1. Title of the project : FAST AND SECURE REAL-TIME VIDEO ENCRYPTION
2. Name of the College & Department : KLE COLLEGE OF ENGINEERING AND TECHNOLOGY, CHIKODI & COMPUTER SCIENCE AND ENGINEERING
3. Name of the Students & Guide :

Students : Name: Balaram R Chougale

USN No.: 2KD19CS024

Email id: [balaramchougale.nice@gmail.com](mailto:balaramchougale.nice@gmail.com)

Mobile No: 8722410680

Name: Basavaraj Arjunagi

USN No.: 2KD19CS025

` Email id: basavarajarjunagi9701@gmail.com

Mobile No.:9353313183

Name: Basavaraj Sollapur

USN No.:2KD19CS026

Email id: basavarajsollapur11@gmail.com

Mobile No.:8496024806

Name: Lakkappa Y Basidoni

USN No.: 2KD19CS044

Email id: lakkappabasidoni2000@gmail.com

Mobile No.:8147831880

Guide : Dr. Bahubali Akiwate

Email id: bahubalimakiwate@gmail.com Contact No.:8971948565

1. Key words : Motion Vector, Message Embedding, Video encryption,Video decryption.
2. Introduction : The project aims to develop a fast and secure real-time video encryption system that incorporates message embedding and motion vector. The system will be designed to ensure that the video data is protected from unauthorized access or interception during transmission over a network or storage.

The video encryption system will utilize advanced encryption algorithms to encrypt the video data, ensuring that the encrypted data cannot be decrypted without the appropriate decryption key. Additionally, the system will incorporate message embedding capabilities, which will enable users to embed messages into the encrypted video stream.

The motion vector will also be utilized in the system to enhance the security of the video data. The motion vector represents the direction and magnitude of the movement of objects within a video frame. By using motion vector, the system will be able to identify regions of interest and apply different encryption methods based on the level of motion detected.

The proposed system will be fast and efficient, ensuring that the encryption and decryption processes do not cause any significant delays in the real-time transmission of the video data. The system will also be designed to ensure that the encryption keys are securely managed to prevent any unauthorized access or compromise.

1. Objectives :
   1. To Embed the message by altering the values of reference picture indices and motion vectors which results in scrambled video.
   2. To avoid the illegal access of the data from unauthorized user and provide reliable data transmission in an effective manner.
   3. To ensure the video security between sender and receiver with the fast growth communication and technology, security of sending confidential video information.
   4. To protect the confidentiality of digital data stored on computer system or transmitted over the internet or any other computer network.
2. Methodology : To achieve the above objective, the following methodology needs to be followed:

* The front end of the project will be implemented using python's tkinter library. The modules necessary for video recording is also implemented and is integrated with the front end.
* AES based encryption and decryption algorithms are implemented which would take video files and encrypted to produce cipher texts in the form of AES bases. The implementation of decryption would be done such a way that there is no loss in the quality, integrity and meaningfulness of the subject data.
* The cryptographic modules are integrated with the frontend to carry out the seamless execution of the intended process.
* Various phases of testing will be conducted such as unit testing, performance testing, integration testing and system testing. The results will be recorded.
* The recorded test data is analysed to yield the areas where the focus is necessary.

