Securing Images with AES and Visual Cryptography Techniques

Submitted in partial fulfilments of the requirements
of the degree of

BACHELOR OF COMPUTER ENGINEERING

by

Toshna Rane (19102058)
Shreya Godbole (19102034)
Parth Gujar (19102056)
Harshal More (19102055)

Guide
Dr. Pravin Adivarekar

Department of Computer Engineering
A. P. SHAH INSTITUTE OF TECHNOLOGY, THANE
University of Mumbai
2022-2023

A. P. SHAH INSTITUTE OF TECHNOLOGY, THANE

CERTIFICATE

This is to certify that the project entitled "**Securing Images with AES and Visual Cryptography Techniques**" is a bonafide work of **Toshna Rane** (19102058), **Shreya Godbole** (19102034), **Parth Gujar** (19102056), **Harshal More** (19102055)" submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of Bachelor of Engineering in Computer Engineering.

_____	_____
Guide Dr. Pravin Adivarekar	Project Coordinator Prof. Rushikesh R. Nikam
_____	_____
Head of Department Prof. Sachin H. Malave	Principal Dr. Uttam D. Kolekar

Date:

A. P. SHAH INSTITUTE OF TECHNOLOGY, THANE

Project Report Approval for B.E.

This project report for Sem-VIII entitled **"Securing Images with AES and Visual Cryptography Techniques"** by **Toshna Rane (19102058), Shreya Godbole (19102034), Parth Gujar (19102056), Harshal More (19102055)** is approved for the degree of ***Bachelor of Engineering*** in ***Computer Engineering***, ***2022-23***.

Examiner Name Signature

1. _____

2. _____

Date:

Place:

Declaration

We declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. We understand that any violation of the above will be the cause for disciplinary action by the Institute and can also invoke penal action from the sources which have thus not been properly citedor from whom proper permission has not been taken when needed.

Toshna Rane (19102058)

Shreya Godbole (19102034)

Parth Gujar (19102056)

Harshal More (19102055)

Date:

Abstract

In this digital era, the need for security of data over the internet is increasing day by day. Images are often used to store and share data securely. Along with data security, data confidentiality and integrity are a major issue while transferring data over the network. Image encryption techniques such as AES image encryption algorithm and Visual Cryptography can be used to provide security to images and image data. In the proposed system, the main role of Visual Cryptography is to store image or image data secured over the network in the form of shares. The image is being encrypted securely using AES encryption algorithm and SHA3-512 algorithm with an added layer of security provided by the DWTCT (Discrete Wavelet Transform based Content Transform) function. The implementation of these algorithms is carried out using python. The results obtained are studied and the system's future scope is discussed.

CONTENTS

LIST OF FIGURES

Abbreviation

SHA-256	Secure Hashing Algorithm
AES	Advanced Encryption Standard
DWTCT	Discrete Wavelet Transform based Content Transform
DES	Data Encryption Standard
VC	Visual Cryptography

CHAPTER 1

Introduction

The main objective of the image encryption technology is to transmit images over the network securely and without any unauthorized access. While transferring images over the network, the confidentiality and integrity of that image is a major concern. Nowadays, Images are often used everywhere in applications over the network to share and store valuable data and therefore needs complete security. Most images are shared and accessed via public networks, thus implementing cryptographic techniques to the image data has become a necessity to protect image data and ensure data privacy. If the images are tampered during transmission, it may cause serious data compromise issues such as information theft, unauthorized access by malicious attackers, and modification attacks to name a few.

Encryption is a technique which provides security to the images. Image Encryption is important because of the emergence of the internet. It relies on the novel concept of taking the sequential or random pixel bits of an image and combining them with logic to create a full set of new pixels that are typical of the original bits. There have been a number of techniques developed to encrypt image data efficiently. These encryption algorithms developed vary in functionality for textual data and multimedia data. Algorithms like Data Encryption Standard (DES), International Data Encryption Standard (IDEA) work well for text-based data while techniques like Blowfish, AES, XOR and RSA are preferred for multimedia data. Many innovators also suggest the combination of steganography and visual cryptography methods for better results.

The algorithm which we are dealing with particularly is the AES encryption algorithm. It is an Advanced Encryption standard often used to encrypt and decrypt images. This algorithm works with secret keys hence it is also known as Secret-Key Encryption. This secret key is used two ways for Encryption and Decryption. The key length determines the number of rounds. A single round includes mixing, transposition and substitution of the input plaintext and transforms it into the final output of cipher text. For better results only using a single algorithm is not sufficient. We combine the AES algorithm with another cryptography technique called Visual Cryptography.

Visual Cryptography is a cryptographic scheme based on the human visual system. In this scheme, the encrypted data is decrypted by the human eye. Due to this, Visual Cryptography doesn't require complex mathematical algorithms to encrypt and decrypt data. The main idea of this approach is to encrypt images into a number of different images called shares. Only when the shares are aligned together in order to match the transparency among the subpixels, the secret message can be seen and recovered. Here the image is divided in 2 shares hence the encrypted message divided into two different Visual Secret Sharing techniques that is hardware friendly and offers backward compatibility. In novel image encryption the two approaches of AES and Visual Cryptography are combined to create a strong algorithm which can withstand the current attacks and also provides efficient protection to the data to be encrypted. The nature of the images encrypted are usually texture based or visually grainy, which gives a clear indication that the particular image is an encrypted image and thus may lead to various attacks or analysis by malicious entities. These might include activities like modification or deletion of image content, various forms of cryptanalysis. In all these scenarios, the image integrity and availability are at a stake. To solve this issue, we introduce a technique that can convert the original encrypted images into visually meaningful ones. These visually meaningful images look like any other normal picture and hide the identity of the encrypted one.

