Advanced Image Steganography Using Pixel-Value Differencing, AES and ChaCha20 Encryption for Medical Data Security

MSc Research Project
MSc In Cybersecurity

Sakshi Suresh Phadtare
Student ID: x22186671

School of Computing
National College of Ireland

Supervisor: Prof. Khadija Hafeez

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Sakshi Suresh Phadtare		
Student ID:	x22186671		
Programme:	MSc in Cybersecurity	**Year:**	2023-2024
Module:	MSc Research Project/Internship		
Supervisor:	Prof. Khadija Hafeez		
Submission Due Date:	12/08/2024		
Project Title:	Advanced Image Steganography Using Pixel-Value Differencing and AES Encryption		
Word Count:	**6962**	**Page Count: 22**	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Sakshi.S.Phadtare

Date: 12/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Advanced Image Steganography Using Pixel-Value Differencing, AES and Chacha20 Encryption for Medical Data Security

Sakshi Suresh Phadtare
X22186671

Abstract

Steganography and cryptography methods are very good and used for security of the data when transmitting with networks. In the medical domain securing patient data is important due to sensitive nature of information which is involved. This project develops an advanced image steganography system aimed at securing medical data with advanced techniques for sensitive patient information like medical records, diagnosis reports and treatment histories. The system is going to combine Pixel-Value Differencing (PVD) with CHACHA20 Poly1305 encryption to protect sensitive patient information. The workflow starts with selecting an image which is having sensitive medical data into which the user's message is going to insert. This message has been encrypted using CHACHA20 Poly1305 which is a good encryption algorithm known for its performance and strongness. The encrypted data is then hidden within the image using PVD which modifies pixel values to hide the information without any visible thing. A comparative analysis will show CHACHA20 Poly1305's is best over AES encryption. CHACHA20 Poly1305 will show faster encryption and decryption times and have better avalanche effect scores which will give higher sensitivity to input changes and increase cryptographic performance. These attributes make CHACHA20 Poly1305 more good and novel as compared to AES in this application. The system is mainly suited for the medical domain by securing that patient data which includes sensitive type of textual information which is securely encrypted and stored. By combining PVD with the advanced CHACHA20 Poly1305 encryption this project is going to give a highly secure and powerful solution for protecting medical data by showing both high performance and novel security features in the field of data steganography.

Keywords: Image Steganography, ChaCha20 Encryption, Medical Data Security, Image Encryption Steganographic Techniques

1 Introduction

1.1 Background

Steganography has been actually derived from the Greek words "steganos" which means covered and "graphie" which means writing (Ghoul et al., 2023) is a method of hiding the information within other data to prevent detection. Unlike cryptography, which makes data, which is unclear to unauthorized users, steganography aims to of course hide or conceal kind of the hidden information (Rahman et al., 2023). This report focuses on image steganography, where secret data is of course embedded within digital images using the redundancy and kind of noise tolerance of image data. Pixel-Value Differencing (PVD) is actually a steganographic technique that do exploit the human eye's sensitivity to differences in pixel kind of intensities (Taha et al., 2022). In PVD, the cover image is divided into non-overlapping blocks which typically consisting of two consecutive pixels. The difference between the pixel values in each block is used to determine the amount of secret data that can be embedded. Larger differences obviously allow for more data to be hidden, while smaller differences restrict the data capacity, thereby preserving the image quality in smoother type of regions. The Advanced Encryption Standard (AES) is a widely adopted symmetric encryption algorithm that of course ensures data security with a series of complex transformations and operations. AES operates on fixed block sizes and uses key sizes of 128, 192, or 256 bits (Sousi et al., 2020). Its robustness against various cryptographic attacks makes it a very very good type of choice and also preferred choice for encrypting sensitive information. By combining AES encryption with PVD, the system ensures that the embedded data is secure and only accessible to users with the correct decryption key. Combining PVD and AES in an image steganography system which of course provides a double type of layer or dual layer of security: the PVD method hides the data within the image, while AES encryption protects the data's confidentiality. This hybrid approach will definitely address the limitations of traditional steganographic methods by enhancing the security of hidden information. The resulting system is very very good and also suitable for applications requiring secure communication, such as confidential data transmission and protection of intellectual type of property.

1.2 Aim of the study

The aim of this study is to develop a good application which has been designed to increase the security of medical data using advanced image steganography techniques. As healthcare systems grow and digital records by protecting sensitive type of patient information like personal health records, diagnostic results and treatment histories has become increasingly important. The project is going to look and solve this pressing need by combining PVD with CHACHA20 Poly1305 encryption into a smooth application.

1.3 Justification

Securing medical data is very important due to its highly sensitive nature and the increasing thing of cyber threats. Medical information which includes patient records, diagnostic reports and personal health details is very valuable by making it a major target for unauthorized access and misuse. Protecting this data is important for protecting patient privacy by maintaining trust in healthcare systems. Also, with the increase of digital health records and telemedicine the volume of electronic medical data is growing for strong security measures.

1.4 Motivation

The motivation behind developing an advanced image steganography system for securing medical data stems from the need to protect sensitive patient information. As healthcare increases, trust on electronic records and digital communication by protecting medical data becomes important. Traditional encryption methods alone may fall short against complex types of cyber-attacks. Combining PVD with CHACHA20 Poly1305 encryption solves this need by giving a strong and multi-layered approach to data security. CHACHA20 Poly1305 provides good performance and strong cryptographic security. The motivation of this project is done by the dual goals of advancing security technology and solving real-world challenges in medical data protection by securing patient trust in an increasingly digital world.

1.5 Research Objectives

There are some research objectives in this report are:

1. To develop an advanced image steganography system to secure different types of medical data which do includes patient records, diagnostic reports and personal health information by securing their confidentiality during transmission and storage.
2. Enhance the PVD algorithm to obviously maximize the amount of data that can be embedded within an image without compromising any kind of visual quality.
3. Conduct a comparative analysis between ChaCha20 Poly1305 and Advanced Encryption Standard (AES) to know their performance in terms of encryption and decryption times as well as their effects on the avalanche effect.

1.6 Research Questions

There are some research questions in this report are:

1. How can advanced image steganography techniques be used to secure sensitive medical data during transmission and storage?
2. What are the comparative advantages of using CHACHA20 Poly1305 encryption over AES encryption in medical data security which is mainly in terms of performance and cryptographic strength?
3. How does the Pixel-Value Differencing (PVD) method secure that encrypted medical data remains hidden within images without noticeable degradation of image quality?
4. Which one is better ChaCha20 or AES?

