Scientific Journal of Impact Factor (SJIF): 4.14
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 6, June -2016

Investigating Approaches for Privacy Preserving Traffic Surveillance

Kushal D. Patel[1], Mihir A. Mishra[1], Pragnesh A. Patel[1], Avani P. Patel[1], Vibhuti P. Patel[1]

[1] *Computer Engineering Department, GIDC Degree Engineering College, Abrama, Navsari*

Abstract- *Traffic surveillance has become essential in many areas to estimate important traffic parameters. Traffic surveillance includes monitoring, restraining and adjusting traffic on the roads to ensure protection and smooth traffic flow. However, there are privacy consequences for citizen's since they are directly captured by camera wherever they travel. In addition, the perceiver can watch the person's travelling habits or activity. This endures threat of personal privacy. Privacy preserving traffic surveillance addresses these privacy breaches. Surveillance should be done in such a way that surveil for the any wrongdoing on the road and preserve the privacy of individuals at the same time. Existing approaches for privacy preserving video surveillance are based on the region of interest (ROI) and hence compromise the privacy. In addition, a few approaches fail to reconstruct the original image. In this paper, we propose approaches that preserve the privacy of citizens while correctly reconstructing the original image.*

Keywords- *Privacy, Edge Detection, HSV (Hue, Saturation, Value), Traffic Surveillance, Video Surveillance*

I. INTRODUCTION

Traffic surveillance is used towards improving transportation efficiency, reducing the congestion on roads and promoting highway safety. Traveler information systems viz. www.masstraveler.com, www.mass511.com www.english.webcam-bruecken.de, www.livetrafficlondon.com, provide various aspects of traffic information [1]. Such websites, broadcast real-time video feeds, which showing traffic flow on the road. Perceiver can record individual's travelling patterns along roads and highways. The observer can colligate that location with other records, such as where a person was in the past. The observer can expend these records for the forecasting of people's future movements and locations. These may induce problems such as watching your travelling habits or activity with specific places (where) and time (when) or with other personal (whom). Privacy preserving traffic surveillance deals these privacy consequences.

For any privacy preserving traffic surveillance application, the following requirements are desirable:

1. Traffic surveillance should be done in a such a way that the frames captured by cameras (fig. 1.a), should be seen by the traffic observer as transformed results (fig.1.b). The observer should merely discover the presence of vehicles and the persons on the road. The personal identity should not be revealed.
2. This transformed result should also be reconstructed in original form as and when required for the security purposes.

a. Original b. Transformed

Figure 1. Privacy preserving Traffic surveillance

In literature, there do exists approaches for privacy preserving video surveillance [2][3][4][5][6][7][8]. However, we observe the following from the existing literature: The approaches proposed in [4][5][6][8] identifies objects in the video that reveal identity of an individual and then apply appropriate methods to protect individual's privacy. Further, these approaches are based on identifying a region of interest (ROI), in which, if region of interest are not correctly identifies than the privacy can be compromised as the missed regions would not be processed to preserve privacy.

1) The schemes proposed in [2][3][7][8] not retains all the user action which may useful for crime investigation in real time. In addition, for the security purpose the processed result should be recovered to original form.

In this paper, we propose three approaches that eliminate the requirement to identify ROIs and do surveillance in real time. In addition, it also retains user actions intact. Further it recovers original frame whenever required.

II. BACKGROUND

Privacy is "*the state or condition of being free from being Observed or disturbed by other people*" [2]. The omnipresent of traffic surveillance cameras raise significant fears of the individual's privacy. In some cases, cameras are mounted in hiding positions, so that people tracked by these cameras have no way of knowing that they are being captured and tracked. Advances in storage and processing technology, the observer can target and record nearly one and all that who travel on a road or highways.Surveillance camera utilized decently can facilitate to disclose any misconduct, but it can cost to privacy of those who does not involved in any malfunction [9]. A fundamental challenge is to invention of surveillance system that helpful to fulfill security demands along with protection of privacy of the individuals. Video captured by CCTV camera can be used to see live traffic on the road. These videos can be stored for the future usage or can be fed to live traffic indicating websites such as www.livetrafficlondon.com. There may threat that these stored videos can be perverted by the observer.

