and denoising of medical images, while the AES algorithm provides strong encryption to ensure confidentiality. To ensure the integrity of the medical image during transmission, the encrypted image is seamlessly and securely embedded within the cover image using the LSB steganographic technique, rendering the changes imperceptible. The proposed method offers a promising solution for securing medical images during their transfer over public networks. The experimental results confirm the efficacy of the proposed method in enhancing the security of medical images while preserving their quality.

II. LITERATURE SURVEY

While usually either cryptography or steganography is employed to ensure security, in this instance, both techniques were integrated to provide enhanced security [1]. To achieve this, transform domain techniques such as DWT and DCT can be employed, and the performance can be assessed based on various parameters [2]. Compression and cryptographic techniques are utilized to secure text files. Compression refers to the process of reducing the number of bits necessary to represent a particular set of data. It is helpful in saving more data. To develop a digital data security application, the combination of the DES (Data Encryption Standard) algorithm with the cryptographic method and the steganographic method with Discrete Cosine Transform (DCT) can be used [3].

The quality of the stego-image can be concluded based on the experiment. In order to improve the security of data files before being sent over the public network, a data security application is provided by this research. Here four levels of security technique for veiling messages are proposed which utilize two levels of cryptography with two levels of

steganography is used [4]. Vernam cipher is modified at each level of cryptography with the automatically originating initial key from the random pixel of camouflage cover. Better camouflage is created to evade interloper attention and realize better performance in terms of steganographic system measurement.[5]. To enhance the system's robustness, we have concentrated on improving the security and steganography processes. Specifically, we have focused on using the LSB method and RGB for the steganography operation. In one technique of image steganography, we have emphasized the MSB bits rather than the typical LSB bits [6]. The experimental findings indicate that the modified method is suitable for embedding a small quantity of data. Several of the methodologies employed in the study rely on the results of the DES, which is a symmetric key algorithm in cryptography [7]. It can be concluded that the combination of these two cryptographic techniques can transmit data through the unsecured channel and provides confidentiality for information hiding. One of the potential limitations of this proposed system is that the input data size may increase, resulting in a larger position array size.[8] SVD is capable of breaking down a matrix into three constituent matrices: a diagonal matrix of singular values, a left orthogonal matrix, and a right orthogonal matrix.

In the field of digital image processing, By minimizing the amount of singular values used to represent an image, SVD can be used to compress images. This is achieved by retaining only the most significant singular values and discarding the rest. The resulting compressed image will have a lower resolution and quality but will require less storage space in memory.

Experiments can be conducted to evaluate the performance of different singular values for image compression. The performance evaluation parameters can include metrics such as image quality, compression ratio, and processing time. The updated method for selecting the singular values that are retained with the related singular vectors in SVD picture compression is proposed in this research. [10] The goal of this technique is to keep the image's edges, which represent a highly important. visible component to human eyes. This is accomplished by permitting a range of percentages, calculated as the total of the singular values that are disregarded, as opposed to a fixed percentage. The variance is used to gauge how edgy a block is, with the block with the highest variance receiving the lowest percentage within the given range. The research aims to improve image compression using SVD by proposing a new method for selecting the singular values that are retained with the related singular vectors. The goal is to preserve the image's edges, which are important visible components to the human eye [11]. The proposed method uses a variable percentage range rather than a fixed percentage to retain the singular values. The range is calculated based on the total of the singular values that are discarded. The variance of the image blocks is used to measure the edge content of each block. Blocks with higher variance (i.e., more edges) are given a lower percentage within the variable range, ensuring that the edges are better preserved in the compressed image.

Overall, this proposed method aims to improve image compression quality by better preserving the edges in the image, which are important visual features. The approach seems promising and could lead to better results compared to traditional fixed percentage methods for selecting singular values in SVD-based image compression.

III. PROPOSED METHODOLOGY

The proposed method for securing medical images during transmission involves a three-step process. First, the medical image is compressed using the SVD approach. Then, The AES algorithm is used to encrypt the compressed image. Finally, the encrypted image is embedded inside a cover image using the LSB steganographic technique, resulting in a stego image that can be transferred via an uncertain channel. At the receiver end, the AES algorithm is used to decrypt the encrypted version of the medical image, thereby obtaining the original medical image. The use of cryptography provides confidentiality to the medical image, as only authorized parties with access to the decryption key can view the original image. The use of steganography provides additional security by hiding the encrypted medical image within a cover image. The utilization of steganography to embed the medical image within a cover image makes it challenging for unauthorized parties to identify the presence of the medical image. Nevertheless, it should be acknowledged that solely relying on steganography for security purposes does not guarantee confidentiality since individuals with access to the stego image and appropriate steganography tools can extract the hidden medical image. Overall, the proposed method seems to provide a good combination of cryptography and steganography to achieve both integrity and confidentiality for medical images. The retrieved medical image is depicted in Figure 1.

