# Achieving Abysmal Security for Multimedia Data using H.264/AVC Algorithm

**Rajesh Gaikwad[1] Swati Maurya[2] Sneha Mishra[3] Nihal Shaikh[4] Affreen Belim[5]**
[1]Assistant Professor [2,3,4,5]Student
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]Shree LR Tiwari College Of Engineering, Maharashtra, India

*Abstract*— Nowadays, the ever increasing and dominant use of large media viz video, image, text transmission systems are increasing the prominence of personal privacy issues. It can't be denied that media transmission systems are necessary to be deployed in order to overcome and mitigate the perception of insecurity caused mainly as a result of terrorist threats and high criminal rate. But in doing that, there arises a significant concern regarding privacy invasion. In this paper, the general model of a typical encryption/decryption system about the security principle is discussed. Data encryption mainly includes the scrambling of the content of image, and video particularly to make the data unreadable, invisible or incomprehensible during cipher text transmission. The objective of this step is to ensure that the content of the data is protected against attackers. Data decryption is basically the opposite of data encryption. It recovers the original data. So as the name suggests, ABYSMAL SECURITY provides privacy protection endlessly and on the other hand reconcile the need for media transmission systems. Here we will elaborate the aspects like description, problem statement, scope, motivation and also the objectives of our project

***Key words:*** H.264/AVC Algorithm, Abysmal Security

## I. INTRODUCTION

### *A. Description*

Here we will elaborate the aspects like description, problem statement, scope, motivation and also the objectives of our project

### *B. Problem statement*

While transferring the data over, network security of this data is important .As we know that whatever task is performed for that reason consumes a lot of CPU memory cycle .Hence encryption and decryption processes too requires it. Therefore these security algorithms consume a good amount of resources encrypting and decrypting the data. So it becomes a must for them to have a great performance complementary to security.

So while we are transferring the data over network the main concern is data is not lost adding to it is that there is no loss of data with faster transmissions. For this purpose we use many different compression algorithms which reduces the size of data during transmission. Hence lossless compression algorithm are used if data being transferred is important and if loss of data is not affordable.

If a compressed file is encrypted, it has better security and faster transmission rate across the network than encrypting and transferring uncompressed file which increases the overhead like size of file and processing time etc. Also identify whether the file has to be first compressed before encrypting or not .If needed then identify the best suited algorithm that should be used for compressing the file according to data type and data size to reduce the overhead of time and increase the efficiency and security to data that is being transferred.

Health related data has different data formats like image, text, video. Thus this data is confidential and needs to be transferred secured. Compression, Scrambling & Encryption play an important role in securing this data against unauthorized attack. Therefore along with security factors like cost and performance of different Scrambling, Compression, Encryption algorithms also need to be considered for practical implementation.

Thus parameters like data type, data size, and compression ratio, key size, key strength, encryption time, decryption time affects the selection of algorithm. So if we want to transfer the file, firstly the file is scrambled then compressed then encrypted. Hence by using these three main techniques we can achieve robust security and excellent performance too.

### *C. Scope and Motivation/Objectives*

The issue of Personal Privacy is increasingly becoming prominent with the white spread use of large video surveillance systems. While the deployment of video surveillance is justified by the perception of insecurity due to terrorist threats and high criminality rate, the rightful fear of privacy invasion is turning into a significant concern. In this project we attempt to reconcile on the one hand the need for video surveillance and on the other hand the concern of privacy protection.

In this project we intend to provide a solution to the problem arising due to loss of privacy as well as result of increase in media surveillance system. The scope of H.264 can be explained as H.264 offers greater flexibility in terms of compression options and transmission support. Similarly AES/DES offers greater flexibility in terms of compression option and transmission support for text, image video.

## II. LITERATURE REVIEW

Here we will elaborate the aspects like the literature survey of the project and what all projects are existing and been actually used in the market which the makers of this project took the inspiration from and thus decided to go ahead with the project covering with the problem statement.

*A. AUTHOR: Secure Image Processing using AES Algorithm: This paper was proposed by BhavanaVerma and SonaMalhotra, Kurukshetra*

Keywords: Cryptography; Digital image; Advanced Encryption Standard (AES) Encryption and Decryption.

