CARDEA: A CONTEXT-AWARE AND INTERACTIVE VISUAL PRIVACY CONTROL FRAMEWORK

by

RUI ZHENG

A Thesis Submitted to
The Hong Kong University of Science and Technology
in Partial Fulfillment of the Requirements for
the Degree of Master of Philosophy
in Computer Science and Engineering

October 2016, Hong Kong

Authorization

I hereby declare that I am the sole author of the thesis.

I authorize the Hong Kong University of Science and Technology to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize the Hong Kong University of Science and Technology to reproduce the thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

_____

RUI ZHENG

CARDEA: A CONTEXT-AWARE AND INTERACTIVE VISUAL PRIVACY CONTROL FRAMEWORK

by

RUI ZHENG

This is to certify that I have examined the above M.Phil. thesis

and have found that it is complete and satisfactory in all respects,

and that any and all revisions required by

the thesis examination committee have been made.

ASSISTANT PROF. PAN. HUI, THESIS SUPERVISOR

PROF. QIANG YANG, HEAD OF DEPARTMENT

Department of Computer Science and Engineering

21 October 2016

ACKNOWLEDGMENTS

First I would like to thank my family for their unconditional support during the past three years. It is their optimistic attitudes as well as patience that helped me walk across all the troubled water among the years.

I would also like to express my deepest gratitude to my advisor Prof. Pan Hui for his support, guidance and encouragement, without which this thesis would not have been possible.

Special thanks to Jiayu Shu, it was a great pleasure to collaborate with her in the past year and I learned a lot from the collaboration. Same thanks gives to Dr. Tongfeng Weng for the enjoyable collaboration on random walks. Other than that, I would like to thank Haris Mughees and Hamza Zia, for countless times we happily talked about everything and I was always surprised by their knowledge, passion as well as determination.

Thanks also goes to all the members in Symlab family. I am fortunate to know so many wonderful people and work as colleague with them. They have helped me a lot in many aspects from daily life to research. Many thanks to Mr. Issac Ma and Mrs. Connie Lau for their administration work.

Last but not least, I would like to thank Prof. Dit-Yan Yeung and Prof. Chi-Keung Tang. It was great fun to take their courses, which guided me to find my interests and thesis topic. I deeply admire the strong sense of responsibility they have on both lecturing as well as supervision of their students. Their research attitudes and hard working will keep motivating me in my future endeavors.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CARDEA: A CONTEXT-AWARE AND INTERACTIVE VISUAL PRIVACY CONTROL FRAMEWORK

by

RUI ZHENG

Department of Computer Science and Engineering

The Hong Kong University of Science and Technology

ABSTRACT

The growing popularity of mobile and wearable devices with builtin cameras, the bright prospect of camera related applications such as augmented reality and lifelogging system, the increased ease of taking and sharing photos, along with advances in computer vision techniques, have greatly facilitated peoples lives in many aspects, but inevitably raised peoples concerns about visual privacy at the same time.

Motivated by the finding that peoples privacy concerns are influenced by the context, in this thesis, we propose Cardea, a context–aware and interactive visual privacy control framework that enforces privacy policies according to peoples privacy preferences. The framework provides people with finegrained visual privacy control using: *i)* personal privacy profiles, with which people can define their context–dependent privacy preferences; *ii)* natural visual indicators: face features, for devices to automatically locate individuals who request privacy protection; *iii)* hand gestures, for people to temporarily update and flexibly inform cameras of their privacy preferences. Benefited

from recent progresses in face and object recognition, Cardea offers a way for context–dependent privacy control in a natural and flexible manner, which differs from tag and marker based systems. We design and implement the framework consisting of Android client app and cloud control server, with convolutional neural networks as core of the image processing module. Our evaluation results confirm such framework is practical and effective, showing promising future for context–aware visual privacy control on mobile and wearable devices.

CHAPTER 1

INTRODUCTION

The concern about visual privacy has been growing in last decade with increasing adoption of video surveillance systems for security reasons. The statistics shows there are 125 video surveillance cameras per thousand people in U.S. by 2014 [1]. Momentum of new technologies such as the Internet of Things (IOT) will keep driving global video surveillance market in following years, which will raise more privacy concerns.

Other than closed-circuit television (CCTV) surveillance systems for security reasons, handheld devices such as camera phones are also used extensively for the recording of meaningful life moments. Recently, coming with the explosion of products in augmented reality (e.g., Google Glass), robotics (e.g., iRobot Create platform), and gaming (e.g., Kinect), is more and more cameras being embedded in these platforms for the enhancement of life experiences. The trend of embedding cameras, especially in wearables, will keep growing, an example of which is smart contact lens [2]. However, the ubiquitous presence of cameras, the ease of taking photos and recording videos, along with "always on" and "non overt act" features threaten individuals to have private or anonymous social lives, raising people's concerns of visual privacy.

More specifically, photos and videos captured without getting permissions from bystanders, and then uploaded to social networking sites, can be accessed by everyone online, potentially leading to invasion of privacy. Malicious applications on the device may also inadvertently leak captured media data [3].

Benefited from research breakthroughs from deep learning community [4], current vision perception systems are advancing fast in their capabilities of understanding image and video contents [5]. Nowadays, recognition technologies can link images to specific people [6, 7, 8], places [9], and general objects [10], making what previously unsearchable now searchable [11], thus reveal far more private information than expected.

Both legal and technical measures have been proposed to resolve visual privacy concerns. For instance, Google Glass is banned at places such as banks, hospitals, and bars [12]. However, prohibition of cameras usage does not resolve the issue fundamentally, instead it may intrude people's rights to capture happy moments. As a result, there are growing needs to design technical solutions to protect individuals' visual privacy in a world with pervasive cameras. Technical solutions that have been proposed so far are still limited, in the way that they are mostly based on static policies, thus users can not flexibly express their individualized privacy preferences based on surrounding contexts when they are captured. Moreover, previous works require users to wear visual markers such as hats [13] for the detection of interested persons, or clip tags such as QR codes [14, 15] for the fetching of privacy polices. Despite technical feasibilities of these approaches, the extra need of setting up markers/tags and the resulting aesthetically unpleasant appearance will hinder users' willingness to adopt these solutions.

Therefore, the motivation of this thesis is to seek a more natural, userfriendly, flexible, and fine-grained mechanism for people to express, modify, and control their individualized privacy preferences. Under this guideline, we propose Cardea, a context-aware and interactive visual privacy control framework, which let individuals control their visual privacy through: *i)* personal privacy profiles, with which people can define their context–dependent privacy preferences; *ii)* different visual indicators: face features and tags, for devices to automatically locates individuals who request privacy protection; *iii)* hand gestures, for people to temporarily update and flexibly inform cameras of their privacy preferences. When using Cardea, the device will automatically compute context factors, compare them with peoples privacy profiles, and finally enforce privacy policies conforming to peoples privacy preferences. To our knowledge, this is one of the pioneering works that leverages deep learning models, more specifically convolutional neural networks (CNN) [16], to enable visual privacy control in a context-specific and interactive manner.

The rest of the thesis is organized as follows: We first review and discuss related works on visual privacy control in Chapter 2. Following that we introduce convolutional neural networks, the core of Cardea's image processing module, and their applications on related computer vision problems. We then give details about the design, implementation and evaluation of Cardea in Chapter 4. Finally, we share our thoughts on possible future work and conclude the thesis in Chapter 5.

CHAPTER 2

RELATED WORKS

2.1 User Studies

Glass-style AR devices and lifelogging devices come into people's lives in recent years, bringing more and more privacy concerns among public, from the perspectives of both recorders and bystanders. Some user studies investigate these concerns by conducting privacy surveys and *in situ* interviews [17, 18, 19, 20]. Here we summarize some findings from these works:

- All user studies find that most participants care about their appearance in recored contents, and welcome a consent mechanism so that they can have controls such as: Stop the recording when they don't want to be recorded; Obfuscation of their identities in recording-time and sharing-time.
- Study in [18] says that lifeloggers care about the privacy of bystanders, and they prefer automated *in situ* controls of privacy contents to relieve the burden of physical control.
- Privacy is vague, and depends on many factors, which we name it as contexts, defined by primitives such as *Who, What, When, Where, Why and How*. All studies confirm that there are many reasons that make contents private. A breakdown of potential design axes for privacy-mediating technologies is proposed in [17].

Inspired by the design axes proposed in [17], in Table 2.1 we reviewed related works by comparing some major factors such as their problem settings, technical solutions, etc.

Table 2.1: Mobile cameras include cameras in smartphones, AR, VR, lifelogging and other wearable devices. Computer vision methods may be assisted with extra sensors such as RFID tags [21], FIR imagers [22]. There are other factors like implementation layer (app level or os level) that are not listed due to space limitation.

year	privacy survey	problem setting		technical solution		enforcement time		privacy object	
		video surveillance	mobile cameras	computer vision	cryptography	in-situ / run time	access / distribution	user	bystander
I-Pic: A Platform for Privacy-Compliant Image Capture [20]									
2016	✓		✓	✓	✓	✓			✓
Recent work which allows people to broadcast their privacy preferences and appearance information to nearby devices through BLE. These preferences are based on social context.									
What You Mark is What Apps See [23]									
2016			✓	✓		✓	✓	✓	
Propose a system that give users control to mark secure regions for third-party applications. It is implemented within Android camera subsystem.									
Sensitive Lifelogs: A Privacy Analysis of Photos from Wearable Cameras [19]									
2015	✓		✓						
Analyze the photos collected in [18], seeking to understand what makes a photo private and what participants said about their images.									
Screenavoider: Protecting Computer Screens from Ubiquitous Cameras [24]									
2014			✓	✓		✓	✓	✓	
Present a framework that controls the collection and disclosure of lifelogging datasets which contain computer screens and possible sensitive contents.									
PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces [25]									
2014			✓	✓		✓	✓	✓	
Introduce a prototype for owners of first-person cameras to 'blacklist' sensitive places (like bathrooms and bedrooms).									
Privacy.Tag: Privacy Concern Expressed and Respected [14]									
2014			✓	✓	✓		✓		✓
Propose using QR code as privacy tag to link an individual with his photo sharing preferences. These preferences are based on web domains.									
Privacy Behaviors of Lifeloggers using Wearable Cameras [18]									
2014	✓		✓			✓	✓	✓	✓
Conducted an *in situ* user study on privacy behaviors of 36 participants who wore lifelogging devices for a week.									
Courteous Glass [22]									
2014			✓	✓		✓			✓
Wearable camera integrated with a FIR (far-infrared) imagers that turns off recording when new persons or specific gestures are detected.									
World-Driven Access Control for Continuous Sensing [15]									
2014			✓	✓		✓	✓	✓	
Propose a general framework that allows objects to explicitly specify its access policies. Policy triggers can be visual indicators or anything that can be detected in other research works.									

Table 2.1: Continued from previous page

year	privacy survey	problem setting		technical solution		enforcement time		privacy object	
		video surveillance	mobile cameras	computer vision	cryptography	in-situ / run time	access / distribution	user	bystander
In Situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-Mediating Technologies [17]									
2014	✓		✓			✓	✓	✓	✓
Investigate the privacy perspectives of individuals when they are bystanders around AR devices. Conducted 12 field sessions in cafés and interviewed 31 bystanders regarding their reactions to a co-located AR device.									
A Scanner Darkly: Protecting User Privacy From Perceptual Applications [26]									
2013		✓	✓	✓		✓	✓	✓	
Perceptual applications can only access transformed objects such as sketches, faces, etc.									
Enabling Fine-Grained Permissions for Augmented Reality Applications With Recognizers [27]									
2013			✓	✓		✓		✓	
Third party AR applications can only access high-level objects such as Skeleton, Hand Position, etc.									
PriSurv: Privacy Protected Video Surveillance System Using Adaptive Visual Abstaction [21]									
2008		✓		✓			✓	✓	✓
Propose a privacy control mechanism for surveillance videos based on closeness between content objects and content viewers. RFID tags are used to improve the detection of people in videos.									
Respectful Cameras: Detecting Visual Markers in Real-Time to Address Privacy Concerns [13]									
2007		✓		✓			✓	✓	✓
A video surveillance system that allows people who wish to remain anonymous wear colored markers such as hats or vests, and their faces will be blurred.									
Privacy Management for Portable Recording Devices [28]									
2004			✓		✓		✓	✓	
Propose an approach that closed closed devices can encrypt data together during recording utilizing short range wireless communication to exchange public keys and negotiate encryption key. Only by obtaining all of permissions from people who encrypt the recording can one decrypts it.									