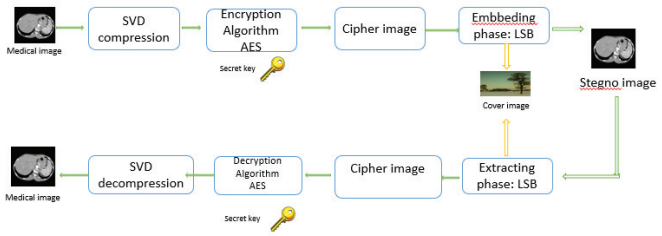

Fig. 1. shows the combination of encryption and steganography

Top of Form

1) Cryptography AES algorithm:

The AES algorithm is an effective method for encrypting and decrypting various forms of data, including images. The fundamental concept behind AES encryption involves taking a plaintext image and transforming it into ciphertext using a key. Subsequently, the same key is utilized to decrypt the ciphertext and recover the original plaintext image.

Here's a high-level overview of the steps involved in AES encryption for images:

1. Convert the plaintext image into a stream of bits.
2. Divide the stream of bits into 128-bit blocks, the block size used by AES.
3. Initialize a 128-bit key, which will be used to encrypt and decrypt the image.
4. Use the key to encrypt each block of bits using the

AES encryption algorithm.

5. Concatenate the encrypted blocks to form the ciphertext.

AES is a widely used and well-regarded encryption standard, and it is very secure when used correctly. However, like all encryption algorithms, it can be vulnerable to attack if the key is not properly secured. To ensure the security of your encrypted image, it is important to choose a strong key, use proper key management procedures, and store the key securely.

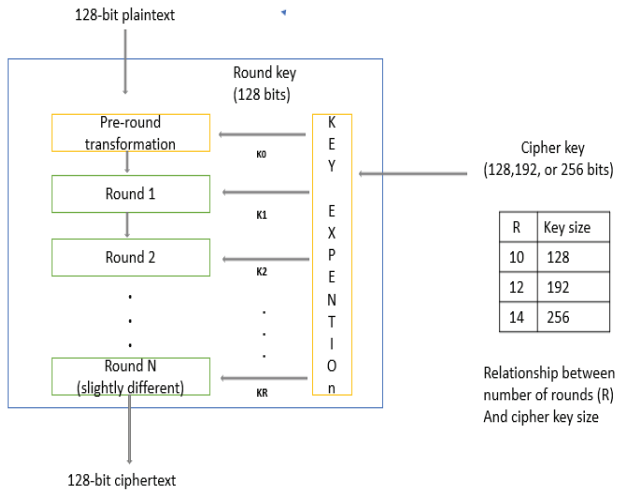

Fig. 2. AES algorithm encryption

B. SVD Compression:

The SVD algorithm is a powerful mathematical tool for image processing. It is used to analyse and manipulate the structure of a matrix, which represents an image. The algorithm provides a low-rank approximation of the original matrix, which reduces the resolution of the image and removes noise. The following is a detailed explanation of the working of the SVD algorithm and what results in it provides.

1) Matrix Decomposition:

A mathematical method called the SVD algorithm is used to divide matrix A into the three matrices U, S, and V. Although matrix S is a diagonal matrix that contains the singular values of A in descending order, matrix U is an orthogonal matrix that contains the left singular vectors of A. The right singular vectors of A are contained in the orthogonal matrix V. These matrices are obtained by performing an eigen decomposition of the matrices A^T A and A A^T. In the context of digital image processing, By decreasing the number of singular values needed to represent the image, the SVD technique can be used to compress images.

