Digital video encryption using modified deformation and formation algorithms

C H Harika
Department of CSE
JSS STU, Mysuru, India

Anusuya M A
Department of CSE
JSS STU, Mysuru, India

***Abstract*—With the advancement of internet technologies in recent years, video technologies have become widely employed in TV, communication, and multimedia, necessitating the need for security on video information Despite the fact that several video encryption techniques have been developed, although it does not provide as much efficiency in terms of encryption and decryption. The process of encryption and decoding They are, nevertheless, more are difficult to deploy as a system and Images and video data are more important in today's online environment. Providing It is critical to protect this data while they are being transported across the network. As a result, the true aim of encryption is to safeguard the data. Traditional algorithms, which are utilized for the encryption of images and text finds it challenging to offer security to the video data since it is large in size and is often utilized.**

***Index Terms*—Encryption, Decryption, Formation algorithm, Deformation Algorithm**

I. Introduction

In today's digital environment, multimedia technologies are becoming increasingly important. The advancement of multimedia technology benefits applications such as video broadcasting, video telephony, video conferencing, and so on. However, maintaining security in video communication is challenging. A huge quantity of data, such as photos, text, music, and videos, is stored in every area, such as industry, hospital, schools, and colleges, and is sent over the network. When we consider hospital data, medical pictures of a patient are collected and exchanged for medical purposes with other doctors in the same or different departments of the hospital.

Rapid advancement of internet and video technologies, we need to provide security as well as authentication for video data. Video security has become increasingly important in recent years as video technologies have become more widely utilised in TV, communication, and multimedia. Video encryption is currently one of the most critical aspects of information security. When compared to image and other data, video data is much larger in size, and it is also used in real-time applications; hence, encoding such data need strong encryption computations. When working with huge amounts of data, variations in the data may arise; as a result, security and synchronization must be maintained effectively. Before being sent over the network, video data is compressed using several compression methods. Visual degradation, speed, compression friendliness, format compliance, cryptographic security, and encryption ratio are all performance criteria that a successful encryption method must have.

Decryption is the inverse of encryption, which involves the unscrambling of data. The two forms of cryptography are symmetric and asymmetric cryptography. Because both the receiver and the sender share the same key in symmetric cryptography, it is also known as secret key encryption. Asymmetric cryptography is public key encryption, in which anybody may encrypt communications using the public key, but only those with paired private keys can decode them, and the security level is determined by the secrecy of the private key.

II. Literature Review

A literature review must include a summary, appraisal, and explanation of the literature relevant to the topic of research chosen. Because video data is massive in size, and providing security to these data needs more robust algorithms, an overview of the articles that provide techniques to offer security to video data has been reviewed here.

M. A. Chandra et al. [1] presented a digital video encryption method that encrypts video frames utilising key frames and a conventional sorting permutation list. The major operation utilised in this article is the bit xor operation, which is used to [1]encrypt data between frames. In this case, two key pictures serve as secret keys, and frames are sorted using a conventional sorting permutation list. For each video, the Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE), and Root Mean Squared Error (RMSE) are computed and their performance is reported. This document also includes a histogram for video frames [2] before and after encryption. The advantage of this technique is that it helps to maintain the system more efficient and safe in terms of cryptography. [3]

P. Yedukondalu et al. [8] [4]introduced the Huffman encryption method for video frame encryption. The video is first transformed to numerous frames, and then, using the block cipher method, the frames are turned to blocks, which are then encrypted. When comparing selective methods to complete encryption, selective approaches require [5] significantly less time. The deformation and formation technique is used for video frame encryption and decryption. Encoding is accomplished by the use of secret keys. A good encrypting algorithm must have a fast encryption or decryption process, a high compression rate, security, encoding and decoding time, and so forth.