2.2 Solutions and Guidelines

As listed in Table 2.1, we conclude previous research works from such aspects:

- **Problem Setting:** Previous researches focused on privacy issues in CCTV, after the spread of smartphones, research focus has been shifted to potential user privacy leakage caused by installed third party applications. A recent trend is the adoption of wearable devices, which make it harder for people to notice that they are being captured. Thus bystander privacy in such settings is gaining more attention these days.

- **Technical Solution:** Encryption and decryption are mostly used when fetching privacy policies, while recognition technologies are mainly used for detection of people and perception of context. Computer vision techniques are also used in policy enforcement stage. Extra economical sensors can be integrated to ease the hardness of computer vision tasks. Wireless technologies are used in some works for the broadcasting of bystanders' privacy policies.

- **Enforcement Time:** *In-situ* control mechanisms pose high requirements of devices' computational power, however fast developments of hardwares and breakthroughs in computer vision encourage researches to try more *in-situ* solutions. Bystander privacy control ideally requires an *in-situ* solution, while user privacy concern usually surfaces at sharing time and is generically easier to be handled.

- **Privacy Object:** Just as other factors, user privacy and bystander privacy don't exclude each other. Essentially user privacy is just a special case of bystander privacy.

- **Other factors:** It is preferable for control mechanisms to be integrated in operation system or even hardware level. Most solutions are based on the assumption that users are trusted. Other design considerations include opt-in vs opt-out, policy push vs policy pull, etc. Each option has advantages and limitations, thus should be considered case by case.

Due to limitation in hardwares as well as algorithms, previous designs are mostly limited on specific settings and simple techniques, though many works mention that policies should be situational, individualized and dynamic. This motivates us to move further in the direction of providing a more general as well as practical control service. From the discussion of related works, we can see that privacy control system design is a complicate task. In current stage it is not possible to solve all problems in one shot, therefore Cardea's design is also limit in such ways:

- Though not limited to, it starts from and aims at protecting bystander privacy.

- Currently only computer vision methods are used, and it tries to provide an *in situ* solution, but relies on a stable connection with a center server. Part of computations are offloaded to center server is because mobile phones can not afford to load all deep learning models and run all computer vision algorithms.

- It is implemented in application layer, thus can not prevent users from using other applications to get raw camera data.
- We choose opt-out policies for aesthetic reason, trying to let photographers enjoy the real world image while still take care of privacy concerns for bystanders who mind their appearances in that image.

2.3 Possibilities and Challenges

The processing power of mobiles and computers are increasing extremely fast in recent years. Nvidia's Tegra Processors [29] are used in many auto-pilot systems. Nvidia's Tegra X1 already achieves 1 teraflops 16bit floating points performance [30]. Many high performance smartphones are now equipped with high end processors such as Qualcomm's Snapdragon 820s [31], which makes them able to run certain heavy computer vision algorithms that is impossible before. A first thought would be deploying state-of-the-art deep learning models on these platforms to extract more accurate context informations. However, context is an abstract concept and thus hard to be defined, thus Cardea is limited in how well context is represented in the design. The way users interact with a system is also important for acceptance of the system, how to ease the burden for bystanders to express their dynamic privacy preferences pose another challenge to our design. From implementation point of view, we have to take care of many things such as resource limitations, issues when scaling up, uncontrolled environments, etc. After an introduction of deep learning and convolutional neural networks in next chapter, we will give details of how we tackle these challenges in Chapter 4.

CHAPTER 3

CONVOLUTIONAL NEURAL NETWORKS

3.1 Deep Learning

Deep learning [32, 4] is part of a broader family of machine learning methods that focus on representation learning. Unlike rule based methods used in early days of artificial intelligence, deep learning targets at tasks that are easy for people to perform but hard for people to describe formally—problems that we solve intuitively. Former methods have proved success in problems that can be completely described by a very brief list of completely formal rules, thus easily provided ahead of time by the programmer. That led to the defeat of world chess champion Garry Kasparov by IBM's Deep Blue chess-playing system in 1997 [33]. However, rule based or knowledge based methods fail at intuitive tasks such as recognizing objects or speech. The reason behind this inability is because these tasks require immense amount of knowledge about the world, and much of this knowledge is subjective and intuitive, thus difficult to articulate in a formal way. The difficulties faced by AI systems relying on hard-coded knowledge suggest that AI systems need the ability to acquire their own knowledge, by extracting patterns from raw data, just like how human learns from experiences. This capability is known as machine learning. It does not take long for people to realize that performance of machine learning algorithms depends heavily on the representation of data fed into these algorithms. Under a good representation, factors of variation can be disentangled and non important factors will be discarded. People used to put lots of efforts on hand designing features to get a good representation for every domain specific problem. Unfortunately seeking a good representation for a problem can be as difficult as solving the problem itself. Deep learning solves this central problem in representation learning by introducing representations that are expressed in terms of other, simpler representations. Deep learning allows the computer to build complex concepts out of simpler concepts, thus achieves great power and flexibility by representing the world as a nested hierarchy of concepts. Fig 3.1 shows a hierarchy relation from AI to deep learning.

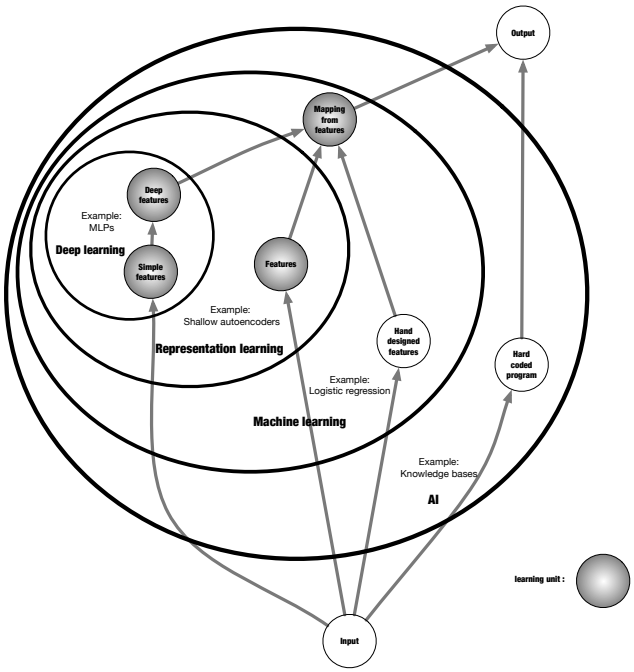


Figure 3.1: Venn diagram showing relations between deep learning, representation learning, machine learning, and AI. An example and work flow are also included for each section.

3.1.1 Three Waves

Deep learning has been rebranded many times under different names, only recently become well known as ”deep learning”. Broadly speaking, there have been three waves of development of deep learning: in 1940s-1960s known as *cybernetics* [34, 35], in 1980s-1990s known as *connectionism* [36], and the current resurgence starts from 2006 [37, 38, 39]. These three waves witness the evolving from simple perceptron, to distributed representation and stochastic gradient descent algorithm, and finally to today's various deep structures. The resurgence of deep learning benefits from the facts: computers are faster, datasets are bigger and a good initialization of model parameters. Faster computers make it possible to train deeper models, bigger datasets relieve deep models from overfitting, and enable them to learn more meaningful mid-level features that are more generalizable, and a good initialization through layer wise pretraining provides a proper prior and makes supervised training on later stages much easier.

Since the early stage of deep learning, neuroscience is regarded as an important source of inspiration. However, it is no longer a predominant guide for the field because we simply do not have

enough information about the brain to use it as a guide. It is seemed as a more general principle of learning multiple levels of composition, which can be applied in machine learning frameworks that are not necessarily neurally inspired.

3.1.2 Breakthroughs

We highlight some of the breakthroughs brought by deep learning in recent years:

- In the ImageNet Large-Scale Visual Recognition Challenge (ILSVRC) 2012, a convolutional neuron network won this challenge for the first time and by a wide margin, bringing down the state-of-the-art top-5 error rate from 26.1% to 15.3% [40], since then the top-5 error rate keeps dropping down each year [41, 42] and in last year dropped to 3.6% using deep residual network (ResNet) [43]. Deep networks also had spectacular successes for pedestrian detection and image segmentation [44, 45, 46] and yield superhuman performance in traffic sign classification [47].

- In March, Google DeepMind's AlphaGo defeated world champion Lee Sedol using deep reinforcement learning [48, 49]. Prior to that, they also showed that a deep reinforcement system is capable of learning to play Atari video games and reaching human-level performance on many tasks [50].

- The application of deep learning on other fields such as speech recognition [51, 52, 53] and machine translation [54, 55] all lead to great successes. The past years surfaced many new trends such as generative adversarial networks, neural Turing machines etc [56, 57, 58, 59, 60]. The years ahead are full of challenges and opportunities to improve deep learning even further and bring it to new frontiers.

3.1.3 Artificial Neural Networks

A Single Neuron

Fig 3.2 shows how to coarsely model a biological neuron: Each neuron receives input signals from its dendrites and produces output signals along its (single) axon. The axon eventually branches out

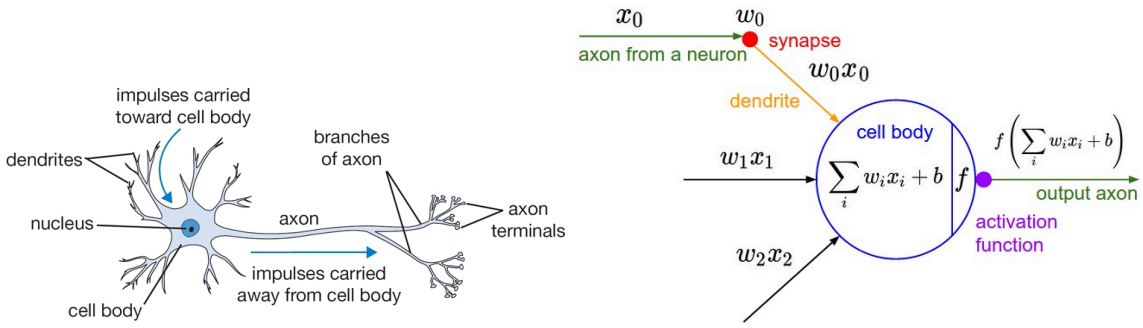


Figure 3.2: A cartoon drawing of a biological neuron (left) and its mathematical model (right). Photo taken from *Module1: Neural Networks* in [61]

and connects via synapses to dendrites of other neurons. In the basic model, the dendrites carry the signal to the cell body where they all get summed. If the final sum is above a certain threshold, the neuron can fire, sending a spike along its axon. In the computational model, we assume that the precise timings of the spikes do not matter, and that only the frequency of the firing communicates information. Based on this rate code interpretation, we model the firing rate of the neuron with an activation function f, which represents the frequency of the spikes along the axon. Historically, a common choice of activation function is the sigmoid function σ, since it takes a real-valued input (the signal strength after the sum) and squashes it to range between 0 and 1. Hereafter in this thesis, we will take standard naming convention and refer a hidden unit as a computational neuron.