Individual privacy compromises when others keep track of individual, as they move on roads. Individual's location and travel patterns can reveal their activities, associations and what people believe to be important or private to them. Often, individuals are unfamiliar with sources, capturing their activities and eventually are unaware that their activities are monitored. Information collected through roadway surveillance can be used to annoy the individual through targeted marketing and advertising [10]. Such information can also be used to harass the individuals through stopping and questioning them. In addition, such information may even be used by stalkers to horrify or even to killing the individual [10]. Video-based surveillance systems are in rapid expansion and are already widely present in our everyday life: there are more than 2.5 million CCTV (Closed Circuit Television) cameras are in operation in the United Kingdom (U.K.) and 25 million worldwide [11]. At the average, a citizen is caught on CCTV cameras 300 times in a day in U.K. [11].

III. RELATED WORK

In [2], Unmanned Aircraft Vehicle (UAV) surveillance system, an Unmanned Aircraft (UA), after capturing video, transmits the encrypted video data to a privacy server. Decryption of encrypted video data performed at a cloud-based privacy server. In addition, videos examined based on the most up-to-date privacy policy. In this approach, after the filter operations, the hygienized video would be directed to the surveillance operator. Surveillance operators can analyze the encrypted video, but it cannot decrypt the video because it does not have the decryption key. In addition, the symmetric key has been shared only with camera, i.e. UA and privacy server. The privacy policy dictated at privacy server as per the varied privacy requirement. Any privacy demands and privacy invasion can be supervised and imposed in real-time at the privacy server [2]. In this approach, initially, the camera requires to communicate with privacy server for the encryption key. One of the restriction of this approach is that the camera may have to wait until the encryption key from privacy server or in other words until it is authenticated by the privacy server. In addition, it requires uninterrupted internet connectivity. Though it is wireless internet connection, there may chance of no wireless internet connection available in some area [2]. In addition, privacy server may face denial of service attack (DoS attack). Therefore, in some event, real time video surveillance may not be possible due to journey of video, initially from UA to privacy server and then from the privacy server to the surveillance operator.

In [3], Dufaux et al proposed a selective scrambling based solution to preserve privacy. In this approach, there is one analysis module that identifies regions of interest which is presumed to incorporate privacy sensitive information. These regions, then scrambled [3]. The scrambling performs in the transform domain by pseudo-randomly alternating the sign of transform coefficients during encoding. In [4], Yu et al. proposed a system called PriSurv, which flexibly alters the method for obscuring Privacy Sensitive Information (PSI) regions according to the relationships between the viewer and the subject's visual information. For this system, they proposed two methods to assure disclosure of an individual's privacy. In [5], Sohn Proposed an approach in which pseudo random sign inversion is imposed to a Region of Interest (ROI). Individual face is encrypted by comprises of random sign bit inversion of non-zeros levels by using the XOR method with multiple keys. However, the encrypted video can be recovered by the brute force attack on sign bits. Limitation of approach in [3][4][5] that the privacy of individual depends on the successful identification of ROI.

In [6], Ivasic-Kos has proposed an approach for person de-identification based on the person's activities. They have employed Gaussian blurring in order to change the obtained human body silhouettes. This method helps to de-identify personal information, while preserving the actionable information, i.e. action performed by a person. However, this approach mainly focuses on single person activity. In [7], Cao et al proposed a scheme by using visual cryptography. In this scheme, from original image, foreground and background are detached. After detachment of foreground component, each foreground image is decomposed into two share images. These foregrounds can be reconstructed only when the two shares are superimposed. Here superimposing is carried out using the XOR operation of the two shares of each foreground [7]. In [13], Upmanyu et al. Proposed an efficient model to accomplish privacy preserving video surveillance. In this approach, they decompose each image into a set of random images (shares). Each separate image solely does not convey any meaningful information about the original frame, while all together, they hold entire information. Their solution derives from a Secret Sharing (SS) scheme based on the Chinese Remainder Theorem (CRT). The limitation of

approaches [7][13] is that if one share is unavailable at the time of reconstruction than one cannot able to reconstruct the original form of video.