Pradeep K. M. et al. [10] [6]introduced the Huffman encryption method. To lower the compression rate, encryption

is performed concurrently with compression for the complete encryption technique. The DCT coefficients are encrypted selectively using a permutation list, and the authors discovered that selective encryption takes less time than complete encryption. Formation and deformation algorithms are used for video data encryption and decryption. They also calculated and analyzed MSE and PSNR dB [7]values and came to the conclusion that the algorithm with the best speed, compression ratio, time of encoding and decoding, and security will obtain the best PSNR.

S. Batham et al. [12] [8] suggested Indexed chaotic sequence based selective encryption of compressed video, which explains the properties of the compressed video. This technique encrypts the compressed intra coded frames and predictively coded frames from Group of Pictures. It employs three algorithms: one for [9] the development of an indexed based chaotic sequence, a second for video compression, and a third for the final process. The major advantage of utilising this method is that it is mostly utilised in real-time application systems, such as digital multimedia encryption, and it also provides excellent security. Because security is a major concern worldwide. It also has a faster pace when compared to other algorithm.

A. Kulkarni et al. [11] [10]proposed comparing several video encryption methods. To maintain a balance between security and compression, the video frames and their audio are time-shifted. The AES method is used to encrypt only a subset of the video's code words. In addition, a random key is utilised in the encryption process. The video gets reshuffled throughout the decoding process. This approach aids in the prevention of intruder attacks and increases security. This method's performance [11]is compared to that of other existing algorithms. They mostly concentrate on symmetric and asymmetric key encryption in this section. The proposed AES method and permutation algorithm are both very secure. The encryption speed is rapid in both this [12]approach and the criss-cross method. These are only a handful of the advantages of the suggested method.

D. Socek et al. [5] [13]developed a correlation-preserving permutation-based digital video encryption method. Sorting permutations are used to encrypt and decode the video frames in the stream, as well as to serve as the encryption process's secret key. Pure permutation and criss-cross permutation are the two types of permutation procedures based on the extraction of a permutation list. Encryption is [14] performed prior to video compression in this approach, with little emphasis placed on compression. According to the performance analysis, this method is efficient and resistant to assaults. Despite the fact that permutation techniques are vulnerable to attack, this modified algorithm is safe.

Y. Negi [6] [15]offered a study of several video encryption methods. Encryption and decryption may be accomplished in two ways: utilising a secret key or a public key. There are two types of encryption methods: complete encryption and selective encryption. Because it encrypts just selected data and reduces data size, the selective method is suitable for real-time systems. This article describes briefly the different encryption [16] techniques, such as the Nave approach, Pure and Zigzag permutation algorithms, Chaos-based method, [17] and Deformation and Formation algorithm, as well as its benefits and drawbacks.

A. Massoudi et al. [13] provide a selective encryption approach that may be used on both images and videos. Selective encryption algorithms reduce the quality of the data to be encrypted while also improving security and scalability. The selective encryption algorithm is assessed using a few criteria. Selective encryption is divided into three categories: before compression, in compression, and post compression. These categories are based on when compression is to be performed in the encryption process, and they have few uses. For selective encryption, the compression technique is always the best option.

III. Proposed Scheme

In this work, we present a novel video encryption technique based on I-frame encryption (video frame). For creating the encrypted I-frame, we used a concept from matrix calculation. In this approach, we gather all video frames, then take each frame one by one and choose a key picture as the key frame for the encryption and decryption process, such that this key image is sent via a secure connection. The following technique is used to encrypt the other frames. After using the encryption method, we aggregate all frames, create an encrypted movie, and deliver it via a basic channel. Encryption and decryption are accomplished using key pictures in this technique. The first frame is not encrypted, and the complete encryption method is employed as well. Encryption is accomplished by the use of a modified deformation method. Collect all video frames from the video, then choose two key images at random as key frames for the encryption and decoding procedure. To jumble the pixels, the first key frame is subjected to a key generating method. Every frame is encrypted with a modified deformation algorithm. Then, by merging all of the encrypted frames, create encrypted video. The encrypted process is decrypted using a modified formation algorithm, which is the reverse process of encryption.

