FALSE COLOR BASED VISUAL PRIVACY PROTECTION

Sruthi Viswanath, Jincy J Fernandez
Department of Computer Science and Engineering,
Rajagiri School of Engineering and Technology, Kochi, India

Abstract : Privacy of a video surveillance has drawn a lot of interest lately. The goal of visual privacy protection is to prevent sensitive information present in an image (or video) from being revealed to the viewers of this content. A reversible privacy protection scheme is proposed that protects all features in a video. False coloring, encryption and Compression is applied on video frames to provide protection. It is not region of interest (ROI)-based and can be applied on entire frames without compromising intelligibility.

Index Terms **- False coloring, Visual privacy protection.**

I. INTRODUCTION

Privacy protection aims to protect the information that an individual wants to keep private by preventing it available to the public domain. In the context of images and videos, we refer to it as visual privacy protection.

Recent advances in computer vision technologies have made the possibility of developing intelligent monitoring systems for video surveillance and ambient-assisted living. By using this technology, these systems are able to automatically interpret visual data from the environment and perform tasks that would have been unthinkable years ago[1]. These achievements represent a radical improvement but they also suppose a new threat to individuals privacy. The new capabilities of such systems give them the ability to collect and index a huge amount of private information about each individual. Next-generation systems have to solve this issue in order to obtain the user's acceptance. Therefore, there is a need for mechanisms or tools to protect and preserve peoples privacy.

The proposed method is a new approach that offers visual privacy protection to all data present in the video, while not depend on either manual or automatic sensitive regions detection, hence offering a simple and robust solution to the protection of visual privacy surveillance, monitoring, and multimedia applications

II. RELATED WORK

Visual privacy protection provides reversible privacy protection tot all features present in an imagery data which can prevent the dissemination of peoples privacy information by using different image security method and restore it when authorized persons are requested. There are many methods to achieve this goal some are discussed here

a) Image Security using Image Encryption and Image Stitching[2]:

Every image to be transmitted is divided into multiple parts and further it gets encrypted and transferred to the receiver, making it difficult for the trespassers to access the original image. Partitioning and encryption on the sender's end make it hard for the intruder to decrypt and have the original image on the other end. Chaotic techniques for image encryption makes the images highly secured and hard to decrypt. A chaotic approach implies a condition of disorder and confusion. It is very sensitive to initial conditions. Even a minute change leads to an entirely.

This work partitions the image into a number of overlapping blocks and each block undergoes encryption process. The encrypted blocks get transmitted to the receiver, where the encrypted block is decrypted. All the decrypted blocks get combined to image stitching algorithm to generate the original image.

This method is not applicable when there are multiple images.

b) Privacy Protection Using the methods of group signature and reversible mosaic[3]:

This system enables both privacy protection and law enforcement utilization of photographs. Using the methods of group signature and reversible mosaics that employ reversible watermarks, the proposed system can prevent the dissemination of facial information of certain people by "hiding" their facial information, but restore it when criminal investigations are warranted.

Anyone with a mobile device who wants his or her facial information to remain hidden from surveillance can relay a request to data-collection access points. A surveillance camera sends an original picture to the server by secure means. The access points then send request data to the server. The server constructs a mosaic of the face of the person who has requested that his or her face be hidden and sends this mosaic to a surveillant. The server stores the images as mosaics to protect all persons who are photographed.

The proposed surveillance camera system achieves both privacy protection and crime prevention. The system considers the rights of individuals to manage the acquisition and distribution of their personal information based on privacy rights. This system allows a surveillant to obtain facial information of only certain people. The study contributes to crime prevention is expected. However, it is thought that this system has much introduction cost on a real surveillance camera system.

c)Protect visual privacy of sensitive content using false coloring[4]:

Although many methods for privacy protection exist, most of them rely on computer vision algorithms, such as the face or person detection, for identifying the privacy-sensitive regions where the protection should be applied to. However, computer vision algorithms are not always accurate and there are cases this algorithm may fail such as bad capture conditions, noise in the images, and non-ideal camera viewpoints. When the computer vision algorithm failed in finding ROI even in a single frame of a video can lead to the loss of the privacy protection efforts. Therefore, a method that is independent on the computer vision algorithms is needed for more good privacy protection.

