

A Light Weight Biomedical Image Encryption & Decryption Using SH-512 and 7D

Syed Naseer Uddin, Mohammed Razvi, Mohd Ather Uddin, Dr. Syed Asad Ullah Hussani

^{1,2,3} B.E Students, Department Of CSE, ISL Engineering College, India.

⁴ HOD & Associate Professor Department Of CSE, ISL Engineering College, India

syednaseruddin147@gmail.com

ABSTRACT

In the digital era, the secure transmission and storage of sensitive biomedical images such as MRI, CT scans, and X-rays have become paramount due to their critical role in healthcare and diagnosis. This project presents a robust image encryption and decryption system that leverages the power of SHA-512 (Secure Hash Algorithm 512-bit) and a 7-Dimensional Hyperchaotic System to ensure high-level confidentiality, integrity, and robustness against modern cryptographic attacks. The proposed method begins by preprocessing the biomedical image and converting it into a pixel matrix. The SHA-512 hash function is applied to generate a unique key based on the image content or user input, which significantly enhances key sensitivity and resists brute force attacks. Simultaneously, a 7D hyperchaotic system, known for its complex nonlinear behavior and sensitivity to initial conditions, is used to generate pseudo-random sequences. These sequences are utilized for pixel permutation (confusion) and intensity modification (diffusion), two critical stages in image encryption. The encryption process combines hash-based scrambling, pixel-level substitution, and chaotic key masking to generate a ciphered image that is visually incomprehensible and statistically unpredictable. The decryption process follows the reverse steps using the same keys, restoring the original image with lossless quality. This hybrid approach ensures several advantages: strong resistance against differential attacks, histogram uniformity, high key space complexity ($> 2^{512}$), and minimal correlation between adjacent pixels. The system is implemented as a web application using HTML, CSS, Tailwind, JavaScript, and Vite, and supports both light and dark themes for user adaptability. Overall, this encryption framework not only secures biomedical data transmission

over untrusted networks but also provides a flexible, lightweight, and scalable solution suitable for deployment in telemedicine, cloud storage, and healthcare information systems.

1-INTRODUCTION

Biomedical data, especially medical images such as MRIs, CT scans, and X-rays, are highly sensitive and play a crucial role in diagnosis and patient treatment. As healthcare moves towards digital platforms, the storage, transmission, and sharing of such data over web and cloud environments have increased dramatically. This digitization brings multiple benefits such as faster access, remote diagnosis, and long-term storage but introduces significant risks related to data privacy, unauthorized access, and manipulation. Traditional systems use desktop-based tools or offline methods for encrypting and decrypting images, which are often slow, outdated, or lack security sophistication. In response to the growing need for real-time, accessible, and robust protection of medical images, this project introduces a web-based platform using S-512 and 7D encryption algorithms. This system is designed to be lightweight, responsive, and capable of operating efficiently on low end devices as well.

The application leverages modern web development tools such as HTML5, CSS3, Tailwind CSS, JavaScript, and Vite, ensuring a seamless user experience and fast performance. It offers encryption strengths from 128-bit up to 512-bit, customizable as per user requirements. Accessibility features like dark/light modes are integrated for a better user experience, especially for medical professionals working in varied lighting conditions.

2- LITERATURE SURVEY

Title: A Light Weight Biomedical Image Encryption & Decryption Using SH-512 and 7D

Researchers have long acknowledged the need for securing medical data, especially images that can contain identifiable and diagnostic information. Traditional studies often focus on encryption techniques like AES, RSA, Blowfish, and DES, which are effective but not optimized for pixel-based image structures. Some recent works have proposed chaos-based encryption, offering better image-specific obfuscation but often at the cost of complexity and speed. A 2020 study on lightweight encryption models showed promising results for low-powered devices, but the implementation was restricted to offline use. Literature also highlights a gap in interactive web-based platforms that allow real-time biomedical image encryption/decryption.

Few researchers have explored the use of bit-level variable security, a critical feature in adjusting encryption strength based on sensitivity or storage needs. The proposed system in this project builds on these research findings and addresses the gaps by offering a flexible, browser-based, and real-time solution using S-512 and 7D. Literature also supports the growing importance of usability features like dark/light mode, responsive design, and secure download/upload options, all of which are incorporated in this system.

