International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Protecting Privacy in Surveillance Systems via Selective Video Encryption

Mr. Nandish M[1], Abdul Rahaman Pasha[2], Mahanth K P[2], Meghana S N[2], Priyanka H R[2]
Assistant Prof., Dept. of CS&E, JNNCE, Shivamogga, India[1]
Research Scholar, Dept. of CS&E, JNNCE, Shivamogga, India[2]

Abstract: The "Privacy Preservation in Surveillance Video Using Selective Encryption" study addresses the issue of privacy in surveillance videos. Video surveillance systems are widely deployed in many public places such as banks, supermarkets, airports, roads, and residential areas. However, the privacy of individuals in these videos is a major concern. The proposed system aims to conceal faces while not interfering with the observation and recognition of human activities. The system uses selective encryption to encrypt only the face region of the frames while other parts of the frame are retained as it is. The proposed method is reversible for revealing faces whenever needed to the authorized person using proper secret keys. The project also aims to ensure the security of the encryption algorithm used and provide a user-friendly interface for ease of use. Overall, this study aims to provide an efficient and scalable solution to the problem of privacy in surveillances.

I. INTRODUCTION

Multimedia communication plays an important role in multiple areas in today's society including politics, economics, industries, militaries, entertainment, etc. [1]. It is of utmost importance to secure multimedia data by providing confidentiality, integrity, and identity of ownership. Multimedia security addresses the problems of digital watermarking, data encryption, multimedia authentication, digital rights management, etc. Multimedia encryption is the core enabling technology that provides confidentiality and prevents unauthorized access to the content. Real-time constraints, large amounts, and unique characteristics of multimedia data inhibit the use of traditional cryptographic algorithms over multimedia data. Digital multimedia (audio, video, photography, etc.) is exposed to a broad spectrum of security problems. We often capture images and videos and share them with friends over a network. There is an increasing concern about the loss of privacy of such data. We have been looking into the security and privacy of multimedia data, during storage, processing, and communication.

Since the capture and processing are by two different devices (often on two different locations), multimedia communication is critical. Popular internet protocols are not secure enough. Therefore, investigations in the security and privacy of multimedia data involve the development of algorithms that especially suits the properties of visual data. Security is often achieved by significant additional computation. Here, image/video data are achieved by exploiting special properties/characteristics of the visual data.

Specific activities in this area include:

* Efficient Video Encryption Algorithms.
* Privacy in Video Surveillance.
* Privacy-Preserving Information Retrieval and Mining.
* Secure and Fast Multimedia Communication.

General Cryptosystem and Encryption Techniques

Encryption is the method by which information is converted into secret code that hides the information's true meaning [2]. The science of encrypting and decrypting information is called cryptography. A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as cipher text.

The various components of a basic cryptosystem are as follows: -

- Plaintext: - In computing, the unencrypted data is also known as plaintext.
- Ciphertext: - The encrypted data is called ciphertext.
- Ciphers: - The formulas used to encode and decode messages are called ciphers or encryption algorithms.
- Key: - A cipher includes a variable as part of the algorithm. The variable is called a key.
- Symmetric Key: -.In symmetric key cryptography, an individual key is used for both encryption and decryption. The sender needs the key to encrypt the plaintext and sends the cipher document to the receiver. The receiver used the similar key (or ruleset) to decrypt the message and recover the plaintext. Because an individual key is used for both functions, symmetric key cryptography is also known as symmetric encryption. Symmetric key cryptography schemes are usually categorized such as stream ciphers or block ciphers. Stream ciphers works on a single bit (byte or computer word) at a time and execute some form of feedback structure so that the key is constantly changing. Block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size. The size of block is fixed in the given scheme. The choice of block size does not directly

affect to the strength of encryption scheme.

•Asymmetric Key: -Asymmetric cryptography uses two keys for encryption and decryption. It depends on the technique of public and private keys. A public key, which is interchanged between higher than one user. Data is decrypted by a private key, which is not transformed. It is slower but more secure. The public key used in this encryption technique is applicable to everyone, but the private key used in it is not revealed. In asymmetric encryption, a message that is encrypted utilizing a public key can be decrypted by a private key, while if the message is encrypted by a private key can be decrypted by utilizing the public key. Asymmetric encryption is broadly used in day to day communication channels, particularly on the internet.

Selective encryption is a new trend in image and video content protection[4]. It consists of encrypting only a subset (region of interest) of the data. Selective encryption aims to reduce the amount of data to encrypt while preserving a sufficient level of security. This computation saving is very desirable especially in constrained communications (real-time networking, high-definition delivery, and mobile communications with limited computational power devices). In addition, selective encryption allows preserving some codec functionalities such as scalability. The purpose of selective encryption algorithms is to encrypt only certain portions of the images, but simultaneously, sufficient images are encrypted to provide trustworthy safety to secure the transmitted images' confidentiality. Not all images need to be encrypted through selective encryption; still, the entire data transmission can be viewed to be secure as a whole. Selective encryption is proficient to improve the scalability of data transmission and also reduces the processing time.