In [8], Prachi proposed an approach based on Bounding Box that discover humans in the video and then de-identify human faces that are detected. There are many modules in their approach to detect faces and its corresponding locations. If anyone module fails, then their approach does not considerably preserve privacy. In some cases, smart camera performs privacy preserving surveillance inside the camera itself [14]. It requires expensive programmable cameras. The camera may be bounded to individual camera algorithms [14]. Altering these algorithms becomes tedious and expensive. These approaches rely on the success of truthful detection of interest regions and do not provide any guarantee of privacy. Moreover, the original video lost in it. In [15], Ralph proposed method based on k-same nearest neighbor. From the privacy protection point of view, this approach assures the desired k-anonymity, the utilities of the resulting averaged faces are often compromised. Specifically, the averaged face may have degraded viewing quality. In addition, it may miss useful facial signatures (e.g. Action or Expressions) due to averaging. For e.g. the ability to distinguish gender or facial expressions from de-identified images may be compromised.

Table 1. Comparison of Approaches for Preserving Privacy in Video Surveillance

Approach	Description	Limitation
Detecting Skin Tones [16]	Substitute skin tones with other colors, hence makes it infeasible to ascertain the race of the individual	It does not conceal the identity completely
Encryption Based on Permutation [17]	Encryption establishes using permutation of the location of the pixels. The permutation based encryption tolerates lossy compression and allows decryption at a later time.	It is based on object selection. If object is not properly discovered, then privacy of individuals may disrupt.
Row Video Decompossion [18]	Video decomposes into object-video streams. The privacy of detecting person is protected by selectively rendering the corresponding objects. The quality of an object-based video decomposition intimately depends on the performance of low-level vision processing.	If segmentation is inadequate, then decompositions of video may be poor or ineffective.
Bounding Box [8]	It discover humans in the video and then de-identify human faces that are detected. There are many modules in their method to detect faces and its corresponding locations.	If any one module fails, then their method does not perform considerably

IV. PROPOSED APPROACHES

In traffic surveillance, privacy preserving transformed results requires in real time. In addition, individual action should be visible in that video for security purpose or for investigating traffic law-breaking events. In Table 1, we give a brief description of various approaches and its limitations for preserving privacy in video surveillance. The schemes [2][3][7][8] not retains all the user action which may useful for crime investigation in real time. In addition, the schemes described in [4][5][6] depends upon on correctly detection of Region of Interest (ROI). Furthermore, to monitor and to adjust traffic on roads, information lost in the transformed result should be minor. Face detection based privacy preservation scheme may not detect some individual in crowded environments. Our three approaches overcome limitation of detection of face or region of interest. Further, our approaches reconstruct original frame as and when it requires.

