International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 5, No.5 (Sep. 2016)

http://dx.doi.org/10.12785/ijcds/050501

Towards Privacy-Preserving Driver's Drowsiness and Distraction Detection: A Differential Privacy Approach

Mahmoud Raafat[1], Bassem Abdullah[2], Mohamed Taher[2] and Mohamed N. Moustafa[2, 3]

[1]Mentor Graphics Corporation, Cairo, Egypt
[2]Department of Computer & Systems Engineering, Ain Shams University, Cairo, Egypt
[3]American University in Cairo, Computer Science and Engineering, Cairo, Egypt

Received 28 Apr. 2016, Revised 31 May 2016, Accepted 3 Jul. 2016, Published 1 Sep. 2016

Abstract: The ubiquitous need for detecting driver's drowsiness and distraction by using a camera mounted inside the car directed to driver's face is driving significant concern about protecting driver's identity from being discovered or exploited by hackers. In this paper, we present a novel technique called block Laplacian Obfuscation Mechanism (bLOM), to privatize the camera data stream by using differential privacy techniques introduced in database domain. We introduce a metric to measure privacy and utility for driver's drowsiness and distraction algorithms. Our experimental results show that in 87% of test cases, bLOM is able to keep the identity of the driver private while still be able to extract facial features needed for driver's drowsiness and distraction detection.

Keywords: differential privacy, face recognition, face features, driver drowiness, driver distraction, Laplace mechanism

1. INTRODUCTION

Traffic accidents occur due to many reasons. Two of the main causes of traffic accidents are driver drowsiness and distraction. According to the latest National Motor Vehicle Crash Causation Survey (NMVCCS) conducted by The U.S. National Highway Traffic Safety Administration (NHTSA), approximately 41% of crashes (more than 800,000 accidents occurred during 5 years) were due to recognition errors made by the driver i.e. due to driver's drowsiness and distraction [1].

Several detection techniques have been proposed in the literature during the last decade for detection of both driver drowsiness and distraction. Many car Original Equipment Manufacturers (OEMs) have already implemented some of these techniques in their production cars. For example, Lexus LS 600h Driver Monitoring System, which was presented in 2006, uses a camera mounted on the top of the steering column cover and a series of integrated near-infra-red LEDs to track the movement of the driver's head. If it determines the driver is looking away from the road ahead at the same time as a collision threat is detected, the system will sound an alert and briefly apply the brakes. [2]. Volvo presented a driver drowsiness detection system in 2007. By placing a sensor on the dashboard to monitor aspects such as in which direction the driver is looking, how open their eyes are, as well as their head position and angle, it is possible to develop precise safety systems that detect the driver's state and are able to adjust the care accordingly [3].

Driver's drowsiness and distraction can be detected using several techniques which are categorized as follows [4]:

- Techniques based on visual features.
- Techniques based on non-visual features.

Most of the techniques based on visual features depend primarily on the successful detection of driver's eyes, mouth or both.

To detect whether the driver is distracted or not, most of proposed algorithms achieve that by detecting driver's head pose and gaze estimation [4]. Detection of driver's face, eyes, and nose plays a big role in determining the gaze direction [5].

On the other hand, there have been trends in automotive industry in the recent years towards interconnecting between Electronic Control Units (ECUs) inside the car using wired buses like (CAN, FlexRay, Ethernet, AVB, …) and between the ECUs and the outside world using wired (USB) or wireless (Bluetooth, Wi-Fi, 3G/4G …) communication protocols.

Email: mahmoud_raafat@mentor.com, babdullah@eng.asu.edu.eg, mohamed.taher@eng.asu.edu.eg, moustafa@ieee.org

These trends will keep increasing in the future with the rapid development of In Vehicle Infotainment (IVI) and Vehicle-to-Vehicle communication (V2V) domains.

Therefore, we can no longer consider any ECU inside a car to be isolated from its neighbor ECUs and so, not completely isolated from the outside world. This opened the door for attackers to find and exploit vulnerabilities in car communication interfaces and gain access to the embedded networks inside the car [6]. Gaining access to the embedded networks inside the car allows the attacker to send and receive any type of data being exchanged between the ECUs. Moreover, the attacker might be able to update ECUs flash memories with their own malicious code. One of the main goals of these attacks is achieving privacy breach, retrieving personal information and sensitive data of the driver [7] [8]. One of the most sensitive data is the feed from sensors and stream from cameras used to detect driver's drowsiness and distraction. Gaining access to this data may allow the attacker to recognize driver's identity and puts driver's privacy at risk.

Most of the presented protection techniques against driver's privacy attacks in the literature focus on providing protection methods over communication protocols. Nader et al. [9] presented an approach to provide privacy among drivers in V2V communication networks, based on the concept of group signatures. Other researchers like Zekeriya Erkin et al. [10] proposed a cryptographic privacy-preserving face recognition technique. They provided a solution to a two-party problem in which one party owns a face image and the other party owns a database of the face images and runs the matching algorithm. Their technique allows to efficiently hide both the biometrics and the result from the second party (which is the server) that performs the matching operation.

