Video Encryption and Decryption using Modified AES Algorithm

[1]**Mr. Pavan Pandey,** [2]**Prof. Zarna Verma**

[1]M.Tech. Scholar, [2]Assistant Professor
Dr Rajendra Gode Institute of Technology and Research, Amravati

*Abstract***: Video encryption is one of the most important technique nowadays for secured transmission. The proposed system uses modified AES algorithm as well as scrambling process in order to provide secured transmission of video. The AES algorithm is used because it is most secured standard for encryption and decryption. Hence the proposed system has been developed using modified AES algorithm and scrambling process, SPYDER (Python 2.7), ANACONDA2.**

*Keywords***: Modified AES algorithm, Scrambling process, SPYDER (Python 2.7), ANACONDA2.**

I. INTRODUCTION

Video encryption is the process of hiding the data by converting it from one form to another. Nowadays there is a rapid growth in the multimedia technologies, where every information can be shared through the network/internet. While sharing the data/information from sender to receiver loss of data may occur in between while transferring. So in order to provide secured transmission, encryption should be done before transferring the data/information to the receiver. Reduction/loss of data can be reduced by encryption process. The encrypted data can be decrypted at the receiver by using the secret key which is for encryption.

The security is required for video during transmission because in distance education the information transferred should not be varied. Encryption is needed for good quality and secured transmission. There are two types of encryption algorithms.
1. Symmetric key cryptography
2. Asymmetric key cryptography.

There are four chief video encryption algorithms
- completely encryption algorithms,
- permutation encryption algorithms,
- selective encryption algorithms and
- perceptual encryption algorithms

The video encryption procedure uses the modified AES algorithm and scrambling process for secured transmission. Here the video quality is maintained after decryption at the receiver.

II. LITERATURE SURVEY

The most important and necessary thing needed for video transmission is security. So in order to provide security, the proposed system uses selective encryption process for providing security during transmission of video and also to increase the transmission of data and robustness of video [1].

This paper provides a video encryption by implementing the S-transform. For improved video encryption selection of rotation of blocks used to generate the S-transform are analyzed. Here the encryption system has high encrypting capability and it also won't affect the coding efficiency. Hence both the perceptive and objective evaluation will be performed with H.264 codec standard [2].

Video encryption has more demand in the research field nowadays in order to provide security. Security becomes more important as increasing the rate of transmission of video. A media can be easily transmitted over the internet but it's not secured. Hence it needs encryption to be taken place before transmission. So many methods are introduced to provide the security for information they are encryption, authentication and digital signatures. The proposed system uses AES algorithm for video encryption [3].

From past few years there is an advancement in the digital content transmission. For secured video transmission some of the encryption algorithms have been applied. Due to some exceptional characteristics special MPEG video encryption algorithms are mandatory, those special characteristics are coding structure, large amount of data and real-time restrictions. The proposed system uses AES algorithm by modifying it in order to reduce the calculation and also to improve its performance [4].

The proposed system uses a secured video encryption algorithm for real time applications. Which uses symmetric key cryptographic technique. Here novel video encryption algorithm is implemented which uses a speakers voice to generate the public key. The public key generated is used as secret key to encrypt the video. This system provides a better encryption time per frame [5].

III. PROPOSED METHODOLOGY

Video encryption is a process of hiding the information/data in order to provide a security during transmission. During transmission of video some information may loss due to insecurity. Some intermediate persons may hack the information and they may change. So in order to avoid all those security should be provided by encrypting the video before transmission. The proposed system uses modified AES algorithm and scrambling process for better and secured transmission. After transferring the encrypted video it should be decrypted at the receiver.

Video encryption and decryption plays a very important role in video processing applications. Video encryption which provides the security for transferring the video. Here initially the transmitted video should be converted into several frames. For each frame encryption is done and it is decrypted later. In order to encrypt initially the frame should be converted into matrix form and scrambling process takes place and that matrix is multiplied by two secret keys one by one then for obtained matrix round cipher method is applied and is converted into image form finally. In order to decrypt the reverse process of encryption should be done. After encrypting all the frames it will be converted into video, hence it is called as encrypted video. The decrypted frames are also converted into video so called decrypted video. The flow diagram below shows the entire process of the proposed methodology.
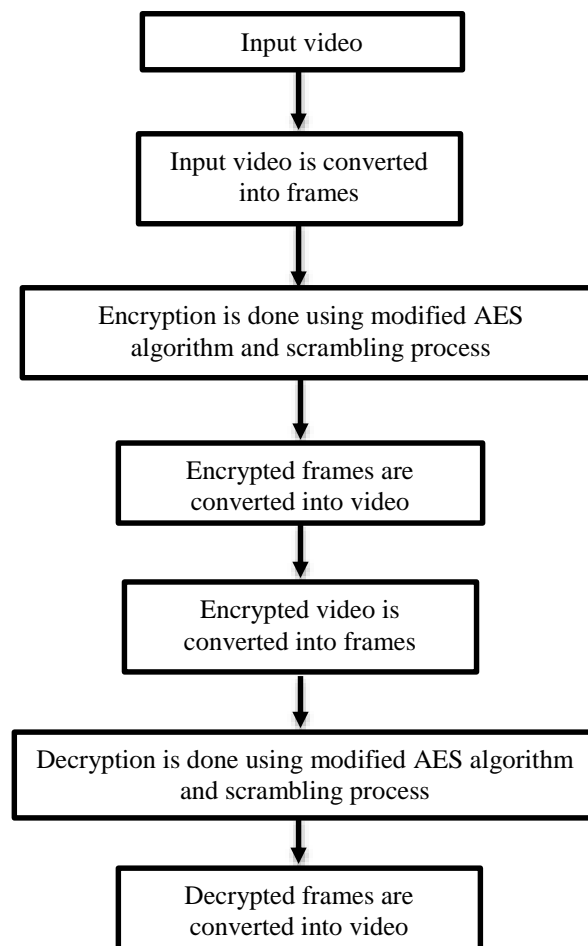
```
                    ┌─────────────────────┐
                    │     Input video     │
                    └─────────────────────┘
                               │
                               ▼
                    ┌─────────────────────┐
                    │  Input video is     │
                    │  converted          │
                    │  into frames        │
                    └─────────────────────┘
                               │
                               ▼
              ┌───────────────────────────────────┐
              │ Encryption is done using modified │
              │ AES algorithm and scrambling      │
              │ process                           │
              └───────────────────────────────────┘
                               │
                               ▼
                    ┌─────────────────────┐
                    │  Encrypted frames   │
                    │  are converted      │
                    │  into video         │
                    └─────────────────────┘
                               │
                               ▼
                    ┌─────────────────────┐
                    │  Encrypted video is │
                    │  converted into     │
                    │  frames             │
                    └─────────────────────┘
                               │
                               ▼
              ┌───────────────────────────────────┐
              │ Decryption is done using modified │
              │ AES algorithm and scrambling      │
              │ process                           │
              └───────────────────────────────────┘
                               │
                               ▼
                    ┌─────────────────────┐
                    │  Decrypted frames   │
                    │  are converted      │
                    │  into video         │
                    └─────────────────────┘
```

