PixSecure: A Lightweight Medical Image Encryption System Using Feature-Based Key Generation

Afham Akram Hasan[1], Mohammad Hisham Hasan[1], Mohammed Nihal[1], Mohammed Sinan[1], Fathimath Raihan[1], and Fathimath Raihan

Department of Computer Science and Engineering, P A College of Engineering, 574153, Mangalore

E-mail:

Abstract

The shift to digital in healthcare has caused widespread sending and storing of sensitive medical pictures making data privacy a key worry. This paper introduces PixSecure, a light encryption system made to protect medical images using a feature-based encryption method. It uses Sobel edge detection to pull out structural features from grayscale images to create strong encryption keys. These keys pass NIST randomness tests, which shows they have high cryptographic strength. PixSecure uses XOR-based encryption with these keys, which leads to effective and secure protection of sensitive data. The system's performance is checked using measures like entropy, correlation, NPCR, and UACI. The outcomes show the system can keep image quality high while ensuring strong security making it a good choice for real-world healthcare settings.

ISBN:97881-19905-39-3

1 Introduction

Digital tech plays a big role in how healthcare systems store, send, and look at medical info these days. As more doctors use online visits and cloud storage patient files, including detailed medical pictures, face more online dangers than before. If someone gets into this private info without permission, it can cause problems beyond just privacy. It can lead to legal issues and make people lose faith in healthcare systems. Old-school coding methods like AES and RSA keep things safe, but they need a lot of computer power. This makes them hard to use for real-time tasks in places with few resources, like country clinics or portable testing tools. Also, these methods don't take advantage of how images are built.

PixSecure tackles this problem by mixing image handling tricks with coding logic. It uses Sobel edge detection to zero in on key parts of medical images. This helps PixSecure make coding keys that don't need much power but still stand up to attacks based on analysis. Using XOR coding also helps make it fast and simple. This means it can fit into current healthcare systems without slowing things down much.

2 Literature Review

Many scientists have tried to protect image data using different methods. Chaos maps have gained popularity for image scrambling and encryption because they're sensitive to starting conditions. But their unpredictability often makes them hard to reverse engineer, which limits their use in regulated fields like healthcare. Edge-based encryption is a newer approach that uses structural features from images to create cryptographic material. Research shows that features extracted by edge detection algorithms like Sobel and Canny are less redundant and work better for key generation. In a study by [2.] Zhang et al. (2021), the researchers used a mix of edge detection and logistic map techniques. This improved randomness but was slow with larger image datasets. Also cryptographic standards suggest using statistical randomness tests to check the quality of generated keys.

ISBN:97881-19905-39-3

The NIST Statistical Test Suite is still the best way to evaluate cryptographic key integrity. Systems that fail these tests tend to have patterns and become predictable making them weak against brute-force and statistical attacks. PixSecure's use of NIST-approved metrics ensures it meets modern encryption standards while staying flexible.

3 Methodology

3.1 Data Acquisition

Medical images were sourced from publicly available datasets, such as those on Kaggle and NIH repositories. These include X-ray and other radiological scans in formats like PNG, JPEG, and BMP.

3.2 Preprocessing

Each image is converted to grayscale to reduce computational load and standardize input. Subsequently, Sobel edge detection is applied to extract the primary contours and shapes of the medical scan.

3.3 Key Generation

-The edge-detected image is transformed into a binary 2D array.

-This array is divided into 3x3 windows, converting each to an integer (0-511).

-These integers are sequentially arranged in a 1D array.

-Adjacent values are averaged, and the result is converted into a binary stream, which forms the encryption key.

-The key undergoes[1] NIST randomness testing to ensure it meets cryptographic standards.

ISBN:97881-19905-39-3

3.4 Encryption

The final binary key is XORed with the edge-detected image to produce the encrypted image. This XOR-based process ensures simplicity while maintaining robust protection.

3.5 Decryption

Decryption is the reverse of the encryption process, using the same key to retrieve the original grayscale image with no perceptual loss or distortion.

3.6 Performance Evaluation

The system is tested using the following metrics:

-Entropy – to measure the randomness of the encrypted image

-Correlation – to verify low similarity between adjacent pixels

-NPCR (Number of Pixels Change Rate) – to measure sensitivity to pixel changes

-UACI (Unified Average Changing Intensity) – to determine average intensity deviation

4 Results show that PixSecure performs comparably or better than traditional encryption systems.

5 Results and Discussion

PixSecure was evaluated across various image sizes and resolutions.

-Entropy values approached the ideal score of 8, indicating high randomness.

-NPCR and UACI values exceeded standard thresholds (>99% and >30% respectively), confirming strong sensitivity to pixel-level changes.

-Correlation coefficients were close to zero, suggesting minimal pixel similarity in encrypted images.