Most of car Manufacturers and tier-1 suppliers nowadays focus on isolation of sensitive and safety critical data from the compromised software and hardware components of infotainment and telematics systems by means of hardware isolation using multi-core processors and software isolation using hypervisors.

In this paper, we present a novel approach to protect driver's private data used in driver drowsiness and distraction detection techniques based on visual features by applying one of the differential privacy techniques. The general idea is to apply the Laplacian obfuscation method to certain frequency components of camera data streams in order to privatize the data before being processed afterwards. This method shall maintain the utility of the drowsiness and distraction detection algorithms by maintain the ability to extract driver's head, eye, nose, and mouth features while preserving driver's identity i.e. making it less likely for face recognition algorithms to succeed in recognizing driver's identity from the privatized data stream.

A. Related Work

Differential privacy is considered a cryptographically motivated definition of privacy that has gained significant attention during the last few years. The first notion of differential privacy was introduced by Dwork [11] in 2006. The goal was to allow a user dealing with statistical databases to retrieve useful information about a population while protecting the privacy of the individuals in the population.

Researches based on the concepts and techniques proposed by Dwork and started to extend them in other domains other than statistical databases. Zhanglong Ji et al. [12] studied how to achieve differentially private machine learning algorithms. Jerome Le Ny, et al. [13] proposed differentially private filtering methods. First, they extended the notion of differential privacy to dynamic systems then they described differentially private mechanisms to approximate stable filters.

Benjamin, et al [14] proposed a support vector machine (SVM) classifier that preserves the privacy of the training data. First, they proposed two mechanisms for differentially private SVM learning, one for learning under finite-dimensional feature mappings, and one for learning with potentially infinite-dimensional feature mappings. Both mechanisms operate by adding perturbation to the output classifier; for each they proved the range of perturbation parameters required in order to guarantee privacy, and they derived the conditions under which the mechanisms yield close approximations to the non-private SVM. Then, they defined a notion of optimal differential privacy as the best privacy achievable among all mechanisms that approximate a non-private SVM. They combined the results on privacy and utility of their mechanisms in order to derive upper bounds on the optimal differential privacy, which states that the level of privacy achieved will be at least as good as the upper bound.

S. Han et al. [15] developed a distributed electric vehicle charging algorithm that preserves differential privacy using Laplace mechanism by perturbation of public signals with Laplace obfuscation whose magnitude is determined by the sensitivity of the public signal with respect to changes in user information.

The literature has widely spread to develop differentially private data processing algorithms such as real-time signal processing [16], classification [17], and dimensionality reduction [18].

Sarwate et al. [19] illustrated the generic methods used for differential privacy. Supposing we have a dataset D and we have an algorithm A that simply computes a function f(D) of the data, and we would like to make it differentially private by adding random obfuscation. They described four key approaches to achieve that:

- Input Perturbation: Adding obfuscation to the data itself before computing the function *f(D)*.
- Output Perturbation: Applying obfuscation to the output of the function. The amount of noise needed to be added will depend on the sensitivity of the function f to the changes in its input.
- Exponential Mechanism: This mechanism is designed for cases where applying obfuscation directly to the output can completely destroy its value i.e. destroy the utility. Given an arbitrary range *R*, the exponential mechanism can be defined with respect to a utility function *u* which maps dataset *D* or output pairs to utility scores. [19]
- Objective Perturbation: This approach can be used when dealing with classifiers suing regular convex optimization. Applying obfuscation to the objective function of the optimization problem shall obtain a differentially private approximation.

2. BACKGROUND

A. Differential privacy

In this section, we review the preliminaries and basic definitions of the notion of the differential privacy.

To understand how differential privacy in statistical works let's consider two databases D and D' that contain the exact same rows except for one entry. In that case, we call these two databases adjacent.

Definition 1 (Adjacent databases). Two databases $D = \{d_i\}_{i=1}^{n}$ and $D' = \{d'_i\}_{i=1}^{n}$ are said to be adjacent if there exists $i \in \{1, \dots, n\}$ such that $d_i = d_j$ for all $i \neq j$.

For simplicity, let us assume D is a database that contains medical records of a population in a city, and D' is the same database as D but after adding a new person which has moved recently to the city. According to Definition 1, D and D' are adjacent.

Now, consider an adversary which have the capability of running multiple queries on the databases D and D'. These queries retrieve the percentage of population that have cancer. Although this type of queries asks only for statistics defined over the full population, it leaks sensitive information about individuals as well. For example, if an adversary runs a query before and after a person moves in the city, she can determine whether that person has cancer or not by simply differencing the outputs of the two queries. This attack is known in cryptography literature as the "Differencing Attack".

Differential privacy aims to provide formal setup to analyze and design countermeasure mechanisms which guarantee that the outcome of any analysis or query on a database is essentially equally likely, independent of whether any individual joins, or refrains from joining the database.

Definition 2 (ε-Differential privacy): Consider a dataset K that contains a set of adjacent databases. For all adjacent databases D and D' in K , a mechanism M preservers ε -Differential Privacy for all $\mathcal{R} \subseteq range(M)$ if it holds that:

$$Pr(M(D) \in R) \leq e^{\varepsilon} Pr(M(D') \in R).$$

The parameter ε indicates the level of privacy preserved: as ε gets smaller a higher level of privacy is preserved.