This method is simple yet effective for visual privacy protection based on false coloring. In image processing, false coloring is mainly used for representing invisible information in an image but nowadays it is used for visual privacy protection. In this method, each pixel value in an input image is mapped to value in color palette, possibly after compression of original pixel data. It is a computer vision independent method that uses simple compression/expansion schemes and false coloring.

The amount of privacy protection by using false colors is not so good as the final result can be computed by interpolating the false color image with the original with different degrees of interpolation. For some applications where intelligibility is more important than privacy, a lower weight can be given to the false-colored result to produce more intelligible images

III. PROPOSED METHOD

The proposed method have 2 phases :Protection Phase and Recovery Phase

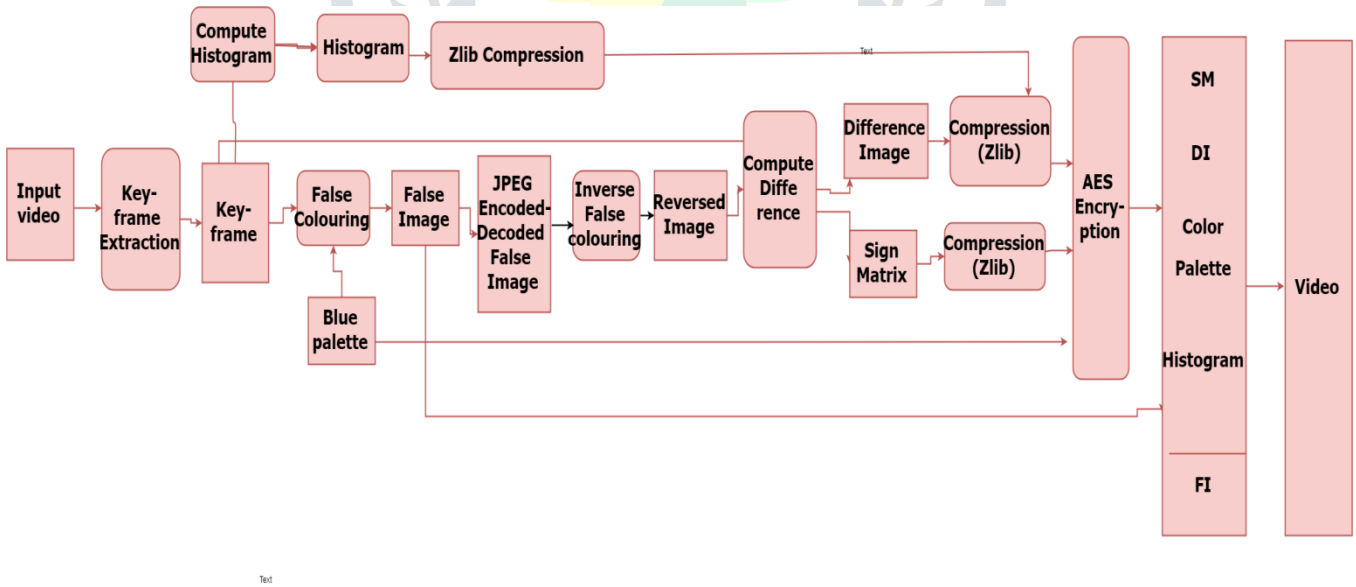

Figure 1:Protection Phase

A. Protection Phase:

During protection phase, the input video undergoes video summarization to extract key-frames instead of considering all the frames. The proposed work consider only key-frames(Frames are considered as key-frames if the histogram difference between two consecutive frames is beyond a threshold[8]). False coloring is applied on every key-frame. For an RGB image, the triplet RGB value is used to used the color palette and it is replaced by value in color palette[5]. In the proposed work, the blue color

palette is used. Let I be the input image, P_c be the color palette, The false color generated by equation 1. The false coloring process is shown in figure 2

$$FI(x,y) = P_c[I(x,y)] \tag{1}$$

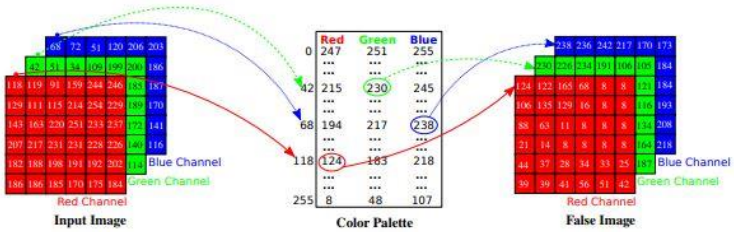

Figure 2

Further, JPEG Encoding and decoding is performed on false image to obtain FI' then Inverse false coloring is performed on FI' to get I'.

