International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 05 May 2024
Page No: 1447 - 1451
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0199

# A Novel Secure and Robust Encryption Scheme for Medical Videos, Images and Reports

*Riyazbanu[1], G.Venkata Kireeti[2] , D.Niranjan Reddy[3] , A.Gowtham Kumar Reddy[4], G.Vamsee Krishna[5]*
*[1]Assistant professor, Department of CSE, KSRM College of Engineering(A), Kadapa (A.P), India.*
*[2,3,4,5]IV B.Tech. Students, Department of CSE, KSRM College of Engineering(A), Kadapa (A.P), India.*
***Emails**: riyazbanu@ksrmce.ac.in[1], 209y1a0562@ksrmce.ac.in[2], 209y1a0550@ksrmce.ac.in[3], 209y1a0506@ksrmce.ac.in [4], 209y1a0555@ksrmce.in[5]*

## Abstract
*The use of medical imaging in telemedicine insurance and other applications has grown significantly in recent years. imaging techniques used in medicine, such as ultrasound, X-rays, computed tomography, and magnetic resonance imaging (MRI). plays a crucial part in the diagnosis of numerous illnesses. The internet has quickly advanced in terms of sharing and transferring large volumes of data. Medical image transmission can be impacted by a variety of attacks and medical image kinds. putting forth a medical data security strategy and outlining the various obstacles that it faces. This strategy attains a high degree of security and withstands many attacks over an extended period of time. A thorough analysis of security methods, including steganography, encryption, and compression, is presented along with a comprehensive assessment of current studies. Ensuring the security of medical images during transmission is crucial in safeguarding patient privacy. Steganography and cryptography are needed for secure transmission in order to maintain data integrity and confidentiality. An application to embed a video or audio content in another file is the project's development. Its focus is on securely and robustly embedding information under a seemingly innocent shroud. This system uses the ideas of cryptography and steganography to make the data more secure. Using an encryption technique that is resilient to various attacks over time is essential for improving the cryptography portion of the system. The paper's goal is to provide an overview and evaluation of each approach's various algorithms using several metrics, including PSNR, MSE, BER, and NC.*

***Keywords:** Steganography, Cryptography, Encryption, Decryption.*

## 1. Introduction
Steganography, derived from the Greek words "steganos" (meaning hidden) and "graphein" (meaning writing), is the art and science of concealing secret information within an innocent-looking cover medium, such as an image, audio file, or text, without arousing suspicion from unintended recipients. Unlike cryptography, which focuses on making a message unintelligible to anyone without the proper key, steganography aims to hide the existence of the message itself. The history of steganography dates back to ancient times, where methods like invisible ink, hidden messages in wax tablets, and even tattooed shaven heads were employed to convey confidential information clandestinely. In the digital era, steganography has found new applications, leveraging the vast array of multimedia formats and the complexity of digital data to embed messages imperceptibly [1]. Modern steganographic techniques involve altering the least significant bits of pixels in images, the least significant samples in audio files, or even the spacing of characters in text to encode hidden information. Advanced algorithms and encoding schemes ensure that the alterations are subtle enough to evade detection by casual observers while still allowing the concealed message to be extracted by authorized parties

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 05 May 2024
Page No: 1447 - 1451
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0199

using the appropriate decryption method or key [2]. Steganography finds applications in various fields, including covert communication, digital watermarking, and copyright protection. While it does not provide the same level of security as cryptography, steganography adds an extra layer of concealment, making it challenging for adversaries to detect the presence of hidden information. As technology continues to advance, so do the techniques and tools used in steganography, highlighting its enduring relevance in the realm of information security and covert communication. Cryptography and steganography are two fundamental techniques employed in the realm of secure communication and information protection [3]. Cryptography is the science and art of encoding messages to ensure their confidentiality, integrity, and authenticity. By utilizing various mathematical algorithms and keys, cryptography enables parties to communicate securely over insecure channels, safeguarding sensitive information from unauthorized access or tampering.On the other hand, steganography focuses on concealing the existence of a message within another medium, such as an image, audio file, or video [4]. Unlike cryptography, which alters the content of the message itself, steganography hides the message in plain sight, making it appear innocuous to unintended observers. This covert communication method has been utilized throughout history, from ancient civilizations embedding messages in wax tablets to modern digital techniques embedding data in digital images or audio files. Both cryptography and steganography play critical roles in modern-day information security, with cryptography forming the backbone of secure communication protocols and steganography offering an additional layer of concealment for sensitive data. As technology advances and threats evolve, the study and application of these techniques continue to be essential in safeguarding digital assets and ensuring privacy in an interconnected world [5].

### 1.1. Domain Description

Network image security refers to the protection of images transmitted over computer networks from unauthorized access, interception, tampering, or misuse. With the increasing reliance on digital images in various domains such as healthcare, finance, and communications, ensuring the security of these images during transmission over networks is crucial [6].