Activations

Depends on the activation, neurons can have different properties and impacts on the whole network. Figure 3.3 shows most commonly used activation functions:

Sigmoid Sigmoid is used historically to simulate the firing rate of a neuron but recent years falls out of favor and is rarely used now. It saturates at either tail of 0 or 1, and at these regions the gradient is almost zero, thus it kills gradients from propagating to previous layers, making deep networks not trainable. Another drawback of sigmoid activation is that neurons in later layers will not receive zero-centered inputs, this will cause all positive or negative gradients on the weights during backpropagation, which may lead to undesirable zig-zagging dynamics in the gradient updates of the weights. However, once gradients are added up across a batch

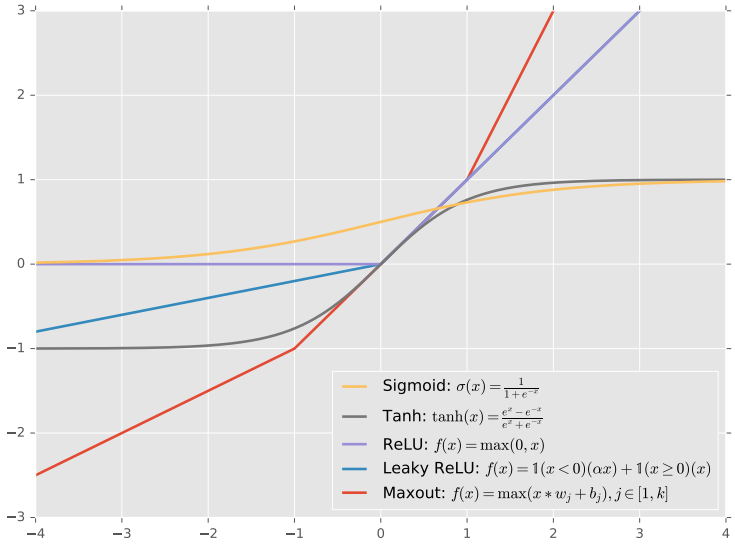


Figure 3.3: Commonly used activation functions.

of data, the final update for the weights can have variable signs, somewhat mitigating this issue.

Tanh Though similar to sigmoid non-linerality in that it also suffers from saturization and thus vanishing gradients problems, tanh is always preferred to sigmoid because its output is zero centered.

ReLU Rectified linear unit becomes popular in recent years. [40] used it in their winning 2012 ImageNet competetion and found that it greatly accelerated the convergence of stochastic gradient descent optimization process. Also comparing to other activations, it is a much more light weight operation since it is a simple thresholding operation. However, ReLU unit can ”die” if a large enough gradient changes the weights such that the neuron never activates on new data.

Leaky ReLU Similar to ReLU, but can help fix the ”dying ReLU” problem by modifying the flat side of ReLU to have a small gradient [62].

Maxout Introduced in [63], Maxout unit enjoys all the benefits of a ReLU unit, and does not have its drawbacks. Maxout activation can implement ReLU activtions and approximate any convex activation function.

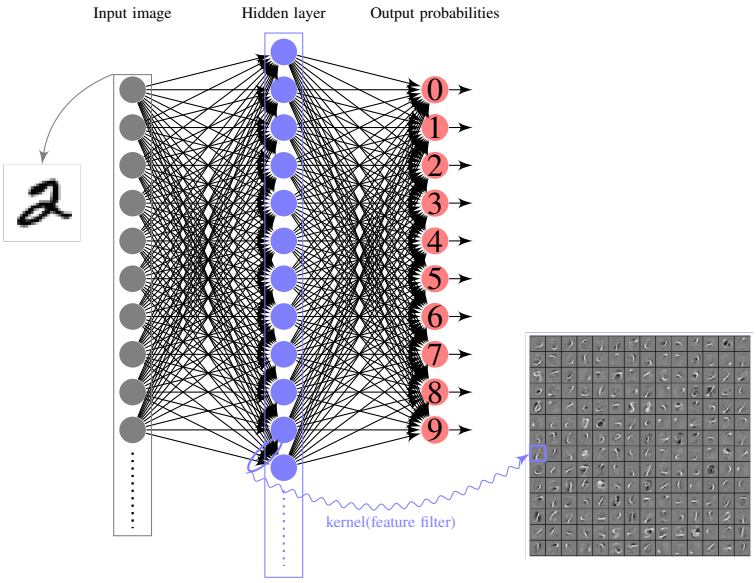


Figure 3.4: A regular feed forward neural network with 1 hidden layer. A 28x28 mnist digit image is flattened and fed into the network, it outputs probabilities of being a certain digit from 0 to 9. The learned kernel for each hidden unit is also shown.

Basic Network Structure

With appropriate loss function, a single hidden unit can function as a linear classifier. However, due to simplicity, its representation power is limited. For example, XOR operation can not be implemented with a single unit, but can be implemented with 3 units. For the network to have enough learning capacity to solve complicate tasks, hidden units are usually aggregated and stacked to form a layer by layer structure. With appropriate regularization, the network can learn powerful features and perform well for many tasks. A regular neural network is shown in Fig 3.4, a deep neural network can have many hidden layers. [64] provides an interactive play ground for tinkering with neural networks.

Backpropagation Algorithm

During the optimization process of loss function, we need to calculate the gradients with respect to all the weights and update them. A naive way is keep all the weights fixed and only tweak one weight to see how it changes loss, thus get its gradient. However, this method is very inefficient since it has to tweak order of the number of weights times to get gradients for all the weights.

The efficient way to do this is backpropagation algorithm. Detailed derivations on backpropagation algorithm can be found on tutorials [65, 61]. We highlight some points here:

- It helps to think of the mapping from input to output that the neural network represents as a computational graph. Each node in this computational graph is simple operation like $+$, $*$, $\max$, or any operation like σ that have a simple derivable gradients. In such way, any complicate mapping function is decomposed into simple unit operations, and backpropagation refers to the node by node backward propagation of gradients from loss to input using chain rule.
- There can be many paths from loss to any variable in the network, gradients flowed through all these paths backwards to this variable get added up when calculating gradient on this variable.
- In neural networks, the preactivations of a layer z and activations of previous layer o have relation $z = w^T o$ where w are the weights between these two layers, it can be seen that gradients for w are proportional to activations o of previous layer, this implies that the scale of the data has an effect on the magnitude of gradients for the weights. When input data is not scaled well, the gradient can be huge, so data preprocessing is a good practice.

Training

Below we list most of the practical concerns when training neural networks:

Data Preprocessing Common data preprocessing steps include mean subtraction, normalization, PCA whitening [66]. Mean subtraction is to zero-center the data. Normalization refers to normalizing the data dimensions so that they are of approximately the same scale. PCA whitening is to first apply PCA on the dataset, followed by a normalization step on the principle components. For most computer vision tasks with big image datasets as input, mean subtraction is enough.

Weight Initialization Mostly used weight initialization strategy is random sampling from a damped gaussian distribution. Improvements on randomly initialization are focused on

calibrating the variances with respect to number of inputs for each neuron such that its output's variable does not blow up. For ReLU units, it is recommended to draw weights from $\sqrt{\frac{2.0}{n}}\mathcal{N}(0,1)$ as suggested in [62]. A recently developed technique called batch normalization explicitly forces each neuron's activations for a minibatch to take on a unit gaussian distribution through whitening among this minibatch [67]. Batch normalization can be interpreted as doing preprocessing at every layer of the network, but integrated into the network itself in a differentiable manner. In practice networks that use batch normalization are significantly more robust to bad initialization.

Regularization $\mathcal{L}2$ regularization $\frac{1}{2}\lambda w^2$ is still the most commonly used regularization term. Other than that, $\mathcal{L}1$ regularization $\lambda|w|$ leads to sparsity in weights, it is useful when the problem is concerned with explicit feature selection. Dropout [68] is a simple but effective way of regularization, in practice it smears activations with a certain probability during training, which can be interpreted as sampling a neural network within the full neural network, and only updating the parameters of the sampled network based on the input data, therefore effectively there are many more neural nets working as an ensemble to eventually perform the classification.

Loss Functions In classification problems, most commonly used data loss functions are hinge loss and cross-entropy loss. Hinge loss is defined as $L_i = \sum_{j \neq y_i} \max(0, f_j - f_{y_i} + 1)$ where L_i and y_i refer to loss and ground truth label of ith sample, f_j is the output score for class j. Hinge loss is used with SVM classifier. Cross-entropy loss is defined as $L_i = -\log(\frac{e^{f_{y_i}}}{\sum_j e^{f_j}})$, and used with Softmax classifier. For regression problems, $\mathcal{L}2$ distance $L_i = ||f - y_i||_2^2$ are normally used. Whenever possible, it is recommended to see if a regression problem can be morphed to a classification problem by quantization of outputs into bins, because classification is an easier task and gives confidences of each class.

Optimization There are many optimization options when training deep neural networks. Starting from vanilla SGD (stochastic gradient descent), integration of momentum improves convergence rate and adaptive algorithms ease the pain of tuning the learning rates. [69] gives a comprehensive overview of related algorithms.

Miscellous To find good hyperparameters such as initial learning rate, regularization strength, it is suggested to use random search over grid search [70] and stage the search from coarse to fine. Bagging of neural networks trained independently is a reliable approach to improve the performance.

3.2 Convolutional Neural Networks

Convolution neural network (CNN) is similar to regular neural network, except that it uses weight sharing to largely decrease the number of parameters, thus having the advantage of being less prune to overfitting and also enable training of deeper networks. It borrows the concept of receptive field from biological vision system, in such a way that a neuron will be only connected to a local region of previous layer. Fig 3.5 (left) shows the connections between a 3 channel input image and a neuron in the first hidden layer. Note that the connections are across the channel dimension, which means if a neuron has a receptive field of size $f_x \times f_y$, and its previous layer has D channels, then the connections this neuron has is $f_x \times f_y \times D$. These $f_x \times f_y \times D$ connections is called a kernel or filter, however people usually refer it as a filter with size $f_x \times f_y$ and normally people set $f_x = f_y$. Weight sharing is achieved when apply a convolution operation on previous layer using the same filter. The output from a filter's convolution operation is referred as a feature map, therefore a hidden layer with D channels/feature maps, is generated from D filters' convolution operations. Fig 3.5 (right) illustrates the convolution operations of two 3×3 filters applied on previous layer which has 3 feature maps each having size 5×5, with stride S and padding P both being 1. It can be easily calculated that if a layer has shape $W \times H \times D$, the convolution of K filters of size $f_x = f_y = F$ with stride S and padding P will generate K feature maps as next layer, each feature map has size $((W - F + 2P)/S + 1) \times ((H - F + 2P)/S + 1)$. And each filter will introduce $F \times F \times D$ weights parameters and 1 bias parameter. After convolution operations, it is often followed with nonlinear activations, using the same nonlinearities listed in last section.

Pooling layer is also commonly used periodically between successive convolution layers. Similar to convolution operation, it also requires a spatial extent F and stride S for pooling operation. However, pooling operations does not apply on channel dimension and the operation is very simple:

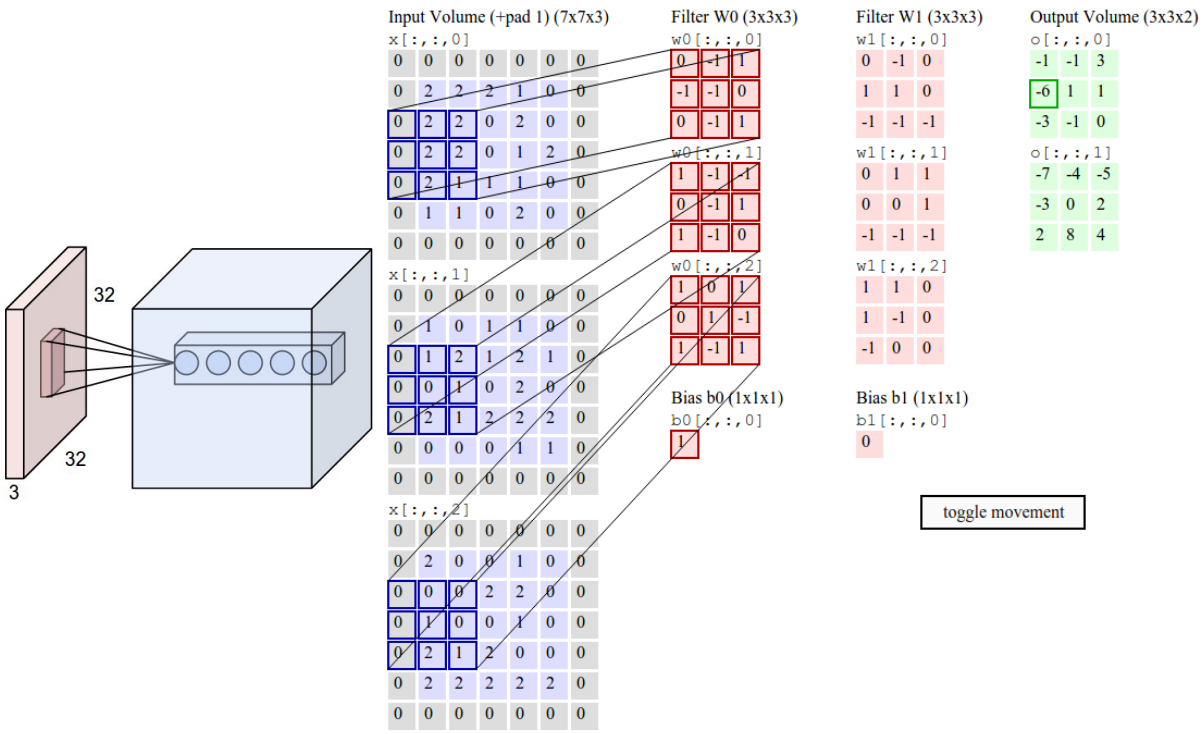


Figure 3.5: Receptive field of a hidden unit (left) and convolution operations of two 3×3 filters (right). Image credit: [61].

max/average pooling is reduce a $F \times F$ block to just a single value via $\max$/$\min$ function. A $F \times F$ pooling on top of a $W \times H$ feature map with stride S will generate a pooled feature map with size $((W-F)/S+1) \times ((H-F)/S+1)$. Though pooling layer can bring certain translation invariance to the network, it will cause too much information loss. It seems likely that future architectures will favor very few to no pooling layers. Local response normalization layer was often used with ReLU neurons but nowadays is also losing favor because in practice its contribution has been shown to be minimal.