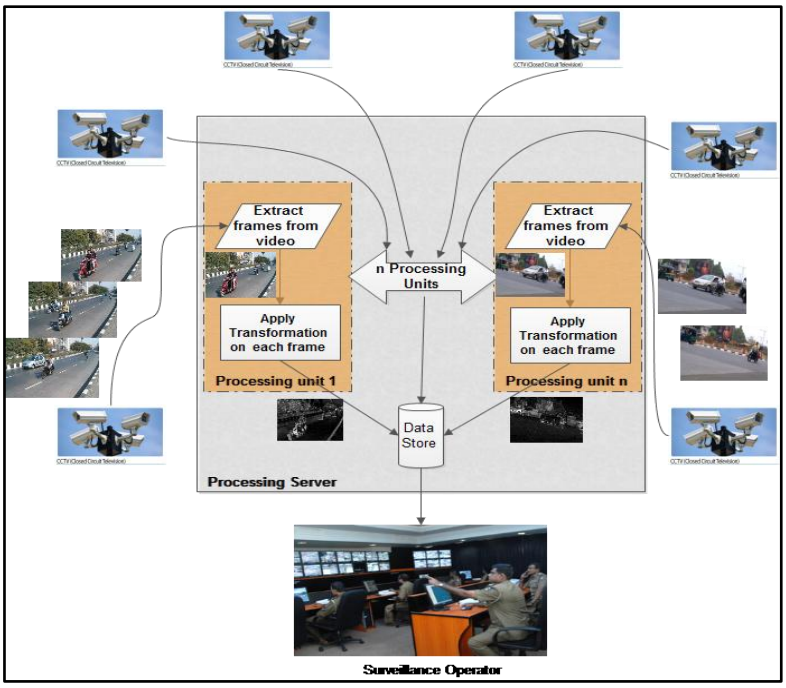


Figure 2. Framework of proposed approaches

The common framework of our three proposed approaches is as shown in fig 2. Initially, video captures by surveillance camera is sent to the processing server. At processing server frames from the video are extracted at the processing unit. Then privacy preserving transformation is applied to each frame. These transformed frames are then transmitted to the observer via secure channel. Here the observer may be any traffic rule regularity officer or any citizen who used traffic website, to predict the traffic on the road.

Approach 1: Scaling and Randomization

We utilized scaling and randomization of each pixel for transformation. In [13], an efficient privacy preserving video surveillance technique using secret sharing (SS) methods has been proposed. In their scheme, each pixel value splits into separate shares and then distributes these shares between different servers. At each server, scaling and randomization apply on each pixel value and then at observer, the original value of the pixel is reconstructed using Chinese Remainder Theorem (CRT). In this scheme if any share would not available at observer than the observer have to wait. Therefore, we eliminate separate server computation. In our approach, we utilize scaling and randomization of each pixel value by applying the following equation at processing server,

$$\mathbf{NP} = (\mathbf{P} * \mathbf{S}) \bmod \mathbf{K} \qquad \mathbf{(1)}$$

Where,

P= Original Pixel Value

S= Scaling Factor,

K= Prime Number, K>255

NP= New Pixel Value

Here, every pixel value (P), in the frame is transformed into new pixel (NP) value using this equation 1 above. Then, every scaled value can be randomized in the range of 0 to K-1. Original pixel value (P) can be recovered using equation 2 below.

$$\mathbf{P} = (\mathbf{NP} * \mathbf{S^{-1}}) \bmod \mathbf{K} \qquad \mathbf{(2)}$$

Here, S^{-1} is a modular multiplicative inverse of S. K is the prime number. The modular multiplicative inverse of S modulo K can be calculated by using the Extended Euclidean Algorithm. If K<255, then NP value ranges from 0 to K-1. However, for the grayscale image, the pixel value is in the range of 0-255. So if K<255, then for some pixel value in the original image which is greater than K, could not be recovered by using the modular multiplicative inverse method for reconstruction of pixels. So the value of K should be greater than 255. Here frame with NP values are transmitted to the observer. This approach is more secure from attacker to reconstruct the original frame from the transformed one.

Approach 2: Edge Based approach

For edge detection Sobel, Robert, Prewitt, Canny, Laplacian of Gaussian, Zero cross methods are usable [19]. Based on the result of an experiment on diverse images on traffic surveillance, we incorporate horizontal and vertical edge based detection in our second approach. In this approach, at first the incoming frame is converted to grayscale from digital color image. Then, we employ the horizontal edge detection operator and then the vertical edge detection using a vertical gradient operator and horizontal gradient operator. A horizontal gradient operator is given by: [-1 0 1] and a vertical gradient operator is given by: $[-1\ 0\ 1]^{T}$ [19]. Then both edge detection results are summed together for better result.

New Frame = Horizontal Edge Detection on original Frame + Vertical Edge Detection on original Frame

It incurs less computational overhead. This approach is faster for real time surveillance. The result of this approach can be useful for broadcasting live feed. For example, processed video by approach 2 can be fed to a traffic suggesting website in real time with privacy protection of the individual.