2 Related Work

2.1 Image Steganography Techniques

2.1.1 LSB Techniques

The two primary image steganography techniques discussed are Least Significant Bit (LSB) Substitution and Transform Domain Techniques (e.g., DCT and DWT). There is a study which is given by (Arya and Soni, 2018) who proposes an enhanced LSB substitution method for steganography, focusing on embedding information from a secret image into a cover image without perceptibly altering its appearance. By modifying only, the least significant bit (LSB) of each pixel in the cover image, the technique ensures that the embedded data remains visually indistinguishable to the human eye from the original image. This approach actually does supports so many types of carrier file formats such as bitmap (BMP), JPEG, and PNG which shows its versatility across different image formats. The paper also evaluates the method's performance by comparing it across different image sizes and formats (BMP, JPEG, PNG) and analyses parameters such as Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) to of course evaluates its hiding capacity. One of the main problem or challenges addressed is achieving a balance between the fairness of the embedded data and its robustness against detection or extraction things. The results also shows that the proposed method achieves high precision in estimating the length of hidden messages and effectively secures image data, as validated with the help of MATLAB implementation. This research also shows the method's performance in enhancing data and image security with the LSB-based steganography which contributes to advancements the communication techniques and digital forensics things.

Another study given by (Rahman et al., 2022) addresses the increasing weakness of data transmission over insecure networks by of course proposing an advanced steganography technique based on the Least Significant Bit (LSB) substitution method. They show the important type of role of steganography in securing communications over the Internet things for growing external threats or things. The proposed approach also focuses on enhancing security, capacity, and robustness in digital images such as RGB, grayscale, texture, and aerial images. Experimental results from numerical things also do validate the performance or effectiveness of their method which shows a good 5.561 percent improvement in PSNR correlation score over existing techniques. Moreover, their approach also achieves a 6.43 percent higher PSNR score across different different dimensions of images with inserted code which shows its good or superior performance in terms of image things and data hidden.

Moreover (Rachael et al., 2020) introduces an enhanced approach to LSB (Least Significant Bit) steganography aimed at hiding or concealing messages during transmission. Showing the thing between steganography and cryptography for enhanced privacy and security, the proposed method has been of course built upon the traditional 1-byte LSB technique to improve concealment kind of performance or effectiveness. The paper also shows a good kind of procedure for image steganography with the help of LSB showing techniques to minimize the detectability of hidden messages. A key thing of their approach includes steganalysis, which includes so many methods for extracting concealed information from steganographic containers. The main and challenge addressed is ensuring that the embedded messages remain undetectable to unauthorized parties, balancing between robust hidden thing and efficient data transmission. Experimental results also show the performance of their technique showing enhanced concealment capabilities compared to conventional LSB methods. The study reports successful reduction in detection rates of hidden messages with the help of steganalysis techniques of course enhance message security and privacy in digital communications. This research contributes to advancing steganographic techniques which of course gives good and practical data or things into securing sensitive information.

After that (Jayapandiyan et al., 2020) introduces an advanced approach to text steganography using an enhanced Least Significant Bit (eLSB) embedding technique aimed at improving the quality and security of cover images compared to traditional LSB algorithms. The proposed method operates in the spatial domain and employs a two-phase encoding process. Initially, metadata and header information are of course generated and embedded into the first few bytes of the cover image. The secret message is then processed and embedded with the help of an optimized approach that analyzes character sequences, thereby optimizing the storage space required for the secret text within the cover image. This optimization results in higher stego image quality relative to conventional LSB methods. A main and of course key challenge addressed by the approach is balancing between maximizing embedding capacity and maintaining cover image quality which do ensures that the embedded messages to unauthorized viewers. Experimental results which show the performance and effectiveness of the eLSB technique, which shows good types of improvements in Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR) and all values compared to standard LSB algorithms. The study also shows the enhanced security and capacity of the proposed method which shows its potential in strengthening text steganography for secure information sharing applications. This research also does contribute to advancing steganographic methodologies which gives a robust framework for embedding and securing sensitive text data within digital images.

In their paper, (Shreelekshmi et al., 2019) presents a novel method to enhance the security of LSB replacement steganography through pre-processing with Inverse Transitions. This approach of course do modify the LSBs of the cover image before embedding data which do ensures that the resulting pixel values after embedding cannot be replicated using traditional LSB replacement methods. By applying inverse transitions, the method has been achieved 100% undetectability against accurate length estimation techniques for LSB replacement, particularly effective for payloads up to 1.5 bits per pixel (bpp) in color images. The proposed method is noted for of course its speed and efficiency which do requires no additional storage overhead and guaranteeing lossless recovery of hidden data for of course distinguishing it from existing steganography techniques. There are some kind of challenges which are addressed include balancing between embedding capacity and maintaining image things, as well as ensuring robustness against steganalysis techniques designed to detect LSB-based data hiding. Experimental results which also shows the method's performance in enhancing security without compromising any kind of data recovery or computational efficiency which make it suitable for resource-constrained applications that demand fast and secure data concealment. This research also gives a good advancement in LSB steganography which gives a practical solution for secure data hiding in digital images with improved things against detection methods.

In their paper (Ali et al., 2019) proposes a novel approach to image steganography using LSB substitution which actually do aim to securely insert information within digital images without detection by unauthorized parties. Recognizing the need for secure communication in modern digital systems, the method also do focus on hiding data things within the random bit positions of pixels. This technique uses the LSB of pixels by modifying them slowly to of course encode hidden messages while maintaining the visual integrity of the image. Experimental results which show the performance of the proposed method which show its ability to hide information effectively. There are some kind of challenges which addressed include achieving a balance between embedding capacity and maintaining visual quality, ensuring that modifications made to the LSBs do not degrade the quality of the stego-image or raise suspicion during steganalysis. The approach also does aim to of course enhance data security by using the ubiquity of digital images on the internet as carrier formats, thereby giving covert communication. So, the proposed LSB substitution method gives a promising solution for securely transmitting sensitive information with the digital media which contribute to advancements in steganographic techniques for protecting confidentiality and privacy in digital communications. This research also shows a good and important step towards enhancing secure data transmission methods in contemporary information systems.

2.1.2 Transform Domain Techniques

Also, there is another study given by (Kalita et al., 2019) who introduces a novel transform domain method for steganography aimed at enhancing data hiding techniques using the Integer Wavelet Transform (IWT). This method also do decompose images into four sub bands (low-low, low-high, high-low, high-high) and selectively modifies three sub bands while preserving the low-low sub band to improve stego image quality. The approach also uses a coefficient value differencing technique to obviously determine the optimal number of secret bits that can be embedded within the coefficients which do ensures efficient use of embedding capacity while maintaining things and robustness. The proposed method also shows good and superior performance across multiple metrics including embedding capacity. The study also includes analyses of histogram deformation and Pixel Difference Histogram for various embedding percentages which do reveal good similarity between stego and original cover images. Experimental results also shows an embedding capacity of 2.3 bits per pixel (bpp) with high-quality stego image outputs, having traditional methods in terms of both capacity and visual fidelity. There are some kind of challenges addressed include optimizing embedding efficiency without compromising image quality and ensuring robustness against detection methods.