The conventional form of a CNN follows the following form:

$$\texttt{Input} \rightarrow [[\texttt{ConvLayer} \rightarrow \texttt{ReLU}] * N \rightarrow \texttt{PoolLayer}?] * M \rightarrow [\texttt{FC} \rightarrow \texttt{ReLU}] * K \rightarrow \texttt{FC}$$

where $*$ indicates repetition, and $\texttt{PoolLayer}?$ indicates an optional pooling layer. Moreover, $0 \leq N \leq 3$, $M \geq 0$ and $0 \leq K < 3$ are common choices. A typical CNN with two feature stages is shown in Fig 3.6. It is preferred to use a stack of convolution layers with small filters rather than one convolution layer with a large filter, because the former allows to express more powerful features of

the input and at the same time with fewer parameters. LeNet [16], AlexNet [40], VGGNet [41] are representatives of this structure. However, the conventional form has been challenged a lot in recent year, many networks that achieve state-of-the-art performance have different repetitive structures such as GoogLeNet [42] and ResNet [43].

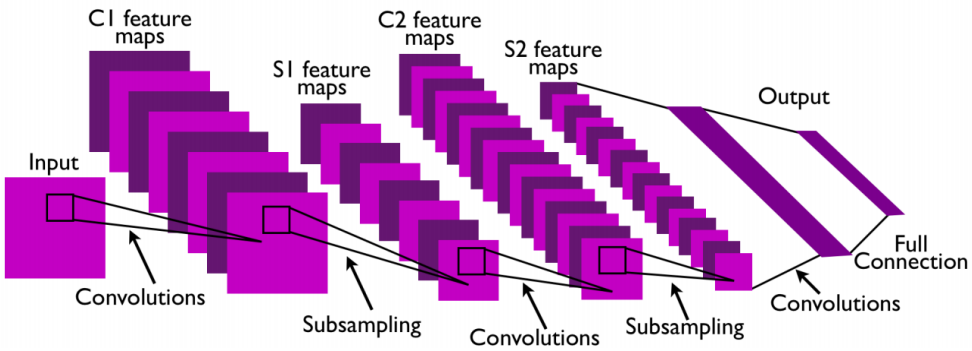


Figure 3.6: A typical CNN architecture with two feature stages.

3.3 Applications

Deep convolutional neural networks have been applied on broad areas from image recognition, video analysis to gameplay. Different from the time in 2012 when it was the major reason behind the winning of ImageNet competetion, nowadays they are basic Lego blocks that will be stacked and tweaked in every possible task. Related applications to this thesis are scene classification, face recognition and object detection. For image classification problems such as scene classification and face recognition, the training dataset is playing an equally important role as the innovation of network structure. Many times conventional CNNs trained on large datasets outperform exquisitely designed CNNs that are trained on smaller datasets by a large margin. Places2 dataset and CASIA-WebFace dataset are among the largest datasets for scene classification and face recognition. The adoption of these classification models is straightforward from their work, therefore we discuss more about how CNNs are used for object detection problems.

From R-CNN to Faster-RCNN

With a powerful CNN like AlexNet that is pre-trained on large dataset, a naive way of using it for object detection problem is classifying a sliding window. However, unlike cascading face detector in OpenCV, the classification of a window involves heavy computations and thus can not afford a sliding window approach. Instead, many methods such as selective search [71], MultiBox [72], EdgeBoxes [73] are proposed to generate region proposals. [74] proposes R-CNN, a region proposal based method that uses region proposals and their convolutional features to train classifiers and bounding-box regressors for object detection, the regional proposals are generated from other methods and features are extracted from a CNN fine-tuned for the detection classes. However, different proposals don't share computations during feature extraction as well as in prediction time, the feature extraction step is slow and requires huge storage for cached features.

He [75] proposed SPP (spatial pyramid pooling) layer to pool convolutional layers to fixed length features, thus enabling variable input size. In forwarding phase, different proposals will be able to share computations, thus it saves time for feature extraction and prediction. However, it still requires first caching features and a post training stage of classifiers and bounding box regressors.

To get rid of the post training stage, Fast R-CNN is proposed in [76] to train the detector in a single stage without caching features and post training steps. The ROI (region of interest) layer proposed in this work is a special case of SPP layer. The network integrates two loss branches which take the roles of classifier and regressor that otherwise would require the post training steps. This has the drawback of still requiring pre-generated proposals, RPN (region proposal networks) is later proposed in Faster R-CNN [77] to generate proposals by the neural network itself, thus get rid of extra proposals from other methods and become a truly end to end training and prediction framework for object detection from raw images. Cardea's gesture detection and recognition module is based on Faster R-CNN.

CHAPTER 4

CARDEA

4.1 System Design

Recalling related works in Chapter 2, what motivates the design of Cardea are the following:

- People's privacy concerns are dependent on context. Although in certain circumstances locations are strong hints of possible privacy intrusion, generally what individuals are doing and with whom are more essential and crucial factors that directly relate to privacy.
- People's privacy preferences vary from each other, thus they should be able to express their personal privacy preferences.
- People's privacy preferences may change from time to time, therefore they need a way to change such preferences easily.

To achieve these objectives, we propose following solution:

- We combine GPS location, grouped scene categories (Table 4.1) and accompanied persons as context that can better represent people's privacy concerns than previous methods. As a result we are able to provide more general as well as finer granularity privacy preference settings for users.
- We use cloud server to host individualized privacy preferences, and user's preference is bound with his facial features. In this way his raw visual information stays locally, preventing the case of visual privacy leakage from hacked servers.
- Other than a simple interface provided to users to update their privacy preferences, hand gestures like  and can be used by user to actively speak out about his preference in the capturing moment, enriching the interaction and adding more flexibilities.

As introduced in chapter 3, breakthroughs made by deep learning community in many computer vision problems such as image classification, face recognition and object detection have guided the proposed solution and shed lights on its practicability. More specifically, given a captured image, Cardea will leverage powerful convolutional neural networks for the recognition of scene context, registered users and gestures. Cardea's design is given in Fig 4.1, it is composed of the client applications and cloud server. It works based on data exchange and collaborative computing involving both client and cloud sides. The major components and interactions include:

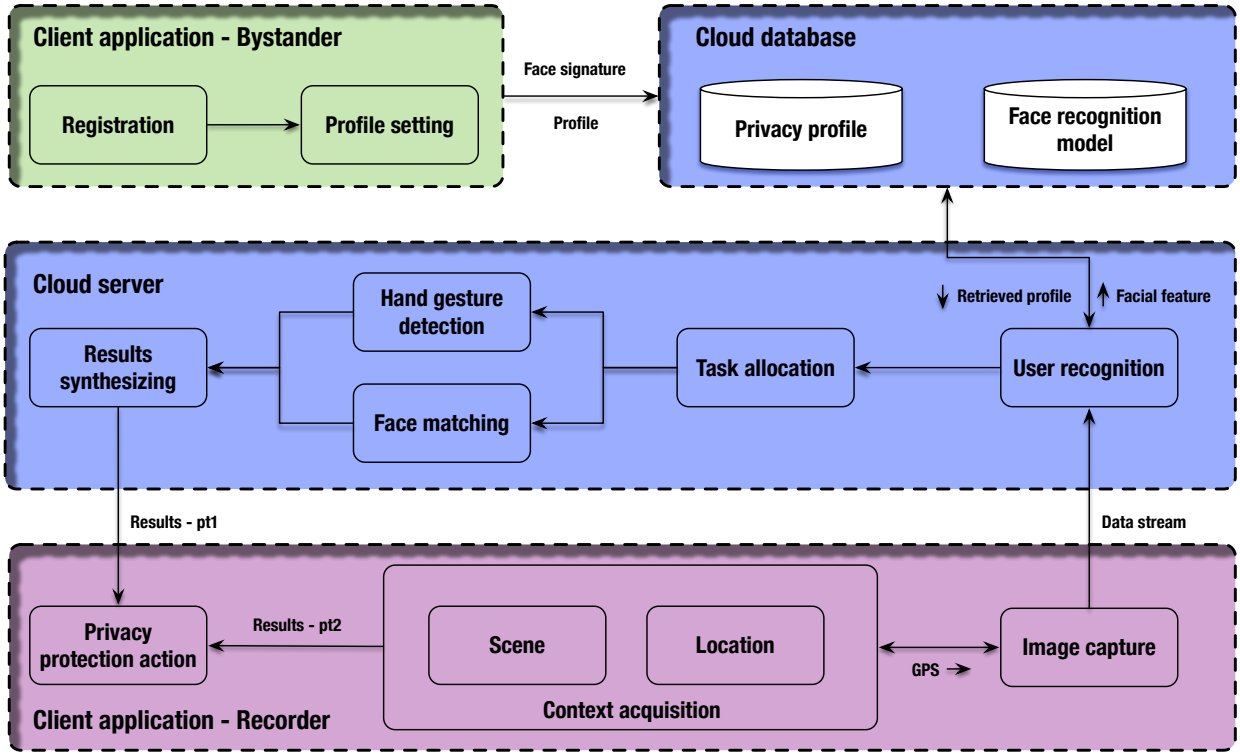


Figure 4.1: System design of Cardea.

Bystander client application: A bystander can use this application to register as Cardea user and define his privacy profile. It will capture a number of face images (about 50–60 images) and extract facial features from these images as his unique face signature. After setting up the context dependant privacy preference, his facial signature and preference will be sent to cloud server for registration and updating of face recognition model.

Recorder client application: A recorder can use this application to take images that will automatically perform privacy protection actions in compliance with all Cardea users' privacy preferences. Given a captured image, it first detects all the faces and extracts the corresponding facial features locally on device, then the features and the captured image (compressed and with all detected faces blurred) are sent to the server for face and gesture recognitions. GPS coordinate is also sent to server in this step to be compared with recognized users' location settings. During the time waiting for response from cloud, it performs scene group prediction task. Finally, predicted scene group and intermediate decision result received from server are combined to decide the actual protection action which will be enforced on the raw captured image.

Cloud server: The cloud server plays two roles: ❶ When receiving requests from Bystander applications, it will store/update users' profiles, and training/updating system's face recognition model automatically; ❷ When receiving requests from Recorder applications, it will initiate face and gesture recognition tasks, as well as partial decision making based on recognition results, and send these intermediate decision results to client for the final step of decision making.

Implementations and evaluation of each module, how Cardea allocates tasks between mobile and cloud, integration and user interactions are discussed in following sections.

4.2 Model Training

4.2.1 Scene Classification

Data Preparing and Preprocessing

For scene classification, we use pre-trained model of Places2 dataset provided by [78]. In the time Cardea project was conducted, Places2 dataset provided by the authors contained 401 categories with more than 8 million training images, and the pre-trained model was based on AlexNet structure [40]. By the time this thesis is writing, the dataset is deprecated and the new Places2 dataset contains 365 categories. And the authors provide more pre-trained models based on different network structures [79].

Table 4.1: Scene categories.