In this project, they proposed a security demonstrate that depicts a plan of successful security for correspondence by AES calculation for encryption and unscrambling. It depends on AES Key Expansion in which the encryption

All rights reserved by www.ijsrd.com 

procedure is somewhat selective or operation of an arrangement of picture pixels alongside the 128 piece key which changes for each arrangement of pixels. In January, 1997 NIST started its push to build up the AES, a symmetric key encryption calculation, and made an overall open require the calculation to succeed DES. With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure, the key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text. The AES algorithm is designed to use one of three key sizes.

*1) Algorithm of AES:*

- Step 1: To input an Image.
- Step 2: Convert this analog image into digital image.
- Step 3: Convert the image pixels into Row and Columns form.
- Step 4: Perform transpose of Columns.
- Step 5: Add these columns using bitwise-Xor operation.
- Step 6: Get the Output.

*B. AUTHOR: Video and Data Encryption Using AES Encryption for Secure Transmission was proposed by International Journal of Scientific & Engineering Research, Volume 6, Issue 4, April-2015*

Keywords: AES Encryption, Data Hiding, Encoding, Embedding data, Steganography, zigzag.

In This paper, video and data is encrypted using AES algorithm for secure transmission. A data hiding process that is combined with encoding and encryption called Steganography is used for embedding messages into video or image to transfer a large amount of secret message. Huffman coding is a technique for lossless data compression and reduction of file size. Huffman coding is used to encode images in a video file. Then the encoded embedded file is encrypted using AES encryption. The process is repeated until the search is done all over the frame. It is decrypted only when the user knows the key. The experimental result shows that the degradation of visual quality is less. The performance of the process is measured by calculating Peak signal to noise ratio, Mean square error rate and Bit error rate.

*C. AUTHOR: Image Compression Using H.264 And Deflate Algorithm proposed by Dr. M. Sundaresan and E. Devika in the year 2016*

Key words: Lossy Compression, Lossless Compression, H.264, Deflate.

Compound image is combination of text, graphics and pictures. Compression is the process of reducing the amount of data required to represent information. It also reduces the time required for the data to be sent over the Internet or Web pages. Compound image compression is done on the basis of lossy and lossless compression. Lossy compression is a data encoding method that compresses data by discarding (losing) some data in the image. Lossless compression is used to compress the image without any loss of data in the image. Image compression is done using lossy compression and lossless compression. In this paper different techniques are used for compressing compound images. The performance of these techniques has been compared. The lossy compression is done using H.264 compression algorithm.

## III. PROPOSED SYSTEM

Information hiding techniques have recently become important in a number of application areas. It is often thought that communication may be secured by encrypting the traffic, but this has rarely been adequate. This project emphasizes on hiding the message rather than enciphering them.

The main aim of this project is privacy protection for multimedia transmission, here focus is mainly on video, image and texts. Security to media will be given in three layers.

*A. Scrambling:*

A Scrambling approach is a method which is employed on almost all commercially manufactured system including image and video systems.

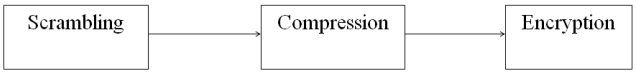
A valuable content scrambling approach is a raising issue as protecting content copyright is important. Image and video scrambling is well employed and general way is to hide unwanted information and disclose an interpretable image and video. There have been many methods regarding image and video scrambling.

The scrambling process we are aiming to implement involves dividing an image or video into NxN blocks. These blocks are then shuffled by some random process. And this shuffled image is then used to transfer the data.

*B. Compression:*

Compression is a reversible conversion of data. This allows a more efficient storage or transfer of data. The inverse process is called decompression. Lossless compression allows 100% recovery of the original data, where a loss of information is a major damage. The conversion to be applied on the images or videos might cause data redundancy.

So the question arises why do we need data compression? Data compression deals with reduction in the size of a data thus making it easier to transmit over a communication channel. However, one must keep in mind that there is always a trade-off between data size and quality. The compressed image is then encrypted using any encryption algorithm. And then it is transferred over the communication network.




## IV. EXISTING SYSTEM

The existing system comprises of either, an algorithm which helps determine transfer of not all possible data's efficiently over a single network. The data transmitted over a single network might either get compressed or encrypted. Scrambling for higher security is not quite used yet over a single network.

Thus, providing efficient as well as encrypted transmission is over a network can be accomplished by this proposed system.