Approach 3: Using HSV color model theory

In HSV (Hue, Saturation, Value), Hue shows how much pure color in a digital color image [19]. Saturation denotes the proportional purity or an amount of white light assorted with a hue. The Degree of saturation is inversely proportional to the amount of white light added [19]. Value (V) denotes lightness or darkness of a color [19]. Hue (H) is presented as the angle that takes values from 0° to 360° [20]. Hue (H) diverges the color from Red at 0°, Green at 120°, Blue at 240° and back to red at 360°/0°. Saturation (S) diverges from 0 to l or it can be represented in percentage from 0 to 100%. When the Saturation, S is 0, color is a gray. When the saturation value is high, the color is white/gray/black, which is depending on the value of intensity [20]. Value (V) or Intensity (I) represented as 0 or as 1. 0 represents as a black and 1 represents as a white.

In our approach, we initially convert RGB (Red, Green, and Blue) to HSV component of each frame. Further, we separate each H, S, V component from the frame. As saturation (S) only highlight intensity, resulting frame after separation of S, does not disclose any identity. Following to separating H, S, and V component, only the S component of each frame is sent to the observer. The security of this approach depends on availability of H, V component because to reconstruct the original frame. To reconstruct, it requires all H, S, V component together.

V. EXPERIMENTAL RESULTS AND ANALYSIS

Here We consider three different Datasets: Dataset 1 (762 frames), Dataset 2 (698 frames) and Dataset 3 (1398 frames), where each of three has dissimilar intensity and brightness. In addition, each of the dataset has a different number of individuals and vehicles on the road in each frame. We examine our three proposed approach with three different resolutions of frames.

All of these frames are of 1920x1080 Full High Definition (FHD) resolutions which are incorporated for High Definition Television (HDTV), 768x576 (576i) resolutions which employed for standard definition television (SDTV) resolution video mode and 320x240 Quarter Video Graphics Area (QVGA) resolutions which is an incorporate for a computer and smart phone mobile display.

In our approach, at processing server, frame extraction rate from Video is 30 frames per seconds (FPS) for all data sets. In addition, in our approach we assume that all this transformed frame from processing server is directed to the observer or to live feed on the internet via secure channel. In addition, transmit time of frames for processing server to observer is real through high bandwidth Internet or LAN. We also assume that for reconstruction purpose our transformed frames are stored into processing server securely.

Table 2. Processing time (seconds) for Approach 1

No. of Frame	Process Time	FPS	Resolution
762	0.074	14	1920x 1080 (FHD)
698	0.14	7	
1398	0.072	14	
762	0.042	24	768x 576 (576i)
698	0.046	22	
1398	0.042	24	
762	0.011	88	320x240 (QVGA)
698	0.012	84	

1398	0.012	84	

In approach 1, we first implements the frame multiplication by S for scaling of the pixel value, then we apply randomization on scaled value by applying mode operation using a prime number K as discussed in equation 1.

Table 2 demonstrates that, by this approach, we achieved 14 frames per second (FPS) for Dataset1, 7 FPS for Dataset2, 14 FPS for Dataset3, for FHD resolution video. By this approach, we achieved 24 frames per second (FPS) for Dataset1, 22 FPS for Dataset2, 24 FPS for Dataset3 for 576i resolutions. In addition, by this approach, we achieved 88 frames per second (FPS) for Dataset1, 84 FPS for Dataset2, 84 FPS for Dataset3 for QVGA resolutions. A processing time of approach 1 is real. So it can be utilized for real time surveillance.

In, fig. 3.a, 3.c, 3.e are original frame extracted from the video and fig. 3.b, 3.d, 3.f respectively, are corresponding transformed frame which is available to the observer by applying approach 1 in such a way that preserve privacy or conceal the identity of an individual. Fig 3.b, 3.d, 3.f demonstrates that from transformed frame, one can able to forecast the traffic scenario on the road.

For instance, one can decide their travel plan from transformed frames, whether to travel on that road or to choose alternative one depending on congestion on the road. In addition, surveillance officers can do surveillance, whether any wrongdoing is happening on the road or not. In addition, user action is intact which can be utilized for finding suspicious activity.

Security of the approach 1 depends on the scaling factor (S) and Prime number (K) in equation 1. For an attacker, to reconstruct the original frames from transformed frames, the attacker must have both these values together. If the S value is higher, than its takes longer time to reconstruct the original frame using brute force attack. For the security purpose, reconstruction can be done as discussed earlier by using equation 2.

