Grenze International Journal of Engineering and Technology, June Issue

Enhancing Security of the Healthcare Sector using Visual Cryptography

Dharshini M[1], Kavitha T[2] and Ancy Jenifer J[3]
[1-3]Karunya Institute of Technology and Sciences, Coimbatore, India
Email: dharshinim@karunya.edu.in, kavithat@karunya.edu, ancyjenifer@karunya.edu

***Abstract*—A novel use of visual cryptography is to ensure safe bio-metric authentication in the healthcare industry. The necessity for strong authentication techniques is due to the growing digitization of records and the growing reliance on electronic health systems. There are now a lot of obstacles because of security and privacy issues with conventional bio-metric authentication techniques.Visual cryptography can be done using many algorithms for image encryption. This paper presents a method to encrypt images using two main encryption algorithms: the Advanced Encryption Standard and the Shamir Secret Sharing Scheme. AES, a widely used symmetric encryption algorithm, provides high security by converting plain text to ciphered text using a key which is symmetric. By using the Shamir algorithm, the system creates and saves encrypted images using visual cryptography. In the health care industries, biometric samples are presented as part of the authentication procedure; these samples are divided into shares and encrypted. The shares are subsequently given to the healthcare professionals, who authenticate patients using their unique shares and the help of the central server. By preventing the disclosure of any critical information to a single party, the visual cryptography technology reduces the possibility of data breaches.**

***Index Terms*— bio-metric authentication, healthcare sector, visual cryptography, security, privacy, advanced encryption, central server, sensitive information, data breaches.**

I. INTRODUCTION

A Safe Encryption System for the Healthcare Industry is needed in order to improve the authentication procedures in the healthcare industry. To guarantee the safety and security of sensitive patient information, Visual cryptography is a novel and extremely safe technique. Sensitive data can be encrypted using visual cryptography and shared in a way that can only be unlocked by combining certain elements. Because it can offer strong and safe authentication procedures, this approach has drawn more interest in the data security community. Strong encryption technologies are essential to ensure the privacy and integrity of that data. Among the set of available encryption algorithms, the Advanced Encryption Standard (AES) stands out for its strong and robust symmetric encryption, suitable for protecting many types of data, including images. In addition to AES, the Shamir project has a secret encryption that uses a private key. It's a simple way to share encryption keys with multiple parties without revealing them. This scheme divides a secret, such as an encryption key, into multiple shares and distributes them to authorized parties. This approach reduces the risk of single-point vulnerabilities and makes key management more secure.

In AES method of encryption, we introduce a user interface designed to encrypt uploaded images using AES

Grenze ID: 01.GIJET.10.2.593

encryption and enable users to download the decrypted images using keys. Through this interface, users can upload their images securely and easily, and during encryption, receive encrypted versions for safe storage or transmission. Also, the interface provides a seamless experience for decryption, allowing users to download their decrypted images using the corresponding keys, thus ensuring confidentiality and integrity throughout the process. Additionally, the Shamir Scheme is implemented for encrypting medical images of patients by dividing them into a specified number of shares, further enhancing the security of image data. In this method, we also extend the encryption capability of our system to include all types of biometric sample images such as fingerprint samples of patients, ensuring the secure transmission and storage of sensitive biometric data.
By understanding the working advanced encryption standard encryption and the Shamir algorithm, and visual cryptography principles into this user interface, a comprehensive solution for secure image encryption and decryption for images, as well as secure handling of biometric samples of registered patients. When compared to conventional authentication techniques, this strategy has a huge benefit. Using visual cryptography adds another degree of protection. The solution makes sure that even in the event that one share is compromised, it remains ineffective without the other shares by encrypting the bio-metric data samples or images. This considerably lowers the possibility of unwanted access and data breaches. To summarize, using these two algorithms, visual cryptographic technique can be implemented with ease and patient's data can be easily stored and accessed only by the authorized users.