The results of this novel method could be used in the medical field, military sector or even forensic department to transmit any confidential message so that the intruders can't gain access or leak the accessed data

CHAPTER 2

Literature Survey

Image data is the most common form of data in today's digital world and thus its security during storage and transmission is a major concern and an important topic of research. There are a variety of methods and techniques to perform image encryption which maintain the integrity and confidentiality of data. Each method has its own benefits and limitations. The method chosen by us is a combination of AES and visual cryptography, two of the most efficient and safe techniques. The results obtained using this technique prove promising for securely encrypting any image data. In [1], Security is a main scheme that secures image, the key and verifies transferred data integrity using MD5, AES encryption algorithm and Visual cryptography. Here data image with different size, length and resolution processed with cryptographic methodology. The retrieval of the original image is with good visual quality. In [2], By combining Encryption and Steganography the hybrid approach for image security has been shown. The image encryption is done using AES Encryption Algorithm. The image encryption technique based on AES is used to convert the original image into a cipher image. The encrypted image is then hidden to provide secret communication so that none other than the communicating parties can judge the communication. The image is hidden behind the cover image using the Steganography concept. Simulation results are shown and analyzed to check the effectiveness of the proposed hybrid approach against various attacks. In [3], the proposed approach is using Dynamic DNA for crucial grounded approach, is suitable to accept colorful forms of data similar to characters, textbook train, image and audio. Random key will be generated at the sender every time and will be used for decoding the ciphertext at the receiver makes

the approach veritably strong against colorful attacks. The proposed approach is delicate to break

by a common cryptanalysis technique. This approach provides two- stage security, bettered trust ability and better time. In [4], VC shares are generated using a general Visual Cryptography model and both these shares are included using the RSA algorithm used in public key cryptography. This algorithm was used to ensure that the secret shares were highly secure and successfully protected from malicious entities that try to alter the bit sequences intended to generate fake shares. In [5], various types of visual cryptography have been surveyed. There are various applications that make advantage of the ideas of visual cryptography. And found out color visual cryptography has become more popular than basic or black and white visual encryption. Numerous systems for binary, grayscale, and color images have been presented in existing literature. Future research in visual cryptography should concentrate on more modern image types like 3D images. In [6], an enhanced (2,2)-VSS scheme with really random shares is proposed. Test findings showed that, in contrast to earlier work, the strategy produces truly random shares as intended. The right values for the first share are chosen using heuristic methods. The second share's extended block values were chosen from six different combinations. The share size obtained is significantly increased. In [7], a visual cryptography method is used wherein, the multiple shares generation method with ECC(Elliptic Curve Cryptography) is used to construct the shares of the secret image. Using an encryption and decryption method compliant with ECC, the shares are separately encrypted and decoded. The private key for the decryption method is created using the CS optimization method. The image's secrecy is maintained, and the reclaimed image is made available as a singular image without the image's quality being compromised in any way. In [8], the authors have discussed how frequently digital products are shared across open networks for communication and hence the security of digital photographs has become crucial. The effectiveness of those encryption strategies is carefully explored and analyzed in order to support the performance of the encryption techniques and to guarantee the security procedures. In [9], The cryptographic method set forward has been put to the test using various input image formats, changing image size, and AES encryption algorithm keys. The proposed algorithm k-n secret sharing scheme divides an image into n shares in a way that allows the original image to be obtained by stacking at least k shares, where k and n. This system may be updated in the future to produce the shares using Visual Cryptography and to substitute a color image for the binary image as the key. The quality of the key sharing photos can be improved. In [10], To address the security weakness of most existing encryption algorithms, whose encrypted images are similar to texture or noise can lead to many attacks and analysis, a new image encryption concept that produces visually meaningful encrypted images that are usually considered as normal

images. of encrypted images is presented. With a large number of encrypted image formats, the proposed concept ensures that it is difficult for attackers to correctly distinguish

and locate encrypted images from all normal images. Thus, the proposed concept is able to protect the original image with a much higher level of security compared to most existing encryption algorithms

CHAPTER 3

Limitation of Existing system

While AES is a widely used and effective encryption algorithm for securing digital data, including images, there are still some limitations to using AES for image encryption. Some of the limitations are:

i. Limited Key Size: AES uses a fixed key size of 128, 192, or 256 bits, which can limit the number of possible keys that can be generated. This makes the encryption vulnerable to brute-force attacks, where an attacker can try different combinations of keys until they find the correct one.

ii. Vulnerability to Known-plaintext Attack: AES is vulnerable to known-plaintext attacks, where an attacker can obtain the key by analyzing the plaintext and ciphertext pairs.

iii. No Protection against Steganography: AES does not provide any protection against steganography, where an attacker can hide information within the image file.

iv. No Resistance to Side-channel Attacks: AES is vulnerable to side-channel attacks, where an attacker can obtain the key by analyzing the power consumption, electromagnetic emissions, or other side-channel information from the encryption process.

v. Limited Compatibility: AES is not compatible with all image formats and may require additional processing to work with certain types of image files.

Upon thorough observation of previous researches made, using Visual Cryptography as a standalone method for encrypting image data has certain limitation too such as:

i. Limited Security: Visual cryptography is a simple encryption technique that can only provide limited security for images. This is because visual cryptography only provides security against unauthorized access by human eyes, and it does not protect against attacks from computers or sophisticated algorithms.
ii. Poor Scalability: Visual cryptography is not scalable for large images or high-resolution images. This is because the encryption process requires a significant amount of space and resources to generate the shares.
iii. Poor Image Quality: The decryption of the shares in visual cryptography results in a low-quality image, which may not be suitable for certain applications.
iv. Vulnerable to Attack: Visual cryptography is vulnerable to several types of attacks, including brute-force attacks and statistical attacks. This is because the encryption algorithm is simple, and the shares generated are deterministic and predictable.
v. Limited Functionality: Visual cryptography can only provide encryption for grayscale images and cannot be used for color images or videos. This limits the functionality of the encryption system.