In another study given by (Liu et al., 2020) who actually introduced an enhanced irreversible image steganography method that combines LSB with PVD techniques to maximize steganographic capacity while preserving image quality. The method also does partition the cover image into non-overlapping blocks, each consisting of three consecutive pixels. The second pixel also serves as the base for embedding secret data using 3-bit LSB substitution, optimizing embedding efficiency. The remaining two pixels in each block are paired with the base pixel and undergo embedding via an improved modulus function-based PVD method.

Experimental results show a good increase in steganographic capacity compared to traditional PVD-based techniques, achieving up to a 135% increase, while ensuring minimal impact on image quality. The method's performance or effectiveness is validated with security which confirms its robustness against common detection techniques. There are some challenges which solve few things like maintaining a balance between input capacity and image things which do secures that the data remains to visual inspection and other things like resistant to steganalysis attempts. The study also shows the method's capability to increase data hiding in images which make it suitable for applications requiring secure and powerful covert communication. So, the combined LSB-PVD steganography method represents a good type of advancement in irreversible image steganography which gives increased capacity and security for digital data concealment.

In their study (Zakaria et al., 2018) introduces a novel steganography method aimed at improving capacity while preserving visual quality and increasing security against steganalysis attacks. The method has been used a data mapping strategy where four secret data bits are mapped to the four most important bits of a cover pixel by minimizing the number of modifications needed per pixel. Mainly only the two least significant bits (LSBs) of each pixel are changed to show the mapping strategy by reducing the risk of steganalysis detection as compared to traditional LSB-based methods. Experimental results have been showed that the proposed approach achieves a 3.48% larger input capacity while increasing visual quality which is been shown by a 3.73 dB increase in Peak Signal-to-Noise Ratio (PSNR). Moreover, the method has been reduced the average modification rate to 0.76 bits per pixel which is thereby reducing the effect on stego-image quality. Security evaluation against Regular and Singular groups (RS) steganalysis and histogram-based detection attacks confirms the trust of method to basic detection techniques by showing its performance in maintaining covert communication integrity. Challenges found which does include optimizing the trade-off between embedding capacity and image fidelity by securing that inserted data remain resistant to detection.

2.1.3 Hybrid Techniques

In their study, (Kalaichelvi et al., 2021) proposes an combined type of approach combining cryptography and steganography to enhance information security in digital communications. The method actually begins with encrypting the message using a revised RSA algorithm to convert it into a secret format which of course ensures confidentiality during transmission. Next, the cover image is having segmentation into edge and non-edge pixel regions using the Canny edge detection technique. Within these segmented areas, portions of the encrypted message (N1 bits in edge pixels and N2 bits in non-edge pixels) are of course embedded with the LSB technique, optimizing data hiding efficiency. Additionally, some important kinds of parameters such as N1, N2, and message length are encoded into the last four pixels of the cover image to generate the stego-image. At the recipient's end, these parameters are extracted from the stego-image to recover the hidden data, which is then decrypted using the revised RSA algorithm's dual-key mechanism for enhanced security. Performance evaluation metrics include entropy and all which shows that the proposed system achieves improved efficiency, security, and all in information hiding. There are some kind of challenges which addressed include maintaining the balance between embedding capacity and image quality while ensuring robustness against steganalysis techniques that could detect modifications in pixel values. The results show the performance of integrating cryptography and steganography for secure data transmission which gives a good solution to safeguard sensitive information across digital networks with enhanced privacy and reliability. This research also contributes things to advancing hybrid techniques in information security, catering to the growing need for robust data protection in modern communication systems.

2.2 Medical Data Security

In the medical domain few studies have been done in image steganography. First study given by (Hashim and Mahmood, 2021) who have been proposed a novel secure image steganography approach called the Pixels Contrast (PC) method which is designed to solve challenges in the medical imaging domain which is mainly issues of low capacity, poor strongness. The proposed method uses a combination of image partitioning with a Henon map the eight-neighbour's method and Huffman coding to increase the security and performance of data hiding. The performance of the PC method has been evaluated using standard medical images and the SIPI dataset with results evaluated through Histogram Analysis, PSNR and all. Another study given by (Broumandnia, 2024) who suggested a steganography mechanism which is been designed to increase data security in medical imaging by inserting secret information within digital images. The method has been used a two-dimensional PVD technique where bits of the secret message are hidden within 8 pairs of non-overlapping pixels of sub-images.

Table 2.1: Comparison Table

Study	Methodology	Key Features	Challenges Addressed	Results
1	Improved LSB substitution steganography	Enhanced LSB method, indistinguishable stego-images	Data hiding capacity, image format compatibility	High precision in message length estimation, suitable for various formats
2	eLSB embedding technique	Spatial domain steganography, high security and imperceptibility	Security, imperceptibility, capacity, robustness	Significant PSNR improvement, robust against steganalysis methods
3	LSB with pixel-value differencing	Integration of LSB and PVD methods, increased capacity	Capacity, image quality, steganalysis prevention	135% capacity increase, robust against steganalysis techniques
4	eLSB with metadata embedding	Improved embedding	Embedding efficiency, image quality, security	Improved stego-image quality, efficient

		efficiency, metadata integration		embedding, metadata integration
5	Integer Wavelet Transform method	Transform domain steganography, four subbands	Embedding capacity, imperceptibility, robustness	High embedding capacity, robust against steganalysis, improved security
6	LSB with modulus PVD	Combined LSB and PVD, enhanced capacity and security	Capacity, image quality, steganalysis detection	Increased steganographic capacity, robust against detection techniques
7	Inverse Transitions for LSB	Preprocessing with inverse transitions, high undetectability	Undetectability, data recovery, security	100% undetectability, efficient data recovery, improved security
8	Cryptography + Segmented LSB	RSA encryption + Canny edge detection, dual-key RSA	Security, embedding capacity, image quality	Enhanced security, efficient embedding, robust against steganalysis
9	Data mapping strategy with LSB	Mapping secret data to MSBs, reduced modifications per pixel	Embedding capacity, visual quality, security	3.48% larger capacity, improved PSNR, reduced modification rate
10	Random LSB substitution	Random LSB positions, imperceptible data hiding	Data hiding, visual integrity, steganalysis prevention	Effective data hiding, imperceptible modifications, practical application

2.3 Own Analysis: Limitations and Approaches

Analysing the current literature which shows so many limitations in existing steganography methods. LSB techniques while simple and powerful mostly struggle with strongness against detection and limited capacity. Transform Domain Techniques improve capacity but introduce soe important computational complexity. Hybrid approaches combining cryptography and steganography gives increased security but face challenges in balancing performance. In medical steganography methods like those proposed by (Hashim and Mahmood, 2021) has been showed good but are mostly have by scalability and adaptability issues which is being solved by my study.