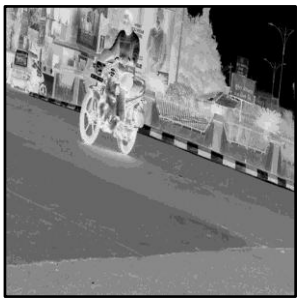
a. Original Image

b. Transformed Image

c. Original Image

d. Transformed Image

e. Original Image



f. Transformed Image

Figure 3. Result of Approach 1

For approach 2, initially we convert incoming frame to Gray scale and then apply horizontal and vertical edge detection on it by applying a vertical gradient and a horizontal gradient operator. In addition, for better results we summed them together.

Table 3. Processing time (seconds) for Approach 2

No. Of Frame	Process Time	FPS	Resolution
762	0.11	14	1920x 1080 (FHD)
698	0.20	7	
1398	0.08	14	
762	0.036	28	768x 576 (576i)
698	0.030	33	
1398	0.036	28	
762	0.015	67	320x240 (QVGA)
698	0.016	63	
1398	0.011	87	

Table 3 shows that, for approach 2, we achieved 14 frames per second (FPS) for Dataset1, 7 FPS for Dataset2, 14 FPS for Dataset3, for FHD resolution video. By this approach, we achieved 2 frames per second (FPS) for Dataset1, 33 FPS for Dataset2, 28 FPS for Dataset3 for 576i resolutions. In addition, by this approach, we achieved 67 frames per second (FPS) for Dataset1, 63 FPS for Dataset2, 87 FPS for Dataset3 for QVGA resolutions.

a. Original Image

b. Transformed Image

c. Original Image

d. Transformed Image

e. Original Image

f. Transformed Image

Figure 4. Result of Approach 2

In, fig. 4.a, 4.c, 4.e are original frame extracted from the video and fig. 4.b, 4.d, 4.f respectively, are corresponding transformed frame which is available to the observer using approach 2 in such a way that preserve privacy or conceal the identity of an individual. Fig. 4.b, 4.d, 4.f demonstrates that from transformed frames one can able to forecast the traffic scenario on the road as describes for approach 1. The weakness of this approach is that once the frame processed by this approach, it becomes difficult to recover from its transformed frame. However, we assume that original frame can be stored on the processing server using any cryptography method before applying the transformation on each frame and can use original frame when there is a requirement of it. This approach can be utilized for live traffic webcasting. In this approach, a processing time is almost similar as approach 1. It eliminates the requirement of detecting the region of interest for preserving privacy of individual's.

Table 4. Processing time (seconds) for Approach 3

No. Of Frame	Process Time	FPS	Resolution
762	0.22	5	1920x 1080 (FHD)
698	0.51	2	
1398	0.24	4	
762	0.153	6	768x 576 (576i)
698	0.144	7	
1398	0.079	13	
762	0.024	41	320x240 (QVGA)
698	0.026	38	
1398	0.026	38	

Table 4 shows that, we achieved 5 frames per second (FPS) for Dataset1, 2 FPS for Dataset2, 4 FPS for Dataset3, for FHD resolution video. By this approach, we achieved 6 frames per second (FPS) for Dataset1, 7 FPS for Dataset2, 13 FPS for Dataset3 for 576i resolutions. In addition, by this approach, we achieved 41 frames per second (FPS) for Dataset1, 38 FPS for Dataset2, 38 FPS for Dataset3 for QVGA resolutions.