Thus, systems which did not attempt to use a combination of these technologies faced the above issues while implementing a successful encryption system for image data. AES and Visual cryptography as individual techniques are susceptible to certain attacks and are hence not suitable for image encryption.

CHAPTER 4

Problem Statement, Objectives and Scope

4.1 Problem Statement

Due to the growing use of the Internet and communication media, image encryption is rapidly increasing. Image sharing through unsafe open channels is vulnerable for attacking and stealing. For protecting the images from attacks, encryption techniques are required. In this project we propose a secure image encryption algorithm that uses both AES and Visual Cryptographic techniques to protect the image.

4.2 Objectives

- To work on AES (Advanced Encryption Standard) algorithm and implementing Visual Cryptography on the Key.
- For secure transmission of image data.
- To generate a visually meaningful encrypted image.
- To protect confidential image data from unauthorized access.
- To develop an efficient user interface for smooth encryption and decryption of images.

4.3 Scope

The scope of the image encryption system with AES and visual cryptography includes the development of a secure method for encrypting digital images using AES encryption and visual cryptography techniques. The primary scope of the system includes:

- Security: The system should provide a high level of security for the digital images by using AES encryption, which is a widely accepted encryption standard. Visual cryptography should also be used to enhance the security of the system.

- User-Friendly Interface: The system should have a user-friendly interface that allows users to easily encrypt and decrypt their digital images without requiring any technical knowledge or expertise.

- Performance: The system should be designed to perform efficiently and quickly, even when working with large image files.

- Compatibility: The system should be compatible with different image file formats, including JPEG, PNG, and BMP.

- Robustness: The system should be robust and resistant to attacks such as brute force and cryptanalysis.

The development of this image encryption system will require the use of programming languages such as Python, and web-framework such as Django for integrating the system code with the user-interface.

CHAPTER 5

Proposed System

5.1 Proposed System Overview

Architecture Diagram

An architectural diagram is a visual representation that maps out the physical implementation for components of a software system. It shows the general structure of the software system and the associations, limitations, and boundaries between each element.

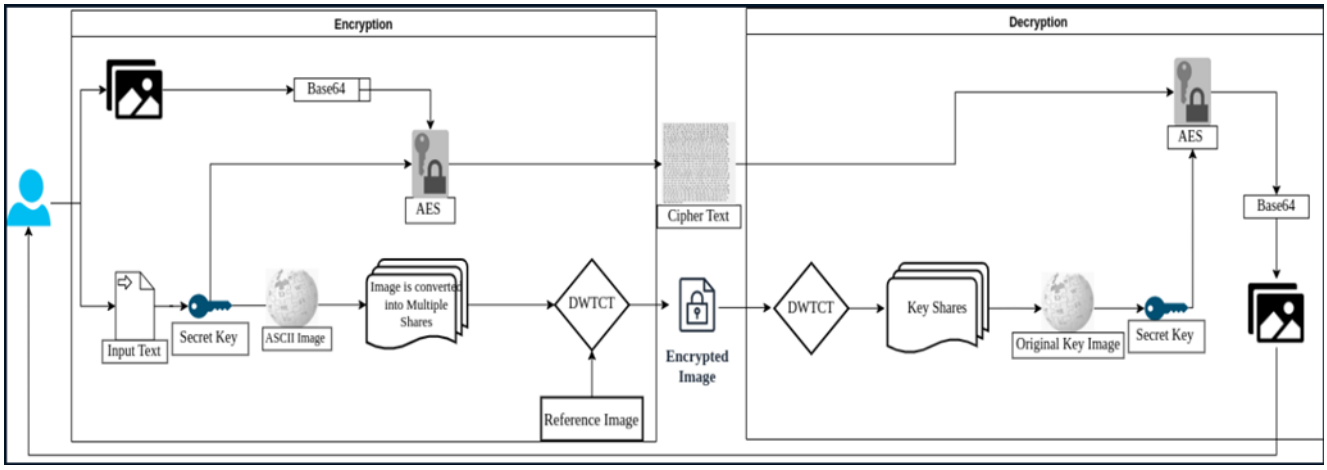

Fig 5.1: Architecture Diagram

Our model first converts an image into base64 format, where groups of 6 bits of data at a time are mapped to inoffensive printable characters. Then the text is hashed into the form of a key for the encryption. Using the characters in the text an image is created which is the split and sent ahead to use in decryption by merging those shares and reforming the key. The cipher text we get from encryption when decrypted uses the key and outputs a base64 encoded text, which we decrypt and get our original image back.

5.2 Design Details

5.2.1 DFD Diagram

DFD or Data Flow Diagram shows the flow of information in a system.

i. DFD Level 0

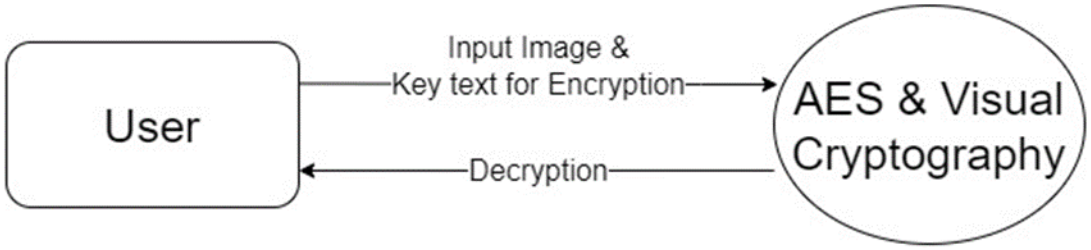

Fig 5.2.1: Data Flow Diagram Level 0

DFD Level 0 or Context Diagram shows the flow of information in the system as a single high-level entity. The user inputs the data to the application and the required results would be displayed to the user.