B. Laplace Mechanism

While many mechanisms have been proposed that achieve differential privacy, the Laplace mechanism is one of the most widely used mechanisms to achieve ε-differential privacy as it is asymptotically optimal when $\varepsilon \to 0$ [20][21][22][23].

Laplace mechanism corrupts the public data by adding random variables drawn from Laplacian distribution as in [13], or by adding random variables to the output of a function operating on database as in [20][21]. Dwork in [11] proved mathematically that in order to guarantee ε-differential privacy by Laplace mechanism, random variables added to the output of a function f shall be drawn from the Laplacian distribution $Lap(\frac{\Delta_f}{\varepsilon})$, where Δ_f is the global sensitivity of function f.

Definition 3 (Global sensitivity): For any query $f: \mathcal{D} \to \mathcal{R}^m$, the global sensitivity of f is defined as follows:

$$\Delta_f = \max\{\|q(D) - q(D')\| : D, D' \epsilon \mathcal{D} \ s.t. \ Adj(D, D')\}.$$

Where $Adj(D, D')$ denotes that the adjacency relation between D and D' is satisfied.

To illustrate Laplace mechanism, consider a database that contain information about a population of a city and consider a query that can retrieve the number of females inside that population. Assume that the gender information about a person inside the population is sensitive information and we would like to privatize this information using Laplace mechanism. First, we need to

calculate the global sensitivity of the query. The maximum difference can occur between two query results of two adjacent databases in that case is equal to one, e.g. a female joins or refrains from the population. Applying obfuscation to query output with Laplacian distribution $Lap(\frac{1}{\varepsilon})$ shall guarantee ε-differential privacy for gender information.

3. DIFFERENTIALLY PRIVATE IMAGES

A. Preliminaries

While the notion of differential privacy was originally defined for databases, the definitions do not cover directly computer vision and image processing domain under consideration. For that end, we start this section by generalizing the notion of differential privacy to be suitable to image processing problems. Next, we show a novel mechanism to produce differentially private images that is still can be used to perform driver drowsiness detection.

As with many image processing algorithms, it is useful to consider the frequency representation of an image. Consider an image IMG, and an integer N, we can define the frequency representation of the image as obtained by the well-known Fast Fourier Transform (FFT) as follows:

$$I = FFT(IMG, N) = \{f(i,j)\}_{i=1,j=1}^{i=2^N, j=2^N}$$

The parameter N controls the size of the produced 2-dimensional frequency representation of the image $f(i,j)$ where the indecies i and j take values in the set $\{1, \dots, 2^N\}$. An example of an image and its frequency representation after applying FFT is shown in Figure 1.

Figure 1. Face image and its corresponding frequency components

Now, using the notation we define the adjacency of two images in a manner which is inspired by the original database adjacency as follows:

Definition 4 (Adjacent images)
Two images $I = \{f(i,j)\}$ and $I' = \{f'(i,j)\}$ are said to be adjacent if there exists a frequency component $f(i,j)$, $(i,j) \in \{1,\dots,2^N\} \times \{1,\dots,2^N\}$ such that $f'(i,j) = f(i',j') \; \forall \; (i,j) \neq (i',j')$.

In other words, the previous definition considers the frequency components of an image as the entries of a database. Two adjacent images are then those who differ on only one frequency component.

The previous definition is very restrictive in the sense that it allows for only one frequency component to differ between adjacent images. We relax the previous definition by considering "blocks" of frequency components. That is, let $b \in \{1,\dots,2^N\}$ denote the number of frequency blocks, by grouping $\frac{2^N}{b}$ frequency components together we end up by an image that has $b \times b$ frequency component groups as shown in Figure 2.

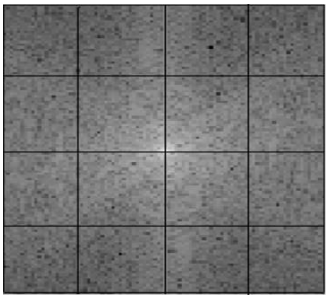

Figure 2. Frequency components grouped into 16 groups

Therefore, it is convenient to introduce the block notation of an image as $I_b = FFT(IMG, N) = f(i,j)_{i=1,j=1}^{b}$ for which we can use to introduce the notion of "block adjacency" of images as follows:

Definition 5 (Block adjacent images). Two images $I_b = FFT(Img, N) \; and \; I'_b = FFT(Img', N)$ are said to be adjacent if there exists a frequency block $(i,j) \in \{1,\dots,b\} \times \{1,\dots,b\} \; such \; that \; f(i',j') = f'(i',j') \; for \; all \; (i,j) \neq (i',j')$.

Unlike the previous definition, two images are considered adjacent if they differ on a block of frequency components of size b. Indeed when $b = 1$, the notion block adjacency boils down to the original image adjacency.

Definition 6 (ε-Block Differential Privacy in image processing). Consider a dataset $\mathcal{D}$ that contains a set of block adjacent images. For all block adjacent images I and I' in $\mathcal{D}$, a mechanism M preserves ε-block differential privacy for all outputs R of the mechanism M holds that:

$$P(M(I) \cong R) \leq e^{\varepsilon} P(M(I') \cong R).$$

The parameter ε indicates the level of privacy preserved: as ε gets smaller a higher level of privacy is preserved. The notion of differential privacy aims to make

an adversary cannot tell from the output of $M(I)$ with high probability that a specific face image I corresponds to which person in dataset.