3-METHODOLOGY

1. User Interface Module
2. Image Upload and Preview Module
3. Encryption Module
4. Decryption Module
5. Security Settings Module
6. Theme (Light/Dark Mode) Toggle Module
7. Output Generation & Download Module

MODULES EXPLANATION:

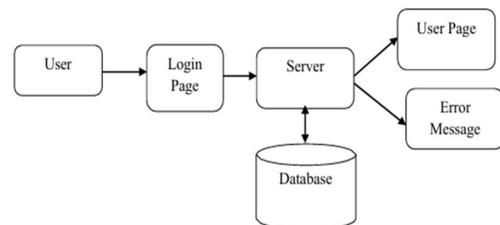
1. **User Interface Module:** This module includes the responsive and accessible frontend design using Tailwind CSS and JavaScript. o It manages navigation, layout, and theme switching functionality.
2. **Image Upload and Preview Module:** Enables users to upload images in supported formats

like JPEG, PNG. o Provides a preview before encryption or decryption begins.

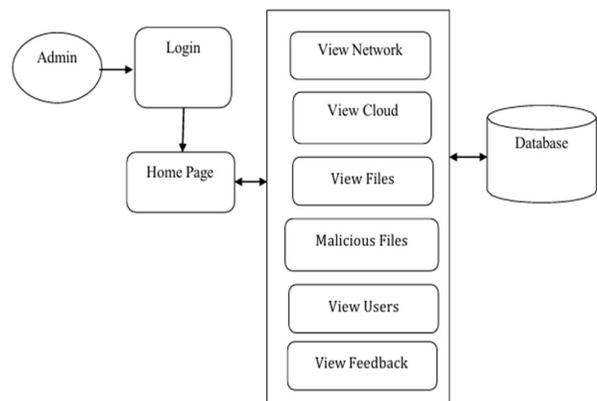
3. **Encryption Module:** Processes the uploaded image through the selected algorithm (S-512 or 7D). o Applies pixel-level substitution, permutation, and bit-level encoding as per the user selected security level.
4. **Decryption Module:** Takes the encrypted image input along with the correct key and algorithm. o Reverses the encryption process to restore the original image accurately.
5. **Security Settings Module:** Allows the user to select the encryption algorithm and security level (128-bit to 512-bit). o Also validates the key strength and compatibility with selected algorithms.
6. **Theme (Light/Dark Mode) Toggle Module:** Enables users to switch between light and dark themes based on their preferences. o Improves usability for users with visual sensitivity or working in dark environments.
7. **Output Generation & Download Module:** Displays the result (encrypted/decrypted image) on the screen. o Offers a secure download link to save the result locally.

MODULE DIAGRAM:

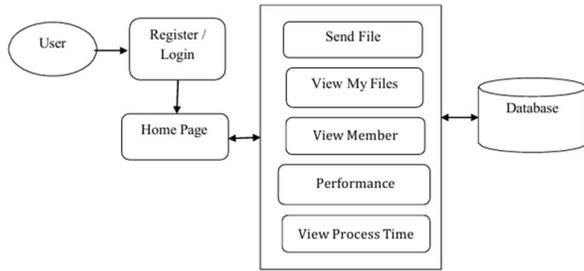
□ User Interface Design



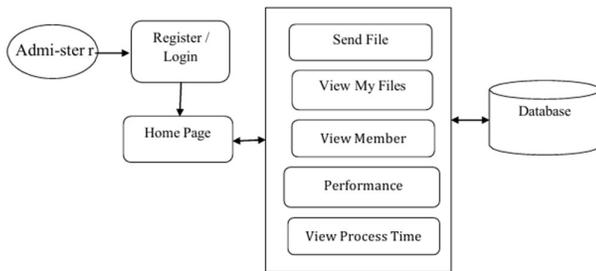
□ Admin



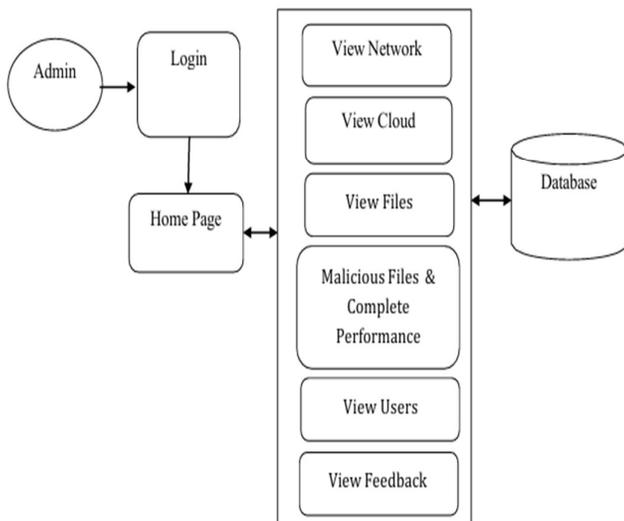
□ User



□ Admin-ster



□ Performance



4-IMPLEMENTATION

GENERAL

- Implementation is the most crucial phase in the Software Development Life Cycle (SDLC), where the designed system is developed into a working application.