ii. DFD Level 1

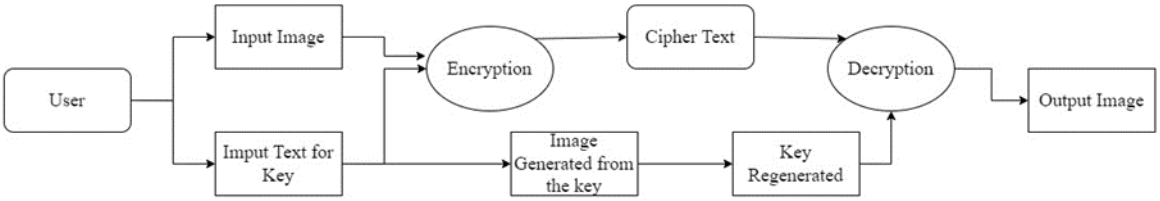

Fig 5.2.2: Data Flow Diagram Level 1

In DFD Level 1, the Context Diagram is decomposed into multiple detailed processes. The data such as audio data, image and the data from the report, is processed with the help of various algorithms. Using this processed data, the model predicts and outputs the results.

5.2.2 Activity Diagram

Activity Diagram

Activity diagram is basically a flowchart to represent the flow from one activity to another activity. The activity can be described as an operation of the system. The control flow is drawn from one operation to another. This flow can be sequential, branched, or concurrent.

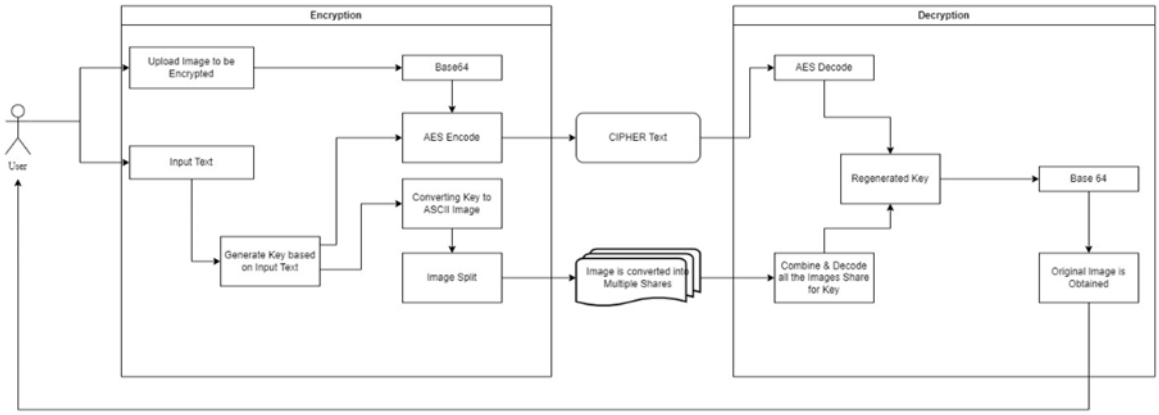

Fig 5.2.3: Activity Diagram

In our system, after landing on the home page, the user is given an option to upload an image to be encrypted, a reference image and a secret key text file. Upon clicking the encrypt button the key image shares, encrypted image and cipher text is generated. For decryption, the user is required to upload the previously obtained key shares and the cipher text to finally obtain the decrypted original image.

5.2.3 Sequence Diagram

Sequence Diagram

A sequence diagram is a Unified Modeling Language (UML) diagram that illustrates the sequence of messages between objects in an interaction. A sequence diagram consists of a group of objects that are represented by lifelines, and the messages that they exchange over time during the interaction.

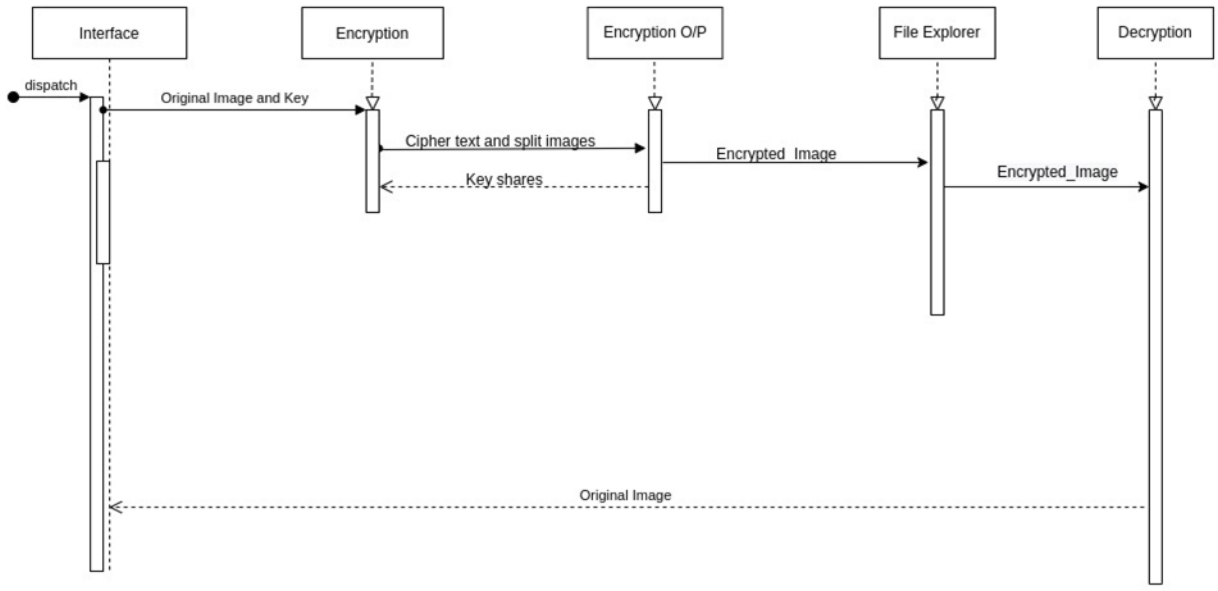

Fig 5.2.4: Sequence Diagram

In our system, Input is given to the interface, after which the encrypted image and the cipher text along with shares of the key image are sent out. To decrypt outputs obtained during encryption are taken as input , giving final decrypted output as the original image.