A. Modified Deformation Technique

To encrypt the video frames, a modified deformation technique is utilised. After extracting the frames from the movie, choose two key frames at random from the collection of frames and label them as Key frame 1 (K1) and Key frame 2 (K2) . K1 is exposed to a key generation method, which randomly scrambles the pixels. The use of a schematic depiction allows the user to quickly and easily comprehend the method. While encrypting the frames, the encryption process begins with the second frame (I2), a simple encryption method is used for the I2 and second key frame (K2), and the result (C2) is first xored with the prior frames, i.e., I1. The fundamental encryption technique is used once again for the output (D2) and generation of the first key frame (K1). Rep the procedure

for all of the frames. Then, using the encrypted frames, create a video (E).

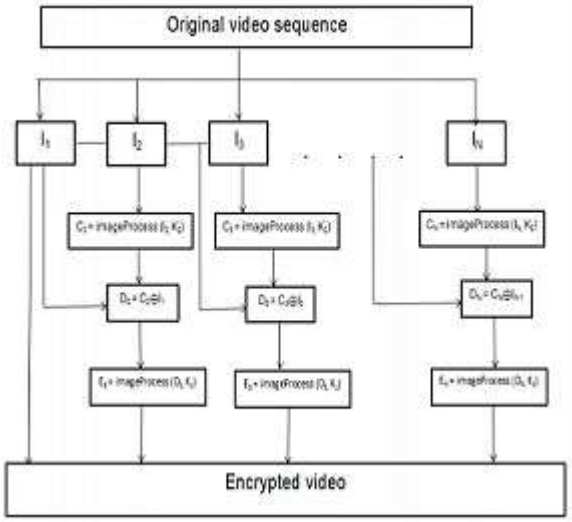

Fig 1: Flow diagram of Modified Deformation Algorithm

B. *Modified Formation Technique*

To decode the encrypted frames, the formation algorithm is utilised. In this approach, the encrypted frames are retrieved from the encrypted video first, and then each frame is decrypted. Two key frames and the first frame must be received from the sender prior to the decryption procedure. The key generating function is applied to K1.The basic image processing technique is used for the encrypted frame (E2) and the first key frame (K1), after which the acquired output (D2) is xored with its preceding frame (initially first frame). Then, to get the original frame of video, the fundamental image encryption technique is performed to the output (C2) and key frame K2. The same procedures are followed for all encrypted frames. Finally, by assembling all of the frames, you may create the final video.

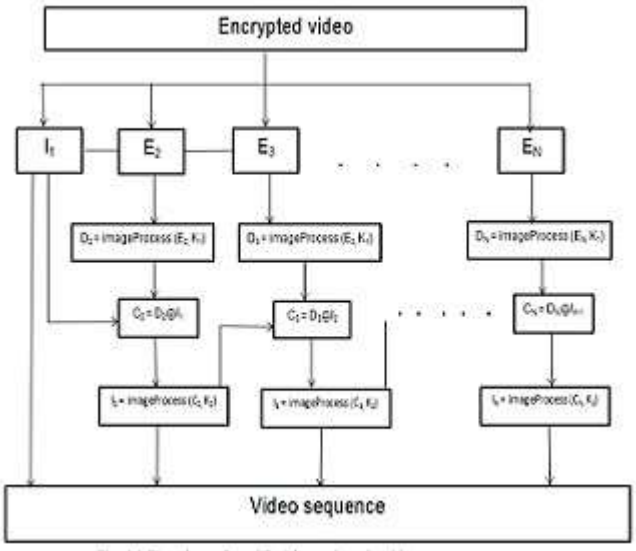

Fig 2: Flow diagram of Modified Formation Algorithm

IV. Proposed Algorithm

A. *Modified Deformation Algorithm*

Video encryption is accomplished by the use of a modified deformation technique, as detailed below. I1, I2, I3,. .....In – Frames K1 is the first key. K2 is the second key.

Step 1: Extract the video frames. V = I1, I2,..... In.