B. The bLOM Algorithm and the utility-privacy tradeoff

In this paper, we propose a mechanism that is based on the input perturbation approach presented in [14] and the Laplace mechanism in order to achieve ε-block differential privacy for face images. The idea of bLOM (block Laplacian Obfuscation Mechanism) mechanism is to apply Laplacian obfuscation mechanism to the blocks of spatial frequency components of face images in order to privatize the data, i.e. to increase the probability that face recognition algorithms will fail to recognize faces belong to which persons face.

There is always a trade-off between privacy and utility [24]. A perfect privacy preserving mechanism for face images might be applying a strong obfuscation technique to a face image that destroys all the face features inside the image. This mechanism will hide the identity of the person perfectly but it will come with a cost that all the useful information inside the image is lost. On the other hand, a poor privacy preserving mechanism may add, for instance, salt-and-pepper noise to a face image that will preserve all the face features inside the image. This mechanism will maintain high level of utility of the data but it is not efficient in preserving the privacy because face recognition techniques will be able to recognize the face in the image after applying a simple Gaussian filter to the image.

C. Analysing face images in the frequency domain

We need to analyze the role of low, mid, and high frequency components in the spatial frequency domain of a face image in order to determine which components or frequency band(s) we will choose to apply obfuscation to. The goal is to maximize the probability of successful detection face features while minimizing the probability of recognizing the identity of the person the face belongs to. Maheshkar et al. already did this analysis in [25]. They presented the following information: Low spatial frequency components of a face image are related to illumination variation and smooth regions like cheeks and forehead of the face which are not important face features to be detected. On the other hand, high spatial frequency components represent detailed information of edge which are so crucial for detecting face features. The middle spatial frequency components represent primarily the basic structures of the face.

The analysis done by Matthias, et al. [26] shows that the most critical spatial frequency band that face recognition algorithms depend on is the mid band, between 8 and 16 cycles per face. They presented results of discriminability measures by computing Fisher Linear Discriminant Analysis, Non-Parametric-Discriminant-Analysis and Mutual Information as a function of spatial frequency. Class discriminability peaked at 16 cycles per face width.

Based on the previous analysis, we can state the following:

Applying obfuscation to low special frequency band will not be a good approach to privatize data.

Applying obfuscation to the high spatial frequency band will not be also a very good approach, as this will corrupt the edge details needed to detect face features and will lead to low utility.

Applying obfuscation to the mid spatial frequency band of a face image will be the best approach to maximize the indistinguishably of a person's identity and minimize the cost of losing useful information i.e. detection of face features at the same time.

D. Global Sensititvy

Sensitivity of spatial frequency components is an essential information for the BLOM algorithm so that we can determine how much obfuscation is needed to be applied to an image in order to preserve privacy. We calculate global sensitivity for each spatial frequency component by constructing a sensitivity matrix. The sensitivity matrix is a matrix that contains global sensitivity value for each spatial frequency component computed for all images in the dataset. The global sensitivity value Δ_f for each component is the difference between the maximum value and minimum value of this component for all images in the dataset. High sensitivity value for a frequency component indicates that the value of the frequency component can vary greatly across the dataset, and vice versa in case of low sensitivity. This information is taken as one of the factors in determining how much noise is added to each frequency component of an image that we want to apply obfuscation to. A simple algorithm to calculate the sensitivity matrix across a dataset of images is illustrated as follows:

***Algorithm* 1:** *Calculating sensitivity matrix for individual frequency components.*

For each image i in the dataset D **then**
    F[x][y][i] = FFT(D[x][y][i])
END For
For each frequency component f with position (x, y) in F **then**
    Sensitivity[x][y] = ||(max((F[x][y]) – min(F[x][y])|| ; where F[x][y] is an array of value frequency component with position (x,y) over all the dataset D
End For
Output Sensitivity

In case we group the frequency components of an image into blocks, we need to modify the previous algorithm to compute the sensitivity matrix Δ_b for each block of frequencies instead of computing for each frequency individually. The modified algorithm is illustrated as follows:

***Algorithm* 2:** *Calculating sensitivity matrix for blocks of frequencies*

For each image i in the dataset D **then**
F[x][y][i] = FFT(D[x][y][i])
END For
For each frequency component f with position (x, y) in F **then**
Sensitivity_f[x][y] = ||(max((F[x][y]) – min(F[x][y])|| ; where F[x][y] is an array of value frequency component with position (x,y) over all the dataset D
End For
For each block b of frequency components
For each frequency component with position (x,y) inside b **then**
Sensitivity_bf[x][y] = Sensitivity_f[x][y]
End For
Sensitivity_b[b] = mean(Sensitivity_bf)
End For
Output Sensitivity_b