3 Research Methodology

3.1 Methodologies Used

3.1.1 AES Encryption

In this project Advanced Encryption Standard (AES) plays a very important role in knowing the security of medical data inserted within images. AES is a symmetric encryption algorithm mainly used for its strongness and performance in data encryption. It operates on fixed-size blocks of data (128 bits) and supports key sizes of 128, 192, and 256 bits which gives a strong level of security by encrypting data with multiple rounds of transformations which do includes substitution, permutation and mixing operations. For this project AES encryption has been used to securely encode the message before it is hidden within the image using Pixel-Value Differencing (PVD). The encryption process includes generating a key which is then used to encrypt the data by making it unreadable without the correct decryption key. AES's performance is mainly advantageous as it allows for quick processing of encryption and decryption tasks which is very important for managing large medical datasets. AES is recognized for its high security and performance. It is mainly adopted in so many applications from securing communications and financial transactions to protecting data in cloud storage and personal devices. AES's security has been derived from its complex structure to known cryptographic attacks by making it a good choice for data encryption.

3.1.2 ChaCha

In this project ChaCha20 encryption has been used to increase the security and performance of inserting medical data within images. ChaCha20 is a modern stream cipher which is been designed to give high security with exceptional performance. It operates with a 256-bit key, and a 64-bit and its encryption process include a series of simple but powerful operations that generate pseudo-random keystreams to securely encode the data. For this project ChaCha20 has been used with Pixel-Value Differencing (PVD) to encrypt the message before hiding it within an image. This combination will secure that the embedded data remains secure and inaccessible without the correct decryption key. ChaCha20's design mainly focuses on speed and strongness which makes it well-suited for applications requiring fast encryption and decryption while maintaining strong security guarantees.

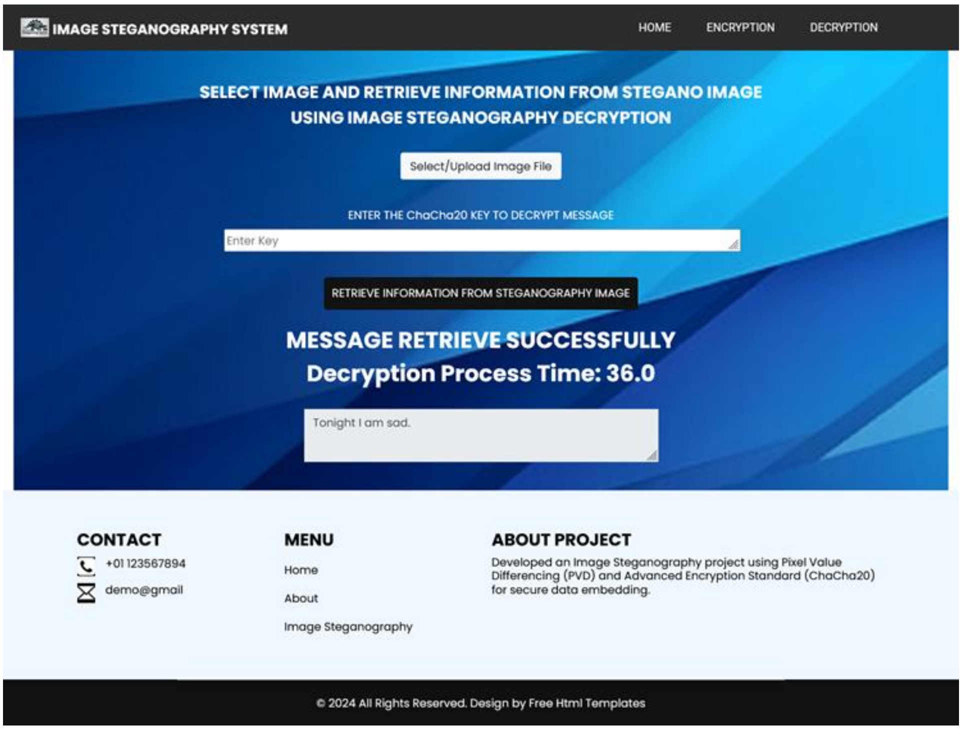
3.1.3 PVD

In this project Pixel-Value Differencing (PVD) has been used to securely insert medical data within images complementing the ChaCha20 encryption method. PVD is a steganographic technique that changes pixel values in a manner that minimally affects the visual quality of the cover image while hiding the data in a good way. This approach does include the pixel values behind a reference image and insert the secret data by making small adjustments to the pixel values. PVD is a powerful method for image steganography. It is mainly used due to its ability to insert data without any kind of problem.

4 Design Specification

This project aims to increase medical data security by inserting patient data within images using an advanced steganography system. The design is going to combine Pixel-Value Differencing (PVD) with CHACHA20 Poly1305 encryption by giving a strong solution for secure data storage. The choice of PVD allows for good hiding of data by changing pixel values in a manner to the human eye which is thereby knowing the steganographic integrity of the image. The encrypted data is then protected by the CHACHA20 Poly1305 algorithm which obviously gives good security features as compared to AES.

The system architecture includes modules for data preprocessing, encryption, steganographic embedding and retrieval. So firstly, patient data is formatted and encrypted using CHACHA20 Poly1305 by knowing confidentiality and integrity. The encrypted data is then inserted into the host image with the help of PVD by using the variability in pixel values to hide the data without any kind of change to the image. For retrieval, the system extracts the inserted data and decrypts it by of course reconstructing the original patient information. This design is going to guarantee that even if the image is caught the encrypted data remains secure. The system is built using Python and combined libraries for image processing and encryption. The deployment includes a user-friendly interface for medical personnel to upload and retrieve patient data in a smooth way. This design not only increases data security but also know things with medical data protection regulations.



SELECT IMAGE AND RETRIEVE INFORMATION FROM STEGANO IMAGE
USING IMAGE STEGANOGRAPHY DECRYPTION

ENTER THE ChaCha20 KEY TO DECRYPT MESSAGE

Enter Key

MESSAGE RETRIEVE SUCCESSFULLY
Decryption Process Time: 36.0

Tonight I am sad.