Step 2: Using the key generation technique, generate K1.

Step 3: Starting with frame I2, execute

C2 is an abbreviation for imageProcess (I2, K2)

D2 is an abbreviation for bitxor (C2, I1)

E2 is an abbreviation for imageProcess (D2, K1)

Step 4: Repeat the preceding steps for all of the frames.

Step 5: Combine all of the frames to create an encrypted video.

.

B. *Modified Formation Algorithm*

This steps decrypted using a modified formation process,as detailed below.

Step 1: Extraction of encrypted frames from encrypted video. E = E1, E2,. ....En

Step 2: Using the key generation technique, generate K1.

Step 3: For each E2 frame

D2 = imageProcess (E2, K1)

C2 is an abbreviation for bitxor (D2, I1)

Ax = imageProcess (C2, K2)

Step 4: Repeat the preceding steps for all of the frames.

Step 5: Combine all of the frames to create a decrypted video.

V. Experimental Results

This paper provides an examination of the suggested encryption scheme's results. Three distinct films have successfully used the formation algorithm. Several simulation results are presented to demonstrate the performance of the video encryption methods. In the field of human–computer interaction, graphical user interfaces (GUIs) are an essential element of software application programming. Its objective is to improve the efficiency and usability of a stored program's underlying logical design, a design discipline known as usability.

The GUIDE tool is used to develop the user interface in this work. GUI development environment (GUIDE) tools are used to create user interfaces for bespoke apps. GUIDE then creates the MATLAB code for building the UI automatically, which may subsequently be adjusted to meet the needs of the user. The GUI in this work comprises four buttons, the first of which is used to load the movie of the user's choosing. The second button, encryption, displays the encrypted video. The third button, decryption, displays the decrypted video. The last button is clear, which acts as a reset button, clearing all loaded data and restoring the GUI to its original state.

The suggested system's GUI is depicted Fig. 3 shows what happens when a user clicks the load video button in the GUI. the relevant screen comes on the screen, where the user may pick the movie of their choosing; if they select the incorrect

film, they can cancel it by clicking clear video. The loading of the movie into the GUI is seen in Fig. 4

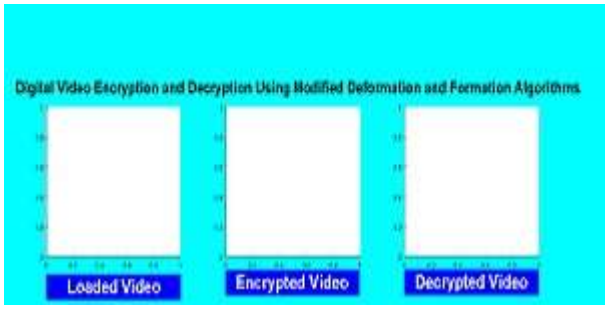

Fig 3: GUI of system

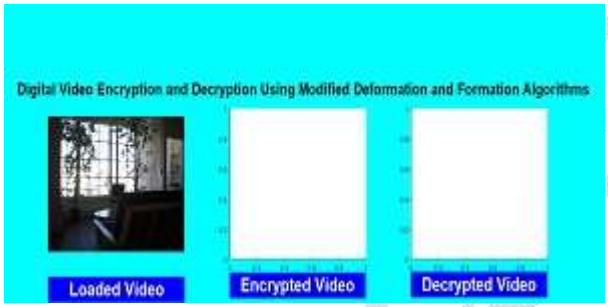

Fig 4: Load the video

If the user wants the encrypted video of the loaded video, he must hit the second button, encryption, which causes the encryption code to execute in the background and the encrypted video to display on the screen, as illustrated in Fig. 5. If the user want to clear the screen, he can do so by pressing the clear button. If a user wants a decrypted video of an encrypted video, he must click the third button, decryption, which causes the decryption code to execute in the background and the decrypted video to display on the GUI, as illustrated in Fig. 6. The fourth button, clear, clears all data and restores the GUI to its original state