Fig 1: Video encryption and decryption process

IV. RESULTS OBTAINED

The output of the video encryption and decryption is shown below. Here the video is converted into frames and it is encrypted and then decrypted as shown in the figure below.
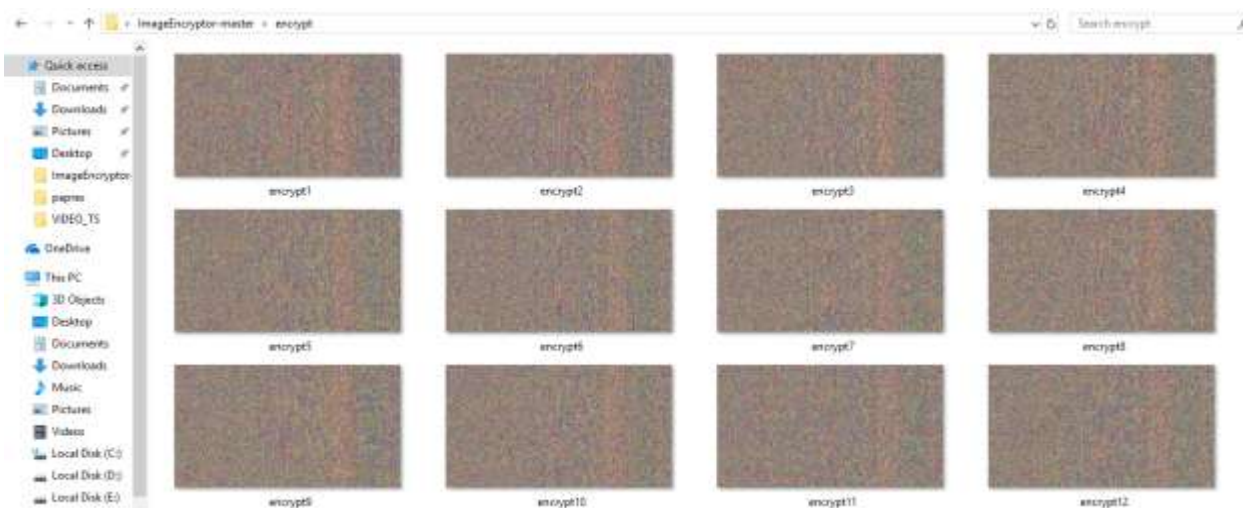

Fig 2: Original images

Fig 3: Encrypted images

Fig 4: Decrypted images

V. CONCLUSION

In this paper video encryption and decryption is done using modified AES algorithm and scrambling process in order to provide the security for the transmission of video. The proposed system here provide a better and secured transmission. The quality of the video after decryption is as original video, hence it provides a better encryption and decryption using AES algorithm.

REFERENCES

[1]   Rupali N. Hole, Megha Kolhekar, "Robust Video Encryption and Decryption using Selective Encryption," International Conference on Nascent Technologies in the Engineering Field, 2017

[2]   A. Kirthanaa, N.Mathan, T.Vino, "Improved perceptual video Encryption and Decryption using S-Transform," International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2015

[3]   Dhananjay M. Dumbere, Nitin J. Janwe, "Video Encryption using AES algorithm," International Conference on Current Trends in Engineering and Technology, IEEE Conference, July 8, 2014

[4]   Ms. Pooja Deshmukh, Ms. Vaishali Kolhe, "Modified AES Based Algorithm for MPEG Video Encryption," ICICES2014

[5]   *Obaida M. Al-Hazaimeh*, *Nouh Alhindawi*, *3Nesreen A. Otoum,* "A Novel Video Encryption algorithm-Based on Speaker Voice as the Public Key," IEEE, 2014

[6]   Nazar AL-Hayani, Naseer Al-Jawad, Sabah Jassim, "Simultaneous video compression and encryption for real-time secure transmission," 8th International Symposium on Image and Signal Processing and Analysis (ISPA 2013).