2) Low-Rank Approximation:

To obtain a low-rank approximation of the original matrix A using the SVD algorithm, we need to retain only the corresponding singular vectors and largest singular values. This low-rank approximation can effectively reduce the resolution of the image and remove noise. The matrices U, S, and V are used to obtain the low-rank approximation of A as follows:

$$\mathbf{A\_\ approx.} = \mathbf{U} * \mathbf{S} * \mathbf{V}^{\wedge}\mathbf{T}$$

3) Image Compression:

The low-rank approximation of the image matrix can be further compressed by removing redundant information. This can be achieved by quantizing the image or by using lossless or lossy compression techniques. The compression ratio achieved by the SVD algorithm is directly related to the number of singular values retained in the low-rank approximation. When more singular values are retained, the compression ratio is higher but the image quality is lower. Conversely, when fewer singular values are retained, the compression ratio is lower but the image quality is higher. Therefore, the choice of the number of singular values to retain is a trade-off between the compression ratio and the image quality, and it depends on the specific application requirements.

a) Image Reconstruction:

The reconstructed image obtained from the low-resolution and denoised image using the SVD technique is suitable for a variety of image-processing applications, including data analysis and compression.

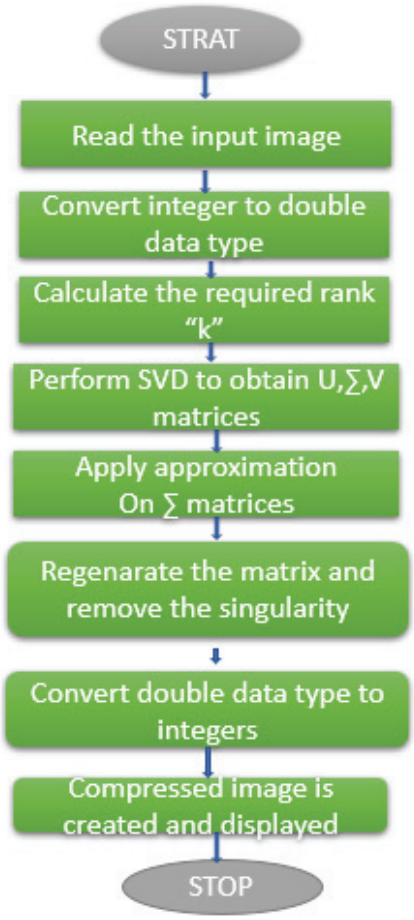

Fig. 3. SVD Compression

The SVD algorithm provides a powerful tool for image processing by reducing the resolution of the image and removing noise. The algorithm is widely used in various fields, including image compression, denoising, data analysis, and image recognition. The results of the SVD algorithm can be

improved by combining it with other techniques such as independent component analysis, principal component analysis, and matrix factorization. The combination of LSB and SVD can be used in a medical image processing project to secure the information contained in medical images.

b) LSB Steganography:

The LSB algorithm is a steganographic technique that involves replacing the least significant bits of the pixel values with bits from the hidden data to embed data within an image file. To implement the LSB algorithm, one can follow the following simple steps:

a) Load the image: Read the image file and load it into memory as a matrix of pixel values.
b) Convert the data to be embedded into binary: The data to be embedded should be converted into binary form.
c) Embed the data: For each pixel in the image, replace the least significant bit of the binary data's red, green, and blue values as represented by bits.
d) Save the modified image: Save the modified image as a new file.
e) Decode the data: To retrieve the embedded data, you can decode the image by extracting the least significant bits from the green, red and blue values of each pixel and converting the extracted bits back into the original data.

It is important to note that the LSB algorithm will affect the quality of the image, especially if a lot of data is embedded within the image. The more data that is embedded, the greater the degradation of the image quality.

Example: Consider the pixels 11111111 (255), which make up the cover picture, and 11100001 (225), which make up the secret image. In the event of an MSB substitution, 11101111 (239) will be the pixel for the stego image, but the outcome of an LSB replacement will be 11111110. (254).

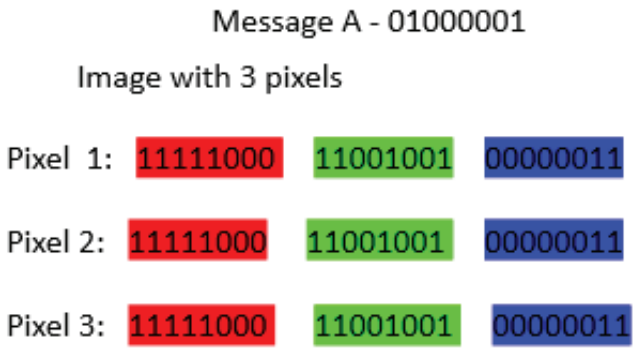

Fig. 4. LSB embedding

C. SVD+LSB:

To combine SVD and LSB steganography, the image is first decomposed into matrices using SVD, and then the least significant bits of either the singular values or singular vectors are replaced with hidden data. The rationale behind this is that the singular values and vectors contain a significant amount of information about the image, and small changes to them are less noticeable and do not significantly impact the visual quality of the image.