☎ +01 123567894
✉ demo@gmail

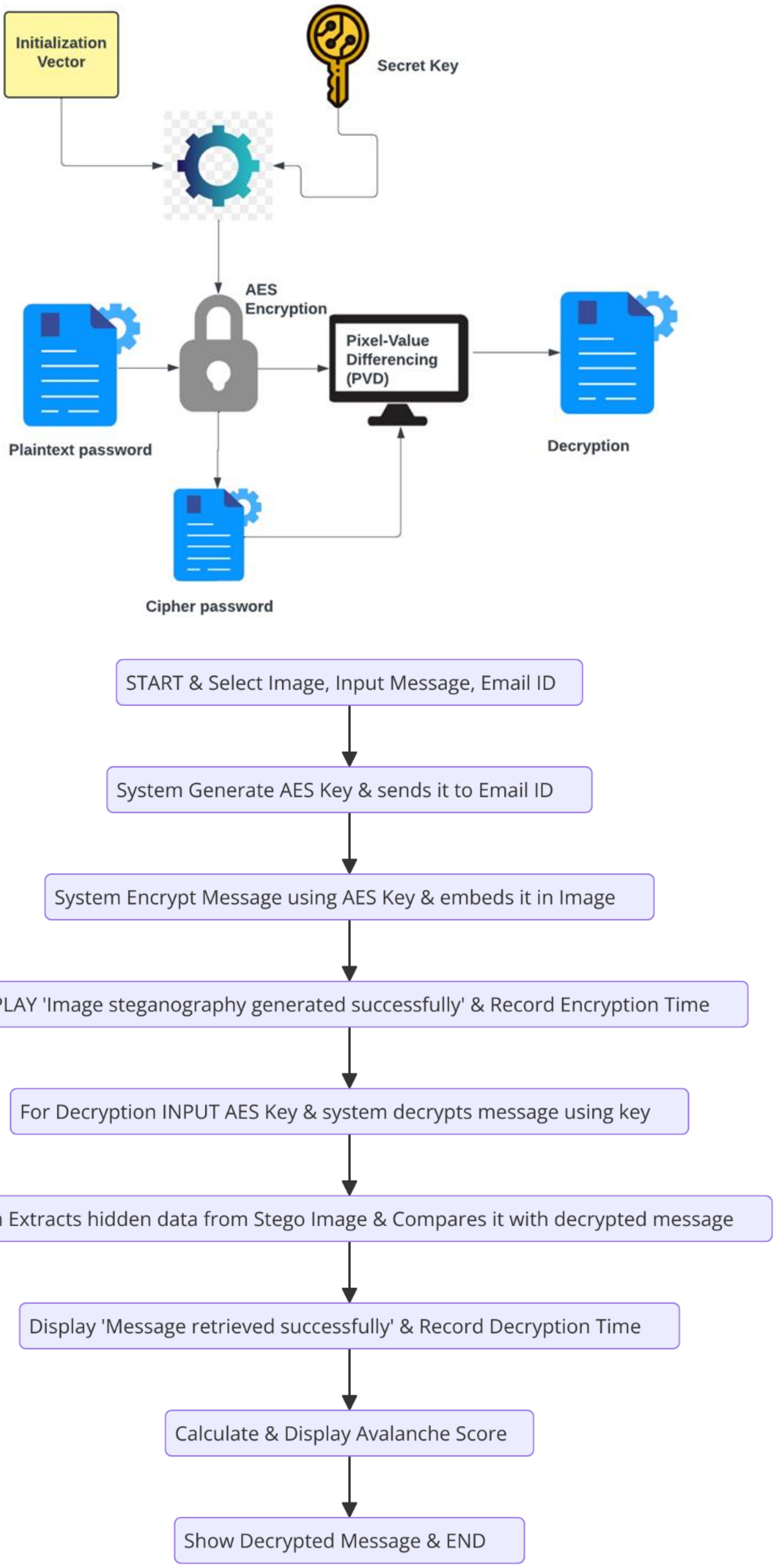
ABOUT PROJECT

Developed an Image Steganography project using Pixel Value Differencing (PVD) and Advanced Encryption Standard (ChaCha20) for secure data embedding.

© 2024 All Rights Reserved. Design by Free Html Templates

Figure 4.1: Web Application Interface

4.1 Algorithm for Proposed System



START & Select Image, Input Message, Email ID

System Generate AES Key & sends it to Email ID

System Encrypt Message using AES Key & embeds it in Image

DISPLAY 'Image steganography generated successfully' & Record Encryption Time

For Decryption INPUT AES Key & system decrypts message using key

System Extracts hidden data from Stego Image & Compares it with decrypted message

Display 'Message retrieved successfully' & Record Decryption Time

Calculate & Display Avalanche Score

Show Decrypted Message & END

Figure 4.2: System Architecture

5 Implementation

The implementation of this advanced image steganography system is used to confirm the security of medical data. The process starts with a user-friendly interface where medical personnel can select an image to host the hidden data. The chosen image serves as the cover for inserting sensitive patient information. The user inputs the message like "Patient ID: 12345. Date: 2024-08-11. Past Medical History: Asthma, treated with albuterol." and their email ID into the system. Upon clicking "Generate PVD Steganography Image with AES" the system starts the encryption process.

The message will have AES encryption by knowing strong protection. The AES encryption key is generated and securely sent to the user's email ID. The encrypted message is inserted into the selected image using Pixel-Value Differencing (PVD). This method will change pixel values in a manner that remains not visible to the human eye. Once the embedding is complete then a success message "Image steganography generated successfully" has been displayed and the encryption process time is recorded.

For decryption, the user inputs the received AES key into the system and clicks "Retrieve Information from Steganography Image." The system is going to extract the inserted data and decrypts it using the given AES key. A message "Message retrieved successfully" confirms the successful extraction and the decryption time has been calculated and displayed. The original message which is "Patient ID: 12345. Date: 2024-08-11. Past Medical History: Asthma, treated with albuterol. " Is going to show on the screen.
The system also calculates the avalanche score by of course measuring the sensitivity of the encryption algorithm to small changes in input. This score knows the strongness of the encryption method used.