Scene Group	Scene Category
Eating	bistro/indoor, bistro/outdoor, cafeteria, coffee_shop, diner/outdoor, dining_hall, dining_room, fastfood_restaurant, food_court, restaurant, restaurant_patio, sushi_bar
Entertainment	bar, discotheque, pub/indoor
Shopping	bazaar/indoor, bazaar/outdoor, clothing_store, general_store/indoor, jewelry_shop, shoe_shop, shopping_mall/indoor, supermarket
Work	conference_center, conference_room, cubicle/office, library/indoor, office, office_cubicles, reading_room
Public	park, street
Mobility	airplane_cabin, airport_terminal, bus_interior, bus_station/indoor, subway_station/platform, train_interior, train_station/platform
Exhibition	art_gallery, museum/indoor
Religion	cathedral/indoor, cathedral/outdoor, church/indoor, church/outdoor, mosque/outdoor, pulpit, temple/east_asia, temple/south_asia
Illness	hospital, hospital_room, nursing_home
Nudity	bathroom, beach, jacuzzi/indoor, sauna, shower, swimming_pool/indoor, swimming_pool/outdoor

Note that in the dataset we used, there is a non-uniform distribution of images per category for training, ranging from 4,000 to 30,000, mimicking a natural frequency of occurrence of the scene. Among the 401 categories, we choose 59 scene categories that are close to daily life and in such scenes people may have privacy concern. In total this subset composed of 1 million training images and 2950 validation images (50 validation images for each category). We also group these 59 scene categories into 10 groups based on contextual similarity as shown in Table 4.1, such that people have similar reasons for privacy concerns in scenes that are in the same group (e.g. people don't want to be captured in bathroom and beach is both because of nudity concerns). The distribution of training images among categories and groups is shown in Fig 4.2.

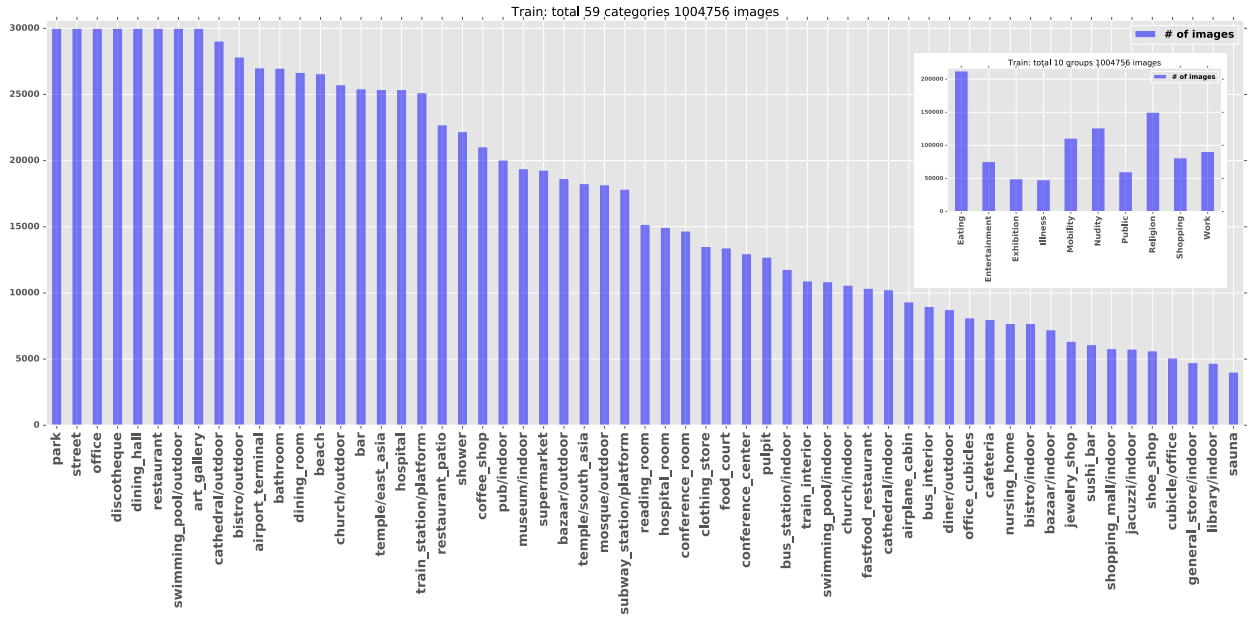


Figure 4.2: Number of images for each category and each group (inset).

Training Procedures

The training step is a standard fine-tuning process, which is extensively used in transfer learning [80, 81]:

❶ Using pre-trained model as feature extractor, we extract the features at *fc7* layer for images belonging to the 59 picked categories. Other than shuffling the features, we also augment the features such that all categories have same amount of features. Though the natural frequencies of occurrence are obviously different among different scenes, we argue that for the purpose of privacy protection, all the scene categories should be equally important, thus categories imbalance is not what we favored. The augmentation step can be implemented using weighted loss layer, but we take simple way of bootstrapping features for categories with less images. After this step, all features are cached and stored in lmdb format.

❷ Train a softmax classifier of the 59 categories using the extracted features. We choose to train a classifier for categories and then add up the output probabilities to predict the group, rather than directly train a group classifier, is because category classifier tells more about the

image, and our desired property is equal weights among scene categories rather than groups.

❸ Both feature extraction and classifier training are implemented using Caffe library [82, 83]. In this step we merge the feature extraction part of pre-trained model and the softmax classifier into a single model by copying weights. Now Caffe has the option of specifying layers with fixed weights, thus simplifying the fine-tuning and deployment process.

Other than improving the validation accuracy from 0.56 to 0.57, shuffling also makes training converges faster. With augmentation to relieve category imbalance issue, the classifier can finally achieve 0.600 validation accuracy on the 59 categories. There is no other benchmarking result specifically on the subset we choose, but recent benchmark gives 53%-56% validation accuracy on the new Places2 dataset with 365 categories [79], suggesting our model is competitive. The higher validation accuracy of our model is due to the smaller scale of classification problem we are dealing with.

Prediction

For prediction, we get probability of a group by summing up the probabilities of all categories belonging to this group, and output the most probable group as prediction of an image. Our model's group prediction accuracy for the validation set is 82.8%. Fig 4.3 shows some prediction examples. As seen from the examples, given an image, the predicted category probabilities are usually distributed to few categories within same group, thus group prediction is resilient to perturbation coming from category prediction. The way we group categories can be seemed as a hard-coded clustering step, which makes prediction more robust to noise. The failure cases are mostly due to natural context ambiguity from a image (e.g. image with object in focus, therefore not enough hints for scene inference). Labeling the 342 non selected categories as an extra group will amplify the ambiguity issue, as doing so will distribute probabilities to the extra group and lead to wrong prediction, even for images with less ambiguity. In other words, a 59 way classifier leads to higher recall for selected scenes and grouping leads to higher accuracy. This is also reflected in confusion matrices shown in Fig 4.4, category confusion matrix shows some clustering structure which is in accordance with the groups we manually assigned. However, only using top 1 category for predic-

Figure 4.3: Scene classification prediction example. Top5 groups (green) and categories (white) are shown with their probabilities.

tion sacrifices prediction accuracy, which can be avoided by grouping as shown in group confusion matrix.

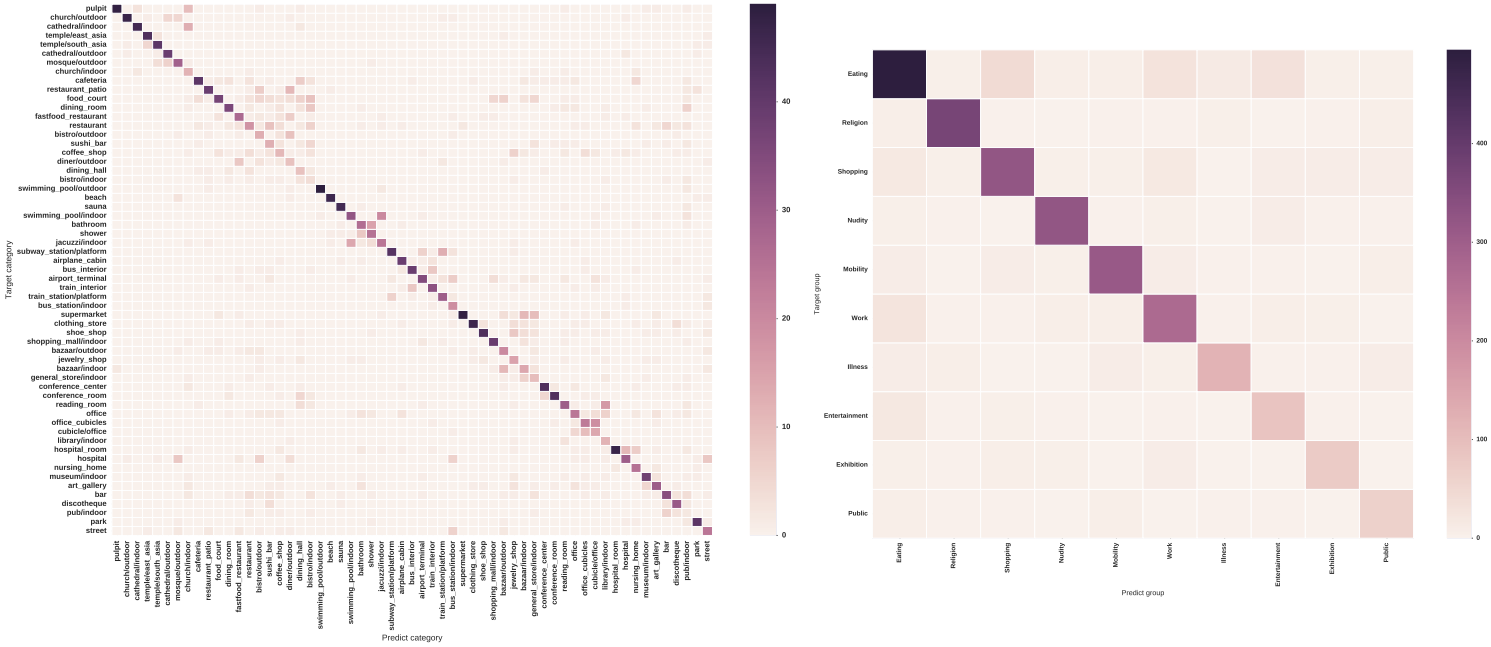


Figure 4.4: Confusion matrices for category prediction (left) and group prediction (right).

4.2.2 Face Recognition

Like scene classification, we select a pre-trained model for face recognition task. More specifically, the pre-trained model will serve as face feature extractor, and we will update the face classifier whenever new users register in Cardea and upload their face features. There are already many deep neural networks deployed in commercial products, like Megvii's Face++ [84], Facebook's Deepface [6], Google's Facenet [8], Sensetime's Deepid [7]. OpenFace [85] is an open source project that is gaining attentions in recent months, it is based on Torch [86]. Because Cardea's other modules are under Caffe framework, we limit our options on open sourced Caffe models. The models in our consideration are VGG face recognition model [87] and Lightened CNN face recognition model [88].

