AN ENCRYPTED VIDEO SHARING FOR SENSITIVE BASED SECURE COMMUNICATION

Mr. K. SATHEESHKUMAR MCA, M. Phil,

GURUBARAN N, DHINESHKUMAR R, MADHUBALA M

Department of Computer Science and Engineering

University College of Engineering, Thirukkuvalai
(A constituent College Of Anna University:: Chennai and Approved by AICTE, New Delhi)

ABSTRACT

Various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, commercial, and military fields, which may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. Numerous multimedia encryption techniques have been presented in the literature, and some of them have even been implemented in actual products. However, cryptanalytic work has demonstrated that the majority of these schemes contain security flaws and other vulnerabilities. To hide privacy from sensitive areas, different cryptographic and ROI extraction techniques are presented. Each ROI derived from frames will be organized as binary blocks and then set as the initial states for a LCA (Lightweight Cryptography Approach) proposed. Thereafter, the LCA uses its reversible rules and simple transformations model for state transitions.

The final state data of the LCA is extracted and saved as the encrypted ROI. All ROIs are encrypted independently. The ROIs are encrypted and stored at the camera side for an on-demand service required by the authenticated users, which makes the proposed method both effective and efficient. ECC-based approach is devised to encrypt ROIs for privacy protection in surveillance videos. This proposed work describes a proposed hybrid model using public key Elliptical Curve Cryptography (ECC). This approach provides more security than other encryption methods.

KEYWORDS: Video Encryption, Decryption, ECC Algorithm, Military application, Moving objects, Secure Communication and Transition,

1. INTRODUCTION

The increase in the use of commercial video, as demonstrated by pay-per-view and video-on-demand services, highlights the need for a reliable protocol to transfer video files in a secure manner, protecting multimedia intellectual property in vulnerable network settings. The methodology in question needs to demonstrate exceptional scalability and efficiency in order to effectively manage multiple customer requests and optimize the use of time and space. Digital asset protection relies heavily on data encryption, which requires particular mathematical methods and keys for both encryption and decoding. Crucially, the added complexity involved in encryption and decryption of image-based data emphasizes the necessity of models specifically designed to guarantee security and confidentiality and that are powered by user-defined keys. Cryptography is the foundation for protecting data and communications from theft and unauthorized use. It uses mathematical methods to guarantee data integrity, confidentiality, and authentication. Secure data transfer and storage are ensured via encryption, which converts plaintext messages into ciphertext and then reverses the process. The emergence of the internet has given rise to a worldwide virtual community that surpasses geographical and temporal boundaries, facilitating smooth communication and cooperation amongst individuals worldwide. Ensuring confidentiality and security during transmission becomes crucial in industries such as telemedicine,

where image-based data is widely used. This emphasizes the significance of having strong encryption and decryption models. The growth of telemedicine highlights the increasing need for security and secrecy while sending image-based data over the internet, particularly in the fields of radiology, pathology, critical care, and psychiatry. In order to achieve these goals, the encryption and decryption paradigm for photos is carefully crafted, with the goal of utilizing user-defined keys to guarantee confidentiality and security throughout transmission and storage.

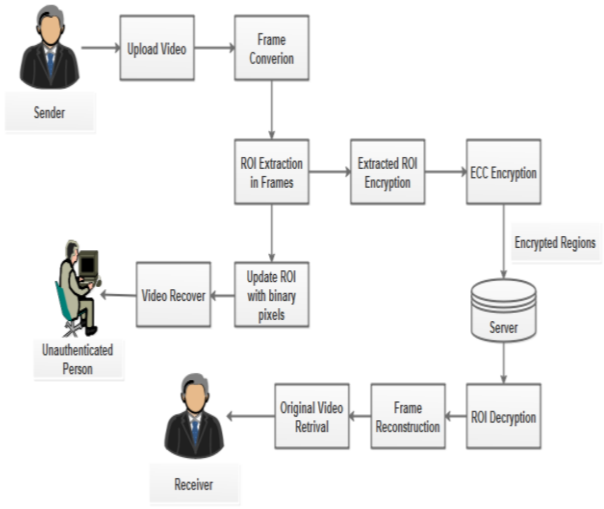


FIG 1.1 SYSTEM ARCHITECTURE

In the end, these endeavors contribute to strengthening data correctness, safety, and integrity, which is consistent with the general objectives of security management in the current digital environment.