5.3 Methodology

Since Visual cryptography and AES are both prone to attacks and are not suitable for image encryption systems as individual technologies, we are proposing a system which uses an algorithm that can survive the current generation of attack scenarios as well as protect from future attacks. In order to this, we are using the best characteristics of both the prior mentioned techniques and combining them to work as a unit. Basically, the algorithm we suggest is divided into two phases: Encryption and Decryption.

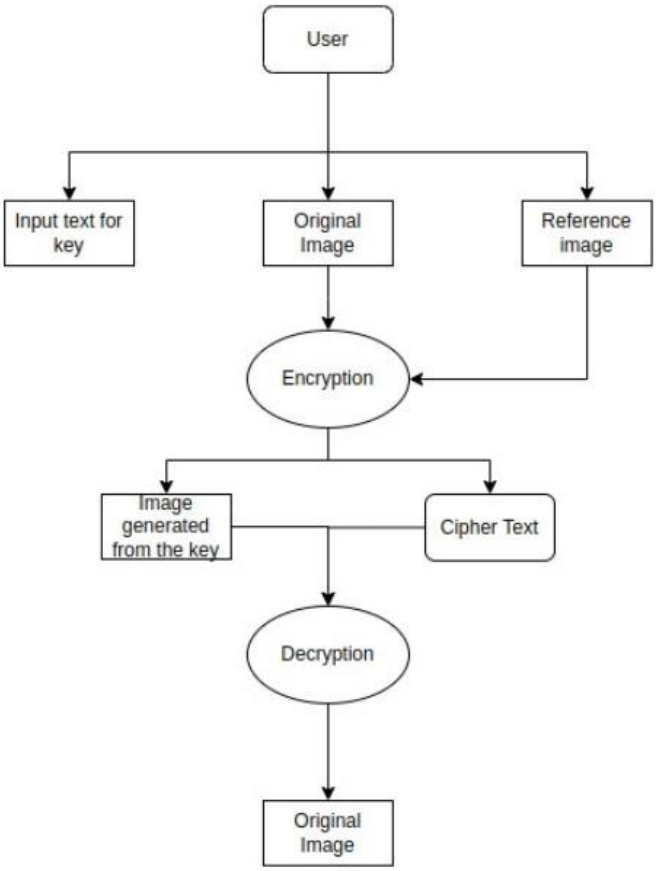

Fig 5.3.1: Flow Chart

During Encryption phase, three inputs are expected which are: the image I to be encrypted, key K and a reference image. The key K is transformed into a secret key called SK with the help of SHA 256 algorithm which is a type of hashing algorithm.

Fig 5.3.2: Working of SHA-256

Next, our original image I is encoded into a base64 string called BI. Base64 is a binary to text encoding scheme and it is commonly used when we need to encode a particular binary data that is required to be stored and sent over the media that is fundamentally designed to deal with only ASCII values. To finally obtain a Cipher text CI, the string BI and secret key SK are both fed into the AES algorithm. The AES algorithm is implemented specifically in Output Feedback (OFB) mode. In the same encryption phase, the original key K is converted to image KI. This procedure is done using ASCII encoding. After the image is generated, it is split into a number of key shares KI1, KI2, KI3…..KIN. These key shared images play a crucial role in the decryption process as well. Now, the reference image and the key shares previously generated are both passed through the DWTC function, where the final encrypted image is created and displayed to the user.

For our system, we use the AES algorithm in the Output Feedback (OFB) Mode. OFB mode is a stream cipher that works by encrypting a fixed-length plaintext data block into a fixed-length ciphertext data block using a secret key.

The basic operation of the AES algorithm in OFB mode image encryption can be explained as follows:

I. Key generation: The secret key is generated using a secure key generation algorithm. A key is usually a binary string of some length, such as 128, 192 or 256 bits.

II. Initialization Vector (IV) Generation: The IV is a random binary string of the same length as the block size of the AES algorithm and is used to initialize the state of the OFB. The IV is generated using a secure random number generator.

III. Encryption: The image data is split into fixed-length blocks, typically of 128 bits. The OFB mode encrypts each block of plaintext data by first encrypting the current IV value using the secret key and the AES encryption algorithm. The resulting ciphertext block is then XORed with the plaintext block to produce the encrypted image block. The current IV value is then updated by encrypting it with the secret key and the AES encryption algorithm. This process is repeated for each block of image data.

OFB mode is a secure encryption method, as it allows one key to encrypt large amounts of data without compromising security. Additionally, the use of an IV value ensures that even if two identical blocks of plaintext are encrypted, the resulting ciphertext will be different due to the unique IV value used for each encryption operation. This makes it difficult for an attacker to decipher the encrypted image data.

After these steps are executed, the DWTCT function plays a key role to generate a visually meaningful encrypted image. The fundamental concept here is that we use a normal reference image and the original image to be encrypted to generate a visually meaningful encrypted image that looks exactly like the reference image.

Working of DWTCT:

I. Convert the original image to a matrix of pixel values.

II. Add DWT to the matrix using a predefined wavelet function such as Haar, Daubechies or Coiflet.

III. Divide the resulting DWT coefficients into several subgroups, each representing a different frequency range.

IV. Apply permutation and replacement process to subgroups with secret key. This process should shuffle the data in a way that makes it difficult for unauthorized persons to recover the original image, but preserves its visual meaning.