E. Block Obfuscation

To privatize an image, for each block of frequency components we add random variables with the same Laplace distribution to frequency components inside that block. If block size is equal to one, this means we will add random variable to each frequency component with a distinct Laplace distribution. Random variable added to each spatial frequency component depends on the global sensitivity of the block this component belongs to Δ_b and the parameter ε, which determines the desired level of privacy. The algorithm of privatizing an image is illustrated as follows:

***Algorithm* 3:** *Applying Laplacian Obfuscation to an image*

For each block b of spatial frequencies of an image **then**
For each component f inside block b **then**
r = Laplace (Δ_b /ε)
f = f + r
END For
END For

4. EXPERIMENTAL RESULTS

In this section, we evaluate the performance of the proposed bLOM algorithm. As we are the first to apply differential privacy techniques to image processing domains, there are no previous performance results to use them for comparison. We first develop metrics to measure utility and privacy performance specific to our case, and then we study the utility-privacy trade-off using extensive numerical experiments. We show that applying the bLOM algorithm to the mid-band spatial frequencies leads to achieving privacy and utility in more than 87% of images while applying the bLOM algorithm to the low and high-band spatial frequencies only achieved privacy and utility in 72%, and 65% of images.

A. Dataset

We used in our experiments face images from "The ORL Database of Faces" [27], which is a widely used database for testing face detection and recognition performance. It contains a set of face images that was taken April 1992 and April 1994 at AT&T Laboratories in Cambridge. The images were taken at different times varying facial expressions and details for 40 persons with different ages (, each one has 10 images giving a total of 400 images.

All images have the same specifications; 92x112 pixels and 256 grey level per pixel.

First, we defined the utility and privacy measures we will be using during the experiment.

B. Privacy and Utility metrics

Various definitions of privacy and utility metrics have been proposed in research literature of statistical databases. When we apply differential privacy techniques to new domain as in our case, we need to define new metrics for measuring privacy and utility specific for these domains. We used the performance of face features detection as a metric for utility and the performance of face recognition as the metric for distinguishability which in indicates the level of privacy achieved. Cascade object detectors in Matlab® were utilized to detect eyes and mouth inside a face image based on Viola-Jones algorithm. The success of extracting eyes and mouth features from a face image is the utility measure needed for drowsiness and distraction detection.

To measure privacy, we used a very common technique in face recognition, which is Principle Component Analysis (PCA). We used the PCA to generate eignfaces for each 40 person in the dataset. For classification, we used Euclidian distance to find the closest neighbor. We defined the privacy measure in this case as failing to correctly recognize a person i.e. failure in classification of a face image in the dataset.

C. Experiment 1: Utility-Privacy tradeoff.

The goal of this experiment is determining the value of ε that will achieve maximum percentage of utility and privacy measures. First, we computed the sensitivity matrix for the dataset using the algorithm described previously. Figure 3 shows the sensitivity matrix computed for all the frequency components over the dataset. Note that we used fftshift function in Matlab to shift the zero frequency component to the center of the matrix. The sensitivity matrix is computed only one time at the beginning of the experiment, and then saved to be used later in the experiment during applying Laplacian obfuscation for each frequency component.

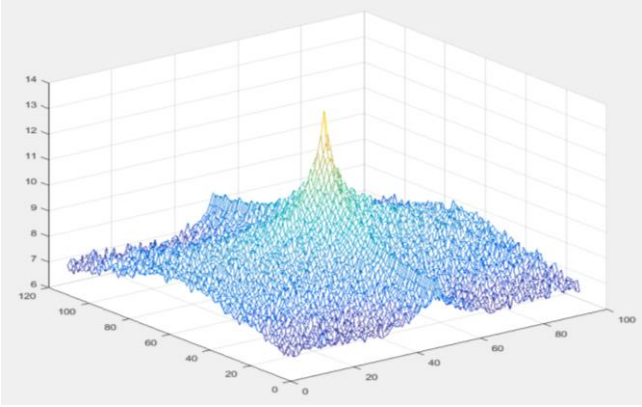

Figure 3. Sensitivity matrix

Then, we generated eignfaces from the 10 images of the 40 persons in the dataset using PCA algorithm. After that, we started with an arbitrary value of ε and then looped for each image in the dataset and applied Laplacian obfuscation with random distribution = Laplace $(\frac{\Delta_f}{\varepsilon})$ to the low, mid, and high blocks of spatial frequency components of the image and then computed the utility and privacy measures for the corrupted image. After computing utility and privacy measures for all images in the dataset, we calculated the percentage of privacy and utility achieved across the entire database under the value of ε and repeated this calculation for multiple values of ε. The results in Fig 4 show that as ε decreases privacy increase and utility decreases. This is because decreasing ε means that more noise is added which increases privacy and decreases utility. We noticed that the maximum percentage of utility and privacy (82%) was achieved after applying Laplacian obfuscation to mid-band frequency components which emphasizes what we have deduced in the previous section as the maximum percentage of images achieving both utility and privacy only reached 72% in case of low-band frequency components and 65% in case of high-band frequency components.