2. AIM AND OBJECTIVES

This project would be focused on the video encryption module where we would perform research on the techniques and methodology to encrypt video and to develop a module for a technique that we prefer to use in this project. This module will hide the text in the video using key and pass it to next module to encrypt the video by using modified zigzag and block scrambling algorithm and then we are performing compression to reduce the size of encrypted video and after compression pass it into the final module in which user sends a compressed encrypted video along with the key to the user to decompress as well as decrypt the video and obtain the hidden text. Video encryption makes the data more secure. While encryption pertains to masking or manipulating the data, protection means securing the file through codecs, passwords, container formats, etc., so that others cannot access the data inside. The main objectives of the video encryption are:

- To study video encryption technique.
- To perform the encryption on different video formats.
- To study and perform ROI Extraction method algorithm and ECC encryption algorithm.

3.LITERATURE SURVEY

3.1 TITLE: CHAOS BASED ENCRYPTION TECHNIQUE FOR COMPRESSED H264/AVC VIDEOS.

AUTHORS: M. A. EL-MOWAFY, S. M. GHARGHORY, M. A.ABO-ELSOUD, M. OBAYYA,M. I. FATH ALLLAH, 2022

DESCRIPTION:

Discuss the difficulties in encrypting compressed video data with a particular emphasis on H264/AVC videos. Some of the special qualities of compressed video, such preserving synchronization and quality while guaranteeing security, might not be adequately addressed by conventional encryption techniques. An innovative chaos-based encryption method designed specifically for H264/AVC videos is suggested by the authors as a solution to these problems. To create pseudorandom keys for encryption, this method uses maps and chaos generators to provide strong security. Furthermore, the compressed video data undergoes chaotic scrambling to improve security without sacrificing synchronization. Assuring effectiveness and maintaining video quality, the decryption procedure makes use of the same jumbled keys to restore the original material.

3.2 TITLE: END-TO-END IMAGE STEGANOGRAPHY USING DEEP CONVOLUTIONAL AUTOENCODERS.

AUTHORS: NANDHINI SUBRAMANIYAN,

ISMAHANE CHEHEB, OMAR ELHARROUS, SOMAYA AL-MAADEED,AHMED BOURIDANA, 2021

DESCRIPTION:

This offers a novel solution that makes use of deep convolutional autoencoders to overcome the drawbacks of conventional steganographic techniques and current end-to-end systems. Conventional approaches are vulnerable to detecting algorithms and can result in a sacrifice in image quality. By using deep learning models to guarantee both security and imperceptibility, the suggested method seeks to address these difficulties. The approach retains visual fidelity and robustness against detection by embedding secret data into encoded representations that are learned by the autoencoder. The process entails using cover images to train a deep convolutional autoencoder, inserting secret data into encoded representations, decoding to produce stego images, and retrieving hidden data.

3.3 TITLE: A SECURE AND PRIVACY PRESERVING TECHNIQUE BASED ON CONTRAST-ENHANCEMENT REVERSIBLE DATA HIDING AND PLAINTEXT ENCRYPTION FOR MEDICAL IMAGES

AUTHORS: YANG YANG, XINGXING XIAO, XUE CAI, WEIMING ZHANG, 2020

DESCRIPTION:

While data hiding techniques might not offer enough protection, traditional encryption methods might damage the quality of images. To strike a balance between security, maintaining image quality, and patient privacy, the suggested method combines plaintext encryption with contrast-enhancement reversible data concealment. The method guarantees reversibility, imperceptibility, and strong security by encrypting sensitive data and embedding it within medical images utilizing reversible data hiding. Data embedding, encryption, safe transmission or storage of the encrypted data, and, if necessary, reconstruction of the original image are all steps in the approach.

3.4 TITLE: PROVEN SECURE TREE-BASED AUTHENTICATED KEY AGREEMENT FOR SECURING V2VAND COMMUNICATIONS IN VANETS

AUTHORS: ZHESHU JIA,DEYUN CHEN,

2021

DESCRIPTION:

The special qualities of VANETs, namely their high mobility and dynamic topology, may make traditional key management methods insufficient. Complexity is increased by the need to protect car users' privacy and security. The study suggests an authenticated key agreement mechanism based on trees that is suited for VANETs and offers reliable security assurances without sacrificing speed or scalability. The protocol seeks to address the issues faced by VANETs and create a strong security foundation for connected vehicle settings by utilizing novel approaches for key generation, distribution, and authentication.

