Security Algorithms and Protocols

Sri Manjusha Tella and Neha Ersavadla

Image And Video Cryptography

1. Abstract

The main aim of this project is to provide security to images and video files using the advanced encryption standard algorithm (AES).

Now a day's almost all digital services such as military and medical imaging systems, internet communication systems and multimedia share most of their information via internet due to the rapid growth of today's technology. These images or videos being transmitted through the network may contain some important information which may be breached by hackers by an intrusion attack and they may use the copied content for other purposes or may alter the existing information causing havoc to the sender and receiver. Thus there is need of a security level in the digital media systems where the images or videos sent are transmitted in an encrypted format to the receiver over the network. The client having received the file should decrypt it using this application so that no third person may hack the file and copy its contents. This application makes the transmission of both image and video files secure over the network.

This application mainly uses the AES algorithm which is considered to be more secure due to its key length. The AES works mainly on the concept of key expansion and is totally reversible which makes the process of encryption and decryption secure. AES is a symmetric block cipher and works on a fixed number of bytes.

2. Introduction

In the last few years the issue of data integrity and security has become one of the main concerns. The data being transmitted via various computer networks may be vulnerable to attacks, which resulted in cryptography techniques. These make the transmitted data secure when encrypted before the process of transmission. The process of converting a series of plain text into its corresponding cipher text s called as cryptography. This process has two parts namely encryption and decryption. The encryption and decryption are the techniques where we uphold the security of a plain text or image and decode the upheld security to know the original plain text or image respectively. AES is a symmetric key encryption algorithm. AES is a block cipher that encrypts 128 bits of data. Some of the main topics in the science of cryptography include confidentiality and authentication

2.1. Confidentiality

The concept of confidentiality ensures that the message can be read by only the intended receiver. This can be fulfilled by the technique of encryption to secure the information being sent from the sender to the receiver. These types of techniques were used in government military applications and now in larger public domains such as e-commerce websites, internet, automatic teller machines and mobile applications.

2.2. Authentication

The concept of proving the information being sent is one's identity. It can be defined as the phenomenon of recognizing the user's identity. It is associated with verifying the user's credentials and requests.

2.3. Image cryptography

The image encryption and decryption plays a major role in the field of securing the information. Thus no hacker or unauthorized user may have access to the original transmitted information via large public networks.

Various image cryptography techniques are being used in various fields such as military and in digital media platform. In this paper we implement the image encryption and decryption using the AES algorithm.

2.4. Video Cryptography

The growth in the platform of digital media has been increased rapidly in the past few years. For example many fields such as military use various videos to train the newly joined people or transfer evidences which are very confidential and classified to them. Such sensitive data should be secured from unauthorized users or hackers.

Thus encrypting the videos solves this problem as the third party people who might have violated rules and had attained access to the videos wouldn’t understand the data content as it is encrypted. The algorithm we use for video cryptography must be efficient in all ways because the size of the data in videos is more. We are implementing the AES algorithm for video cryptography in this project paper.

3. Background And Related Work

The work on encrypting the videos and images has been in process from many years in order to secure the data being transmitted via huge networks from hackers and other access denied users. Many algorithms have been developed for efficiency and applied in real time applications. The digital media encryption is one of the major fields using the science of cryptography. The image cryptography is mainly classified into categories based on the image

color scales, random permutations method or vector quantization methods. Similarly the video cryptography is categorized based various characteristics namely completely layered encryption, using permutation or selective encryption. Many other parameters contribute and influence the working of these processes.

4. Methodology

4.1. AES Algorithm

Both the image and video cryptography is done using the Advanced Encryption Standard Algorithm. It is of three types namely AES-128, AES-192, and AES-256. This classification is based on the length of the key used in the algorithm. The AES encryption algorithm mainly consists of four different transformations such as substitute byte, shift row, mixing columns and adding a round key. The decryption algorithm is the reverse process of the above four transformations stages.

4.2. Image Cryptography

This process mainly includes the ability to get the original image pixels. We need to create a strong encryption image so that it may not be vulnerable to any attacks. It should be efficient and faster in a way such that the data gets transferred faster from the sender to the receiver. The other important thing to consider is the perfect quality of the original image as a result of the image decryption process.