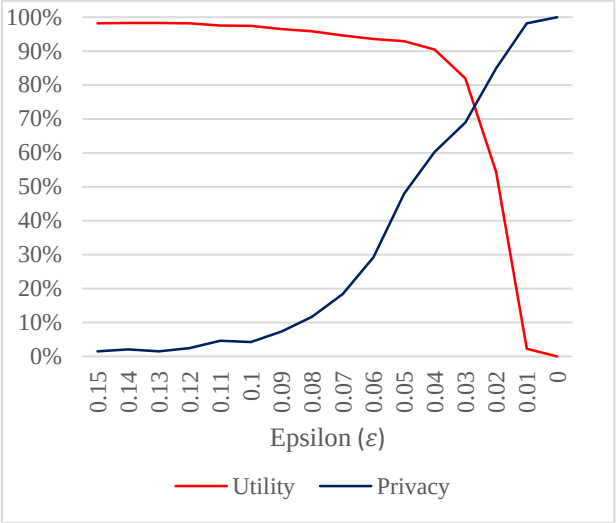

Figure 4. (a) Utility vs privacy graph when obfuscation is applied to low-band frequency components.

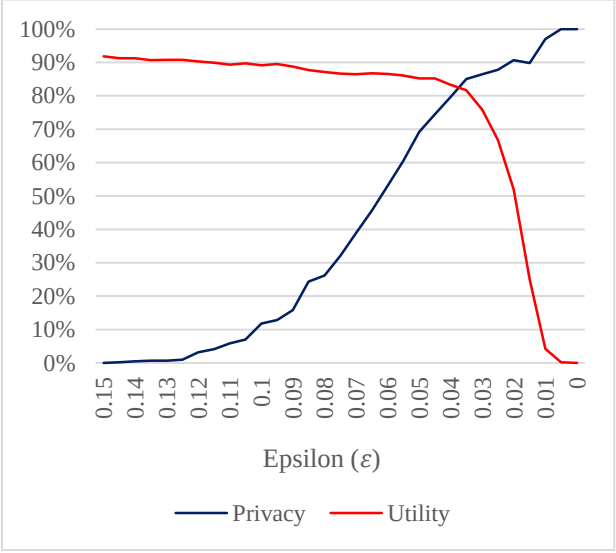

Figure 4. (b) Utility vs privacy graph when obfuscation is applied to mid-band frequency components.

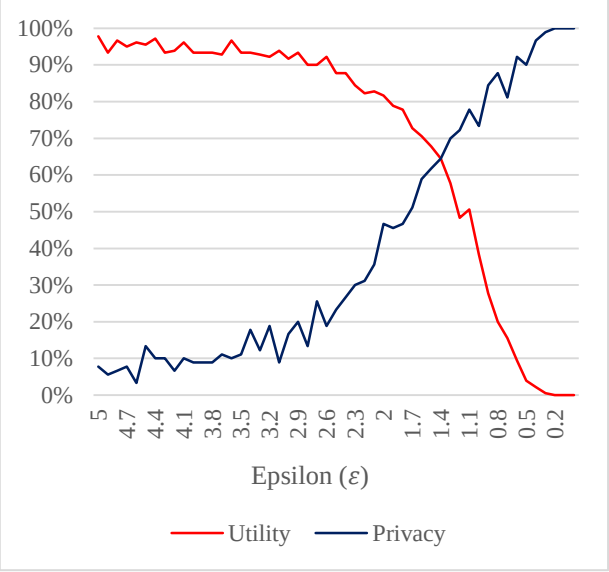

Figure 4. (c) Utility vs privacy graph when obfuscation is applied to high-band frequency components.

D. *Experiment 2: Effect of block size*

Having noted from the previous experiment that the maximum percentage of privacy and utility achieved after applying obfuscation to mid-band frequency components, moved on to analyze the effect of the block size on the output of bLOM algorithm.

In this experiment, we repeated the same steps done in experiment 1 for mid-band frequency components but we varied the block size used in bLOM algorithm.

We calculated the block sensitivity matrix and applied Laplacian obfuscation with random distribution = Laplace ($\frac{\Delta_b}{\varepsilon}$) to each block of frequency components in the mid-band. We noticed that increasing the block size starting with block size equal to one has led to better performance of bLOM algorithm, which reached 87% of privacy and utility with block size between five and ten as shown in Figure 5(a). After that point, the performance of the algorithm started decreasing as the block size increases. The percentage of utility and privacy for example reached a maximum of 70% when the block size was equal to twenty as shown in Figure. 5(b).

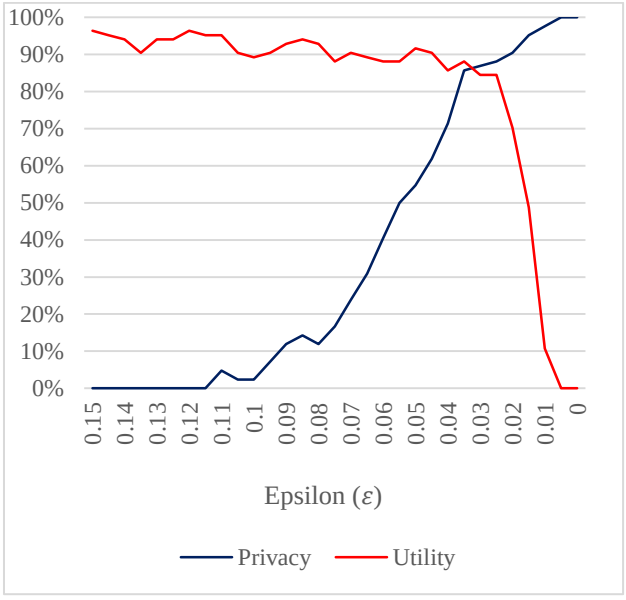

Figure 5. (a) Utility vs privacy graph when obfuscation is applied to mid-band frequency components with block size = 10.