a) Load an image and convert it to a grayscale matrix
b) Perform SVD on the grayscale matrix to get the unitary matrices U, D, and V and the singular values and vectors
c) The least important bits of the single values or vectors are changed to conceal secret data, which have a lower impact on the visual quality of the image, as they contain a large portion of the image information.
d) Reconstruct the grayscale matrix using the modified singular values or vectors
e) Convert the grayscale matrix back to a colour image and save it

This technique may not be very secure and could be easily detected by steganalysis methods. More advanced techniques, such as using singular value thresholding or using the singular vectors in a more sophisticated way, may be required to achieve a higher level of security.

IV. EXPERIMENTAL RESULTS

The proposed method, which involves combining LSB steganography and AES encryption has been implemented using MATLAB, with the addition of SVR compression to ensure the preservation of image quality. A matrix is divided into three smaller matrices using the mathematical approach known as SVD, which represents the original matrix. In medical image hiding, SVD can be used to represent a medical image as a series of singular values, which can be manipulated to conceal information within the image.

The results of a medical image-hiding experiment using SVD or LSB will depend on the specific implementation and the quality of the data being used. In general, the results will show the effectiveness of the method in hiding information within the medical image while maintaining the quality of the image and the accuracy of the information being hidden.

The image is a matrix of 512 by 512. Every pixel is represented in the matrix by a number from 0 to 512. We are looking for compression of that image using the SVD image compression method. Using this method, we will retrieve some information from the image but the image quality has to remain good.

SVD on the matrix A:

[U, S, V,] = svd (A);

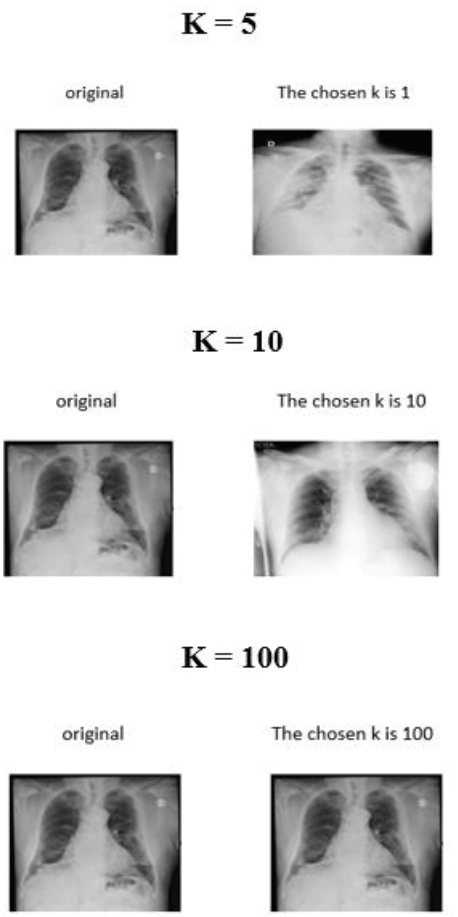

Fig. 5. IMAGE 1(SVD compression for different singular value "k"

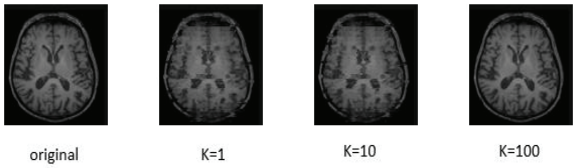

Fig. 6. MAGE 2 (compression for different singular value "k"

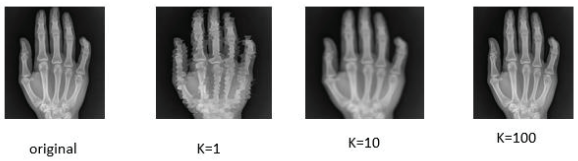

Fig. 7. MAGE 3 (compression for different singular value "k"

TABLE I. SVD ALGORITHM RESULTS

IMAGE 1			IMAGE2			IMAGE3		
K	CR	CI	K	CR	CI	K	CR	CI
5	175.5	160.5	5	176.5	160.8	5	177.3	161.5
10	88.9	150.6	10	83.7	151.2	10	84.5	152.2
100	7.8	170	100	7.9	170.99	100	8.1	171.5