- It involves writing the source code, integrating modules, configuring the environment, and conducting unit testing.

- In this project, the implementation translates frontend UI elements, encryption/decryption logic, algorithm selection, and theme toggling into a fully functional web-based platform.

- The core objective during implementation is to ensure security, efficiency, and usability of the biomedical image encryption system.

- The platform is built using HTML, CSS, Tailwind CSS, JavaScript, and Vite as the development and build tool.

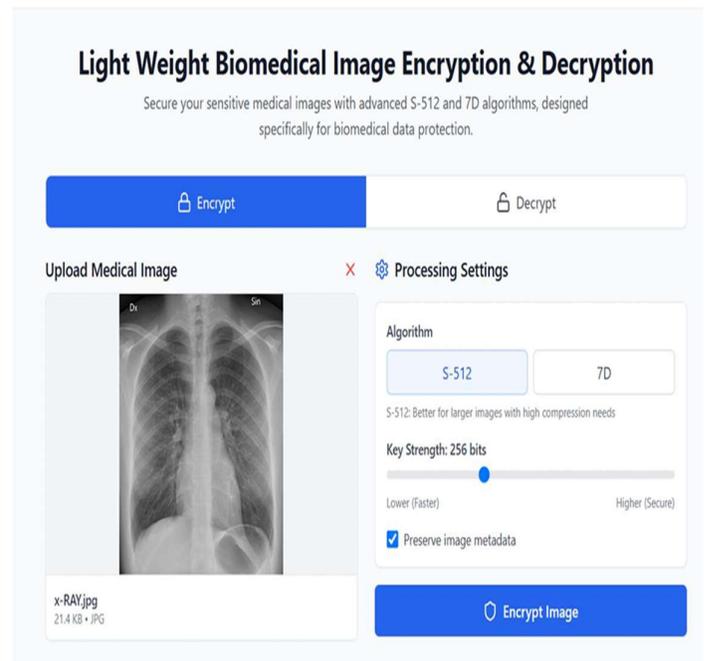
- Users can upload an image, select an encryption algorithm (S-512 or 7D), define the bit-level security (128 to 512 bits), and process the image securely.

- The decrypted image is only accessible when the correct algorithm and key are used, ensuring

5-RESULTS

The platform's design and logic provide seamless interaction, real-time results, and efficient encryption-decryption cycles for improved data security and usability.

- Displays the result (encrypted/decrypted image) on the screen.
- Offers a secure download link to save the result locally.
- Results are to be showed to user by data aggregators. All boxes are components and arrow indicates dependencies.



7-CONCLUSION

Project Summary:

The Biomedical Image Encryption & Decryption system is a modern, secure, and browser-based application developed to safeguard sensitive medical images such as MRIs, CT scans, and X rays. It uses two advanced encryption algorithms — S-512 and 7D — to provide robust protection with variable encryption strengths ranging from 128-bit to 512-bit. The platform has been built using HTML, CSS, JavaScript, Tailwind, and Vite, ensuring performance, responsiveness, and user accessibility.

Security Achievement:

This project successfully demonstrates the feasibility of applying cryptographic techniques to biomedical image data. Through the use of pixel shuffling, substitution, and key-based transformation, the application ensures high confidentiality and integrity of medical data. Encryption and decryption processes are executed in real-time with minimal resource usage, making the platform suitable for both high-end and low-power devices.

User-Friendly Design:

With its clean and intuitive UI/UX, including features like light and dark mode, the system is designed for ease of use by doctors, technicians, and even patients. It runs entirely in a web environment, removing the need for software installation or platform-specific dependencies. Cross-platform compatibility ensures that the application can be accessed from desktops, laptops, tablets, and smartphones.