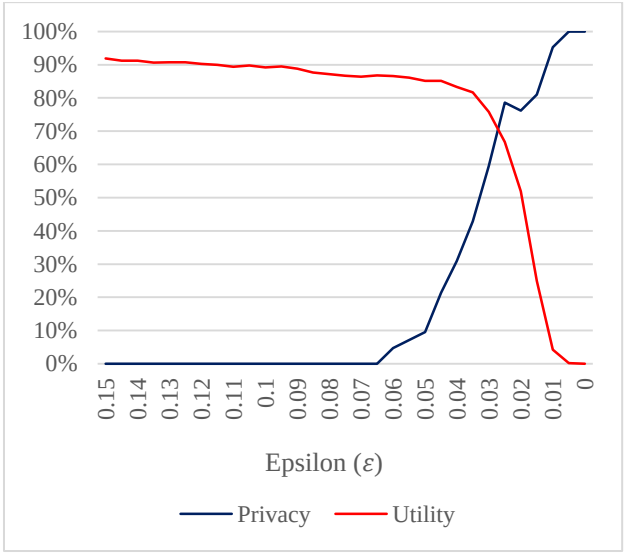

Figure 5. (b) Utility vs privacy graph when obfuscation is applied to mid-band frequency components with block size = 20.

E. *Experiment 3: End-to-End Evaluation.*

In this experiment, we performed end-to-end evaluation of the bLOM algorithm we propose. We demonstrated how applying bLOM algorithm to a face image can preserve the privacy of the person and maintain the utility of the useful information in the image at the same time. As shown in Figure 6, before applying Laplacian obfuscation, the identity of the person was recognized successfully and all his face features were extracted (face, eyes, nose, mouth). After applying

Laplacian obfuscation to the image, facial recognition algorithm has failed and as it identified a wrong person, which means that person's identity was preserved while all face features were extracted successfully indicating that that utility remained unaffected after applying Laplacian obfuscation.

Figure 6. (a) Face recognition before adding noise.

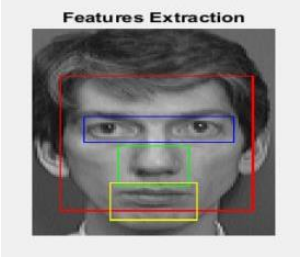

Figure 6. (b) Face Features detection before adding noise.

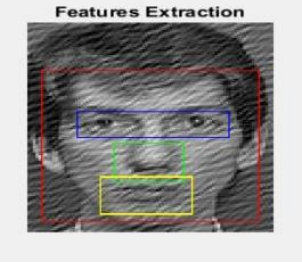

Figure 6. (c) Face Features detection after adding noise.

Figure 6. (d) Face recognition after adding noise.

5. CONCLUSION

In this paper, we presented a novel approach to make computer vision and image processing algorithms differentially private. We proposed the bLOM algorithm , which is differential privacy technique in which we apply Laplacian obfuscation to images in order to privatize them. We showed experimentally that applying obfuscation to the camera data stream after tuning Laplace distribution parameters lead to preserving the identity of the driver in 87% of test cases, while also maintaining the ability to extract driver's eye, and mouth features, which are the building blocks for driver's drowsiness and distraction detection.

REFERENCES

[1] National Highway Traffic Safety Administration. (2015). Fatality Analysis Reporting System Encyclopedia. [Online]. Available: http:// www-fars.nhtsa.dot.gov/

[2] www.testdriven.co.uk/lexus-ls-600h/

[3] https://www.media.volvocars.com/

[4] S. Kaplan, M. A. Guvensan, A. G. Yavuz and Y. Karalurt, "Driver Behavior Analysis for Safe Driving: A Survey," in IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 3017-3032, Dec. 2015.

[5] S. Langton, H. Honeyman, and E. Tessler, "The influence of head contour and nose angle on the perception of eye-gaze direction," Perception Psychophys., vol. 66, no. 5, pp. 752–771, Jul. 2004

[6] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on, Budapest, 2013, pp. 1-12.

[7] K. Koscher, A. Czeskis,F. Roesner,S . Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, and H. Shacham, "Experimental security analysis of a modem automobile," in 2010 IEEE Symp. Security and Privacy, Oakland, CA, 2010, pp. 447-462.

[8] R. Brooks,S . Sander,J . Deng,a nd 1. Taiber," Antomobile security concerns;' IEEE Veh. Technol. Mag., vol. 4, no. 2, pp. 52-M, 2009.

[9] N. M. Rabadi and S. M. Mahmud, "Privacy Protection Among Drivers in Vehicle-to-Vehicle Communication Networks," 2007 4th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 2007, pp. 281-286.

[10] Cynthia Dwork, "Differential Privacy" http://research.microsoft.com/pubs/64346/dwork.pdf.