V. Apply inverse DWT to the encrypted sub bands to obtain an encrypted image.

There are many variations of this basic algorithm, and additional steps can be added to improve the security and visual quality of the encrypted image.

For the Decryption procedure, two inputs are required: the cipher text and the previously generated encrypted image. A user interface will be created to input the image and key text as well as display the decrypted images to the user. During decryption, our previously generated key shares are obtained from the visually meaningful encrypted image and then these key shares are used to reconstruct the original key image KI. To convert this key image to key text we use ASCII decoding. The key thus obtained is transformed to secret key SK using SHA- 256 hashing algorithm. After this procedure is completed, the cipher CI and secret key SK are sent as input into the AES decryption algorithm. The output of this algorithm is a base64 encoded string message of the original image. Finally, this encoded image is decoded to generate our original image as output to the user.

To obtain the key shares from the visually meaningful encrypted image, the DWTCT function works as follows in the decryption process:

I. Obtain the encrypted image and the secret key used for encryption.
II. Apply DWT to the encrypted image using the same wavelet function and decomposition level used during the encryption process.
III. Divide the resulting DWT coefficients into several subgroups, each representing a different frequency range.
IV. Create the same chaotic sequence used during the encryption process.
V. Apply an inverse chaotic transform to each subgroup of the encrypted image using the same chaotic sequence to obtain the encrypted sub-bands of the original image.
VI. Apply inverse DWT to the mixed sub-bands to obtain the original image.
VII. Generate the hidden key shares.

The AES algorithm operating in OFB (Output Feedback) mode for image decryption is a process that reverses the encryption process to obtain the original plaintext image data. The decryption process uses the same secret key and initialization vector (IV) used during the encryption process. The steps to decrypt an image encrypted with the AES algorithm in OFB mode are as follows:

I. Key generation: The same secret key used during the encryption process is used for decryption.

II. Initialization Vector (IV) generation: The same IV used during the encryption process is used for decryption.

III. Decryption: Encrypted image data is divided into fixed-length, typically 128-bit blocks. OFB mode decrypts each block of ciphertext data by first encrypting the current IV value with the secret key and the AES encryption algorithm. The resulting ciphertext block is then XOR-encoded with the encrypted image block to produce a cleartext image block. The current IV value is then updated by encrypting it with the secret key and the AES encryption algorithm. This process repeats for each block of encrypted image data.

IV. Original image reconstruction: Once all encrypted image blocks are decrypted, they can be combined with the original plaintext image.

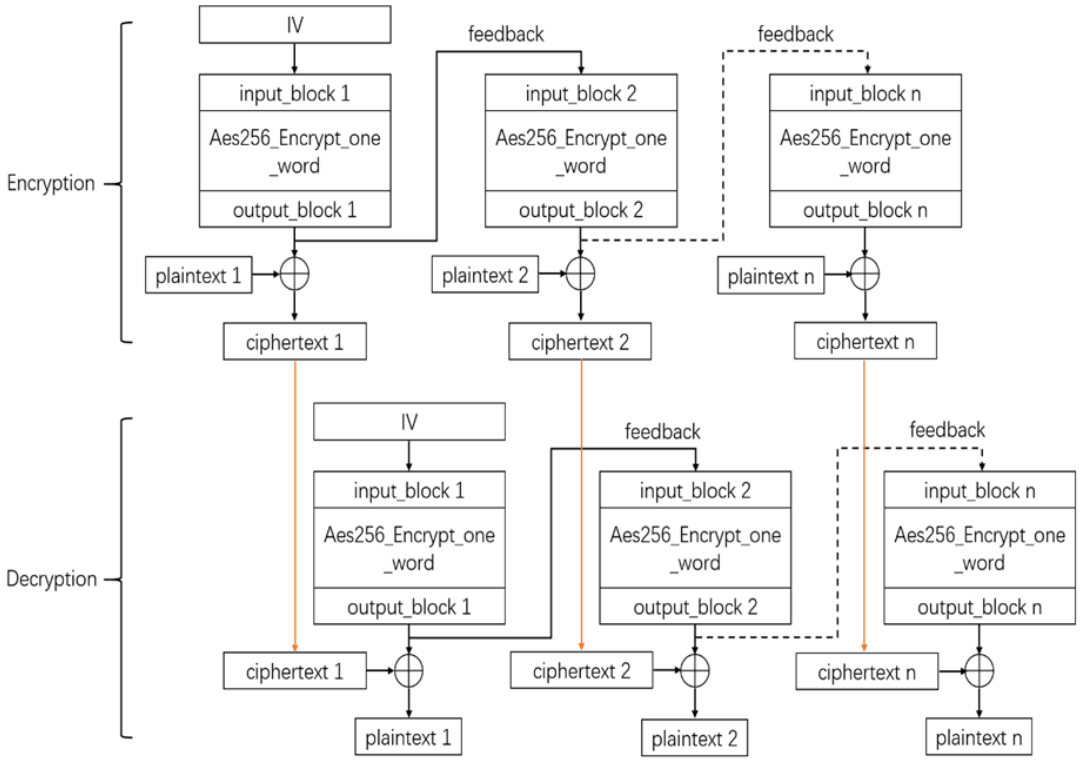

Fig 5.3.3: Working of AES in OFB mode

The algorithm is thoroughly analyzed in terms of efficiency by using images of different quality and resolution as well as keys with varying sizes.

CHAPTER 6

Experimental Setup

6.1 Requirement Analysis and details about input to systems or selected data.

Operating Systems such as Windows, Linux or Mac can be used, A minimum of 8 GB RAM is required to process the heavy models. At least 2.8Ghz CPU speed would be required. Visual Studio Code is a code editor redefined and optimized for building and debugging modern web and cloud applications. For running a project in data science or data visualization, one could use Jupyter notebooks inside VS Code. Python is an interpreted, high-level, and general-purpose programming language. The entire GUI and processing in this project will be done in python. In this project, we are going to use python's web-based framework, Django. Django is used to integrate the backend system code with the frontend to provide a smooth user interface to the users. CSS is used to style an HTML document. CSS describes how HTML elements should be displayed. Bootstrap is a framework which is used to create user interfaces in web applications. It provides CSS, JS and other tools that help to create the required interfaces.