## V. ALGORITHMS USED FOR IMPLEMENTING THE SYSTEM

1) H.264/AVC or MPEG-4 algorithm is used to implement the following proposed system. It is a recently completed video compression standard jointly developed by the ITU-T VCEG and the ISO/IEC MPEG standards

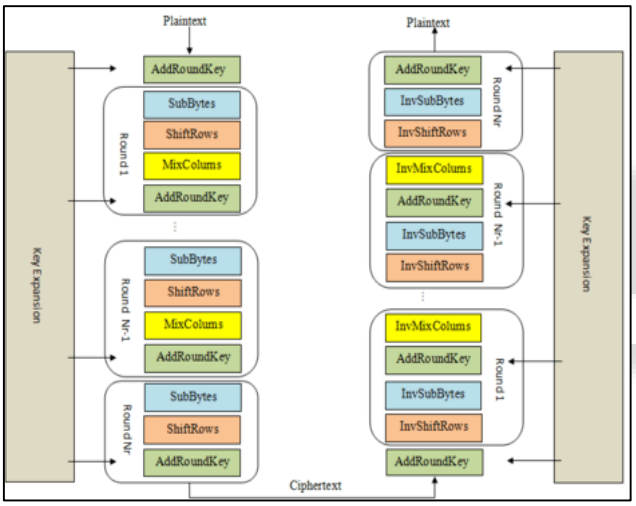
All rights reserved by www.ijsrd.com 

committees. The standard promises much higher compression than that possible with earlier standards. Further it supports flexibility in coding as well as organization of coded data that can increase re silence to errors or losses.

2) The Advanced Encryption Standard (AES) Algorithm
Encryption with AES The encryption phase of AES can be broken into three phases: the initial round, the main rounds, and the final round. All of the phases use the same sub-operations in different combinations as follows:

*A. Initial Round*

- Add Round Key
- Main Rounds
- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key
- Final Round
- Sub Bytes
- Shift




*B. Decryption in AES*

To decrypt an AES-encrypted cipher text, it is necessary to undo each stage of the encryption operation in the reverse order in which they were applied. The three stage of decryption are as follows:

*1) Inverse Final Round*

- Add Round Key
- Shift Rows
- Sub Bytes
- Inverse Main Round
- Add Round Key
- Mix Columns
- Shift Rows
- Sub Bytes

*2) Inverse Initial Round*

- Add Round Key

## VI. Application Architecture

The Figure 5.1 shows block diagram of the system. The system consists of a sender and a receiver. At the Sender side the user first scrambles the given data, then compresses it using algorithm, later encrypt the given data using encryption algorithm. At the receivers end, first using the common key decryption is performed, then reverse compression of the given data is performed and finally reverse scrambling using the h.264 algorithm is applied. Now, where the reverse algorithm the major chunk is provided by maintaining the data size and avoiding distortion thus making system more efficient than other.

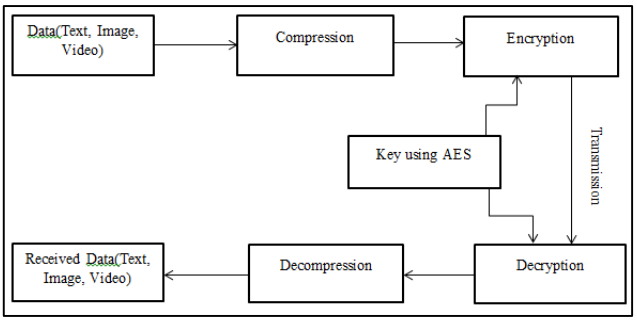



Fig. 5.1: Architecture of the ASS

## VII. Conclusion

The issue of leaking of important data while transferring it is a basic concern of everyindividual. With the above project one can safely transfer data over a network. Thus,resulting in important information not falling in the hands of any other unwanted user.

## References

[1] Secure image processing using AES Algorithm: This paper was proposed by Bhavana Verma and Sona Malhotra, Kurukshetra
[2] Video And Data Encryption Using AES Encryption For Secure Transmissionwas proposed by International Journal of Scientific & Engineering Research,Volume 6, Issue 4, April-2015
[3] Image Compression Using H.264 And Deflate Algorithm proposed by Dr. M. Sundaresan and E. Devika in the year 2016

All rights reserved by *www.ijsrd.com* 