[11] Ji, Z., Lipton, Z.C., Elkan, C.: Differential privacy and machine learning: a survey and review (2014). arXiv preprint arXiv:1412.7584

[12] J. Le Ny and G. J. Pappas, "Differentially Private Filtering," in IEEE Transactions on Automatic Control, vol. 59, no. 2, pp. 341-354, Feb. 2014.

[13] S. Han, U. Topcu and G. J. Pappas, "Differentially private distributed protocol for electric vehicle charging," Communication, Control, and Computing (Allerton), 2014 52nd Annual Allerton Conference on, Monticello, IL, 2014, pp. 242-249.

[14] Erkin, Zekeriya, et al. "Privacy-preserving face recognition." Privacy Enhancing Technologies. Springer Berlin Heidelberg, 2009.

[15] A. D. Sarwate and K. Chaudhuri, "Signal Processing and Machine Learning with Differential Privacy: Algorithms and Challenges for Continuous Data," in IEEE Signal Processing Magazine, vol. 30, no. 5, pp. 86-94, Sept. 2013.

[16] L. Fan and L. Xiong. Real-time aggregate monitoring with differential privacy. presented at 21st ACM Int. Conf. Information and Knowledge Management (CIKM '12).

[17] K. Chaudhuri, C. Monteleoni, and A. D. Sarwate. (2011, Mar.). Differentially private empirical risk minimization. J. Mach. Learn. Res. [Online]. 12, pp. 1069–1109.

[18] M. Hardt, K. Ligett, and F. McSherry. (2012). Advances in Neural Information Processing Systems 25.

[19] Dwork, Cynthia, and Aaron Roth. "The algorithmic foundations of differential privacy." Foundations and Trends in Theoretical Computer Science 9.3-4 (2014): 211-407.

[20] S. Costea and N. Tapus, "Input Validation for the Laplace Differential Privacy Mechanism," Control Systems and Computer Science (CSCS), 2015 20th International Conference on, Bucharest, 2015, pp. 469-474.

[21] Q. Geng and P. Viswanath, "Optimal Noise Adding Mechanisms for Approximate Differential Privacy," in IEEE Transactions on Information Theory, vol. 62, no. 2, pp. 952-969, Feb. 2016.

[22] M. S. Keil, A. Lapedriza, D. Masip and J. Vitria, "Preferred Spatial Frequencies for Human Face Processing Are Associated with Optimal Class Discrimination in the Machine", PLoS ONE, vol. 3, no. 7-2590, 2008.

[23] L. Sankar, S. R. Rajagopalan and H. V. Poor, "Utility-privacy tradeoff in databases: An information-theoretic approach", IEEE Trans. Inf. Forensics Security, vol. 8, no. 6, pp. 838-852, 2013.

[24] Maheshkar, Vikas, et al. "FEATURE IMAGE GENERATION USING LOW, MID AND HIGH FREQUENCY REGIONS FOR FACE RECOGNITION." The International Journal of Multimedia & Its Applications 4.1 (2012): 75.

[25] "The Database of Faces" http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html

[26] Geng, Quan, and Pramod Viswanath. "The optimal mechanism in differential privacy." arXiv preprint arXiv:1212.1186 (2012).

[27] Rubinstein, Benjamin IP, et al. "Learning in a large function space: Privacy-preserving mechanisms for svm learning." arXiv preprint arXiv:0911.5708 (2009).

Mahmoud Raafat is a MSc. of Engineering student at Computer & Systems Department, Faculty of Engineering, Ain Shams University. He received his BSc. degree from Computer & Systems Engineering Department, Faculty of Engineering, Ain Shams University in 2011. He has five years of professional experience as an embedded software engineer working in the automotive industry. He worked in various projects related to vehicle telematics, infotainment, and engine control. He is now working in Mentor Graphics Egypt as a senior embedded software engineer. He has research interests in Advanced Driver Assistance Systems (ADAS) and autonomous vehicles.

Bassem Abdullah received his Ph.D. in Electrical and Computer Engineering from University of Miami, Florida, USA in 2012, and his M.Sc. and B.Sc. degrees in Electrical Engineering from Ain Shams University, Cairo, Egypt, in 2007 and 2000, respectively. He is an Assistant Professor at the Computer and Systems Engineering Department, Ain Shams University. His research interests include computer vision, machine learning and embedded systems in biomedical and automotive applications.

Mohamed Taher received the PhD degree in electrical and computer engineering from the George Washington University in 2006. He is an associate professor in the Department of Computer and Systems Engineering at Ain Shams University. His research interests include high-performance computing, reconfigurable computing, embedded systems, and computer architectures.

Mohamed Moustafa received his PhD in electrical engineering from the City University of New York in 2001. He has been active in the industry. From 1998 to 2003 he was senior principal research scientist at L-1 Identity Solutions corporate research center, NJ, USA (now part of Saphran-Morpho, France).

He is a member of the IEEE, the IEEE Computational Intelligence Society, and the IEEE Technical Committee on Pattern Analysis and Machine Intelligence. He is a founding member and the vice chair of the IEEE Computational Intelligence Society chapter in Egypt. He holds three US patents in the field of biometrics and digital image processing.