ISBN:97881-19905-39-3

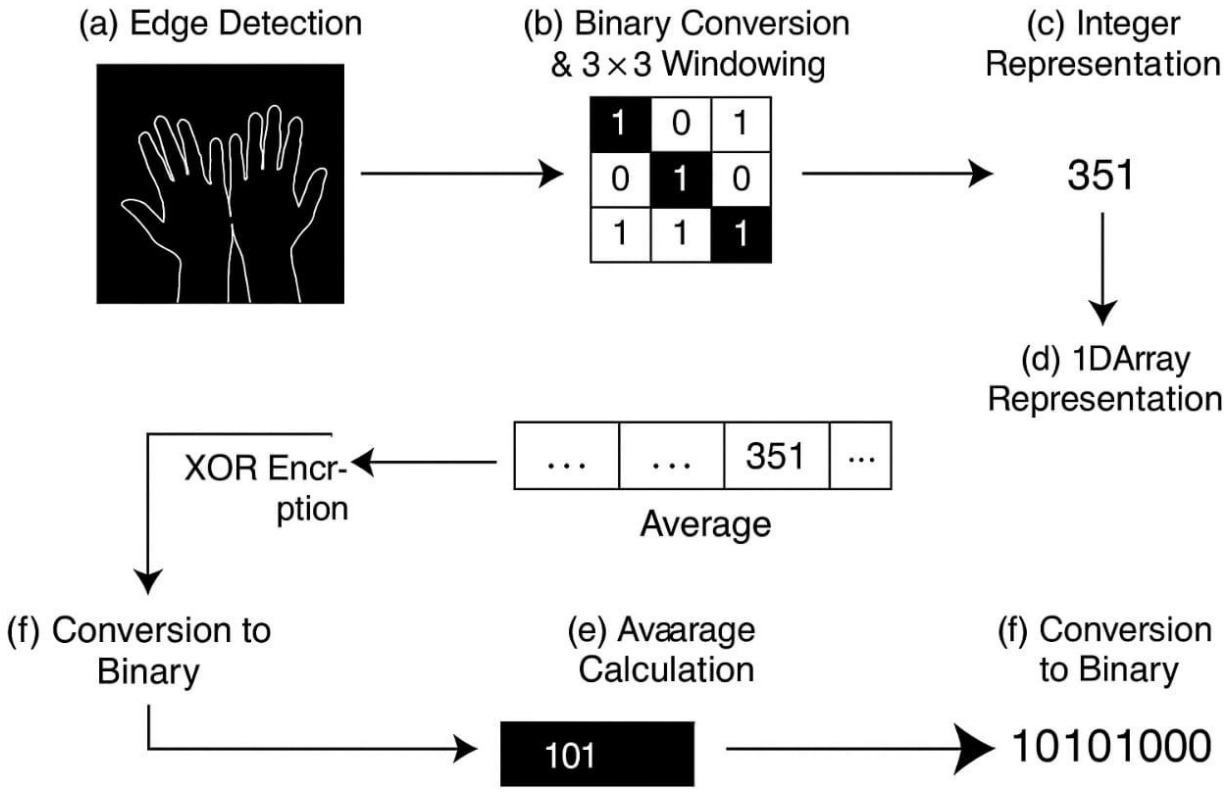

Figure 1: Encryption Process

The algorithm maintained high decryption fidelity, allowing accurate restoration of original medical data. Furthermore, computational efficiency tests revealed that the system can operate effectively on mid-range hardware, confirming its suitability for deployment in resource-constrained medical environments.

6 Conclusion

PixSecure offers a smart solution for safeguarding medical images, which is essential for maintaining patient privacy in our modern world. It's built to be quick, flexible, and strong when it comes to data security. This makes it a great fit for both bustling city hospitals and rural healthcare facilities. The system employs feature-based key generation and XOR encryption, keeping things straightforward and efficient. Tests have shown it to be incredibly

ISBN:97881-19905-39-3

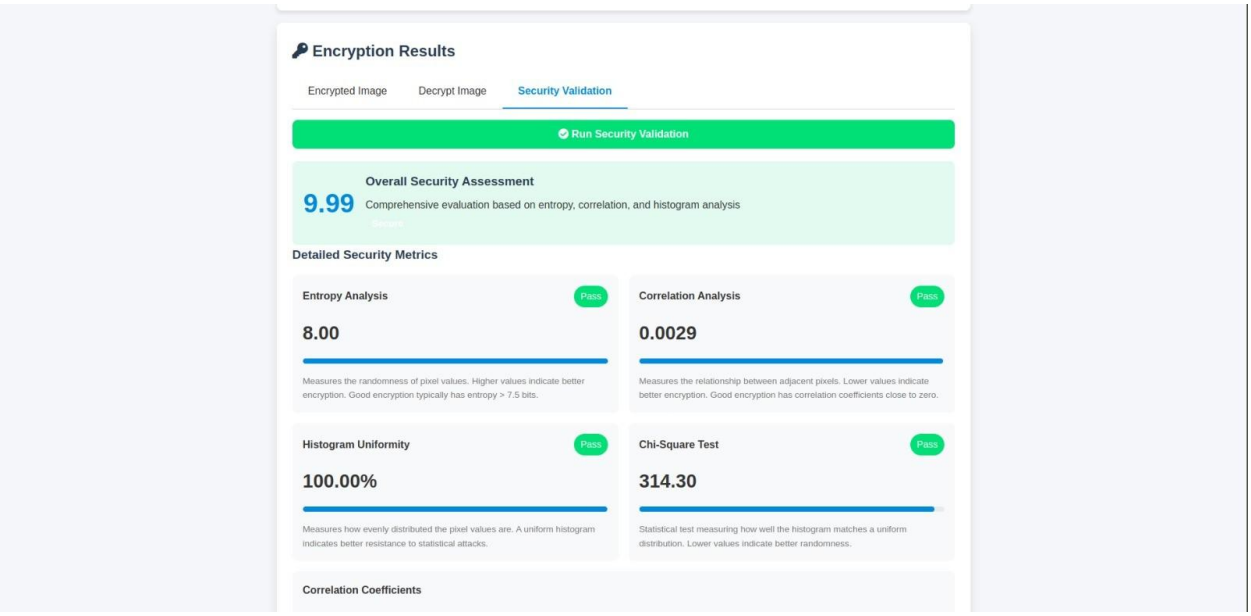

Figure 2:

reliable and sturdy.

Looking ahead, PixSecure plans to extend this approach to secure Electronic Health Records (EHRs) and is also looking to integrate artificial intelligence to detect any unusual activities during the encryption process.

References

(1) Nist, 2010.

ISBN:97881-19905-39-3