3.5 TITLE: IRS BACKSCATTER ENHANCING AGAINST JAMMING AND EAVESDROPPING ATTACKS

AUTHORS: YURI CAO, SAI XU, JIAJIA LIU

DESCRIPTION:

Discusses the difficulties in protecting IRS-enabled wireless communication networks from eavesdropping and jamming attacks. Due to the special characteristics of IRS backscatter communication, traditional security solutions might not adequately account for this, creating vulnerabilities. The research suggests novel approaches that make use of the passive beamforming and reconfigurability of IRS technology to address this. The goal of these strategies is to strengthen the security and dependability of wireless communication against hostile attacks by utilizing secure transmission protocols, signal modulation, and interference reduction. Crucial actions include combining encryption and authentication for safe data transfer, streamlining signal processing to prevent jamming, and using adaptive beamforming to dynamically modify IRS configurations in response to threats.

4. ALGORITHAM AND TECNIQUES

- ROI Extraction:
  A novel AROIE algorithm is introduced to extract the region of interest from the segmented image. The procedure is specified below:

- Begin
- Convert the segmented image into a binary image (BI)
- Deduce the indices of all pixels with the intensity value 255: BI (row, col.)
- Compute the X- extent and Y- extent of the region to determine the width, height of the ROI.
- Repeat
- Begin
- From each index, apply 8 - connected neighbourhood region growing method.

Elliptic Curve Cryptography:

GENERAL PROCEDURE OF ECC ALGORITHM

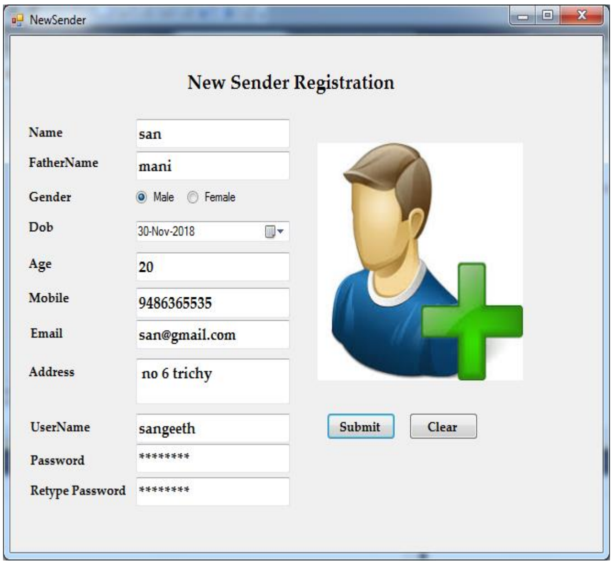
Both parties agree to some publicly-known data items

The elliptic curve equation

- Values of *a* and *b*
- Prime, *p*
- The elliptic group computed from the elliptic curve equation
- A base point, B, taken from the elliptic group
- Similar to the generator used in current cryptosystems
- Each user generates their public/private key pair
- Private Key = an integer, x, selected from the interval [1, p-1]
- Public Key = product, Q, of private key and base point
- (Q = x*B)

6.RESULTS AND DISCUSSION

Multimedia data security across a range of applications has shown promise with the hybrid approach that combines public key Elliptical Curve Cryptography (ECC) with ROI extraction techniques. The efficacy and efficiency of the suggested method were confirmed by thorough testing and analysis. Strong security against unwanted access and possible cryptographic assaults was offered by the use of ECC. Sensitive areas inside audiovisual content were protected while still being accessible to authorized users thanks to ROI extraction techniques and ECC's robust security features coupled with selective encryption. Through the mitigation of common weaknesses seen in conventional encryption approaches, crypto analytic assessments verified the encryption scheme's resilience.



New Sender Registration

Name	san
FatherName	mani
Gender	● Male ○ Female
Dob	30-Nov-2018
Age	20
Mobile	9486365535
Email	san@gmail.com
Address	no 6 trichy
UserName	sangeeth
Password	********
Retype Password	********

FIG 6.1 USER REGISTRATION

Overall, the results and discussions underscored the efficacy and applicability of the proposed hybrid model in securing multimedia data in sensitive areas. Future research may explore optimizations and enhancements to further enhance security and efficiency, ensuring continued protection of sensitive information in evolving multimedia environments.