$$I'(x,y) = P_c^{inv}[FI'(x,y)] \tag{2}$$

False coloring is not a one to one operation so same false image can't be obtained from inverse false coloring. This is done by comparing each pixel value in FI' with lookup table and select least difference value

$$I'(x,y) = \underset{i\in\{0,1,..255\}}{\arg\min} |\, P_c[i] - FI'(x,y) \,| \tag{3}$$

Histogram of input image is created so that it help for image recovery during recovery phase. Then I' is subtracted from I to get difference image(DI) and sign of difference image is stored in sign matrix(SM).

$$DI = |\, I(x,y) - I'(x,y) \,| \tag{4}$$

$$SM = \begin{cases} 1, if I(x,y) - I'(x,y) < 0 \\ 0, otherwise \end{cases} \tag{5}$$

Zlib compression[6] is performed on histogram, difference image, and sign matrix. Outputs of compression and color palette are encrypted using AES Encryption[7] . Encrypted data is written to Tiff file along with false image(I) and write these images as video

B. Recovery Phase

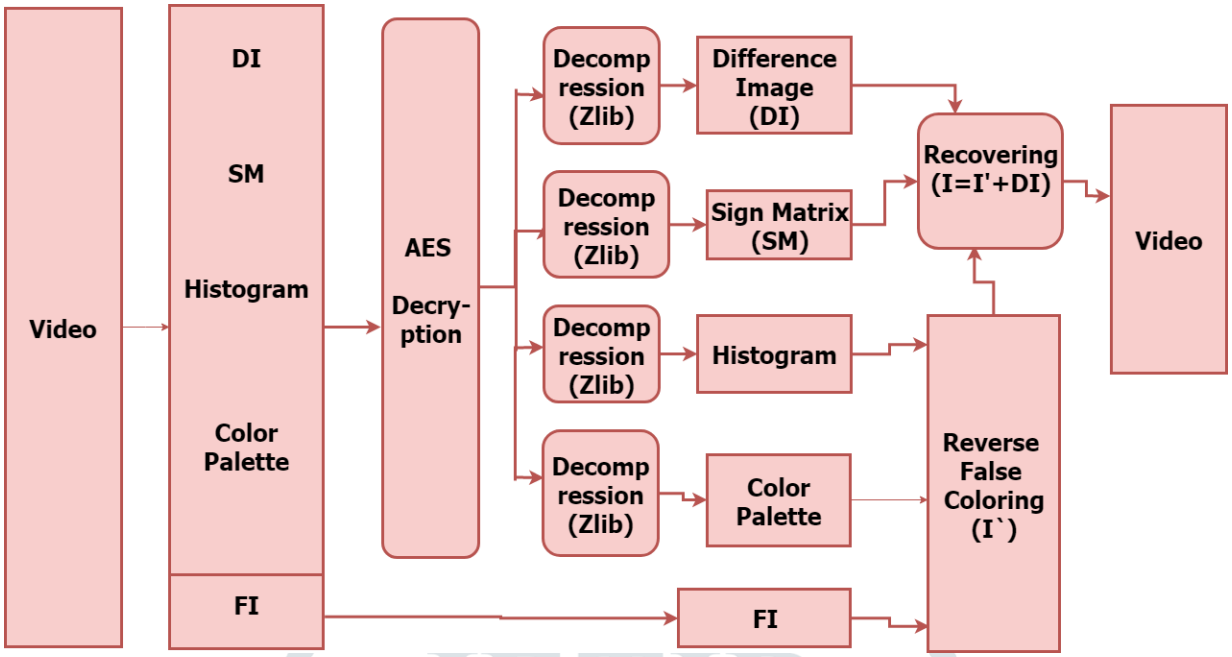

Figure 3:Recovery Phase

In the Recovery phase, original key-frame video is recovered from the protected video. For recovery, a secret key is needed that is known to only to an authorized person. Frames are extracted from protected video and read data such as false image, encrypted palette value, encrypted compressed input image histogram, encrypted compressed difference image, and encrypted compressed sign matrix. These encrypted values are given for AES decryption then Zlib decompression which gives output difference image, sign matrix image, histogram and color palette. Inverse false coloring is done on false image using color palette and histogram to get inverse false image (FI'). Using FI', DI and SM construct recovery image(R(x, y))[5].