(a) (b)

Figure 1: (a) Original image (b) Encrypted image

An example of selective encryption is shown in Figure 1 In this example, the face part of individuals who are present in the image is encrypted whereas the rest of the part in the image is transmited as it is.

II. LITERATURE SURVEY

This section provides a brief description of the various techniques that were reviewed to get better knowledge about the various research and development works that have been done in the area of privacy preservation in surveillance video. The proposed work consists of two main stages i.e., face detection and region of interest encryption. The survey presented in this chapter is based on recent works in these two domains.

KHALID M. HOSNY[1] et.al depicts "Privacy Protection in Surveillance Videos Using Block Scrambling-Based Encryption and DCNN-Based Face Detection", The problem statement mentioned in the research paper is that with the increasing use of surveillance cameras in various settings, people's privacy is at risk. While surveillance cameras are important for safety and security, they can also capture sensitive information, such as people's faces, without their consent. Therefore, there is a need for a method to protect people's privacy in surveillance videos. The solution statement proposed in the research paper is to use a novel method for surveillance video privacy protection using block scrambling-based encryption and DCNN-based object detection. The proposed method involves the following algorithms: DCNN-based face detection, Block scrambling-based encryption, Chaotic logistic map-based encryption. The proposed method is designed to protect the privacy of people in surveillance videos by detecting their faces, scrambling them, and encrypting them using a secure key. Advantages of this method are privacy protection, precession, cryptographic, fortification, low processing time, suitable for real time application, reversible. Limitations are may not be effective in low-quality surveillance video, scalability, vulnerability.

Alem Fitwi, Yu Chen [2] et.al proposed "Privacy-Preserving Selective Video Surveillance" The widespread use of video surveillance systems raises concerns about privacy violations and unauthorized access to personal information. Existing mass-surveillance systems often lack the capability to selectively capture and analyze video frames containing aggressive or suspicious behavior, leading to privacy breaches. Therefore, there is a need for a privacy-preserving selective video surveillance (PriSev) method that can address these concerns by enabling selective-surveillance while safeguarding individuals' privacy.The proposed

solution in this paper is the PriSev method, which enables selective-surveillance while preserving privacy. The method involves the use of a lightweight dynamic chaotic image enciphering (DyCIE) scheme for onsite object detection and frame encryption at the network edge where the video is created. At the fog/cloud layer, frame decryption is efficiently performed followed by deep-neural-network (DNN) based frame-filtering and selective storage that runs on a surveillance server. In addition, a multi-agent system is introduced for the exchange of deciphering keys between the sending and receiving agents. The experimental study and performance analyses show that the proposed PriSev method is able to efficiently perform privacy-preserving selective surveillance in real-time. Advantages are selective, efficient, optimization, secure, robust. Limitations are resource-intensive, specialized, latency.

Alem Fitwi, Yu Chen [3] et.al explained "Privacy-Preserving Surveillance as an Edge Service Based on Lightweight Video Protection Schemes Using Face De-Identification and Window Masking" The problem statement addressed in this paper revolves around the need for privacy-conscious surveillance in the context of the widespread deployment of CCTV cameras and the potential invasion of individuals' privacy. The authors highlight concerns about the collection of private information without consent and the need to address privacy breaches in video surveillance systems. They emphasize the importance of making cameras privacy-conscious by design and propose a Privacy-preserving Surveillance as an Edge service (PriSE) method with a hybrid architecture to detect privacy attributes like windows, faces, and perpetrators. The key issues addressed are Privacy concerns arising from the constant invasion of individuals' privacy due to the deployment of a myriad of edge cameras in urban and suburban areas. The need to develop a surveillance system that is privacy-conscious by design and addresses the interception of videos in transit, potential abuse of CCTV cameras and videos by operators, and the balance problem between privacy and usability. The challenges associated with privacy attribute identification, image scrambling methods, and object-detection technologies in preserving privacy in surveillance systems. The authors aim to tackle these issues by proposing a lightweight foreground object scanner and a video protection scheme that operates on edge cameras and fog/cloud-based models to detect and mask privacy attributes, thereby ensuring end-to-end privacy protection. The solution proposed in the paper involves the Privacy-preserving Surveillance as an Edge service (PriSE) method, which comprises a hybrid architecture with a lightweight foreground object scanner and a video protection scheme. The PriSE method aims to detect privacy attributes such as windows, faces, and perpetrators, while ensuring end-to-end privacy in surveillance systems. The algorithm used for the solution includes the following Simplified Foreground-object Detector, Frame Privacy-preserving Scheme, Window and Face Objects Detection and Masking, Detection and Classification of Fugitives. Advantages are comprehensive, efficient, secure, obfuscation, alerting. Limitations are resource-intensive, sophistication, latency, trade-off, dynamic.