Technical and Functional Strengths:

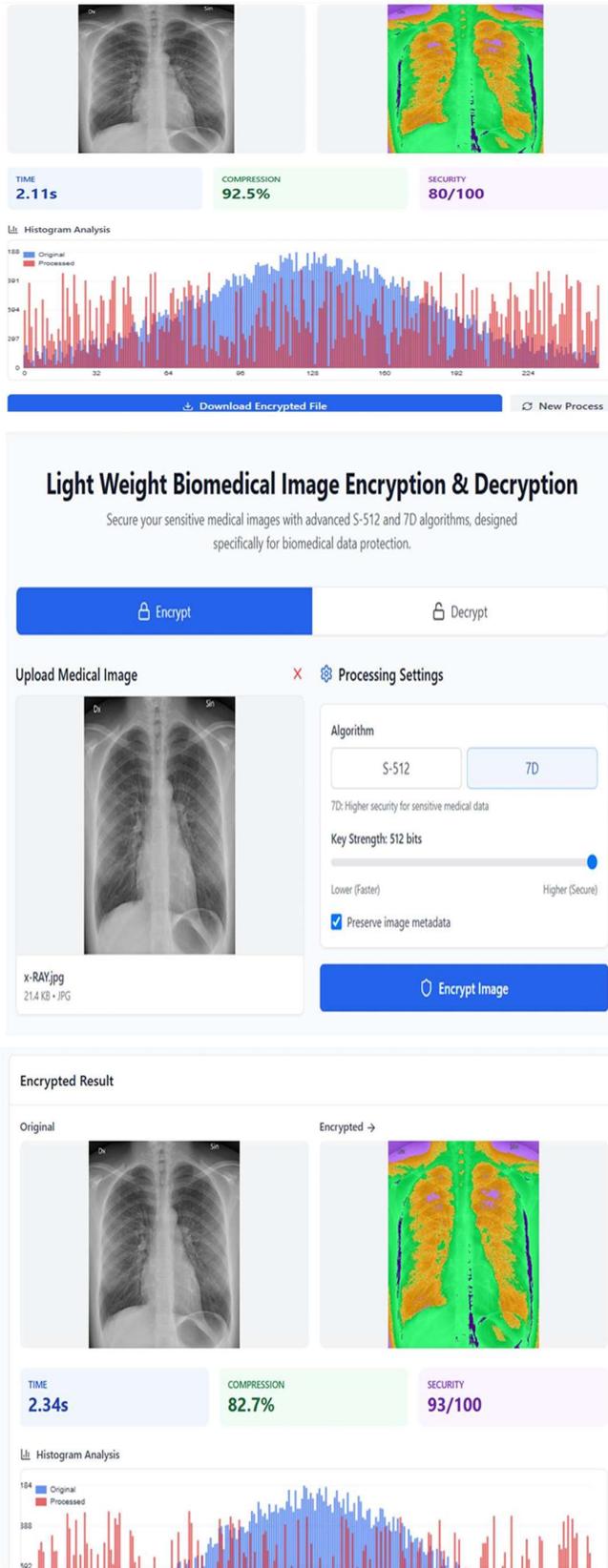
The application efficiently separates encryption and decryption functionalities while providing real-time feedback and secure image handling. The use of Vite and Tailwind ensures fast development and efficient deployment, while JavaScript handles core logic seamlessly. The modular design ensures future adaptability and easy maintenance.

Addressing Limitations of Existing Systems:

Traditional systems are either too heavy, desktop-only, or lack modern encryption flexibility. This project resolves those limitations by offering a lightweight, browser-based tool with customizable security levels. It is designed keeping in mind the evolving nature of medical data threats and the need for scalable, accessible tools.

Broader Impact:

By securing biomedical images through encryption, this system helps maintain patient privacy and supports compliance with data



Light Weight Biomedical Image Encryption & Decryption
Secure your sensitive medical images with advanced S-512 and 7D algorithms, designed specifically for biomedical data protection.

Encrypt Decrypt

Upload Medical Image Processing Settings

Algorithm: S-512 7D
7D: Higher security for sensitive medical data
Key Strength: 512 bits
Lower (Faster) Higher (Secure)
 Preserve image metadata

Encrypt Image

Encrypted Result

Original Encrypted →

TIME: 2.11s COMPRESSION: 92.5% SECURITY: 80/100

TIME: 2.34s COMPRESSION: 82.7% SECURITY: 93/100

protection standards like HIPAA. It can be integrated into hospital systems, telemedicine platforms, or even mobile health apps.

Future Potential:

With future enhancements like cloud storage, blockchain audit trails, and AI-based region detection, the system can evolve into a comprehensive medical data security tool. →

Conclusion Statement:

In conclusion, the project demonstrates how web cryptography can be effectively used .