The algorithms are given two inputs, an image and a key. The image we want to encrypt is given as the input to the algorithm and the corresponding key in a hexadecimal format. The output is same size that of the input image. For the process of encryption - firstly, we divide the input image into a 4 * 4 matrix format. Then we determine the number of rounds based on the key length. Suppose the number of rounds is n, we will perform about (n-1) rounds which include the four transformation stages. The final round does not consist of the mixing columns transformation stage. For the process of decryption - the reverse process of the encryption is used to get the original image as an output and the encrypted image and the key are given as inputs. The transformation stages that are to be implemented in all the rounds are inverse substitution byte, inverse shift rows and inverse mixing columns.

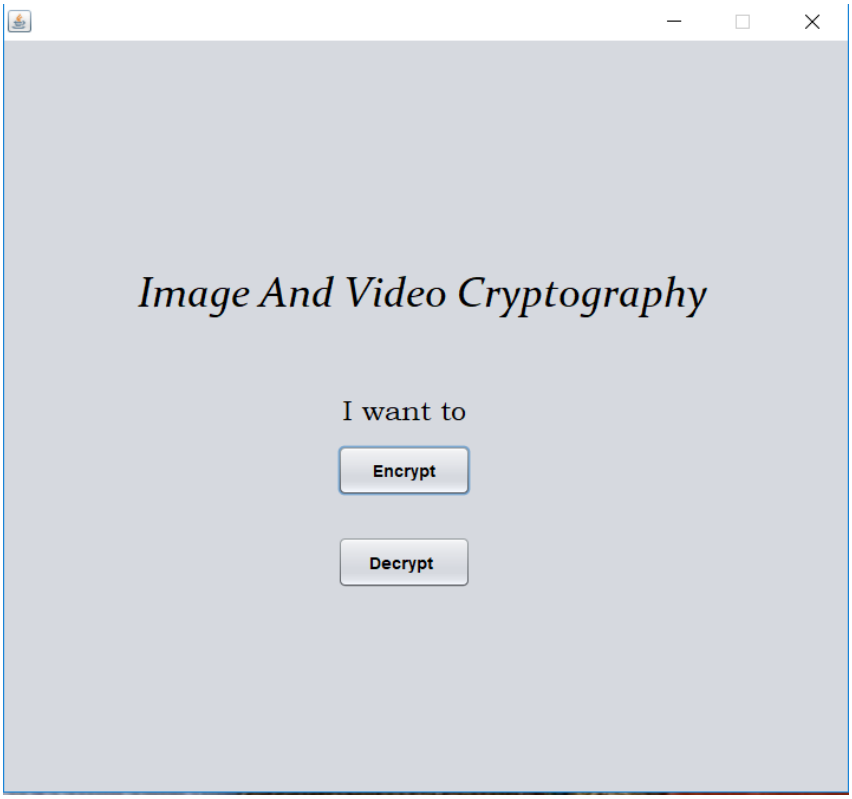
4.3. Video cryptography

The video encryption algorithms have become one of the major areas of concern for securing the data being transmitted in the forms of digital media through public networks. We are implementing the AES algorithm for video encryption and decryption. For the process of encryption - firstly, the video is divided into a number of frames using a video editor. These frames cannot be considered as images as they also contain the audio information along with the picture. The transformation stage of shuffling will randomly shuffle all the frames and they are sent into a block or stream. This shuffling is done so that the resultant audio is not

understandable when we play the video. We can implement this shuffling by a random unique key generation. This key will be sent to the receiver in order to crack the shuffling methodology when decryption is done. The code words obtained for each frame are encrypted and sent to the receiver which makes the data more secure and beyond human interception. For the process of decryption - the receiver must run the algorithm on the code words to get the original video. Later the receiver should reshuffle all the frames which are decoded using the shuffling key which will result in the original video.