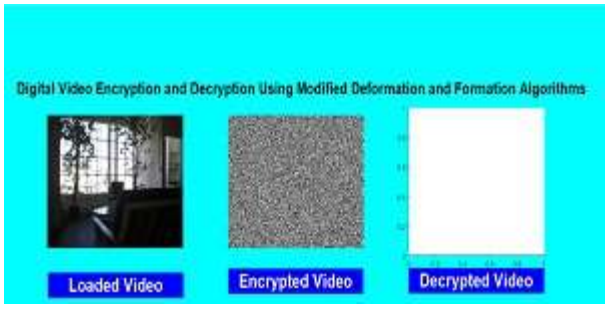

Fig 5: Encrypted video

Fig 6: Decrypted Video

The time necessary for each video is computed and given in Figure 7 depicts a graph produced for the time required by different movies for encryption and decryption. The length of time required for the encryption and decryption processes is determined on the kind and size of the video. The suggested algorithm's results demonstrate that the time required for encryption is more than the time required for decryption

	Encryption time (seconds)	Decryption time (seconds)
Air.avi	7.1	4.1
Bunny.mp4	32.0	21.4
Best.3gp	30.2	24.1
Aa.3gp	13.5	10.3

Fig 7: Time required for encryption and decryption process for different videos

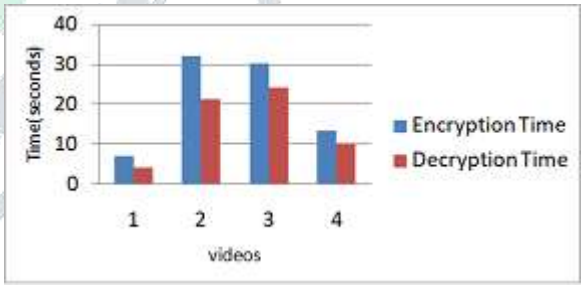

Fig 8: Graph plotted for time required by different videos for encryption and decryption

Error measurements are critical for determining video quality. The greater the video quality, the higher the PSNR value, and the lower the MSE value. The PSNR and MSE values for each video are shown in Figure 9.

	PSNR (db)	MSE
Air.avi	92.7	0.06
Bunny.mp4	91.8	0.07
Best.3gp	88.1	0.1
Aa.3gp	88.8	0.09

Fig 9:PSNR and MSE values for different videos

Figure 10 depicts the graph produced for the PSNR values, whereas Figure 11 depicts the graph printed for the MSE values.

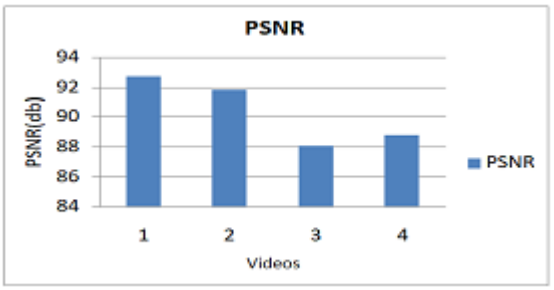

Fig 10: Graph plotted for PSNR values

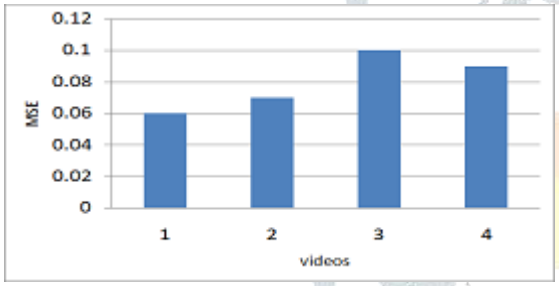

Fig 11: Graph plotted for MSE values

VI. Conclusion and Futurework

Video encryption and decryption utilising improved deformation and formation methods are presented in this study. Frames are taken from video and then encrypted and decrypted using the appropriate techniques. The time necessary for the encryption and decryption processes for various movies is recorded, and it is discovered that the time varies depending on the kind and size of the video. A graphical user interface is created for the purpose of assisting the user in efficiently using the system. The findings demonstrate that the algorithms operate well on video formats such as avi, mpeg, and mp4, and that MSE and PSNR values are computed for various videos in order to assess the video quality and system efficiency. The results demonstrate that the proposed algorithms work satisfactorily.