Alem Fitwi, Yu Chen [4] et.al discussed "Secure and Privacy-Preserving Stored Surveillance Video Sharing atop Permissioned Blockchain" The problem addressed is the lack of privacy and security in traditional video surveillance systems, which can lead to breaches and abuse of personal information. The paper proposes a solution using blockchain technology to ensure secure and privacy-preserving sharing of stored surveillance videos. The proposed solution is a mechanism based on a permissioned blockchain, smart contracts, and an enciphering algorithm. This solution aims to create a decentralized, reliable system with secure and privacy-aware sharing of stored surveillance videos. The enciphering algorithm is based on discrete cosine transform, advanced encryption standard, and a block shuffling algorithm. The system is designed to provide a high level of security and privacy for the stored surveillance videos while still maintaining the usability and clarity of the video data. Advantages high level security and privacy, authorization, usability and clarity, decentralized, reliable, less-vulnerable. Limitations are less-anonymity, limitation in scalability.

Xianhao Tian and Peijia Zheng [5] et.al talk of"Robust privacy-preserving motion detection and object tracking in encrypted streaming video a preprint" The problem statement discussed is they consider a non-interactive video motion detection and tracking system involving only two parties: the video data owner and the cloud server. The owner has limited storage and computation resources and needs to outsource data storage and computing tasks to the cloud. The paper focuses on addressing privacy concerns related to the storage and processing of video data on the cloud server, particularly in scenarios involving sensitive content such as human faces and card security codes. The goal is to develop a secure motion detection and tracking scheme that allows for effective detection, robust tracking, and fast computation while ensuring privacy and security of the video data. The solution proposed in the research paper involves the development of a reliable multi-object tracking scheme based on Kalman filtering by adaptively refining the observation data. The authors propose a secure motion detection and tracking scheme that allows for effective detection, robust tracking, and fast computation in encrypted bit stream video. They introduce the feature DNRC, a clustering algorithm, and a motion tracking scheme to achieve these objectives. Advantages are Robust Performance, Privacy Preservation, Efficient and Low-Computation Load, Superior Performance. Limitations are Limited Scope, Experimental Conditions, Manual Parameter, Lack of Comparative Analysis.

Shuli Cheng [6] et.al depicts "A Selective Video Encryption Scheme Based on Coding Characteristics" Problem statement

discussed is to propose a selective video encryption scheme that combines video coding and encryption algorithms to protect video information with higher security, addressing the challenges of compatibility, security, and timeliness in video encryption. Solution is to have proposed a selective video encryption scheme that utilizes the H.264/AVC encoding algorithm and the advanced encryption standard (AES) with dynamic key generation to encrypt video slices independently. The scheme encrypts important semantic elements in the video stream, such as IPM, MVD, residual coefficient, and delta_QP, to ensure the visual perception security of video encryption. Advantages Utilizes H.264/AVC Encoding, Enhanced Security, Dynamic Key Generation, Real-Time Key Updating, Better Encryption Effect. Limitations are Limited Space for Semantic Element Renderings, space limitation, Complexity of 4-D Hyper chaotic System, . Limited Comparative Analysis, Dependency on Specific Video Coding Standard.

Huining Li and Kun Wang [7] et.al proposed "A Selective Privacy-Preserving Approach for Multimedia Data" The problem statement discussed is to address the challenges and security issues associated with multimedia data, such as privacy breaches, data leakage, and unauthorized access, and to propose a selective privacy-preserving approach that maximizes privacy weights while ensuring resource and time constraints are met. The solution proposed in this research paper is a selective privacy-preserving approach for multimedia data that allocates encryption resources according to the privacy weight and execution time of each data package. The proposed method categorizes data packages into multiple groups based on the level of privacy weight and decides whether a data package needs to be encrypted or not. To prevent malicious attacks during data transmission and storage, the approach randomly divides data into two parts and performs XOR operations with a generated cipher key in different cloud storage servers. The proposed method also considers resource and time-delay constraints in multimedia systems and formulates a single objective optimization problem with constraints of time delay and resources to figure out the maximum total privacy weights from a set of variables containing the amount of data package types, the privacy weight for each data package, and the operation time for the data with encryption and non-encryption. Advantages are can be used in many type of data, time efficient, adaptable. Limitations are problem in adaptability, energy intensive,