To compare performance of features extracted from the two models, we run t-SNE visualization [89] on the features of a small dataset we previously collected for emotion sensing. Fig 4.5 shows the t-SNE visualization result. It seems VGG feature and Lightened CNN feature have similar performance, at least on this small dataset. Though it is found that comparing to Lightened CNN model, VGG model is more robust to variations and its features show better transferability [90], the

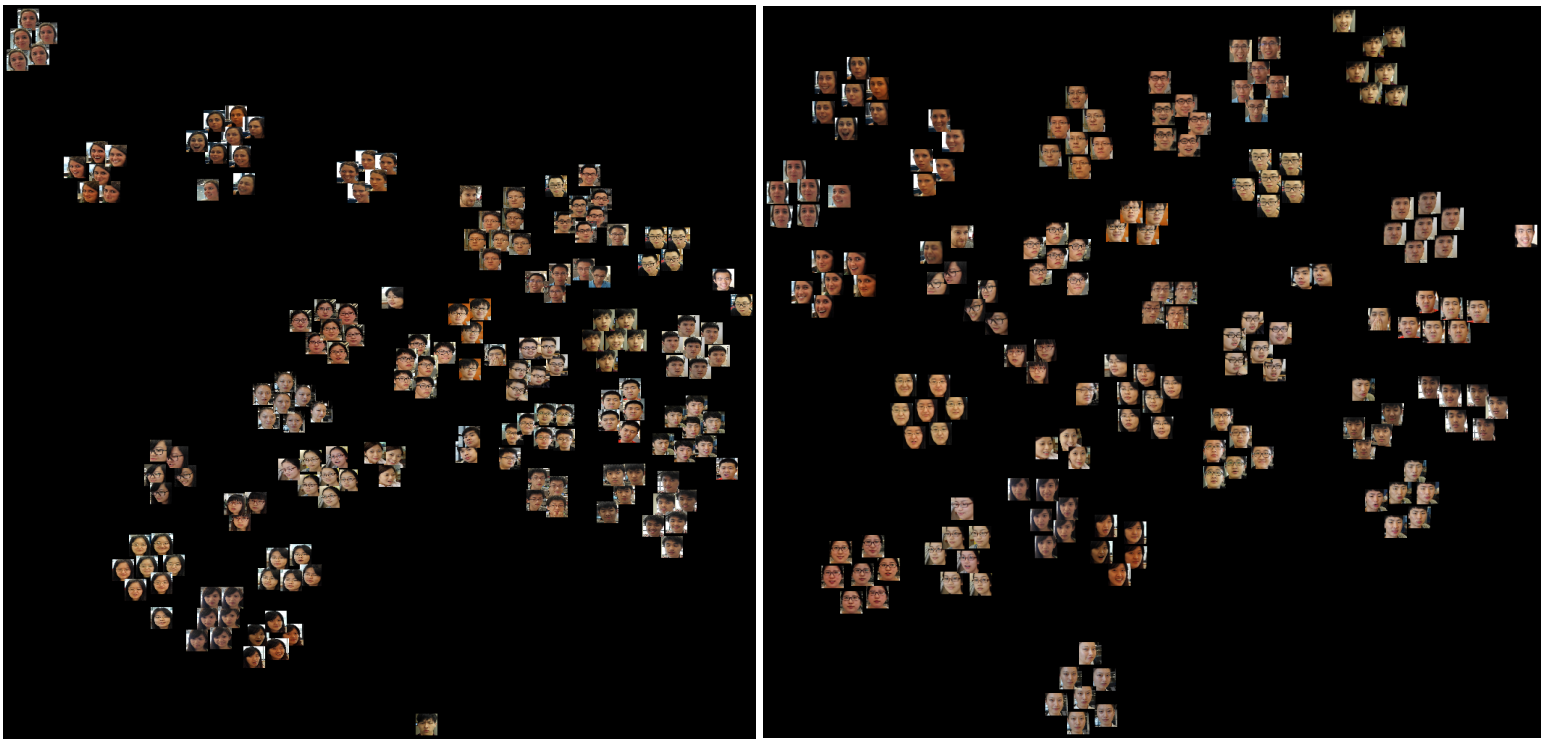


Figure 4.5: t-SNE visualization of VGG *fc8* layer features and Lightened CNN *fc1* layer features.

model size is more than 500MB, 10 times bigger than Lightened CNN model. And the released VGG model has a feature dimension of 4096, while Lightened CNN model has a feature dimension of 256. Our experiment on different Android smartphones shows it takes 10 times longer to extract VGG features. Table 4.2 shows the forwarding time we tested on different smartphones. It can be seen VGG model consumes much more memory that it can only run on phones with memory larger than 3GB. Due to above concerns, we use Lightened CNN model in our implementation.

Table 4.2: Time of single facial feature extraction and batch facial feature extraction (10 faces).

	Xiaomi Mi 3W Snapdragon 800 2GB RAM	Galaxy Note 4 Snapdragon 805 3GB RAM	Xiaomi Mi 5 Snapdragon 820 4GB RAM
1 VGG CNN	N/A	N/A	$\sim$ 2780 ms
10 VGG CNN	N/A	N/A	$\sim$ 26740 ms
1 Lightened CNN	$\sim$ 508 ms	$\sim$ 330 ms	$\sim$ 303 ms
10 Lightened CNN	$\sim$ 6602 ms	$\sim$ 3071 ms	$\sim$ 2031 ms

Detection and Alignment

Lightened CNN model takes aligned face as input, requiring that the distance between midpoint of eyes and midpoint of mouth is 48, and y value of midpoint of eyes is 40, as shown in Fig 4.6. We use OpenCV's haar cascade [91, 92] frontal face detector. The limitation it brings to Cardea is only frontal faces will be detected and recognized. We set *minNeighbors* (the parameter specifying how many neighbors each candidate rectangle should have to retain it) to be 3 to ensure a relative high recall for face detection. To remove false positive, we further apply skin color filter (range $[0, 48, 60] - [30, 255, 255]$ in HSV color space) on retained rectangles. Following that, we use Dlib library's HOG [93, 94] based face detector as a second stage filter. Note that Dlib's face detector has higher accuracy comparing to OpenCV's face detector, but is much slower if applied directly on a high resolution image, therefore it is used as a filter on small rectangular areas. Dlib's facial landmarks detector [95] is also used in later face alignment stage, it can detect 68 facial landmarks [96, 97]. With the detected landmarks and required alignment condition about inputs to the CNN model, we can calculate the homography matrix that is finally used to align faces. The steps for detection and alignment is shown in Fig 4.6, and we implemented it as a JNI library for Android platform [98].

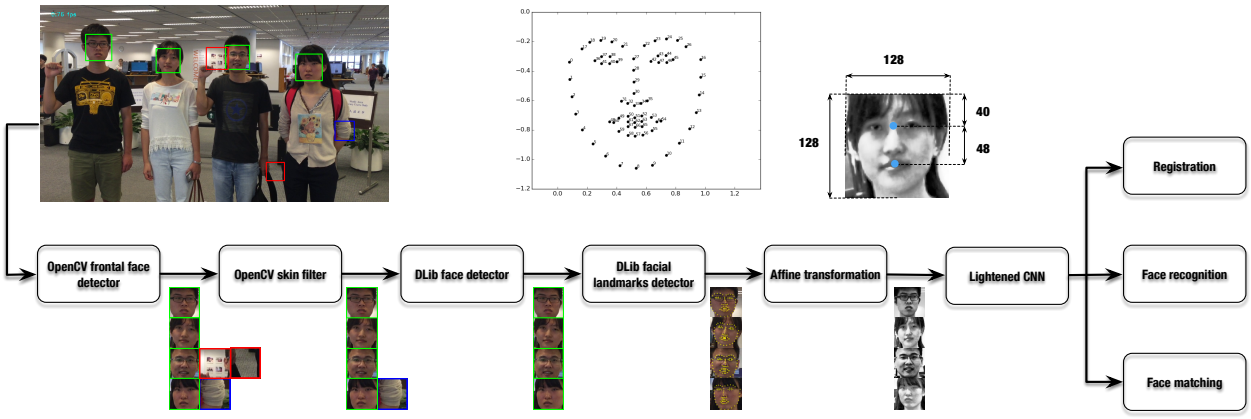


Figure 4.6: Face detection and alignment workflow.

Recognition

All the facial features uploaded by registered users are used to train a classifier in the cloud server, using LIBSVM library [99]. During prediction, we enable probability estimations $p_i, i \in 1, \cdots, N$, where p_i is the probability of being user i. For each facial feature, if $\max_i p_i \leq T_p$, then we treat it as from an unknown person who hasn't registered in Cardea, otherwise it is from the user who has the highest probability and his privacy preference will be fetched for further processing. Threshold T_p is an empirical parameter, a proper value of T_p makes sure registered users are recognized correctly, and non-registered bystanders are recognized as unknown person. It is dependant on the face database scale, but the proper value can always be found through cross validation.

Matching

Face matching occurs when a recognized user A has also specified and uploaded features of person B with whom he doesn't want to be captured, it is to determine whether B also appears in this captured image. Note that B is not necessarily a registered user of Cardea. It is required that n_B, the number of B's facial features uploaded by A should be more than 10. A simple way is pointing the camera on B's photo but from different angles. Then for every detected face C other than A in the image, its feature f_C will be compared with n_B features of B uploaded by A. `Cosine` similarity is used as distance metric. Among n_B distances between f_C and B's features, we can calculate the ratio r of distances which are shorter than a threshold T_d, if the ratio r is higher than a threshold T_r, then C and B are the same person, thus B appears with A in the same image and A's privacy will be protected. By tuning, we find $T_d \in (0.4, 0.6)$ and $T_r \in (0.4, 0.8)$ shows good enough performance. In Fig 4.7, we plot the distribution of distance between same person's Lightened CNN features and different person's Lightened CNN features. The features are extracted from all the faces in ORL face database [100], which consists of 400 images from 40 distinct subjects, 10 images per subject. Each subject has photos with different variations, such as: with/without glasses, open/closed eyes, and different facial expressions. It is obviously seen that distances between features of same person and features of different persons are well seprated, especially for the case of `cosine` similarity.

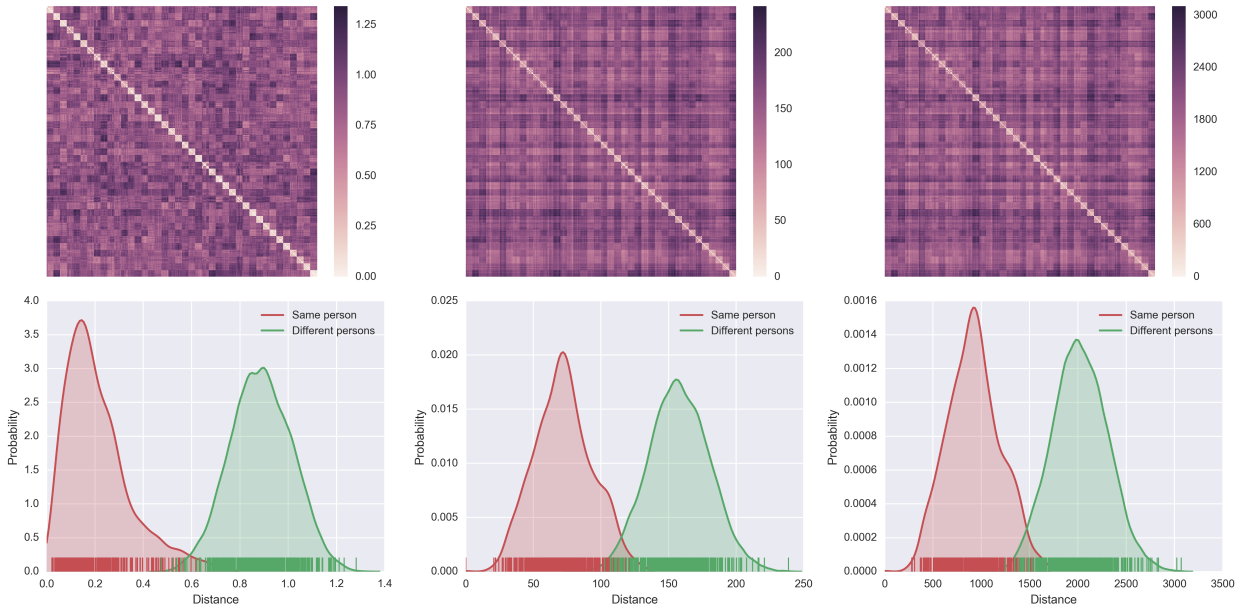


Figure 4.7: Distance matrix (top) and distance distribution (bottom) of Lightened CNN features using `cosine` similarity (left), l_1 norm (center) and l_2 norm (right).

4.2.3 Gesture Recognition

In Cardea, "yes" (✌) and "no" (✋) gestures have the highest priorities and are used to temporarily overwrite privacy preferences. To recognize gestures in real world images, the first step is detection of hands, and it turns out to be the most challenging part in this sub task. Skin color based hand detector will fail dramatically in images with cluttered background. A much more robust method will be using multiple proposals [101] based on hand shape, context, and skin color. However, it takes an extremely long time to detect hands in one image. Finally, we choose to use state-of-the-art detection framework faster R-CNN [77] to train a gesture detector in an end-to-end manner.