In, Fig. 5.a, 5.c, 5.e are original frame extracted from video and Fig. 5.b, 5.d, 5.f respectively, are corresponding transformed frame which is available to the observer using approach 3 in such a way that preserve privacy or conceal the identity of an individual.

a. Original Image

b. Transformed Image

c. Original Image

d. Transformed Image

e. Original Image

f. Transformed Image

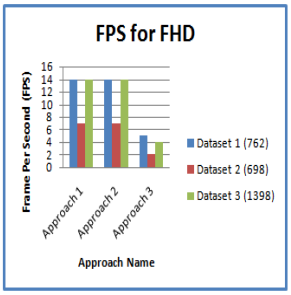
Figure 5. Result of Approach 3

The security of approach 3 depends on availability of H and V component. If 3 components altogether are available, then only we can reconstruct original frame. In addition, one component solely out of three, does not reveal any information. In our approach, only S component available to the observer from processing server via secure channel. It does not disclose any identity. Here, we assume that, the H and the V component are stored at processing server securely. However, for more security, we assume that H and V component is stored separately by applying any encrypted method at processing server. By using H, S, V component R, G, B value can be reconstructed using equations given in [19] for HSV to RGB conversion. The processing time of approach 3 is slightly higher than the other two approaches. However, this approach can also be utilized for real time traffic surveillance. In addition, approach 3 can be useful for travel planning as well as for surveillance officers to do traffic surveillance. In addition to our three approaches, we out with the background subtraction method by using image averaging approach.

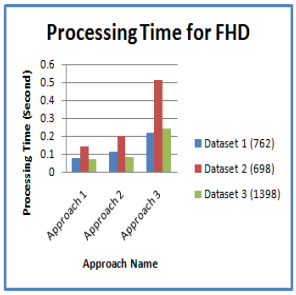
In this experiment, we, initially, average few frames and then subtract each frame from average frame. We found that, the resulting frame, preserve the privacy of individuals. However, we cannot reconstruct original frame back from resulting frame. This approach can work if and only if the background is properly extracted. For example, it is not giving perfect results at traffic stopping points like a traffic signal where the person and vehicle are stopped. It is working perfectly only if the vehicle or person is in motion.

Comparison between our three approaches

Fig. 6.a, 7.a, 8.a shows comparison respectively, for FHD, 576i, QVGA resolutions. Similarly, fig. 6.b, 7.b, 8.b, shows comparison of processing Time between three different approaches for three different data sets. We can say that as compared to approach 1 and approach 2 processing time for an approach 3 is higher. In addition, approach 3 processes lesser number of frames per second.

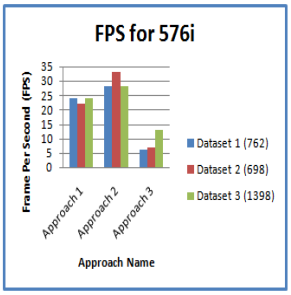


a. FPS for FHD

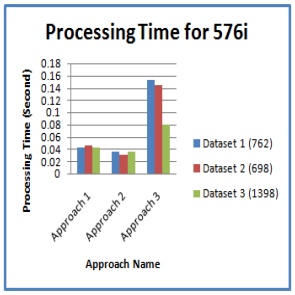


b. Processing Time for FHD

Figure 6. a) FPS and b) Processing Time for FHD

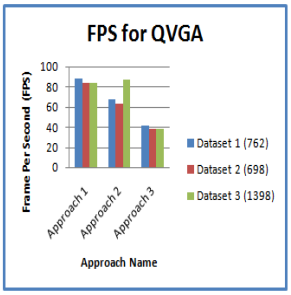


a. FPS for 576i

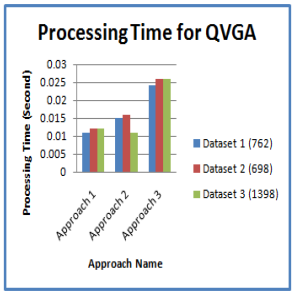


b. Processing Time for 576i

Figure 7. a) FPS and b) Processing Time for 576i



a. FPS for QVGA



b. Processing Time for QVGA

Figure 8. a) FPS and b) Processing Time for QVGA

VI. CONCLUSIONS

The privacy issue is crucial concerns for traffic surveillance. In this paper, we investigate approaches that overcome the problem of detection of region of interest for privacy preservation during traffic surveillance. In addition, it allows reconstructing the original frame for security purposes. From the analysis, our result shows that processing time is real and retains useful information for surveillance. In addition, it can prevent tracking of the person during traffic surveillance. The approaches can be equally applicable for any kind of video surveillance.

