ABSTRACT
Aiming at the need of personal privacy protection in video surveillance, especially in the traffic surveillance, we discuss in this paper, approaches for preserving privacy for traffic surveillance. We propose three approaches so that the observer can only view a transformed form of surveillance to protect individual privacy. In the first approach, we utilize randomization based techniques using modular arithmetic that first scale the pixel value and then randomize it using prime numbers. Our first approach secure pixel value as well as preserves the privacy of citizens. However the first approach incurs more computational overhead. In our second approach, we use color model theory, i.e. Hue-Saturation-Value (HSV) model to hide person’s facial information to preserve privacy. We show that our second approach is faster than the first approach. However, the second approach is less secure. In the third approach, we apply edge based, i.e. horizontal and vertical edge detection on capture frame to hide person identity. In addition, a third approach is faster than the other two approaches and thus it can be very useful for real time traffic surveillance.

Categories and Subject Descriptors
K.4.1 [Computers And Society]:
Public Policy Issues

General Terms
Security

Keywords
Privacy, Edge Detection, HSV (Hue, Saturation, Value)

1. INTRODUCTION
Traffic surveillance is used towards improving transportation efficiency, reducing the congestion on roads and promoting highway safety. Traveler information systems such as www.masstraveler.com, www.mass511.com and www/english.webcam-bruecken.de provide various aspects of traffic information [1]. Such websites, broadcast real-time views from cameras showing traffic flows, or traffic jams. It makes possible the tracking of travelers along roads and highways throughout. The observer can connect that location with other records, such as where that person has been in the past. The observer can use these records for the prediction of people’s future movements and locations. These may cause problems like watching your travelling habits or activity with specific places (where) and time (when) or with other personal (with whom). Privacy preserving traffic surveillance addresses these privacy breaches.

Surveillance should be done in a such a way that the frames captured by cameras (figure 1.a) should be obfuscated, and results seen by traffic observer are only the transformed results (figure 1.b), i.e. the observer can only see the presence of vehicles and can only detect the presence of the driver of the vehicles or pedestrian on the road. The identity of the driver or pedestrian on the road should not be revealed. This result also can be recovered or reconstruct in original form as and when required for security purposes. Therefore, the transformation should be lossless.

2. PROPOSED APPROACHES
The basic flow of our three proposed approaches is as shown in figure 2. At the beginning, video capture by surveillance camera are sent to the computational server at which frames from the video are extracted. Then transformation is applied to each frame. These transformed frames are sent to the observer via secure channel. Here the observer may be any traffic rule regularity officer or any citizen who can use traffic website as mentioned in section 1.

Figure 1. Privacy preserving Traffic surveillance

Figure 2. Flow Diagram of proposed approaches

Approach 1: Scaling and Randomization
In [2], an efficient Privacy Preserving video surveillance technique using Secret sharing (SS) methods has been proposed. In the SS method, it splits any data into multiple shares (at different server) such that no share by itself has any useful information, but together, they retain all the information of the original data. However, In our approach we use scaling and randomization of each pixel, use in [2] and we eliminate separate server computation, i.e. the computation of pixel value (share) at different server, for traffic surveillance. In our approach, we do scaling and randomization of each pixel value by using the following equation at computational server,

\[ NP = (P * S) \mod K \]

Here,
- \( P \) = Original Pixel Value
- \( S \) = Scaling Factor,
- \( K \) = Prime Number, \( K > 255 \)
- \( NP \) = New Pixel Value
Every scaled value can be randomized in the range of 0 to K-1. If K<255 then NP value will be in the range of 0 to K-1. However the value of pixel value is in the range of 0-255. So if K<255 then for some pixel value which is greater than K could not be recovered by using finite field multiplicative inverse method for reconstruction of pixels. So the value of K should be greater than 255. In addition, if the value of the NP is greater than 255, then NP value might be greater than 255. This can be adjusted by using modular arithmetic operation. Here frame with NP values are sent to the observer. Results of approach 1 are as shown in figure 3.

![Figure 3. Results of approach 1](image)

This approach is more secure from attacker to reconstruct the original frame from the transformed one. However, for such computation, it requires more time for processing.

Approach 2: Edge Based approach

In this approach, we first apply horizontal edge and then 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]' [3]. 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

![Figure 4. Results of approach 2](image)

In addition Edge detection method (approach 2) is faster than approach 1. The results of approach 2 are as shown in figure 4. It incurs less computational overhead. This approach is faster for real time surveillance.

Approach 3: Using HSV color model theory

In HSV (Hue, Saturation, Value), Hue shows how much pure color in a digital image [3]. Saturation refers to the relative purity or an amount of white light mixed with a hue. The Degree of saturation is inversely proportional to the amount of white light added [3]. Value is the lightness or darkness of a color [3]. In our approach, we first convert RGB (Red, Green, and Blue) to HSV component of each frame. As saturation (S) only highlight intensity, it does not disclose any identity. So it is useful for preserving privacy. So after separating H, S, and V component, only the S component of each frame is sent to the observer. The results of this approach are as shown in figure 5.

![Figure 5. Results of approach 3](image)

3. Results

In our ongoing research, we consider processing time for each frame to convert into privacy preserving frame for various traffic datasets. Table 1 shows the processing time of our proposed approaches. Here for three proposed approaches, we consider three different Datasets: Dataset 1 (762 frames), Dataset 2 (698 frames) and Dataset 3 (1398 frames).

<table>
<thead>
<tr>
<th>Approach</th>
<th>Number of Frames</th>
<th>Average frame processing time (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scaling &amp; Randomization (Approach 1)</td>
<td>762</td>
<td>2.82</td>
</tr>
<tr>
<td></td>
<td>698</td>
<td>6.87</td>
</tr>
<tr>
<td></td>
<td>1398</td>
<td>2.69</td>
</tr>
<tr>
<td>Edge detection Based (Approach 2)</td>
<td>762</td>
<td>0.28</td>
</tr>
<tr>
<td></td>
<td>698</td>
<td>0.55</td>
</tr>
<tr>
<td></td>
<td>1398</td>
<td>0.24</td>
</tr>
<tr>
<td>RGB to HSV (Approach 3)</td>
<td>762</td>
<td>0.29</td>
</tr>
<tr>
<td></td>
<td>698</td>
<td>0.57</td>
</tr>
<tr>
<td></td>
<td>1398</td>
<td>0.32</td>
</tr>
</tbody>
</table>

The efficiency of first approach can be further improved by using parallelism for computation on each individual pixel.

4. Conclusion

We discussed various privacy preserving approaches which can prevent tracking of the person during traffic surveillance. Here we proposed three approaches which may be very useful for real time traffic surveillance at the same time preserve privacy of individuals.

5. References