Yohan Beugin [8] et.al discussed "Building a secure and privacy-preserving smart camera system", The problem statement discussed is that current commercially available smart camera systems often prioritize convenience and ease of use over security and privacy, leaving users vulnerable to potential privacy violations. This work aims to address this issue by proposing a user-controlled smart camera system that prioritizes privacy and security while maintaining usability and functionality. The proposed solution is user-controlled smart camera system that uses pairing techniques and cryptography to ensure privacy and security. The system consists of one or several cameras, one or several Android smartphones running the application and belonging to users of the system, an

untrusted cloud storage server and a communication network. The system encrypts every frame of the recorded videos, and the encrypted frames are stored on a cloud storage server that has no access to any decryption material. The encrypted frames can be pulled from there by the smartphone application. The users who have access to the corresponding decryption keys on their smartphone can then decrypt and view the videos. The encryption keys are rotated at every fixed epoch by the camera. The proposed algorithm uses a combination of existing pairing and encryption techniques to build a secure and privacy-preserving system. Advantages are privacy, security, confidentiality, integrity, authenticity. Limitations are technical knowledge is needed, high-cost.

Pavan Kumar Vadrevu and Sri Krishna Adusumalli [9] et.al discussed "A Review on Privacy Preservation Techniques in Surveillance and Health Care Data Publication" The problem statement discussed revolves around the need for effective privacy preservation techniques in the context of surveillance and healthcare data. Specifically, the manuscript aims to address the challenges related to safeguarding personal privacy in the collection, storage, and publication of surveillance and healthcare data. Solution to this is to address the problem statement of effective privacy preservation techniques in surveillance and healthcare data. For video surveillance data, the manuscript discusses different privacy-preserving anonymization operations, such as smart cameras that cover sensitive or confidential information in videos, cryptographic mechanisms to protect video streams, and blockchain-based data processing approaches. For healthcare data, the manuscript reviews various personal privacy preservation methods, including anonymization techniques, homomorphic encryption, attribute-based encryption, and storage path encryption. Advantages are inclusive, insightful, comprehensive, informative. Limitations are vulnerable, less-effective.

Khattab O. Khorsheed [10] et.al discussed "Enhancing the performance of video encryption used for security and privacy protection in secure multimedia transfer", The problem statement of the research paper revolves around the need for secure multimedia transfer over unsecure networks. The authors highlight the vulnerability of data exchanges over unsecure networks and emphasize the crucial nature of multimedia security. The solution proposed in the research paper involves the development of an algorithm that affords premium security in a relatively short computational phase. This algorithm is designed to cope with different video sizes and types, as well as multiple devices. The proposed solution aims to enhance the performance of video

encryption, ensuring the confidentiality of video transfer while addressing the computational complexity associated with real-time video processing. Advantages are premium security, adaptability, less computational complexity. Limitations are proposed algorithm is not clear, omission, oversight

III. PROPOSED METHOD

The encryption system is implemented using python with Tkinter under the windows environment. The developed system is tested by considering videos of several size and duration. Performance of the system is measured using the parameters such as MSE and PSNR for position permutation and pixel scrambling techniques. The system consists of two parts sender side which consists of the encryption part and the receiver side which consist of the decryption part. In the encryption part, the frames were extracted from the original video, then the face region is detected from the extracted frames, and after that, the detected face region is encrypted using the logistic map method, then finally the encrypted video is obtained. In the decryption phase frames are extracted from the encrypted video, and face regions are decrypted from the extracted frames is to get the original video.

The details of system design involving different stages such as detecting faces in the video and encrypting the face regions are presented in this chapter. The algorithms and flowcharts for different stages are also presented.

The Encryption method for privacy-preserving system is based on two stages:

1. Face detection
2. Face encryption

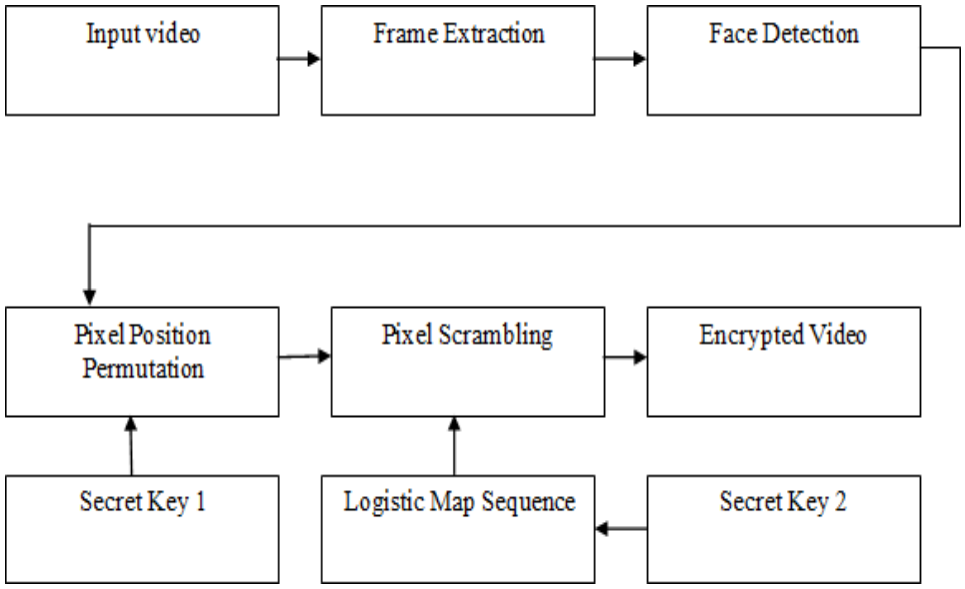

Figure 2: Video Encryption Architecture

The block diagram of the system is shown in Figure 3.1. The input to the system is surveillance video. From the input video, frames are extracted. From the extracted frames face regions are extracted using Viola-Jones method.

3.1 Viola-Jones AdaBoost Algorithm

In the Viola-Jones object detection algorithm, the training process uses AdaBoost to select a subset of features and construct the classifier. A large set of images, with a size corresponding to the size of the detection window, is prepared. This set must contain positive examples for the desired filter (e.g., only front view of faces), and negative examples (no faces).

Viola-Jones algorithm works in four stages:

Haar-features selection: -A Haar-like feature consists of dark regions and light regions. It produces a single value by taking the difference between the sum of the intensities of the dark regions and the sum of the intensities of light regions.
Creating of integral images: -A given pixel in the integral image is the sum of all the pixels on the left and all the pixels above it.
Adaboost Training: -This algorithm selects the best features from all features. It combines multiple "weak classifiers" (best features) into one "strong classifier". The generated "strong classifier" is the linear combination of all "weak classifiers".
Cascade Classifier: - It is a method for combining increasingly more complex classifiers like AdaBoost in a cascade which allows negative input (non-face) to be quickly discarded while spending more computation on promising or positive face-like regions.