Future work will involve increasing security by encrypting key images and attaching a digital signature to them, as single key images are used for both encryption and decryption. The selective encryption method may be employed, and the time required can be recorded.

References

[1]M. Chandra, R. Purwar, and N. Rajpal, "A novel approach of digital video encryption," *International Journal of Computer Applications*, vol. 49, pp. 38–42, 07 2012.

[2]P. Ramasamy, V. Ranganathan, S. Kadry, R. Dama ševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—tent map," *Entropy*, vol. 21, no. 7, 2019. [Online]. Available: https://www.mdpi.com/1099-4300/21/7/656

[3]M. Bakhtiari and M. Maarof, "An efficient stream cipher algorithm for data encryption," *International Journal of Computer Science Issues*, vol. 8, 05 2011.

[4]K. Pradeepkumar.M, "An efficient and secure video encryption technique for real time systems," *International Research Journal of Engineering and Technology (IRJET)*, vol. 03, 11 2016.

[5]S. Cheng, L. Wang, N. Ao, and Q. Han, "A selective video encryption scheme based on coding characteristics," *Symmetry*, vol. 12, no. 3, 2020. [Online]. Available: https://www.mdpi.com/2073-8994/12/3/332

[6]Ashwitha and T. Murari, "Study and analysis of various video encryption algorithms," 12 2017, pp. 1–5.

[7]N. Geetha and D. K. Mahesh, ""efficient video encryption using rrs algorithm"," *Int. J. Pure Appl. Math*, vol. 118, pp. 885–890, 2018.

[8]S. B. Virendra Kumar Yadav, ""icsecv: An efficient approach of video encryption"," *IEEE*, vol. 57, 2014.

[9]D. G. Costa, S. Figuer êdo, and G. Oliveira, "Cryptography in wireless multimedia sensor networks: A survey and research directions," *Cryptography*, vol. 1, no. 1, 2017. [Online]. Available: https://www.mdpi.com/2410-387X/1/1/4

[10]K. H. A. Kulkarni, S. Kulkarni and A. More, "Proposed video encryption algorithm v/s other existing algorithms: A comparative study"," *nternational Journal of Computer Applications*, vol. 65, 03 2013.

[11]T. Adiguna and Hendrawan, "Secure h.264 video coding using aes/cfb/pkcs5 padding encryption on various video frames (i, p, b)," *2016 10th International Conference on Telecommunication Systems Services and Applications (TSSA)*, pp. 1–5, 2016.

[12]W. Salama, H. Elkamchouchi, and Y. Abouelseoud, "New video encryption schemes based on chaotic maps," *IET Image Processing*, vol. 14, 10 2019.

[13]D. C. O. M. H. K. Daniel Socek, Spyros Magliveras and B. Furht, ""digital video encryption algorithms based on correlation-preserving permutations"," *Information Security Volume*, June 2007.

[14]V. Memos and K. Psannis, "Encryption algorithm for efficient transmission of hevc media," *Journal of Real-Time Image Processing*, vol. 12, 05 2015.

[15]Y. Negi, ""a survey on video encryption techniques"," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, pp. 234–237, April 2013.

[16]O. O. K. M. Abomhara, O. Zakaria, "An overview of video encryption techniques"," *International Journal of Computer Theory and Engineering*, vol. 02, pp. 103–110, February 2010.

[17]N. Mao, L. Zhuo, X. Li, and J. Zhang, "An efficient video encryption scheme for h.264 compressed bitstream," *2011 7th International Conference on Advanced Information Management and Service (ICIPM)*, pp. 89–94, 2011.