II. Related Works

Kalubandi et al. [1] proposed a secure method for image encryption using AES algorithm and visual cryptographic techniques. First, the images are encrypted using the AES algorithm and for conversion of keys into shares visual cryptographic scheme is implemented. The Cryptanalysis is performed to prove the security of the proposed method. This method is implemented using the programming language python.
Dalia Alsaffar et al. [2] performed a comparative analysis of two major cryptographic algorithms. Here, the AES algorithm and RSA algorithm were chosen for the image encryption process, and their performance was examined. The AES algorithm produces better encryption quality of images and the RSA algorithm coefficient tends to be closer to zero value, providing a stronger correlation
Rajangam et al.[3] proposed a medical secure image encryption technique that generates biokeys based on distance metrics, providing robust security measures for healthcare data. One potential limitation is the need for accurate distance metrics, which may be challenging to define for some medical images.
Castro, Impedovo, and Pirlo [4] developed a secure scheme for encryption of medical images, particularly focusing on secure fingerprint-based transmission in healthcare environments. A limitation could be the reliance on fingerprint data, which may not always be available or reliable.
Zhang, Ren, Shafiq, and Gu [5] introduced a privacy protection framework for security of medical image without dependency on key, combining visual cryptography and trusted computing to secure sensitive medical data. A limitation may be the reliance on trusted computing hardware, which may not be universally available.
Shammi et al. [6] presented an optimized shares creation and visual cryptography technique to secure bio- metric data effectively. Possible limitations include the need for careful optimization and the potential loss of bio-metric information during the encryption process.
Liu et al. [7] proposed a novel spatiotemporal chaos model and DNA computing approach for encrypting multiple medical images, ensuring high-level information security. A limitation could be the complexity and resource requirements of spatiotemporal chaos modeling.
El-Shafai, Khallaf, El-Rabaie, and Abd El-Samie [8] introduced a cryptography framework for medical image based on deep extracted features using neural auto-encoders, enhancing security in smart IoT healthcare applications. Limitations may include the need for extensive labeled data for training and potential overfitting.
Lata and Cenkeramaddi [9] provided a comprehensive review of deep learning applications in medical image cryptography, summarizing key advancements in this field. The review itself does not have specific limitations, but the applicability of deep learning methods may vary depending on the available data.
JADDOA and Kurnaz [10] explored the critical role of cybersecurity in image encryption, emphasizing its significance in safeguarding sensitive healthcare data from potential threats. The limitations may depend on the specific cybersecurity measures discussed in the paper.

III. Proposed Methodology

Security and privacy issues are brought up by the transmission and storage of images such as fingerprint samples, iris scans, and so on. Adding visual cryptography to the bio- metric identification procedure can offer another degree of protection,type of encryption or message can be split up into several portions and given to several people. Taken as a whole, these shares can unlock the concealed knowledge, but taken separately, they reveal nothing about the original secret. Individuals' bio-metric characteristics would be gathered and transformed into bio-metric templates in this proposed study, which would thereafter go through visual cryptography. The resultant shares will be safely sent to various healthcare-related organizations, including clinics, hospitals, and insurance providers. Once the person has been authenticated, these entities can pool their shares to recreate the original bio-metric template and confirm the person's identity. The bio-metric data is secured during storage and transmission thanks to the use of optical cryptography, reducing the possibility of unwanted access. These algorithms ensure a safe and successful identification process by more efficiently analyzing and comparing bio-metric characteristics. In general, By fusing bio-metric authentication methods, it aims to improve security, privacy in the healthcare sector. The suggested effort has the potential to transform the authentication procedure and advance the creation of safe healthcare systems.

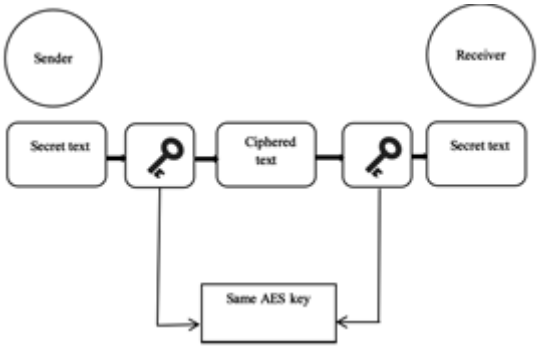

Fig 1: Advanced encryption standard architecture

Module 1: Acquisition and Processing of Biometric Data: The goal of this module is to collect bio-metric information from people working in the healthcare industry. Fingerprints, face photos, and retinal scans are just a few examples of the data that the system will record and collect. Accurate data collection may necessitate specialized technology and sensors.This module will examine the accuracy and reliability of the gathered data after receiving the bio-metric data. To guarantee accurate authentication results, it will assess elements including picture resolution, clarity, and uniqueness.