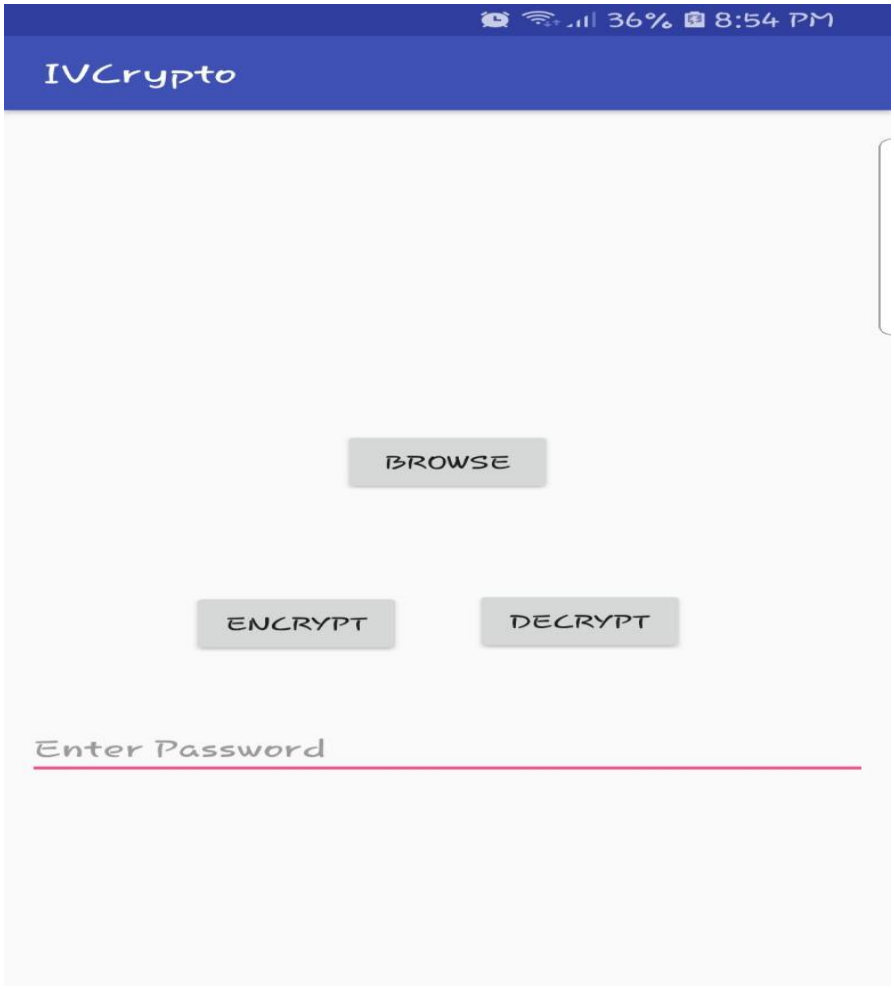
5. Experiments and Analysis

We have developed the java code for the image encryption and decryption which works efficiently. We have developed a java application for image and video cryptography using java swings. We have chosen java swings as it has easier and understandable graphical user interface through which we could make it more interactive. We have used the AES algorithm for encryption and decryption. We also used secure hash algorithm to verify the password for encrypting and decrypting the image and video files. The password is not stored anywhere so it's necessary for the user to remember the password otherwise it is hard to recover the encrypted file. The below screen shot shows the java application we have created.



We have also created an android application which encrypts and decrypts both images and videos. We named the android application as IVCrypto. We used AES algorithm for image

and video cryptography. We need to enter the password to encrypt or decrypt the files. The below screen shot shows the android application we have created.



6. Conclusion and Future Work

The image and video cryptography is implemented using the AES algorithm; this algorithm offers mostly efficient encryption quality which makes the data transmission more secure. The time required for the image and video encryption using AES algorithm is less when compared with the DES algorithm which makes it more efficient in large domain and real time applications.

The future enhancement can be done by making the encryption process of the images and videos more secure by converting them into their corresponding color scales. This process might take lesser time and work efficiently by encrypting the data using the color scales. The video cryptography can be made more secure by encrypting each and every frame of the video and shuffling the frames so that no third party can hack the system and compromise data integrity.

7. Bibliography

https://arxiv.org/ftp/arxiv/papers/1412/1412.8490.pdf

http://www.iraj.in/journal/journal_file/journal_pdf/3-27-139087843544-48.pdf

https://www.ijser.org/researchpaper/An-image-encryption-and-decryption-using-AES-algorithm.pdf

http://www.cs.man.ac.uk/~banach/COMP61411.Info/CourseSlides/Wk2.3.AES.pdf

https://www.cse.wustl.edu/~jain/cse571-11/ftp/l_05aes.pdf

https://ieeexplore.ieee.org/document/6966311/

https://arxiv.org/ftp/arxiv/papers/1303/1303.3485.pdf