The medical image-hiding experiment's results are currently under evaluation and will be compared to the results obtained using the LSB method without encryption. In the LSB method, the image is embedded into a cover image. The evaluation process will be based on the PSNR (Peak Signal-to-Noise Ratio) and MSE (Mean Square Error) values, which can be calculated using the following equations:

MSE is a metric used to measure the similarity or difference between two images. It is calculated by taking the difference between the pixel values of the original and the processed image, squaring them, and taking their average. A lower MSE value represents minimal distortion and greater similarity between the two images. The formula for calculating MSE is:

$$\text{MSE} = \frac{1}{A} \times \frac{1}{B} \sum_{C=0}^{A} \sum_{D=0}^{B} (\text{X(c, d)} - \text{y(c, d)})^2 \quad (1)$$

Where c and d are the numbers of rows and columns respectively. A and B are the total numbers of rows and columns, x is the cover image, and the Oswego image.

PSNR: PSNR is a metric used to measure image quality by comparing the maximum possible power of a signal to the amount of noise that corrupts the signal. The higher the PSNR value, the better the image quality, as the signal is stronger relative to the noise.

$$\text{PSNR} = 20 \log_{10} \left(\frac{MAX_f}{\sqrt{MSE}}\right) \quad (2)$$

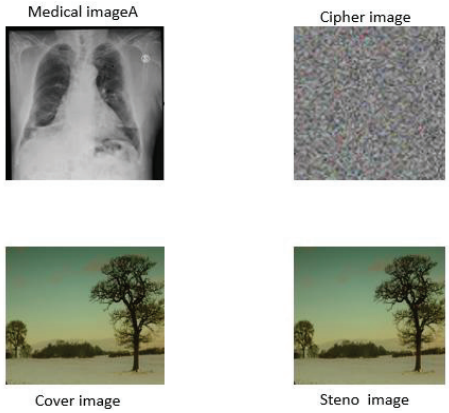

Fig. 8. Image A trasformation of cipher image, and cover image

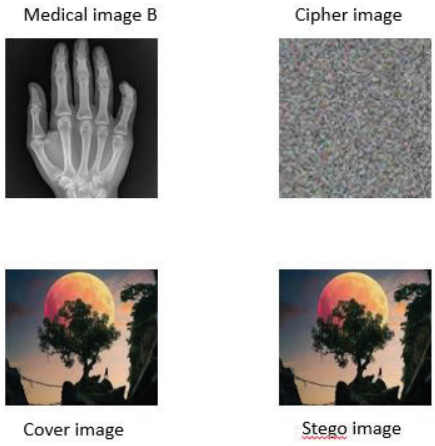

Fig. 9. Image B trasformation of cipher image and cover image

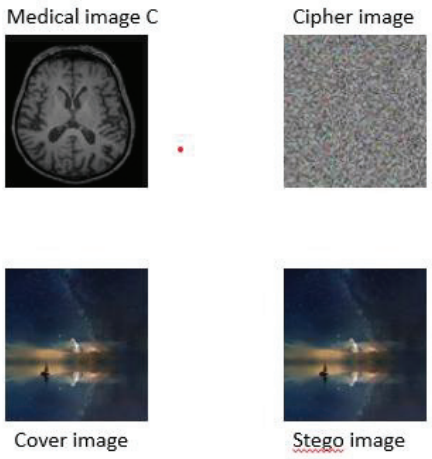

Fig. 10. ImageC transformation of cipher image, and cover image

TABLE II. PSNR AND MSE RESULTS

IMAGES	PSNR	MSE
A	71.567	0.00048
B	62.476	0.00057
C	62.567	0.00065

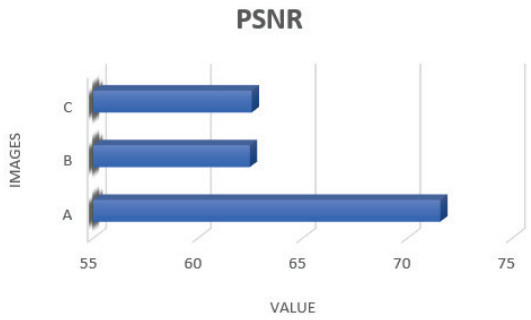

Fig. 11. Graph for PSNR

This graph represents the model's image quality accuracy based on the PSNR matrix.