Module 2: Encryption and Visual Cryptography:

To encrypt the bio-metric templates, this module uses method, use visual possible to split a secret image or template into several shares, each of which retains all of the original data's content. As a result of the shares' distribution among many organizations, reconstruct data combination of these encryption keys needed safe the biometric are managed by this module. It makes certain that the keys are handled, transferred, and kept safely to thwart tampering and unwanted access.

Module 3: Confirmation and Decryption:

Using the encrypted bio-metric templates, this module manages the real authentication procedure. During the authentication attempt, retrieved bio-metric data. To ascertain if the stored and input bio-metric features are similar or dissimilar, a variety of matching methods and techniques are used. This module assesses the authenticity of the person trying authentication based on the comparison results. It uses decision-making algorithms to determine whether the bio-metric data is valid and to give or refuse access based on that determination.

IV. Results and Discussions

Using AES, an interface is launched using streamlit to encrypt the patient images and download the decrypted images. The encrypted image cannot be accessed easily unless correct key values are chosen and entered by the user who is trying to access the patient’s data. The signup page, login option, the dashboard interface is added to the interface before the encryption and decryption.

TABLE I. LIST OF ALGORITHMS USED

S.No	Encryption Algorithm	Work Done	Data used
01	Advanced encryption standard	Interface of encryption and decryption	Patient medical images
02	Shamir secret scheme	Harris corner detection to capture key points	Images and Fingerprint samples