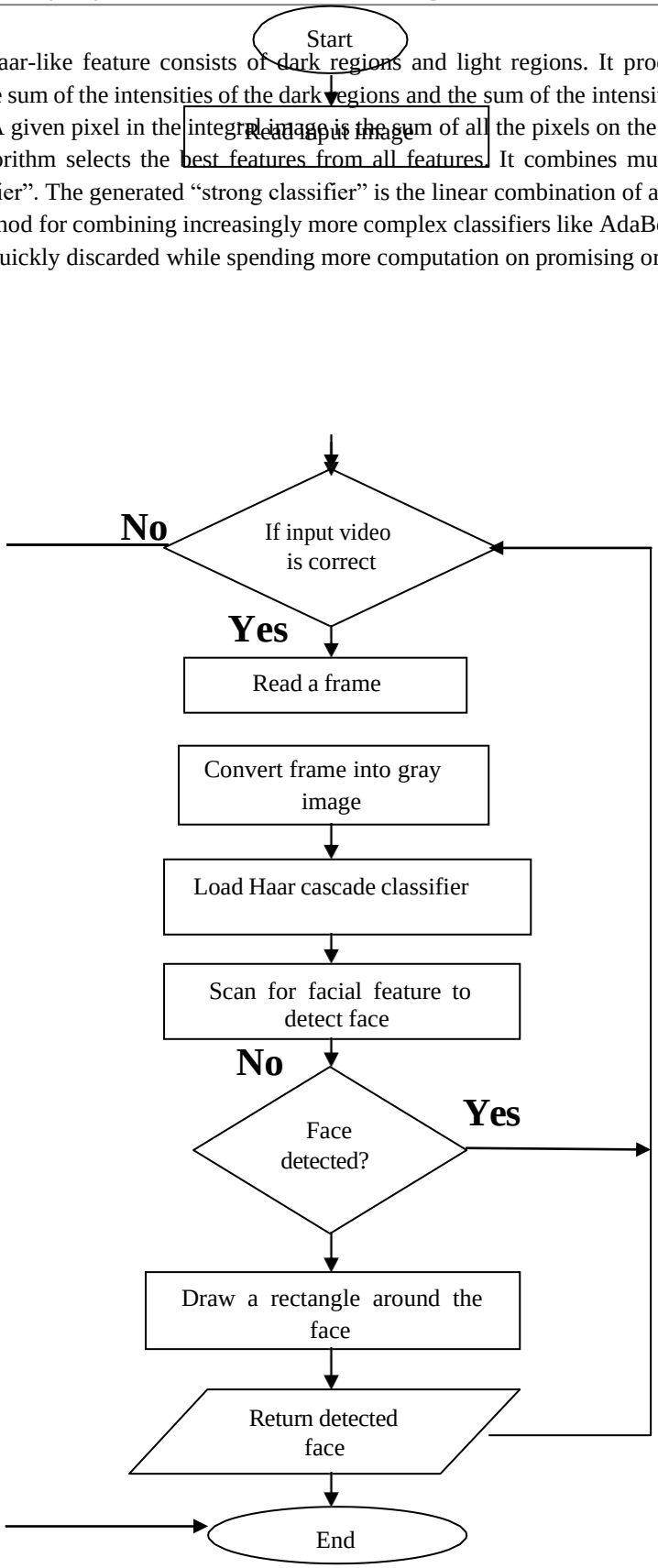

Figure 3: Flow chart for Face detection using Viola-Jones method

3.1.1 Face region detection stages in Viola-Jones method

Step 1:- Read input video
Step 2:- Read a frame/image
Step 3:- Convert frame/image into gray image
Step4:- Load Haar cascade classifier
Step 5:- Scan for facial feature to detect face
Step 6:- Face detected
Step 7:- Draw a rectangular around the face
Step 8:- Return detected face.

IV. RESULTS AND ANALYSIS

The different experiments conducted along with the results of the developed system are presented in this chapter. The performance of the system is being analysed based on various relevant parameters.

4.1 Experimental Setup

The encryption system, developed using Python with Tkinter on a Windows platform, underwent rigorous testing using videos of various sizes and lengths. System performance was evaluated using metrics such as Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) for position permutation and pixel scrambling techniques. It comprises two main components: the sender side, responsible for encryption, and the receiver side, handling decryption. During encryption, frames are first extracted from the original video. Subsequently, the facial region within these frames is identified. Following this, the detected facial area undergoes encryption using the logistic map method, resulting in the production of the encrypted video. Conversely, in the decryption phase, frames are extracted from the encrypted video. Then, the facial regions within these frames are decrypted, allowing for the reconstruction of the original video.

4.2 Snapshots

Figure 4: Frames extraction

Figure 5: Face detection using viola-jones algorithm

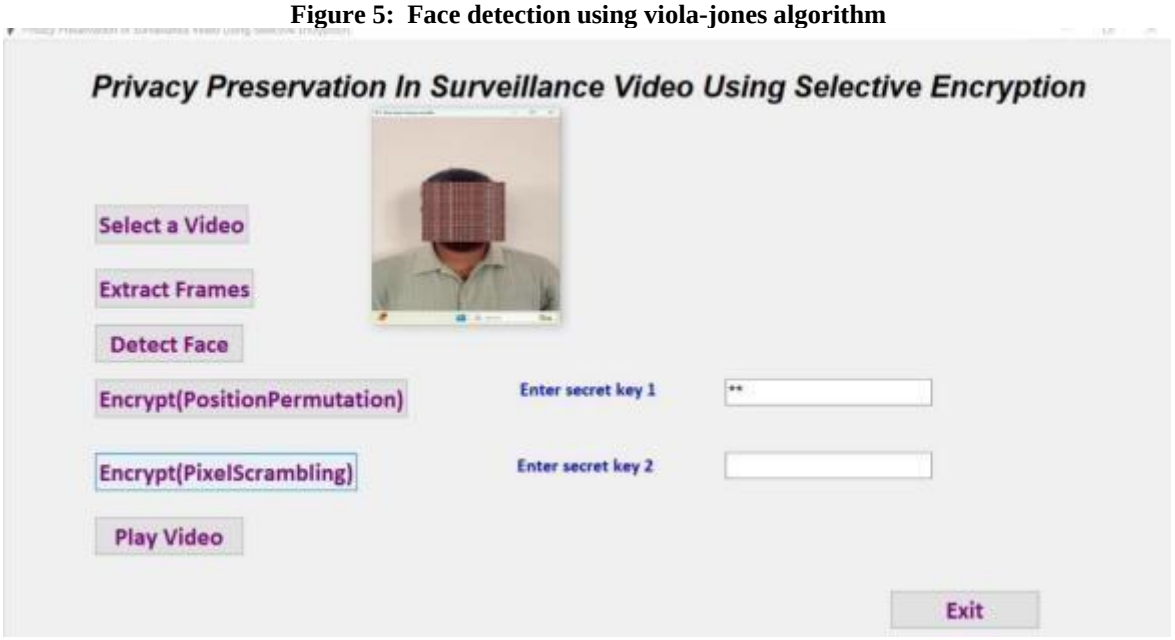

Figure 6: Encrypted image

4.3 performance Analysis

Peak signal to noise ratio (PSNR) is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of loss compression codecs. The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality. The performance is measured by computing the Mean Square Error (MSE) and Peak signal-to-noise ratio(PSNR) value for encrypted image and original image.