6.2 Prerequisites for using the model

For using image encryption system, the user is required to have an image to be encrypted, a random reference image and a text file containing any text that could be considered as the secret key file. For the Decryption process, the user should have the previously obtained key shares along with the Cipher text file generated in order to successfully decrypt the image.

6.3 Software and Hardware Set up

i. Hardware requirements

- Operating Systems
- 8 GB RAM
- i5 Processor

ii. Software requirements

- VSCode, PyCharm
- Python 3.8 and above.
- HTML, CSS, JavaScript, Bootstrap

The execution of the proposed system is carried out on Dell Vostro 3500 having Intel Core i5-1135G7 CPU running at 2.42 GHz and consisting of 8GB RAM. The algorithms are implemented using Python 3.10.2. The project also includes a user-friendly interface to carry out the encryption and decryption process.

CHAPTER 7

Result

The execution of the proposed system is carried out on Dell Vostro 3500 having Intel Core i5-1135G7 CPU running at 2.42 GHz and consisting of 8GB RAM. The algorithms are implemented using Python 3.10.2. The project also includes a user-friendly interface to carry out the encryption and decryption process. If the user wants to carry out encryption on any image, they are asked for three inputs- The original image to be encrypted, a reference image and a text file which contains a secret key. The output obtained by the user's system are- the encrypted image, two key shares and a text file containing the cipher text. When the user wants to perform decryption, they are asked to provide the key shares and the cipher text as input in order to obtain the original image back.

The user interface is as follows:

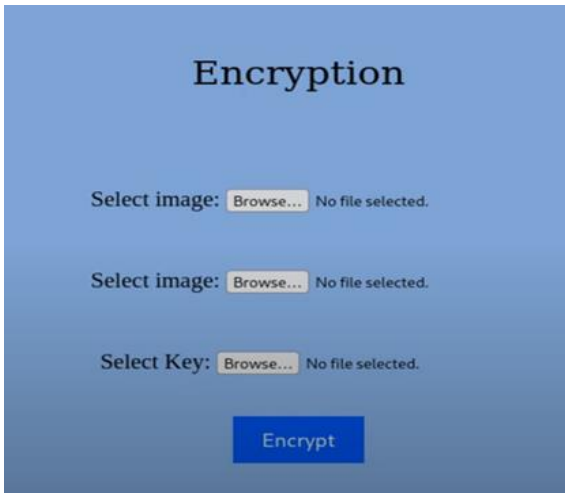

Fig 7.1: Encryption window

Fig 7.2: Decryption window

The following are the images given as input by the user.

Fig 7.3: Image to be sent for encryption

Fig 7.4: Reference image

The outputs obtained by the user on clicking the ’Encrypt’ button is, a text file containing the cipher text and the following images: -

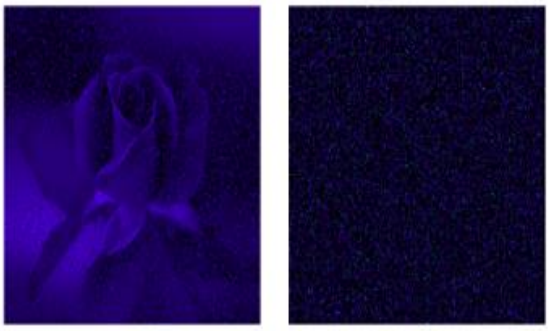

Fig 7.5: Key shares generated

Fig 7.6: Encrypted image

CHAPTER 8

Project Plan

Our project started in July 2022, and after finalizing the topic and objectives, we began working on it. Phase one covered project conception, project study, and design layout. In phase two, we designed our proposed system, and in the final third phase, we completed project implementation, and submitted a research paper along with our results.