(6)

$$R(x,y) = FI'(x,y) + s * DI(x,y)$$

Where s is computed as:

(7)

$$s = \begin{cases} 1, if SI(x,y) = 0 \\ -1, otherwise \end{cases}$$

Construct video from these recovered frames (R(x, y)).

IV. Result and Discussion

Read input video and extract key frames from video using histogram technique. The input video containing car had around 270 frames. It extracts 11 frames from . avi format video. Key-frames frames are shown in Figure 4.

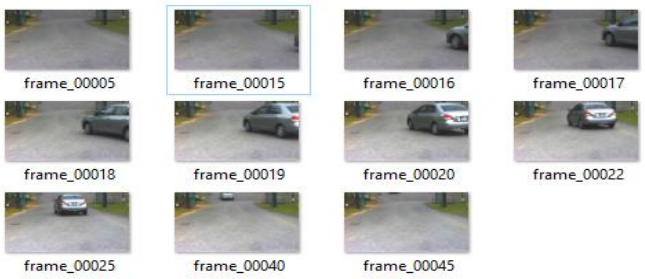

Figure 4

After key frame extraction, each frame undergoes a series of operations such as false coloring, compression and encryption to make it protected. Blue color palette is used for false coloring. Figure 5 shows input image and Figure 6 show false colored image.

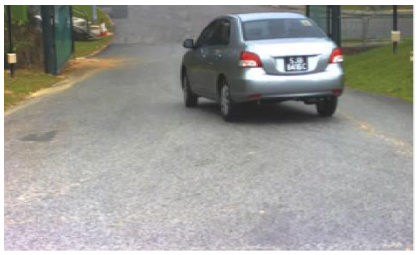

Figure 5

Figure 6

JPEG compression is performed on false image with threshold 80. Figure 7 show before and after JPEG compression

Figure 7

Inverse false coloring is performed on encoded decoded false image to get inverse image. Figure 8 show Inverse JPEG Encoded-Decoded False Image

Figure 8

Inverse JPEG Encoded-Decoded False Image is subtracted from input image to get difference image and sign matrix. Figure 9 and 10 show Difference image and sign matrix image

Figure 9

Figure 10

Zlib compression is performed on difference image, sign matrix and histogram of input image then compressed data along with color palette is encrypted in to cipher format using AES algorithm. After encryption False image is written to tiff file along with encrypted difference image, sign matrix, histogram, color palette. Each frame in video is converted to protected Tiff files and then make video using this Tiff file. Output of protection phase is a video with protected frames. On recovery, read each frame from protected video and given to decryption, decompression and recovery to get original key-frames. Figure 11 shows Recovered Image.

Figure 11

Construct video using these recovered images to get recovered original CCTV footage.

a. Selection of color palette :

Analyzed different color palettes and chosen 3 color palettes based on their preserving privacy efficiency.

- Input image, false image, Difference image and sign matrix using Blue color Palette:

- Input image, false image, Difference image and sign matrix using Green Color palette:

- Input image, false image, Difference image and sign matrix using Purple color palette:

Among them, the Blues palette has a more monotonic variation of colors, Green is extremely erratic, and the Purple is in-between. The color palettes also influences the quality of the recovery. For the Blues palette, is more monotonic than the other two palettes, the quality of the recovery is very well and therefore the difference image contains very small values. However, for the other two palettes the recovery is progressively less effective due to their less regular variations across the color scale. Based on visually determination Blue palette is selected since it give most accurate reversal of a target face but if security is the primary concern, one should select a palette with more random variation to avoid reconstruction of the original data by unauthorized users.

b. Face detection:

Done experiments to check the privacy of the protected video. Applied face detection algorithm on protected data to find faces in the video, but the algorithm returns zero faces. The face detection algorithm used is based on Haar Feature-based Cascade Classifiers and OpenCV. This face detection algorithm searches faces in input using a trained model and extract and returns the location of faces in the input. The proposed system protects the privacy of protected data by making it unable to extract any sensitive information from video by human observers or face recognition algorithms. Figure 12 and 13 shows input and protected frame.