REFERENCES

[1] I. Azogu and H. Liu, "Privacy-preserving license plate image processing," *2011 IEEE GLOBECOM Work. GC Wkshps 2011*, pp. 34–39, 2011.

[2] Y. Kim, J. Jo, and S. Shrestha, "A server-based real-time privacy protection scheme against video surveillance by unmanned aerial systems," in *2014 IEEE International Conference on Unmanned Aircraft Systems, ICUAS 2014 - Conference Proceedings*, 2014, pp. 684–691.

[3] F. Dufaux and T. Ebrahimi, "Scrambling for video surveillance with privacy," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2006, 2006.

[4] X. Yu, K. Chinomi, T. Koshimizu, N. Nitta, Y. Ito, and N. Babaguchi, "Privacy protecting visual processing for secure video surveillance," *Proc. - Int. Conf. Image Process. ICIP*, pp. 1672–1675, 2008.

[5] H. S. H. Sohn, E. T. AnzaKu, W. De Neve, Y. M. R. Y. M. Ro, and K. N. Plataniotis, "Privacy Protection in Video Surveillance Systems Using Scalable Video Coding," *2009 Sixth IEEE Int. Conf. Adv. Video Signal Based Surveill.*, pp. 424–429, 2009.

[6] I. Ivasic-Kos, M. ;Iosifidis, A. ; Tefas, A. ; Pitas, "Person De-identification in Activity Videos," in *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on*, 2014, no. 26–30 May, pp. 1294 – 1299.

[7] Xiaochun Cao ;Na Liu ; Ling Du ; Chao Li, "Preserving privacy for video surveillance via visual cryptography," in *Signal and Information Processing (ChinaSIP), 2014 IEEE China Summit & International Conference on*, pp. 607 – 610.

[8] P. Agrawal and P. J. Narayanan, "Person de-identification in videos," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 3, pp. 299–310, 2011.

[9] J. Wickramasuriya, M. Alhazzazi, M. Datt, S. Mehrotra, and N. Venkatasubramanian, "Privacy-protecting video surveillance," in *Electronic Imaging 2005*, 2005, pp. 64–75.

[10] C. Slobogin, *Privacy at risk: The new government surveillance and the Fourth Amendment*. University of Chicago Press, 2008.

[11] A. Cavallaro, "Privacy in Video Surveillance," *IEEE Signal Processing Magazine*, vol. 24, no. 2, pp. 168–169, Mar-2007.

[12] R. N. Fries, M. R. Gahrooei, M. Chowdhury, and A. J. Conway, "Meeting privacy challenges while advancing intelligent transportation systems," *Transportation Research Part C: Emerging Technologies*, vol. 25, Elsevier, pp. 34–45, 2012.

[13] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar, "Efficient privacy preserving video surveillance," *Proc. IEEE Int. Conf. Comput. Vis.*, pp. 1639–1646, 2009.

[14] A. Chattopadhyay and T. E. Boult, "PrivacyCam: A privacy preserving camera using uCLinux on the blackfin DSP," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, 2007.

[15] R. Gross and L. Sweeney, "Towards Real-World Face De-Identification," in *Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007. First IEEE International Conference on*, 2007, pp. 1 – 8.

[16] A. M. Berger, "Privacy mode for acquisition cameras and camcorders," 6,067,399, 2000.

[17] S. Carrillo, P. ; Kalva, H. ; Magliveras, "Compression Independent Object Encryption For Ensuring Privacy In Video Surveillance," in *Multimedia and Expo, 2008 IEEE International Conference on*, 2008, pp. 273–276.

[18] F. Z. Qureshi, "Object-video streams for preserving privacy in video surveillance," *6th IEEE Int. Conf. Adv. Video Signal Based Surveillance, AVSS 2009*, pp. 442–447, 2009.

[19] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*. Prentice Hall, 2007.

[20] G. Prashanth Kumar and M. Shashidhara, "Skin Color Segmentation for Detecting Human Face Region in Image," in *International Conference on Communication and Signal Processing*, 2014, pp. 1–5.