Gantt Chart

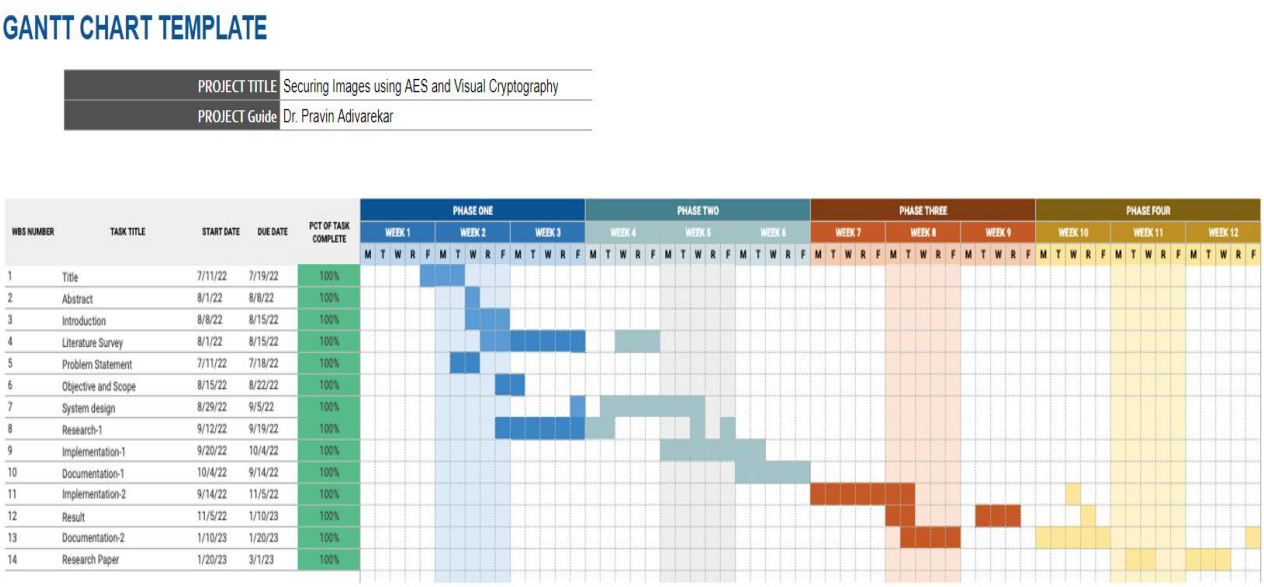

Fig 8.1: Gantt Chart

CHAPTER 9

Conclusion

Thus, we have successfully implemented a secure image encryption system using AES algorithm, Visual cryptography and the Discrete Wavelet Transform function. The encrypted images generated by our system are visually meaningful in nature and not like the usual noise or texture based which proves to be a huge differentiating factor from other general image encryption system. The unique image encryption methodology proposed in this paper has been successfully tested on numerous images with varying resolutions as well with varying key sizes for the AES algorithm. It is observed that the visually meaningful encrypted images are of good quality in all of the tested scenarios

CHAPTER 10
Future Scope

In future, this system could be further enhanced by improving the quality of the key shares generated which would in turn positively affect the efficiency of the algorithm proposed. Furthermore, an advanced SSL (Secure Sockets Layer) could be deployed to securely transfer encrypted outputs to the user. Additional security measures could also be executed to control various image processing attacks like translation, rotation and scaling of key shares. An image encryption system that combines AES, visual cryptography, and DWTCT function is a promising technology that has a wide range of potential future applications. Some potential future scopes or applications for this technology could also include:

- Secure Communication: The image encryption system can be integrated with messaging apps to provide secure communication. The system can encrypt the images and messages before transmitting them, ensuring that only the intended recipient can decrypt and view them.

- Medical Applications: The system can be used in the medical field for secure transmission of patient information, including X-rays and CT scans. This would help ensure the privacy of patients' sensitive information.

- E-commerce: The image encryption system can be integrated with e-commerce platforms to provide secure transmission of product images and other sensitive information between buyers and sellers.

- Defense and Intelligence: The system can be used in defense and intelligence applications for secure transmission of sensitive information between military and government agencies.

- Banking and Finance: The system can be used in the banking and finance industry to provide secure transmission of financial information, such as bank statements, tax returns, and other sensitive financial documents.

- Cloud-based Image Encryption: The image encryption system can be integrated with cloud-based services to provide secure storage and transmission of images. This would help ensure the privacy of users' images and sensitive information stored in the cloud.

Overall, the future scope of an image encryption system implemented using AES, visual cryptography, and DWTCT function is quite promising. The technology has the potential to secure communication, protect sensitive information, and enhance privacy in various industries.

References

[1] Rao, Anjana; Suma, D (2018). [IEEE 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS) - Bengaluru, India (2018.12.20-2018.12.22)] 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS) - A Novel Image Encryption Algorithm with Image Integrity Check., (), 98–104. doi:10.1109/csitss.2018.8768797

[2] Saini, Jaspal Kaur; Verma, Harsh K (2013). [IEEE 2013 IEEE Second International Conference on Image Information Processing (ICIIP) - Shimla, India (2013.12.9-2013.12.11)] 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013) - A hybrid approach for image security by combining encryption and steganography. , (), 607–611. doi:10.1109/ICIIP.2013.6707665

[3] Akiwate, Bahubali; Parthiban, Latha (2018). [IEEE 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS) - Belgaum, India (2018.12.21-2018.12.22)] 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS) - A Dynamic DNA for Key-based Cryptography. , (), 223–227. doi:10.1109/CTEMS.2018.8769267

[4] K. Kaur and V. Khemchandani, ”Securing Visual Cryptographic shares using Public Key Encryption,” 2013 3rd IEEE International Advance Computing Conference (IACC), Ghaziabad, India, 2013, pp. 1108-1113, doi: 10.1109/IAdCC.2013.6514382.

[5] R. Bhatnagar and M. Kumar, ”Visual Cryptography: A Literature Survey,” 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 78-83, doi: 10.1109/ICECA.2018.8474649.

[6] Mustafa Ulutas, Rifat Yazici, Vasif V. Nabiyev and Guzin Ulutas, Secret ¨ Sharing Scheme With Improved Share Randomness, IEEE, 2008, ISBN 978-1-4244-2881-6/08.

[7] K. Shankar and P. Eswaran,” RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique”, J CIRCUIT SYST COMP, vol. 25, no. 1650138,

[8] Pakshwar, Rinki, Vijay Kumar Trivedi and Vineet Richardia. ”A survey on different image encryption and decryption techniques.”, IJCSIT) International Journal of Computer Science and Information Technologies 4.1, 2013.

[9] Kumar, M. Arun, and K. Jhon Singh, ”Novel Secure Technique using Visual Cryptography and Advance AES for images.”, International Journal of Knowledge Management and e-learning, Vol. 3, No. 1, pp. 29-34, 2011.

[10] Bao, L., Zhou, Y. (2015). Image encryption: Generating visually meaningful encrypted images. Information Sciences, 324, 197–207. doi:10.1016/j.ins.2015.06.04

Publications

Paper 1: Securing Images with AES and Visual Cryptography Techniques

Conferences:

[1] 4th INTERNATIONAL CONFERENCE OF EMERGING TECHNOLOGIES 2023, BELGAUM, INDIA

Status: Paper Accepted

[2] 2023 IEEE World Conference on Applied Intelligence and Computing (AIC 2023)

Status: Paper Submitted