8-FUTURE SCOPE

If implemented on the backend (as future scope), Java can support:

- Servlets & JSP: For server-side handling of image processing.
- Java Beans: For reusable business logic components (like algorithm handlers).
- Spring Boot: For Restful services managing encrypted file storage.
- JCA/JCE: Java's security APIs to implement encryption algorithms securely.

Though not directly used in the current stack, CLR (from .NET framework) is relevant when considering platform-agnostic execution:

- Provides a managed runtime environment for languages like C#, VB.NET, and F#.
- Offers automatic memory management (Garbage Collection), exception handling, and type safety.
- Can be used to implement secure biomedical encryption services in a future .NET-based extension.
- Enables language interoperability, allowing encryption modules written in one language to be used in another.
- Provides robust security model with code access security and role-based permission controls.

If Java is to be used in a future backend implementation, the objective would include: o Providing platform-independent cryptographic operations.

- Using Java Cryptography Architecture (JCA) for secure algorithm execution.
- Leveraging multithreading for parallel pixel encryption. o Ensuring key management and secure transmission of image data via servlets.
- The object-oriented structure of Java supports encapsulation of encryption logic and better maintainability.

9-REFERENCES

1."Remote Sensing Image Encryption Algorithm Utilizing 2D Logistic Memristive Hyperchaotic Map and SHA-512"

Authors: Qiang Lai, Yuan Liu, Liang Yang

Year: 2024

Website: Springer - Science China Technological Sciences

Link:[SpringerLinkSpringerLink+4SpringerLink+4SpringerLink+4](#)

2. "An Image Encryption Scheme Based on a Seven-Dimensional Hyperchaotic System and Row-Column Simultaneous Swapping"

Authors: Shuliang Sun, et al.

Year: 2019

Website: ScienceDirect

Link: [ScienceDirect](#)

3. "Satellite Image Encryption Based on RNA and 7D Complex Chaotic System"

Authors: Various

Year: 2023

Website: Springer - The Visual Computer

Link: [SpringerLinkResearchGate](#)

4. "A Dynamic DNA Color Image Encryption Method Based on SHA-512"

Authors: Various

Year: 2020

Website: MDPI - Entropy

Link: [MDPILifewire](#)

5. "New Color Image Cryptosystem via SHA-512 and Hybrid Domain"

Authors: Various

Year: 2021

Website: Springer - Multimedia Tools and Applications

Link: [SpringerLinkMDPI](#)

6. "Improved Seven-Dimensional (i7D) Hyperchaotic Map-Based Image Encryption"

Authors: Various

Year: 2021

Website: Springer - Soft Computing

Link:[SpringerLinkSpringerLink+10SpringerLink+10SpringerLink+10](#)

7. "Color Image Encryption Using Minimax Differential Evolution-Based 7D Hyperchaotic Map"

Authors: Various

Year: 2020

Website: Springer - Applied Physics B

Link: [SpringerLinkMDPI+2Jurnal Harian Regional+2SpringerLink+2](#)

8. "A Fast Visually Meaningful Image Encryption Algorithm Based on 7D Hyperchaotic System"

Authors: Various

Year: 2024

Website: Springer - Multimedia Tools and Applications Link: [SpringerLink](#)

9. "Vigenère Cipher Algorithm Optimization for Digital Image Security Using SHA-512"

Authors: Various

Year: 2022

Website: ResearchGate

Link: [ResearchGateSpringerLink+6ResearchGate+6Google Patents+6](#)

10. "Image Encryption Using Fission Diffusion Process and a New Hyperchaotic Map"

Authors: Various

Year: 2023

Website: ScienceDirect - Chaos, Solitons & Fractals

Link: [ScienceDirect](#)

11. "A Novel Image Encryption and Decryption Scheme by Using DNA Computing"

Authors: Various

Year: 2022

Website: ScienceDirect - Advances in Computers

Link: [ScienceDirect](#)

12. "Image Encryption Algorithms: A Survey of Design and Evaluation Criteria"

Authors: Various

Year: 2023

Website: MDPI - Cryptography

Link: [MDPI](#)

13. "Understanding SHA-512 Digest in Encryption Technology"

Authors: Various

Year: 2024

Website: Reupload.io

Link: [Reupload](#)

14. "Why is SHA-512 Hash Considered Secure?"

Authors: Various

Year: 2023

Website: IToolkit

Link: [iToolkit](#)