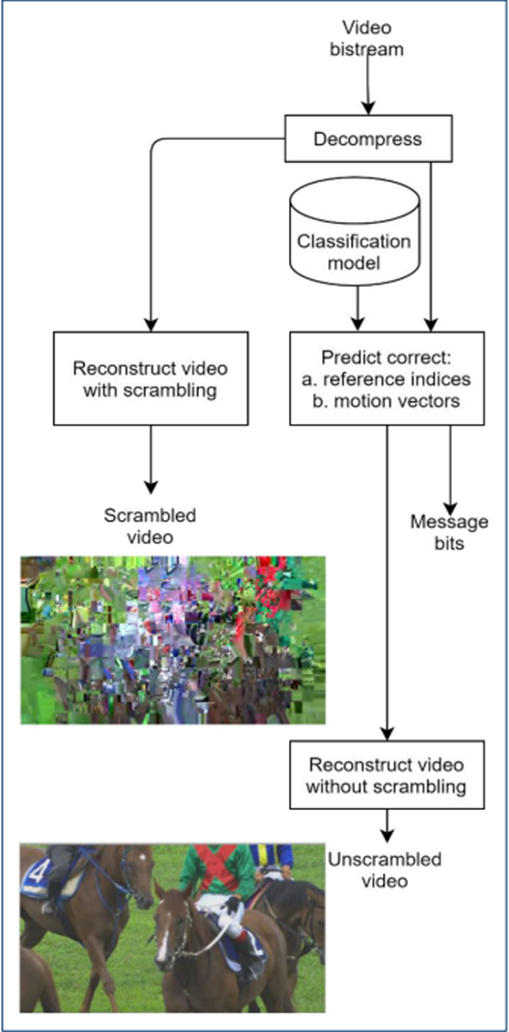
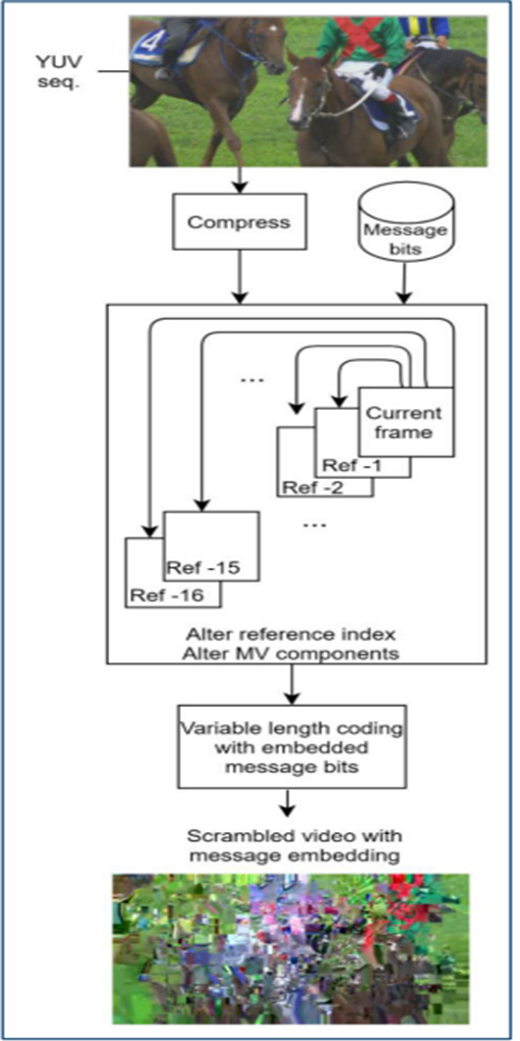


Figure a. Encryption Figure b. Decryption

The above figure shows that message embedding is achieved by altering the values of reference picture indices and motion vectors which results in scrambled video. To extract message bits, an authorized decoder builds a classification model per video sequence and uses it for predicting the true values of the reference indices and motion vectors. As such, message bits are extracted and the video is correctly reconstructed to its unscrambled state.

1. Result and Conclusions :

The system should be able to encrypt video data as it is being captured, transmitted or stored, using a fast and secure encryption algorithm. It should also allow for the embedding of a message within the encrypted video data. The motion vector information can be used to further enhance the security of the encrypted video data by adding a layer of complexity to the encryption process. By using motion vector information, the encrypted video data will be harder to decipher, as it will not be possible to accurately predict the next frame based solely on the previous one. The expected outcome of the project is a system that can be used in various applications where real-time video encryption is required, such as video surveillance, live streaming, and video conferencing. The system should be designed to be efficient, easy to use, and compatible with different devices and platforms. Additionally, it should be secure enough to protect against various types of attacks, including replay attacks, man-in-the-middle attacks, and eavesdropping.

1. Scope for future work :

* Real-time video encryption with message embedding and motion vector can be used to secure video conferencing systems used in business, education, and healthcare. This technology can help protect sensitive information exchanged during virtual meetings and prevent unauthorized access to the video stream.
* Real-time video encryption with message embedding and motion vector can also be used in broadcasting and media industries to protect copyrighted content from piracy and illegal distribution. This technology can help ensure that only authorized viewers have access to the video stream.
* Military and defense organizations often use video communication for strategic planning and coordination. Fast and secure real-time video encryption can help to ensure the confidentiality and security of these communications.