If I of size m x n is the original image and K is the encrypted image then

MSE is given by: $MSE = 1/mnn-1\ [I\,i\,,j-K\,i\,,]$

The PSNR is given by the following equation.

$PSNR = 20.\,log\ 10(MAXf\ )$ …. (4.2)

SL.NO	Encrypted Image	MSE	PSNR in dB
1	Frameenc 1	10.268	27.900
2	Frameenc 15	10.235	27.928
3	Frameenc 112	10.266	27.902
4	Frameenc 238	10.269	27.899
5	Frameenc 363	10.253	27.913

Table 1: MSE and PSNR for sample frames

4.3.1 Histogram Analysis

An image histogram is a graphical demonstration that shows a visual impression of the spread of pixels through calculating the number of pixels at each level. The histogram is an approximate representation of the distribution of numerical or categorical data. To construct a histogram, the first step is to divide the entire range of values into a series of intervals.

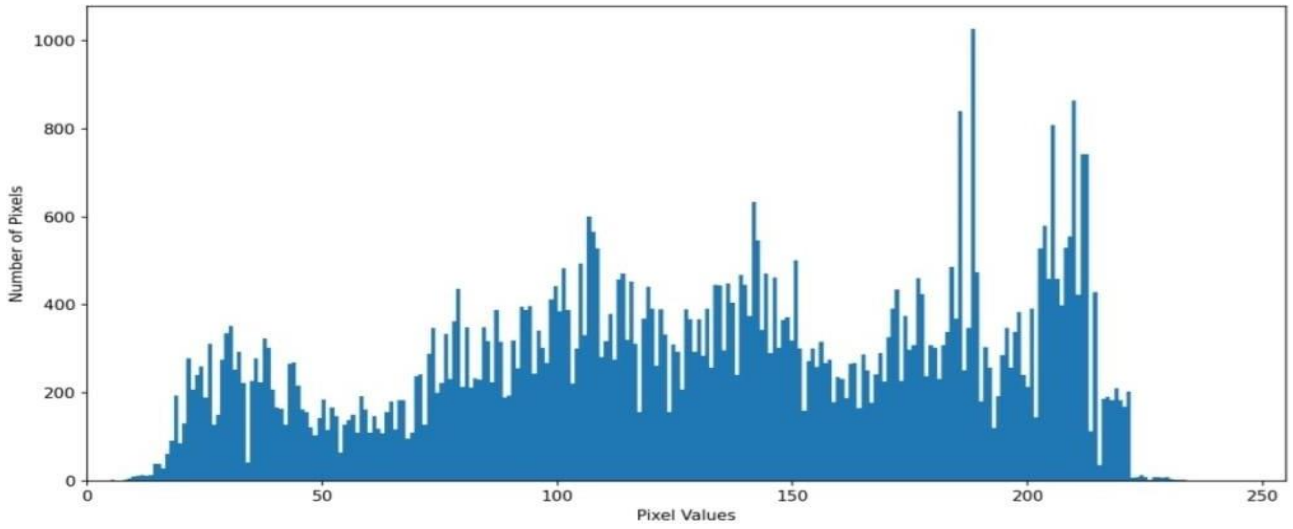

Figure 7: Histogram of Original image

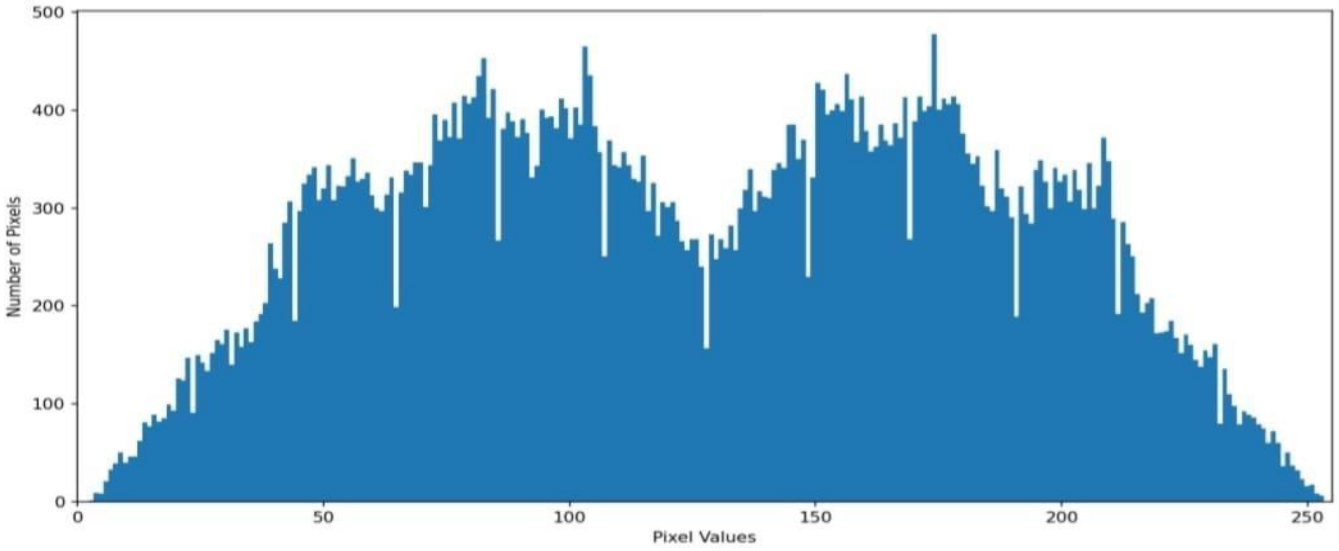

Figure 8: Histogram of Encrypted image

CONCLUSION

The design and implementation of a system for privacy preservation in surveillance video is presented in this report. In the proposed system, face region is selected as region of interest for privacy preservation. Here the aim is to conceal faces while not interfering with the observation and recognition of human activities. The proposed method is reversible for revealing faces whenever needed to the authorized person using proper secret keys. Face region in the frames are detected using Viola-Jones method. Once the face is detected, the face region of the frame is encrypted in two stages. In the first stage pixel permutation method is used and in the second stage, pixel scrambling is used. The proposed method uses two secret keys. If both the keys are matched, then only the frames get decrypted properly. The performance evaluation of the system exhibits efficient encryption which is evident from the obtained results.

REFERENCE