Data Preparing and Preprocessing

VGG group has shared a comprehensive dataset of hand images collected from various different public image data set sources in [101, 102]. It contains 5628 images, which is composed of 4069 training images, 738 validation images, 821 testing images respectively, each image is with annotations of hand bounding boxes. However, this dataset can only let us train a hand detector. To

achieve the goal of recognizing gestures, there are two solutions in our consideration:

- First train a hand detector using this dataset, then train another hand gesture classifier using other commonly used gesture datasets and pipe them together.
- Take this dataset as a subset of images with "natural" gestures, then prepare extra images with "yes" and "no" gestures including annotations by ourselves, and train a "natural/yes/no" gesture detector end-to-end.

The first solution is not an end-to-end solution, and the specific "yes" and "no" gestures may not be included in those standard gesture datasets, then we will still need to prepare our specific gesture dataset like in second solution. Therefore, we choose the second solution, based on the observation and also assumption that annotated hands in VGG's hand dataset are in natural relaxing modes, thus will not be treated as "yes" or "no" gestures. The annotations of VGG dataset are tilted rectangles shown as yellow ones in Fig 4.8, we re-annotate the dataset using bounding boxes of the original annotations shown as blue rectangles.

We crawled 527 images with "yes" hand gestures, and 363 images with"no" hand gestures. Note that in a crawled image, it may contain different types of hand gestures as shown in Fig 4.8, which is not a problem so long as gesture types are annotated correctly (*remind* that all gestures in VGG dataset are treated as "natural" class). These images are crawled from Google and Flickr image search with keywords such as "victory sign", "stop gesture", "palm gesture" and so on, many of them are focused on the hands thus don't contain many background pixels. We rescale these images in different scales and then pad zeros on rescaled images. In Faster-RCNN python implementation [103], an input image is rescaled to around 1000×1000 before fed to region proposal network. If without padding data augmentation step, the bounding boxes of hand gestures will be huge in many crawled images that are focused on hands, which makes the learned model not able to detect small hand gestures and also not perform well on the regression of large hand gestures. Another reason for the padding step is to counter data imbalance of three classes. After augmentation, we have a dataset of 13843 images, including 5628 images from VGG dataset, 4712 augmented images mostly with "yes" gestures and 3503 augmented images mostly with "no"

gestures. Fig 4.8 shows some sample images with annotations from this composed dataset. We wrote a tool [104] to annotate the crawled images.

Figure 4.8: Training hand gesture dataset composed of VGG hand dataset (top) and augmented crawled dataset (middle and bottom). Blue, red and green annotations denotes "natural", "no" and "yes" gestures.

Training Procedures

Using the composed dataset, we fine-tune the *conv3_1* and up layers of VGG16 pre-trained model provided by Faster-RCNN library, jointly with region proposal layers and detection layers that are not part of VGG16 pre-trained model. Features from *conv5_3* layer of VGG16 network are shared

between region proposal network (RPN) and Fast-RCNN [76] detection network, RPN uses them to generate proposals, and region of interest (ROI) pooling layer in detecting network uses them for bounding box regression and classification. There are two methods to train a shared feature extraction network. One is an alternating optimization method with following steps: ❶ Train an RPN M_1 initialized from VGG16 pre-trained model M_0, ❷ Generate training proposals P_1 using RPN M_1, ❸ Train Fast R-CNN model M_2 on proposals P_1 initialized from M_0, ❹ Train RPN M_3 from M_2 without changing convolutional layers, ❺ Generating proposals P_2 using RPN M_3, ❻ Train Fast R-CNN model M_4 on proposals P_2 initialized from M_3 without changing convolutional layers, ❼ Add M_3's RPN layers to Fast R-CNN model M_4. Another method is an approximate joint optimization method by training with stochastic gradient descent as usual, which is easier, faster and achieves similar performance [103], so we use the second training procedure.

Prediction

During prediction, we set Non-Maximum Suppression (NMS) threshold as 0.4 and confidence level threshold as 0.7. Figure 4.9 shows some examples of gesture detection and recognition results in natural environment. It can be seen that the trained model can handle cluttered background such as in shopping environment, and indoor dark lighting condition. It is interesting to notice that bounding boxes for "natural" hands are bigger, reflecting the fact that we select re-annotated the VGG dataset for "natural" class using bounding boxes of the original annotations. The model has a good recall in terms of hand detection, however, its gesture recognition is sensitive to motion blur, palm angles and gesture size. We think the good recall of hands comes from the comprehensive VGG dataset, and the not so good recognition result is because the "yes/no" dataset we composed does not have a good quality because gestures are focused in many images, especially for "no" gestures, which is reflected by the observation that "yes" gesture recognition performs better than "no" gesture.

Figure 4.9: Examples of gesture detection and recognition.

4.3 System Integration

4.3.1 Deployment on Android

Ideally, for a privacy control framework, we prefer a design that does not require cloud server and all the algorithms run locally on mobile devices. In the current design and implementation, cloud server exists mainly for two reasons: ❶ Storage center for profiles and hosting face recognition model; ❷ RPN in gesture recognition task is written in Python language, thus gesture recognition can not run on Android smartphones easily. However, these are not hard restrictions, possible improvements are discussed in Chapter 5.

The deployment of Caffe models for scene classification and facial feature extraction on smartphones is based on Caffe-android-library [105], we modified its code [106] to support loading multiple Caffe models, batch feature extraction, and only forwarding to a specified layer during feature extraction, which saves useless computations from fully connected layers. There are other libraries for deploying neural networks on mobile, such as Torch-android [107] and MXNet [108]. The de-

ployed scene classification model (based on AlexNet structure) has a size of 230MB, which is not small. However, its prediction is very fast, and can be easily fitted into the time slot when client is waiting response from cloud server. The facial feature extraction model (based on Lightened CNN structure) has a relatively bearable size of 33MB. Comparing to AlexNet, Lightened CNN model has smaller filter sizes, but with many more feature maps, therefore in run time, Lightened CNN model consumes about 1GB memory, which makes it not able to run on smartphones with less than 2GB memory as shown in Table 4.2. Possible ways to decrease model size and optimization of resource consumptions are also discussed in next chapter. Other lighter models we deployed on android include OpenCV face cascading model (less than 1MB) for face detection, and Dlib shape predictor (90MB) for facial landmarks detection.

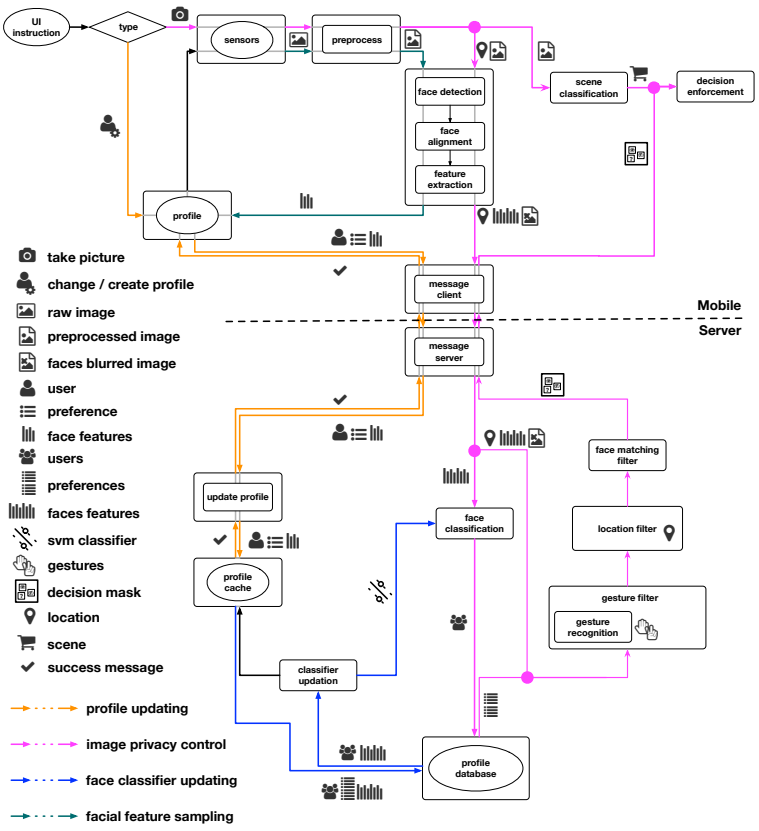
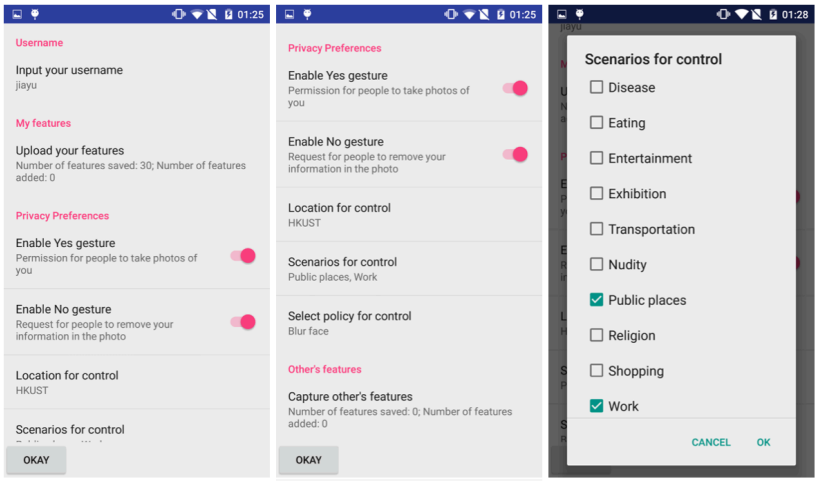


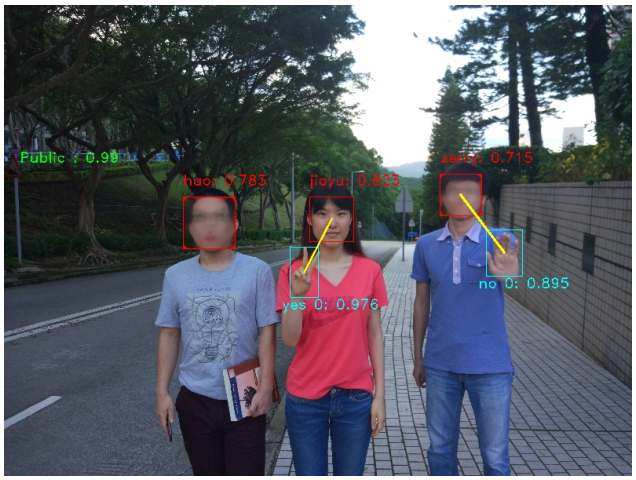
Figure 4.10: Dataflow of Cardea

4.3.2 Dataflow and Integration

Fig 4.10 shows the detailed structure and dataflow of Cardea, which is mainly composed of the following steps (a demo video about the usage can be found in [109]):



(a) Registration and profile updating interface



(b) Privacy protection example

Figure 4.11: Cardea user interface and privacy protection results. In (a), *jiayu* registers as a Cardea user by extracting and uploading her face features. She specifies HKUST, two scene groups for privacy protection. She also enables "yes" and "no" gestures. In (b), a picture is taken in HKUST. 3 registered users, one "yes" and one "no" gesture are recognized. The scene is correctly predicted as "Public". *jiayu*'s face is not blurred due to her "yes" gesture. Prediction probabilities are also shown in (b).

Registration and Profile updating: The interface provided to a bystander for registration and updating of his profile is shown in Fig 4.11a. He is able to select one or more scene categories, one location for control, as well as enable gestures or not. In two cases his facial features will be packaged with his privacy preferences: one is in registration time and the other is when he wants to update his facial features in the cloud. This registration and updating message will be send to server, if it is an updating message without feature updating, then his user profile in cloud will be updated immediately and he will receive a "success" notification, otherwise this message will be first buffered in a profile cache, and only after the next successful face classifier updating will he receive the "success" notification.

Face classifier updating: In the server, the face classifier will be updated intermittently. For every time interval ΔT, if there is cached messages that brings new facial features, it will ❶ block the

queue of prediction messages from doing face recognition, ❷ merge profile cache with profile database, ❸ retrain a face classifer and ❹ unblock queued prediction messages.

Image capturing: When a recorder uses Cardea to take a image, extracted facial features, GPS coordinate as well as face-blurred image will be packaged as prediction message and sent to server for processing. In the server side, after faces recognition and profiles retrieval, it will start the cloud part of decision making process for every face bounding box, after which what will be returned to the client side is a decision mask that specifies among all the detected faces, which should be blurred, which should be kept and which should be further determined based on the scene results calculated on the client side. In client side, while waiting for response from server it will calculate the scene result. With received decision mask, it makes final decisions on every face and enforces the privacy protection actions complied with everyone's preference.