This implementation will guarantee that sensitive medical data which do includes patient information can be securely hidden within images. The combination of PVD and AES encryption gives a dual layer of security by making it highly good for protecting confidential type of medical records from unauthorized access. The use of email for key distribution and detailed time tracking for encryption and decryption processes further increases the reliability of the system.
Algorithm for Image Steganography System with PVD and AES Encryption
Step 1: Select Image
Step 2: Input Message
Step 3: Enter Email ID
Step 4: Encrypt Message
Step 5: Embed Encrypted Message
Step 6: Send Encryption Key
Step 7: Display Success Message
Step 8: Decrypt Message
Step 9: Retrieve and Display Message
Step 10: Calculate Avalanche Score

6 Evaluation

6.1 Experiment 1

Table 6.1 presents the encryption and decryption times for the AES algorithm which is been applied to images of different sizes before a text change. The table includes three entries each representing different image file sizes (100 KB, 500 KB, and 1024 KB) and their corresponding encryption and decryption times measured in milliseconds. For the 100 KB image the encryption process takes 9331.29 ms while decryption is faster at 36 ms. As the image size increases to 500 KB the encryption time rises to 25690.68 ms with decryption time obviously increasing to 115.01 ms. For the largest image size of 1024 KB encryption time further go to 45495.97 ms and decryption time to 189.01 ms.

Table 6.1: Encryption and Decryption Time Before Changed Text

Enc/Dec Algo	Image File Size (kb)	Enc Process Time(ms)	Dec Process Time(ms)
AES	100	9331.29	36
AES	500	25690.68	115.01
AES	1024	45495.97	189.01

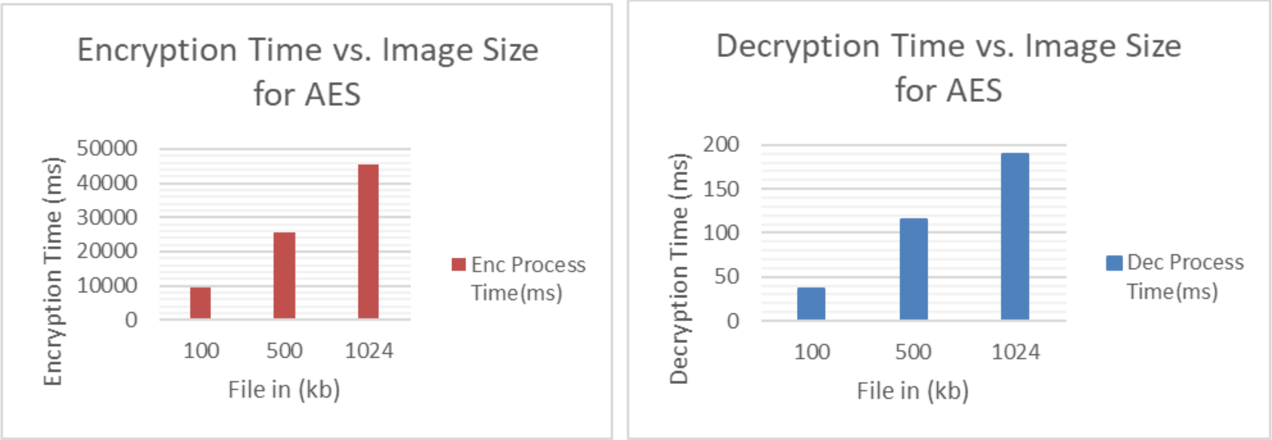


Figure 6.1: Graph for AES

6.2 Experiment 2

Table 6.2 outlines the encryption and decryption times for the CHACHA20 algorithm applied to images of varying sizes (100 KB, 500 KB, and 1024 KB) before a text change. This data provides insight into the performance of the CHACHA20 encryption algorithm in handling different image file sizes. For the 100 KB image, the encryption time with CHACHA20 is 8637.92 ms, which is slightly lower compared to AES for the same size, while the decryption time is 36 ms, identical to AES. As the image size increases to 500 KB, the encryption time grows to 26408.34 ms, & the decryption time increases to 125.08 ms. For the largest image size of 1024 KB, the encryption time reach 43259.36 ms, & decryption time extend to 219.92 ms.

Table 6.2: Encryption and Decryption Time Before Changed Text

Enc/Dec Algo	Image File Size (kb)	Enc Process Time(ms)	Dec Process Time(ms)
CHACHA	100	8637.92	36
CHACHA	500	26408.34	125.08
CHACHA	1024	43259.36	219.92

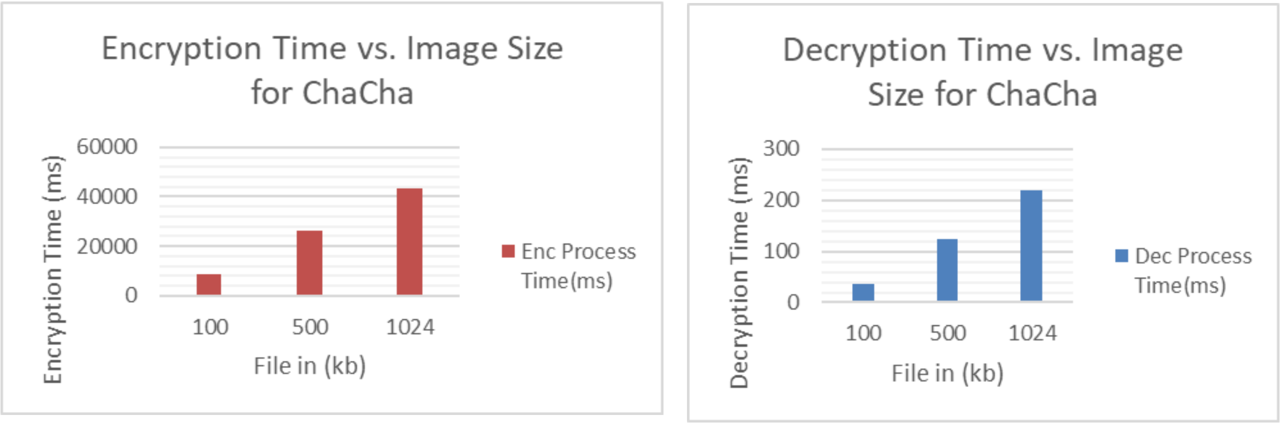


Figure 6.2: Graph for ChaCha

6.3 Experiment 3

Table 6.3 presents the encryption and decryption times for the AES algorithm applied to images of various sizes (100 KB, 500 KB, and 1024 KB) after a slight text change. This table shows how the performance of AES is affected by text modification. For the 100 KB image, the encryption time is 8683.88 ms, which is slightly longer compared to the time recorded before the text change, while the decryption time is 34 ms, marginally faster. As the image size increases to 500 KB, the encryption time rises to 26766.48 ms, with decryption time increasing to 104.01 ms. For the 1024 KB image, encryption time extends to 44673.56 ms, and decryption time is 188.01 ms.