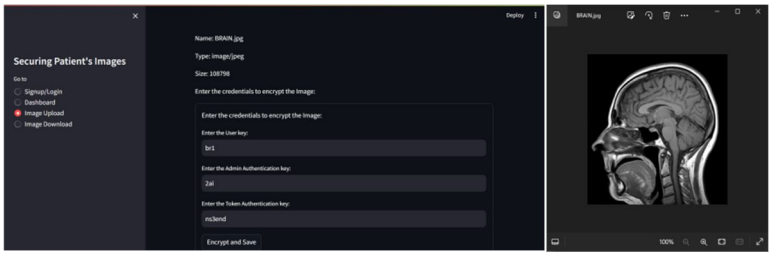

Fig.2. AES Encrytion of a patient's image

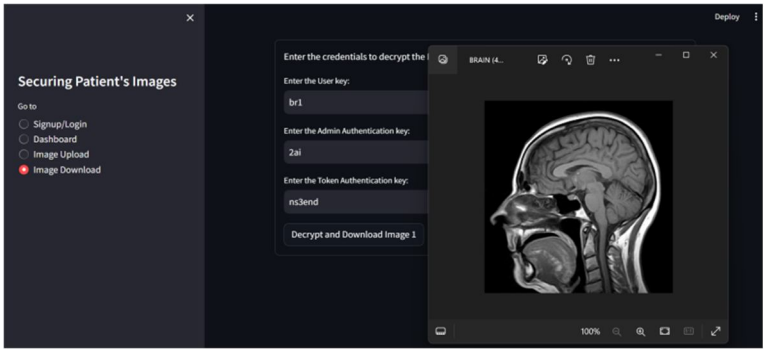

Fig.3. AES Decryption of the image

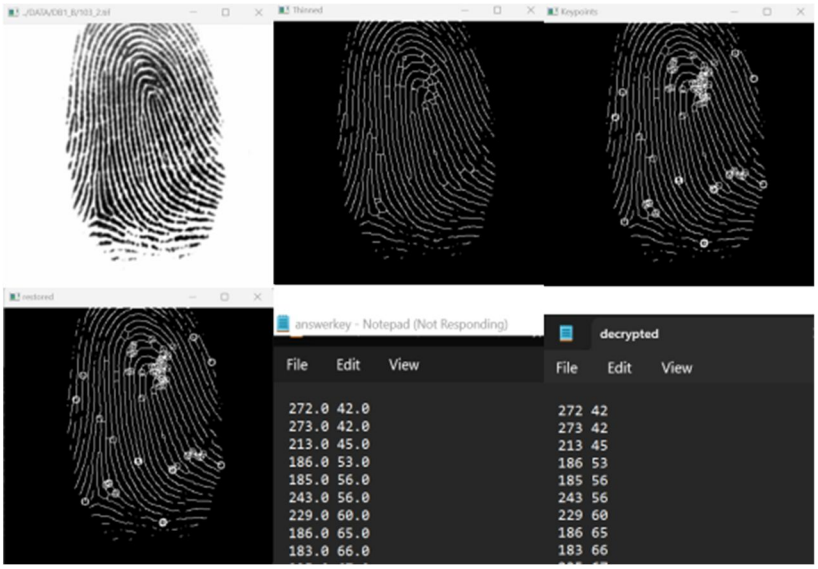

Fig.4. Encryption of a patient's fingerprint sample

Using Shamir scheme, during encryption of a patient's sample biometric data like fingerprint samples, here the keypoints are captured to retrieve the original image and values are written to answerkey and decrypted key files and stored.

V. Conclusion

In conclusion, the healthcare industry can reap a number of significant advantages by deploying a safe bio-metric authentication system that leverages visual cryptography. This system uses bio-metric authentication approaches that are distinct and challenging to counterfeit, which successfully answers the growing concerns over data security and privacy in the healthcare industry. By dividing the bio-metric template into pieces and making sure that the original template is not kept or transmitted, the use of visual cryptography provides an extra degree of protection.

Upcoming Projects

To protect patient privacy and confidentiality, the healthcare industry needs a reliable bio-metric authentication solution. This research suggests a new method for bio-metric authentication in healthcare called Visual Cryptography (VC). Through the use of VC, a cryptographic technology, confidential information can be encrypted and shared among several people in the form of shares. Patients' bio-metric information, such as fingerprint or iris scans, is divided into shares and encrypted using VC in this system. Then, in order to guard against unwanted access, these shares are kept apart in various databases. The time complexity can be dealt with in upcoming works for faster encryption than the proposed work, in such a way that even if shares are increasing, the time taken to encrypt should be less than now.

References

[1] Kalubandi, V., Vaddi, H., Ramineni, V., & Loganathan, A. (2016). A novel image encryption algorithm using AES and visual cryptography. 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), 808-813.

[2] Alsaffar, D., Sultan Almutiri, A., Alqahtani, B., Alamri, R., Fahhad Alqahtani, H., Alqahtani, N., Mohammed alshammari, G., & Ali, A.A. (2020). Image Encryption Based on AES and RSA Algorithms. 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), 1-5.

[3] Rajangam, V., Kumar, S. S., Narayanan, S., Sangeetha, N., & Avudaiammal, R. (2022). Medical Image Encryption Using Distance-Based Biokey Generation. In Aiding Forensic Investigation Through Deep Learning and Machine Learning Frameworks (pp. 195- 218). IGI Global.

[4] Castro, F., Impedovo, D., & Pirlo, G. (2023). A Medical Image Encryption Scheme for Secure Fingerprint-Based Authenticated Transmission. Applied Sciences, 13(10), 6099.

[5] Zhang, D., Ren, L., Shafiq, M., & Gu, Z. (2023). A Privacy Protection Framework for Medical Image Security without Key Dependency Based on Visual Cryptography and Trusted Computing. Computational Intelligence and Neuroscience, 2023.

[6] Shammi, L., Shyni, C. E., Nisa, K. U., Bora, R. K., & Saravanan, S. (2022, December). Securing Biometric Data with Optimized Share Creation and Visual Cryptography Technique. In 2022 6th International Conference on Electronics, Communication and Aerospace Technology (pp. 673-679). IEEE.

[7] Liu, H., Teng, L., Zhang, Y., Si, R., & Liu, P. (2024). Mutil-medical image encryption by a new spatiotemporal chaos model and DNA new computing for information security. Expert Systems with Applications, 235, 121090.

[8] El-Shafai, W., Khallaf, F., El-Rabaie, E. S. M., & Abd El-Samie, F. E. (2022). Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications. Neural Computing and Applications, 34(13), 10629- 10653.

[9] Lata, K., & Cenkeramaddi, L. R. (2023). Deep learning for medical image cryptography: A comprehensive review. Applied Sciences, 13(14), 8295.

[10] JADDOA, A. A. J., & Kurnaz, S. (2023). Cyber Security Role in Image Encryption. Intent Research Scientific Journal, 2(7), 20-44.