### 1.2. Importance

First and foremost, a reliable encryption scheme safeguards patient confidentiality by preventing unauthorized access to medical records [7]. Medical videos, images, and reports often contain highly personal information, ranging from diagnoses and treatment plans to sensitive imagery. Any breach in security could lead to devastating consequences, including identity theft, discrimination, or even blackmail [9]. Moreover, robust encryption enhances data integrity by protecting against tampering or alteration of medical records. In a field where accuracy is critical, ensuring that medical information remains unaltered is essential for maintaining trust between patients and healthcare providers [8]. Without proper encryption, malicious actors could potentially manipulate medical data, leading to misdiagnoses, inappropriate treatments, or compromised patient safety. Furthermore, a novel encryption scheme addresses the evolving landscape of cybersecurity threats. As technology advances, so do the tactics used by cybercriminals to breach systems and access sensitive information. By continuously innovating encryption techniques, healthcare organizations can stay ahead of these threats and adapt to new challenges in data security [10].

## 2. Architecture of the Model

This defines the working process of the project which we are designed in it. That it shows first we are going to take the cover image to cover the secret message, then we are going to take the secret message that may be a different file as the user required, that secret file will be preprocessed and that goes to the hiding network that stego

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 05 May 2024
Page No: 1447 - 1451
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0199

image will be formed means the cover image is displayed. For extraction the stego image will goes to extraction network that will process and secret file will be extracted in Figure 1.

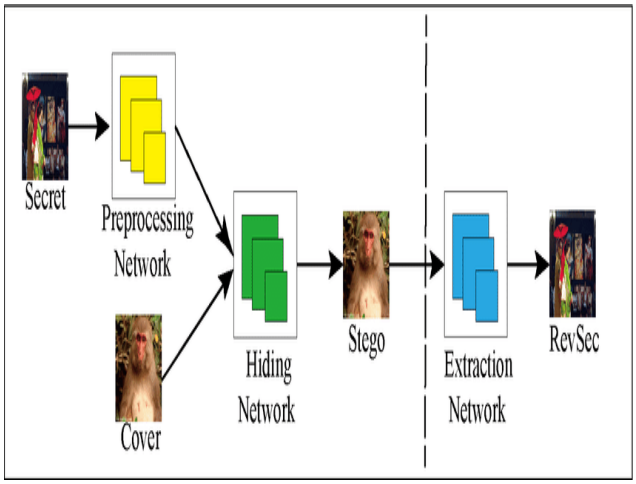


**Figure 1 System Architecture**

### 2.1.Proposed Solution

To address these challenges, we propose a novel encryption scheme designed specifically for medical videos, images, and reports. Our approach leverages a combination of cryptographic techniques, access control mechanisms, and data compression algorithms to achieve both security and efficiency. Firstly, we employ advanced encryption algorithms such as AES (Advanced Encryption Standard) to ensure robust protection of medical data against unauthorized access. Additionally, we integrate access control mechanisms based on role-based authentication, enabling fine-grained control over who can access specific types of medical information. This ensures that only authorized healthcare professionals can decrypt and view sensitive patient data. Furthermore, our encryption scheme incorporates data compression techniques optimized for medical data, reducing storage requirements and transmission overhead without compromising data integrity. By carefully selecting compression algorithms tailored to the characteristics of medical images, videos, and reports, we minimize loss of diagnostic information while maximizing efficiency. Moreover, our scheme supports secure transmission of encrypted medical data over networks, employing protocols such as SSL/TLS to safeguard against eavesdropping and tampering during data exchange. Importantly, our encryption scheme is designed with scalability and interoperability in mind, allowing seamless integration with existing healthcare IT systems and standards. This ensures compatibility with Electronic Health Record (EHR) systems, Picture Archiving and Communication Systems (PACS), and other medical information management platforms commonly used in healthcare facilities. Additionally, our solution is adaptable to various deployment scenarios, including cloud-based storage, on-premises servers, and mobile devices, catering to the diverse needs of healthcare organizations.

### 2.2. Data Flow Architecture

Another name for the DFD is a bubble chart. A system can be represented using this straightforward graphical formalism in terms of the input data it receives, the different operations it performs on that data, and the output data it generates. One of the most crucial modelling instruments is the data flow diagram (DFD). The components of the system are modelled using it. These elements consist of the system's procedure, the data it uses, an outside party that communicates with it, and the information flows within it. DFD illustrates the flow of data through the system and the various transformations that alter it. It's a visual method that shows how information moves and changes that are used in the data transfer process from input to output. The bubble chart is another name for DFD. Any level of abstraction can be utilised to portray a system using a DFD. DFD can be divided into phases that correspond to escalating functional detail and information flow in Figure 2.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 05 May 2024
Page No: 1447 - 1451
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0199