Table 6.3: Encryption and Decryption Time After Changed Text

Enc/Dec Algo	Image File Size (kb)	Enc Process Time(ms)	Dec Process Time(ms)
AES	100	8683.88	34
AES	500	26766.48	104.01
AES	1024	44673.56	188.01

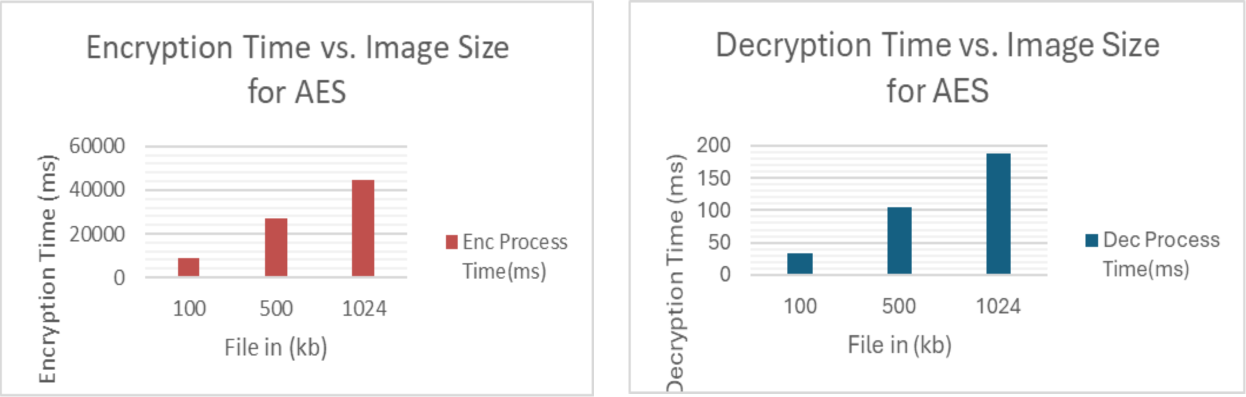


Figure 6.3: Graph for AES

6.4 Experiment 4

Table 6.4 details the encryption and decryption times for the CHACHA20 algorithm applied to images of various sizes (100 KB, 500 KB, and 1024 KB) following a text change. This table provides insights into the performance impact of modifying the encryption key on CHACHA20. For the 100 KB image, the encryption time is 8643.19 ms, showing a slight increase from the pre-text change time, while the decryption time remains at 36 ms. As the image size grows to 500 KB, the encryption time rises to 25070.27 ms, and the decryption time increases to 117.02 ms. For the largest image size of 1024 KB, encryption time extends to 43214.67 ms, and decryption time reaches 185.01 ms.

Table 6.4: Encryption and Decryption Time After Changed Text

Enc/Dec Algo	Image File Size (kb)	Enc Process Time(ms)	Dec Process Time(ms)
CHACHA	100	8643.19	36
CHACHA	500	25070.27	117.02
CHACHA	1024	43214.67	185.01

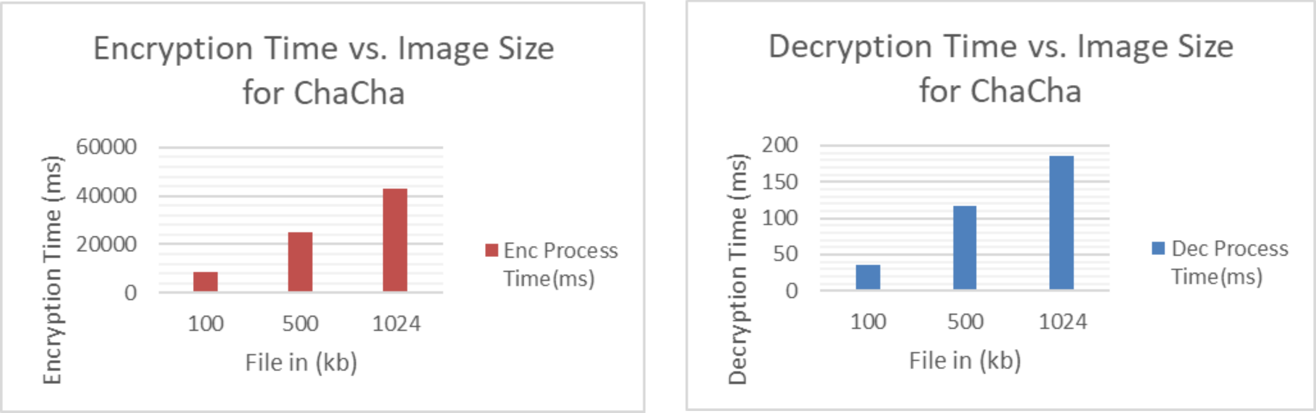


Figure 6.4: Graph for ChaCha

6.5 Experiment 5

Table 6.5 presents the avalanche effect scores for AES and CHACHA20 algorithms which is been applied to images of different sizes (100 KB, 500 KB, and 1024 KB). The avalanche effect measures how a small change in the input (such as modifying a bit) affects the output showing the sensitivity of the encryption algorithm to changes in the input data. For AES the avalanche scores are 50.61 for a 100 KB image, 49.60 for a 500 KB image and 53.20 for a 1024 KB image. These scores show the algorithm's sensitivity to changes in the input data with a minor increase in the score for larger images which obviously show that AES maintains a consistent but slightly change in avalanche effect across different image sizes. For CHACHA20 the avalanche scores are 49.52 for a 100 KB image, 53.79 for a 500 KB image and 52.08 for a 1024 KB image.

Table 6.5: Table of Avalanche Effect

Enc/Dec Algo	Image File Size (kb)	Avalanche Score
AES	100	50.60724234
AES	500	49.59785523
AES	1024	53.19926874
Enc/Dec Algo	**Image File Size (kb)**	**Avalanche Score**
CHACHA	100	49.52380952
CHACHA	500	53.78590078
CHACHA	1024	52.0754717