Figure 12

Figure 13

c. Structural similarity:

Structural Similarity Index (SSIM) is a perceptual metric that provides a good approximation to perceived image distortion[9]. In the proposed model SSIM values of recovered video frames with respect to the input video frames is 0.946131. There is a small difference between the input video and recovered video but it still keeps sensitive data in the frame without distortion .Figure 14 shows input frame and recovered frame

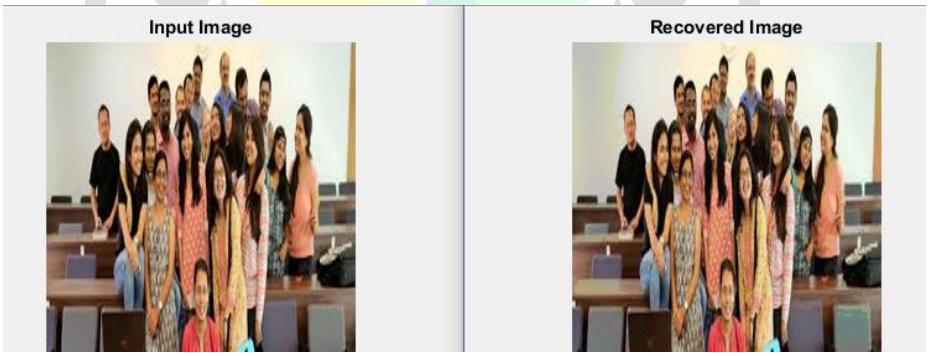

Figure 14

V. CONCLUSION

Proposed work is a method for visual privacy protection using false coloring. Key-frames are extracted from the input video and it undergoes several operations like false coloring, compression, and encryption to make it protected. During Recovery, the original video is recovered from protected video using operations like decryption, decompression, etc. This method is a simple and robust solution to the protection of visual privacy surveillance, monitoring, and multimedia applications. It strikes a balance between various criteria that are important in visual privacy protection, namely privacy, intelligibility, reversibility, security, and robustness.

The primary advantage of this method is that it can be applied on the entire image does not require any prior face detection or other sensitive regions detection so it is a computer vision independent method and protection is continuous. Color

palette depends on privacy along with intelligibility. In this work, Color palette is selected based on an accurate reversal of a target face but if security is the primary concern, one should select a palette with more random variation to avoid reconstruction of the original data by unauthorized users.

REFERENCES

1] J. R. Padilla-Lopez, A. A. Chaaraoui, and F. Florez-Revuelta, "Visual privacy protection methods: A survey, " Exp. Syst. Appl. , vol. 42, no. 9, pp. 41774195, 2015.

[2] Jyoti T. G. Kankonkar, Prof. Nitesh Naik "Image Security using Image Encryption and Image Stitching"', Proceedings of the IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC)

[3] Kento Kobayashi, Keiichi Iwamura, Kitahiro Kaneda, Isao Echizen, "Surveillance Camera System to Achieve Privacy Protection and Crime Prevention, "', 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

[4] Serdar C iftci, Pavel Korshunov, Ahmet Oguz Akyuz, and Touradj Ebrahimi "Using False Colors to Protect Visual Privacy of Sensitive Content"'

[5] Serdar C iftci , Ahmet Oguz Akyuz, and Touradj Ebrahimi, Member, IEEE " A Reliable and Reversible Image Privacy Protection Based on False Colors", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 20, NO. 1, JANUARY 2018

[6] Savan Oswal , Anjali Singh , Kirthi Kumari " DEFLATE COMPRESSION ALGORITHM ", International Journal of Engineering Research and General Science Volume 4, Issue 1, January-February, 2016.

[7] Sneha Ghoradkar, Aparna Shinde "Review on Image Encryption and Decryption using AES Algorithm. ", International Journal of Computer Applications (09758887) National Conference on Emerging Trends in Advanced Communication Technologies (NCETACT-2015).

[8] Sanjoy Ghatak "Key-frame extraction using threshold technique. ", International Journal of Engineering Applied Sciences and Technology, 2016

[9] Zhou Wang, Member, IEEE, Alan C. Bovik, Fellow, IEEE Hamid R. Sheikh, Student Member, IEEE, and Eero P. Simoncelli, Senior Member, IEEE,"Image Quality Assessment: From Error Visibility to Structural Similarity. ", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 13, NO. 4, APRIL 2004