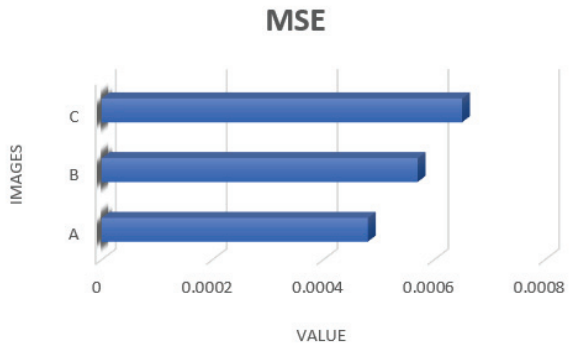

Fig. 12. Graph for MSE

This graph represents the model's image quality accuracy based on the MSE matrix.

V. CONCLUSION

The proposed method seems to provide a comprehensive approach to securing medical images by combining cryptography and steganography. The SVD approach for image compression can help to maintain image quality, while the use of AES encryption can provide confidentiality for the medical image. Furthermore, Using LSB steganography to embed the encrypted medical image into a cover image can help to conceal its presence and can add a further layer of protection. It should be noted that the effectiveness of the combined SVD and LSB steganography method in medical image hiding relies heavily on the strength of the encryption key and the robustness of the steganographic technique. Common measures that evaluate how comparable the original and reconstructed images are, including PSNR and MSE, can be used to assess the reconstructed image's quality. Three distinct kinds of medical images were used to assess the performance of the suggested approach, and each image's PSNR and MSE values were calculated.

REFERENCES

[1] G. Prashanti, B. V. Jyothirmai, and K. S. Chandana, 'Data confidentiality using steganography and cryptographic techniques', in 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2017, pp. 1–4.

[2] R. Sharma and S. Bollavarapu, 'Data security using compression and cryptography techniques', International Journal of Computer Applications, vol. 117, no. 14, 2015.

[3] A. Solichin and E. W. Ramadhan, 'Enhancing data security using DES-based cryptography and DCT-based steganography', in 2017 3rd International Conference on Science in Information Technology (ICSITech), 2017, pp. 618–621.

[4] H. Al-Ghuraify, A. A. Al-Bakry, and A. T. Al-Jayashi, 'Quaternion Security Using Modifying Vernam Cipher With Image Steganography', The International Journal of Multimedia & Its Applications (IJMA) Vol, vol. 11, 2019.

[5] M. A. Islam, M. A.-A. K. Riad, and T. S. Pias, 'Enhancing security of image steganography using visual cryptography', in 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), 2021, pp. 694–698.

[6] N. V. S. Reddy and Others, 'Improving security in Image Steganography using MSB Bit differencing and Cryptographic algorithm', in 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), 2018, pp. 228–230.

[7] D. Bhat, V. Krithi, K. N. Manjunath, S. Prabhu, and A. Renuka, 'Information hiding through dynamic text steganography and cryptography: Computing and informatics', in 2017 international conference on advances in computing, communications and informatics (ICACCI), 2017, pp. 1826–1831.

[8] K. M. Aishwarya, R. Ramesh, P. M. Sobarad, and V. Singh, 'Lossy image compression using SVD coding algorithm', in 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2016.

[9] P. Varghese and G. A. S. Saroja, 'DWT, DCT and SVD Based Hexagonal Image Compression', in 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT), Erode, India, 2021.

[10] R. Ranjan, P. Kumar, K. Naik, and V. K. Singh, 'The HAAR-the JPEG based image compression technique using singular values decomposition', in 2022 2nd International Conference on Emerging Frontiers in Electrical and Electronic Technologies (ICEFEET), Patna, India, 2022.

[11] A. H. Bentbib, K. Kreit, and I. Labaali, 'Randomized tensor singular value decomposition for multidimensional data compression', in 2022 11th International Symposium on Signal, Image, Video and Communications (ISIVC), El Jadida, Morocco, 2022.

[12] M. A. Usman and M. R. Usman, 'Using image steganography for providing enhanced medical data security', in 2018 15th IEEE Annual

Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, 2018.

[13] S. S. Yadahalli, S. Rege, and R. Sonkusare, 'Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques', in 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2020.

[14] N. Nahar, M. K. Ahmed, T. Miah, S. Alam, K. M. Rahman, and M. A. Rabbi, 'Implementation of android based text to image steganography using 512-bit algorithm with LSB technique', in 2021 5th International Conference on Electrical Information and Communication Technology (EICT), Khulna, Bangladesh, 2021.

[15] P. Subhasri, S. Santhoshkumar, A. Sumathi, C. Balakrishnan, and F. Kurus Malai Selvi, 'Efficiency enhancement using least significant bits method in image steganography', in 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2022.