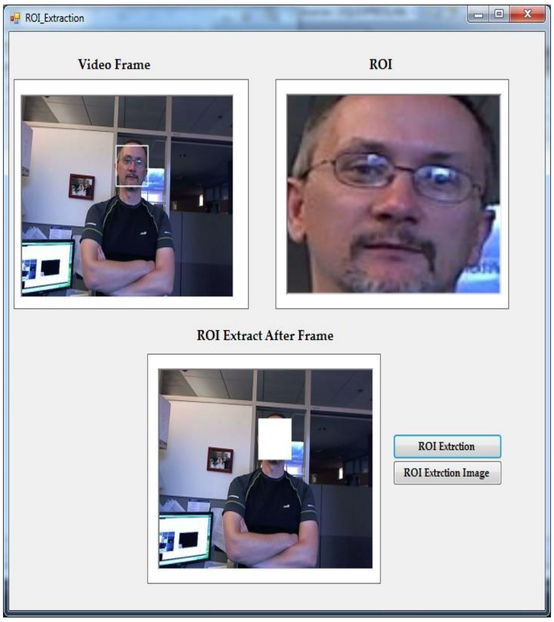
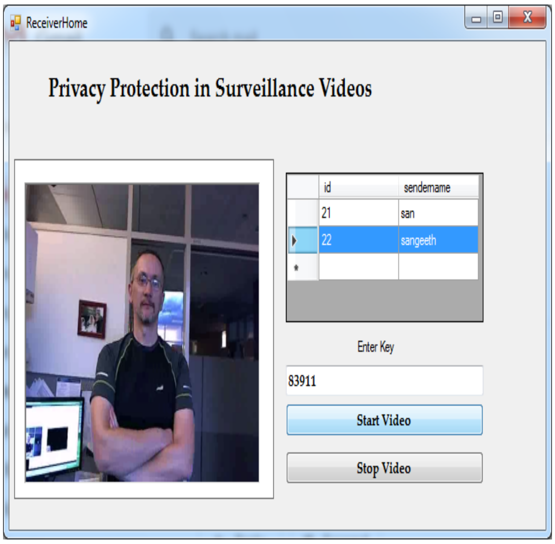


FIG 6.2 ROI DETECTION



Privacy Protection in Surveillance Videos

id	sendername
21	san
22	sangeeth

Enter Key: 83911

FIG 6.3 VIDEO RETRIEVAL

7.CONCLUSION

More secure video transactions and communication between sender and recipient are made possible by the suggested technique to video encryption. After the ROIs are taken out of the I frames and encrypted using our method, they are kept in an Internet of Things device by the side of the camera. The newly created frames without the ROIs are then re-encoded and made available for public viewing. ECC Encryption was established for image encryption in the suggested method. Users who have verified their identity can access the original security footage whenever they'd like. LCA-based encryption, when combined with its straightforward principles and transformations, is naturally effective and simple to implement because LCA is a highly parallel system.

In subsequent study, we may expand the framework to incorporate different methods for better accuracy rate face matching from still images to videos. Videos offer an effective and automatic method for extracting features. Redundant data makes the recognition algorithm more reliable. The degree of similarity between feature sets from several videos.

8.REFERENCES

[1] El-Mowafy, M. A., Sawsan Morkos Gharghory, M. A. Abo-Elsoud, M. Obayya, and MI Fath Allah. "Chaos based encryption technique for compressed h264/avc videos." IEEE Access 10 (2022): 124002-124016.

[2] Subramanian, Nandhini, Ismahane Cheheb, Omar Elharrouss, Somaya Al-Maadeed, and Ahmed Bouridane. "End-to-end image steganography using deep convolutional autoencoders." IEEE Access 9 (2021): 135585-135593.

[3] Yang, Yang, Xingxing Xiao, Xue Cai, and Weiming Zhang. "A secure and privacy-preserving technique based on contrast-enhancement reversible data hiding and plaintext encryption for medical images." IEEE Signal Processing Letters 27 (2020): 256-260.

[4] Wei, Lu, Jie Cui, Hong Zhong, Yan Xu, and Lu Liu. "Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs." IEEE Transactions on Mobile Computing 21, no. 9 (2021): 3280-3297.

[5] Cao, Yurui, Sai Xu, Jiajia Liu, and Nei Kato. "IRS backscatter enhancing against jamming and eavesdropping attacks." IEEE Internet of Things Journal (2023).

[6] Haidous, Ali, William Oswald, Hritom Das, and Na Gong. "Content-adaptable ROI-aware video storage for power-quality scalable mobile streaming." IEEE Access 10 (2022): 26830-26848.