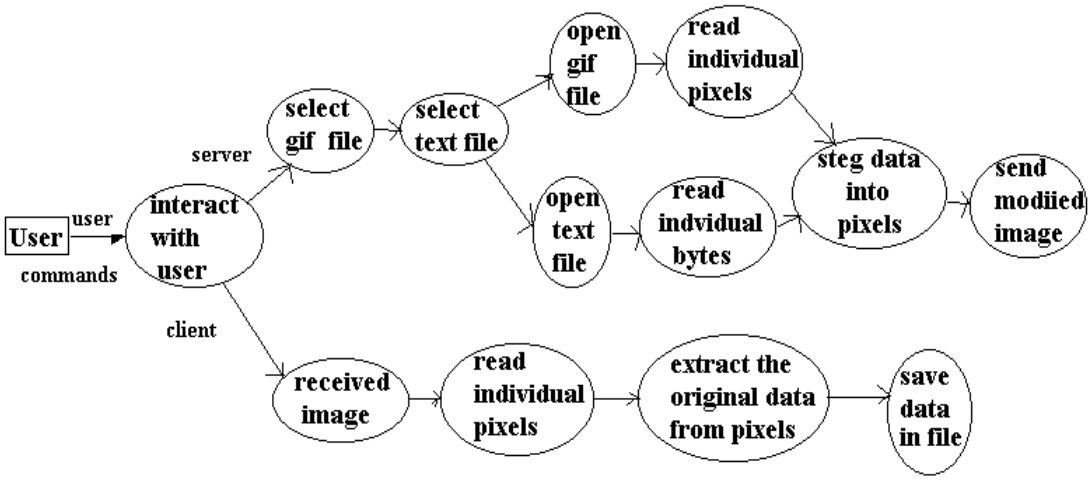


**Figure 2 DFD Architecture**

## 3. Advantages and Result

### 3.1. Advantages

- Provides all types of Files Embed and De-Embed
- Many options for users friendly with application.
- Provides Compression and File Security.
- Current Steganography is High Security

### 3.2. Result

This project has been solved by these two major concepts on Encryption and Decryption of the images that hides the sensitive data in the medical field. That scopes to enhance the data secured, tampering of the data will not be occured in this. The data of the patient will be safely secured and hided for the unknown user in the application. In this we have another option that to compress the size of the file and shws the exact size of the covered file. It embeds all types of the files and gives the high security in this proposed system.

## Conclusion

You can use steganography to communicate covertly. The theoretical and practical boundaries of steganography have been examined. We discussed how the DES and RSA techniques have been used to improve the audio and video steganographic system and offer a secure communication method. During the message's embedding, a stego-key was applied to the system. Key-based steganography is more secure than non-key steganography. This is because it is impossible for a malicious party or third party to recover the encoded message without knowing the valid key. For this reason, we employ steganography in a few of the following: concealing data on a network in the event that a network branch exists. posting confidential information online in order to prevent transmission. Integrating remedial audio and video data in case of corrosion occurs from a poor transmission

## References

[1]. Sari, Christy Atika, Giovani Ardiansyah, and Eko Hari Rachmawanto. (2019). An improved security and message capacity using AES and Huffman coding on image steganography. TELKOMNIKA, 17(5), 2400- 2409.

[2]. Sharma, N., & Batra, U. (2020). Performance analysis of compression algorithms for information security: A Review. EAI Endorsed Transactions on Scalable Information Systems, 7(27).

[3]. Jeromel, A., & Žalik, B. (2020). An efficient lossy cartoon image compression method. Multimedia Tools and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 05 May 2024
Page No: 1447 - 1451
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0199

Applications, 79(1-2), 433-451.

[4]. Adhanadi, F., Novamizanti, L., & Budiman, G. (2020). DWT-SMM-based audio steganography with RSA encryption and compressive sampling. Telkomnika, 18(2), 1095-1104.

[5]. Setyaningsih, E., Wardoyo, R., & Sari, A. K. (2020). Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution. Digital Communications and Networks...

[6]. Chai, X., Wu, H., Gan, Z., Zhang, Y., Chen, Y., & Nixon, K. W. (2020). An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding. Optics and Lasers in Engineering, 124, 105837.

[7]. Dehshiri, M., Sabouri, S. G., & Khorsandi, A. (2021). Structural similarity assessment of an optical coherence tomographic image enhanced using the wavelet transform technique. JOSA A, 38(1), 1-9.

[8]. Osama F. AbdelWahab, et al. (2019). Hiding data in images using steganography techniques with compression algorithms. Telkomnika, 17(3), 1168- 1175.

[9]. Tsai, C., Shih, W., Lu, Y Huang, J., and Yeh, L. (2019). Design of a Data Collection System with Data Compression for Small Manufacturers in Industrial IoT Environments. Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1-4.

[10]. Anand, A., Singh, A.K. (2020). An improved DWT- SVD domain watermarking for medical information security Computer Communications Volume 152, Pages 72-80.