[1] Khalid M. Hosny, Mohamed A. Zaki, Hanaa M. Hamza, Mostafa M. Fouda, and Nabil A. Lashin. "Privacy Protection in Surveillance Videos Using Block Scrambling-Based Encryption and DCNN-Based Face Detection“,IEEE Idaho State University, Pocatello, ID 83209, USA, vol 7, 3 October 2022

[2] Alem Fitwi, Yu Chen. "Privacy-Preserving Selective Video Surveillance“, State university Binghamton, Binghamton, NY 13902, USA, 6607-7281,vol 6, 2020

[3] Alem Fitwi, Yu Chen, Sencun Zhu, Erik Blasch, and Genshe Chen. "Privacy-Preserving Surveillance as an Edge Service Based on Lightweight Video Protection Schemes Using Face DeIdentification and Window Masking“, State university Binghamton , Binghamton, 557-569, vol 9, 2021

[4] Alem Fitwi, Yu Chen. "Secure and Privacy-Preserving Stored Surveillance Video Sharing atop Permissioned Blockchain" , arXiv:2104.05617v1 [cs.DC], 356-369, vol 12, 2021

[5] Xianhao Tian, Peijia Zheng, Jiwu Huang. "Robust Privacy-Preserving Motion Detection And Object Tracking in Encrypted Streaming Video“, arXiv:2108.13141v1 [eess.IV], vol 5 , 2021

[6] Shuli Cheng ,"A Selective Video Encryption Scheme Based on Coding Characteristics",University publication, 1-15, vol-13, 2020

[7] Huining Li, Kun Wang, Xiulong Liu, Yanfei Sun, Song Guo. "A Selective Privacy-Preserving Approach for Multimedia Data", The Hong Kong Polytechnic University, 245-257, vol 12 , 2023

[8] Yohan Beugin. "Building a Secure and Privacy-Preserving Smart-Camera System“, arXiv:2208.09776v1 [cs.CR], vol 7, 2022

[9] Pavan Kumar Vadrevu, Sri Krishna Adusumalli in Surveillance and Health Care Data Publication" , International Journal of Engineering Research & Technology (IJERT),Published by, www.ijert.org, ISSN: 2278-0181, vol 8, 2021

[10] Khattab O. Khorsheed, Omar G. Abood, Shawkat K. Guirguis. "Enhancing the Performance of Video Encryption Used for Security and Privacy Protection in Secure Multimedia Transfer" International Journal of Engineering &Technology, 7 (4) (2018) 6167-6170, vol 10 , 2018