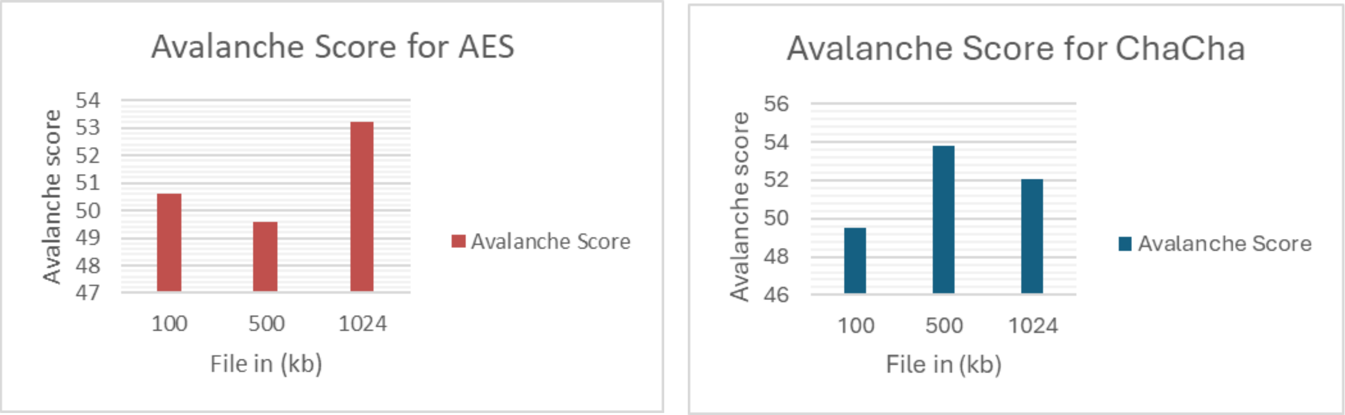


Figure 6.5: Avalanche Graph

6.6 Comparison Analysis with AES vs ChaCha

When comparing AES and ChaCha20 for encryption and decryption in the medical data security ChaCha20 has been showed good performance and novelty. Although both algorithms have been given strong security ChaCha20 consistently performs better as compared to AES in terms of processing time. For image files of different sizes ChaCha20 gives faster encryption and decryption times as compared to AES by making it a better choice for applications demanding quick data processing. The avalanche effect which measures the sensitivity of the algorithm to changes in input is good for ChaCha20.

7 Conclusion and Future Work

7.1 Conclusion

This project has been successfully developed a complex image steganography system that increases the security of medical data with the combination of Pixel-Value Differencing (PVD) and CHACHA20 Poly1305 encryption. The main objective was to create a robust method for inserting sensitive patient information within images while maintaining both security and performance. The system operates by first selecting an image which serves as the host for the hidden data. Users input their message which is then encrypted using CHACHA20 Poly1305. This modern encryption algorithm is known for its speed and strongness which gives good performance as compared to traditional encryption methods like AES. The encrypted message is then hidden within the image using the PVD technique. PVD changes the pixel values in a manner that inserts the data without important visual things by confirming that the information is secure.

7.2 Limitations and Future Works

While the developed image steganography system has been showed good performance in securing medical data there are so many limitations and areas for future improvement. One limitation is the system's performance on a single image format which may not be compatible with all types of images. Future iterations could obviously increase compatibility by supporting a huge range of image formats and sizes. Future work could focus on optimizing the PVD algorithm and the encryption process to reduce computational demands and improve performance for large-scale medical data. Also, the system is currently handling only textual data which is been inserted in images. Expanding its capabilities to have other types of medical data, like complex diagnostic images or audio recordings could make it better and useful in broader medical things. Finally, the user interface and overall user experience could be improved. Simplifying the process of selecting images, inputting messages and managing encryption keys could make the system more accessible to users with different levels of technical expertise. Future work could include developing a better interface and combining user feedback to change the system's functionality and ease of use.

References

1. Arya, A. and Soni, S., 2018. Performance evaluation of secrete image steganography techniques using least significant bit (LSB) method. *Int. J. Comput. Sci. Trends Technol*, *6*(2), pp.160-165.
2. Rahman, S., Uddin, J., Khan, H.U., Hussain, H., Khan, A.A. and Zakarya, M., 2022. A novel steganography technique for digital images using the least significant bit substitution method. *IEEE Access*, *10*, pp.124053-124075.
3. Rachael, O., Misra, S., Ahuja, R., Adewumi, A., Ayeni, F. and Mmaskeliunas, R., 2020. Image steganography and steganalysis based on least significant bit (LSB). In *Proceedings of ICETIT 2019: Emerging trends in information technology* (pp. 1100-1111). Springer International Publishing.
4. Jayapandiyan, J.R., Kavitha, C. and Sakthivel, K., 2020. Enhanced least significant bit replacement algorithm in spatial domain of steganography using character sequence optimization. *Ieee Access*, *8*, pp.136537-136545.
5. Kalita, M., Tuithung, T. and Majumder, S., 2019. A new steganography method using integer wavelet transform and least significant bit substitution. *The Computer Journal*, *62*(11), pp.1639-1655.
6. Liu, H.H., Su, P.C. and Hsu, M.H., 2020. An improved steganography method based on least-significant-bit substitution and pixel-value differencing. *KSII Transactions on Internet and Information Systems (TIIS)*, *14*(11), pp.4537-4556.
7. Shreelekshmi, R., Wilscy, M. and Madhavan, C.V., 2019. Undetectable least significant bit replacement steganography. *Multimedia Tools and Applications*, *78*(8), pp.10565-10582.
8. Kalaichelvi, V., Meenakshi, P., Vimala Devi, P., Manikandan, H., Venkateswari, P. and Swaminathan, S., 2021. A stable image steganography: a novel approach based on modified RSA algorithm and 2–4 least significant bit (LSB) technique. *Journal of Ambient Intelligence and Humanized Computing*, *12*, pp.7235-7243.
9. Zakaria, A.A., Hussain, M., Wahab, A.W.A., Idris, M.Y.I., Abdullah, N.A. and Jung, K.H., 2018. High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution. *Applied Sciences*, *8*(11), p.2199.
10. Ali, U.A.M.E., Sohrawordi, M. and Uddin, M.P., 2019. A robust and secured image steganography using LSB and random bit substitution. *American Journal of Engineering Research (AJER)*, *8*(2), pp.39-44.

11. Ghoul, S., Sulaiman, R. and Shukur, Z., 2023. A review on security techniques in image steganography. *International Journal of Advanced Computer Science and Applications*, *14*(6).
12. Rahman, S., Uddin, J., Zakarya, M., Hussain, H., Khan, A.A., Ahmed, A. and Haleem, M., 2023. A comprehensive study of digital image steganographic techniques. *IEEE Access*, *11*, pp.6770-6791.
13. Taha, M.S., Rahem, M.S.M., Hashim, M.M. and Khalid, H.N., 2022. High payload image steganography scheme with minimum distortion based on distinction grade value method. *Multimedia Tools and Applications*, *81*(18), pp.25913-25946.
14. Sousi, A.L., Yehya, D. and Joudi, M., 2020. Aes encryption: Study & evaluation. *CCEE552: Cryptography and Network Security*.
15. Hashim, M.M., Mahmood, A.A. and Mohammed, M.Q., 2021. A pixel contrast based medical image steganography to ensure and secure patient data. *International Journal of Nonlinear Analysis and Applications*, *12*(Special Issue), pp.1885-1904.
16. Broumandnia, A., 2024. Two-dimensional modified pixel value differencing (2 D-MPVD) image steganography with error control and security using stream encryption. *Multimedia Tools and Applications*, *83*(8), pp.21967-22003.