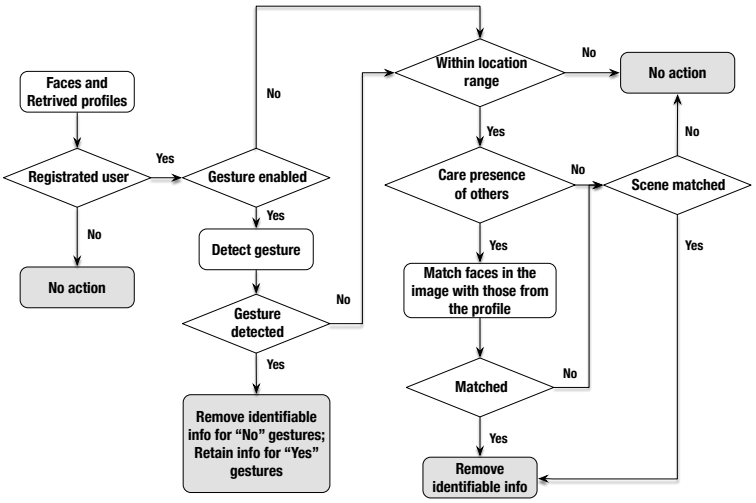


Figure 4.12: Steps of decisions about actions to be applied on detected faces.

Decision making: Fig 4.12 gives the detailed decision steps. Note that in this process, we need to match a detected gesture with the right face or people who issued the gesture, currently we simply take the nearest face of a detected gesture as the person who issued this gesture, thus it requires the user to put his hand near his face when sending "yes/no" gestures. As seen from the figure, when the detected face is recognized as a registered user, and context including location, scene, presence of other people and gesture matched with the user's profile, this detected face will be removed. An

example is shown in Fig 4.11b. For other cases, the face will be kept but it may cause removal of other faces in the face matching step.

Concurrent requests: To enable concurrent requests from different client apps, we implement multiple "recognition" workers to process the queued messages from all the clients, recognition results from different workers will be collected and put into a result queue, followed by multiple "mailing" workers to make decision masks and mail the decision masks back to corresponding blocked client threads. We tested with a server configuration - "Intel i7-5820K CPU, 16GB RAM, GeForce 980Ti Graphic Card(6GB RAM)" and the campus's Wi-Fi network, the time from start sending message to receive server's response is $1-2s$, depending on the message type. The total time from capturing moment to the enforcement of protection actions is $2-4s$, depending on how many faces detected. Most time is spent on facial feature extraction and message data transmission. Note that processing in the server side is relatively fast, gesture recognition of one image takes $200-300ms$, while the time spent on SVM face classifier and face matching is negligible. With 6GB GPU RAM, the server can serve 3 gesture recognition workers at the same time, supporting 5-10 concurrent requests. The implementation of Cardea is hosted in [110].

4.4 Evaluation

In this section, we present evaluation results along 3 axes:

1) ***vision micro–benchmarks***, to evaluate the performance of different computer vision tasks, including scene classification, face recognition and matching, and hand gesture recognition. Note that when doing this evaluation, based on the categories shown in Table 4.1, we modify the scene categories and groups (add more categories and remove few categories and regroup them) hoping that it would cover more daily scenes (e.g. "Exhibition" group is removed). After this modification, we have 9 groups composed of 98 categories (1.9 million images) shown in Table 4.3. We also retrain the scene classification model, and get 55% category validation accuracy and 83% group validation accuracy. **All evaluations in this section are based on this new scene classification model.**
2) ***system overall performance***, according to final privacy protection decisions and users' privacy preferences.

Table 4.3: Nine general scene groups

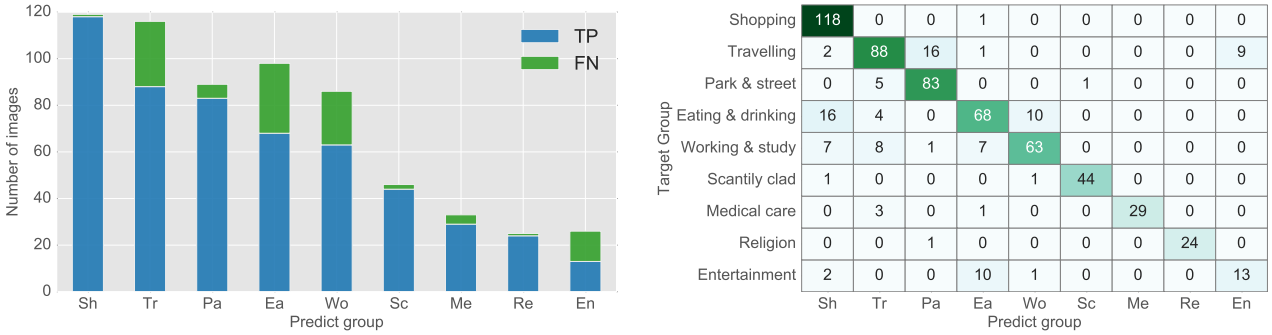
Group name	Abbreviatin	Scenes #	Examples
Shopping	Sh	20	clothing store, market, supermarket
Travelling	Tr	9	airport, bus station, subway platform
Park & street	Pa	12	downtown, park, street, alley
Eating & drinking	Ea	18	bar, bistro, cafeteria, coffee shop, fastfood restaurant, food court
Working & study	Wo	9	classroom, conference center, library, office, reading room
Scantily clad	Sc	12	beach, swimming pool, water park
Medical care	Me	2	hospital room, nursing home
Religion	Re	11	cathedral, chapel, church, temple
Entertainment	En	5	amusement park, ballroom, discotheque
All		*98*	

3) ***runtime and energy consumption***, which shows the processing time of each part, and energy consumed on one image.

4.4.1 Scene Classification

We recruited 8 volunteers and asked them to take pictures "in the wild" belonging to 9 general scene groups. After manually annotating these pictures, we had 759 images in total, with 638 images in 9 scene groups we are interested in. We then predict scene group for each image using the scene classification model we trained.

The number of images and classification result of each group are shown in Figure 4.13a. The true positives (TP) refers to images that are correctly classified, and false negatives (FN) are those classified as other scene groups. Overall, we can achieve 0.83 recall (TP/(TP+FN)), and 5 scene groups are with recall more than 0.90. It is worth mention that the recall of scene groups *Scantily clad (Sc)*, *Medical care (Me)*, and *Religion (Re)* exceed 0.95, which provides strong support to



(a) Recall **(b)** Confusion matrix

Figure 4.13: Scene classification evaluation results.

protect users' privacy in sensitive scenes.

We also give the detailed classification confusion matrix in Figure 4.13b. It shows that most FN of *Eating & drinking (Ea)* are classified as *Shopping (Sh)* or *Working & study (Wo)*, and most FN of *Wo* are classified as *Ea* or *Sh*. The reason is that boundaries between *Sh*, *Ea*, or *Wo* are not clear. For example, shopping malls have food courts, or people study in coffee shop. The same reason accounts for the confusion between *Park & street (Pa)* and *Travelling (Tr)*. Moreover, for scene categories such as pub and bar, people may group them into *Ea* or *En*. Therefore, a safe way is to select more scene groups, for instance, both *Ea* and *En* when you go to a pub at night.

In general, the evaluation results from images captured "in the wild" demonstrate that most of scenes can be correctly classified, the performance is especially satisfactory for those sensitive scenes.

4.4.2 Face Recognition and Matching

We first select 50 subjects from LFW dataset [111] who has more than 10 images as registered users. Note that subjects in the CASIA WebFace Database used to train the lightened CNN model do not overlap with those in LFW. For each subject, we extract at least 100 face features form Youtube video to simulate the process of user registration. In total, we get 5042 feature vectors. These features are then divided into the training set and validation set. In addition, we collect user test set and non–user test set to evaluate the face recognition accuracy. The user test set is

composed of 511 face feature vectors from online images of all 50 registered users. The non–user test set consists of 166 face feature vectors from 100 subjects in LFW database whose names start with "*A*" as non–registered bystanders.

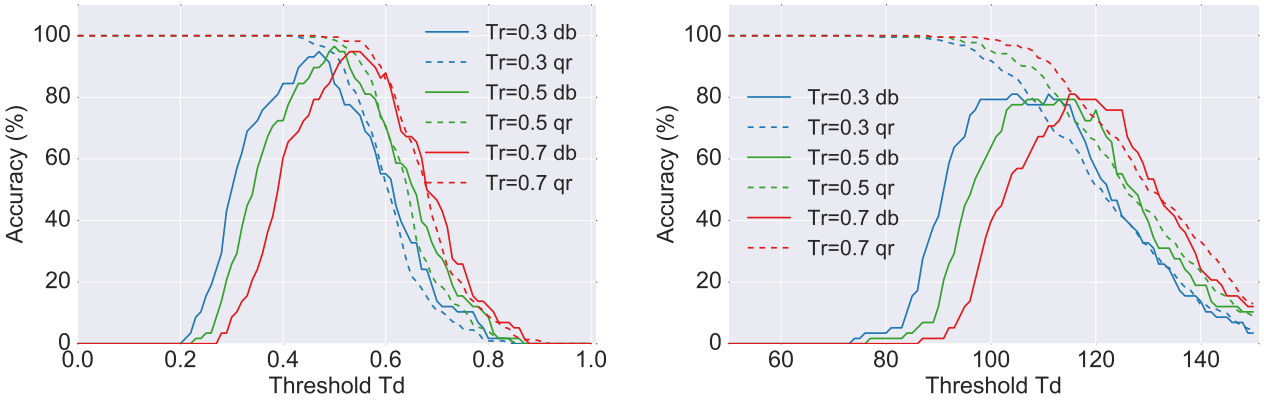
(a) Training accuracy

(b) Testing accuracy with threshold T_p

Figure 4.14: Face recognition accuracy.

Figure 4.14a shows the recognition accuracy as to validation set and user test set with different numbers of features per person used for training. The accuracy refers to the fraction of faces that are correctly recognized. The results show the model trained with $10 \sim 20$ features per person can achieve near 100% accuracy on the validation set and over 90% accuracy on the user test set. Little improvement can be achieved with more training data. Figure 4.14b shows the overall accuracy with probability threshold T_p. For non–user test set, the accuracy means the fraction of faces that are not recognized as registered users. As a result, the accuracy will increase for the non–user test set but decrease for the validation set and user test set when T_p goes up. To make sure that registered users can be correctly recognized, and non-registered users will not be mistakenly recognized, we choose T_p to be $0.08 \sim 0.09$, which achieves over 80% recognition accuracy for both users and non–users. It is worth mentioning that the proper value of T_p should be decided case by case through such experiment for different databases with different scales.

To evaluate face matching performance, we still use the user test set. Subjects who have more than 10 features are regarded as the database group, the rest are the query group. Similar to face recognition accuracy, we break face matching accuracy into two parts: for persons belonging to the database group, we need to correctly match features only to the correct person; for persons



(a) Cosine distance

(b) Euclidean distance

Figure 4.15: Face matching accuracy with different distance threshold T_d and ratio threshold T_r.

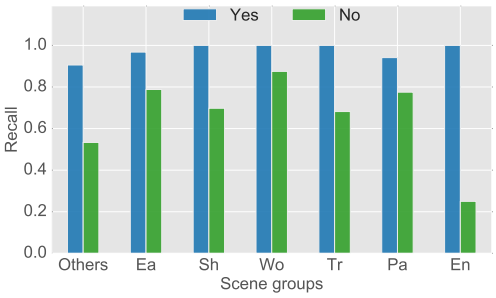
not belonging to the database group, we should not match features to anyone. Figure 4.15 shows the matching accuracy with Cosine distance and Euclidean distance respectively. The results show that Cosine distance can achieve better performance with near 100% accuracy for both situations in which people belong to the database group or the query group. The preferable parameters would be distance threshold $T_d \approx 0.5$, and ratio threshold $T_r \approx 0.5$.

Overall, the face recognition and matching methods we employ with appropriate thresholds T_p, T_d, and T_r can effectively and efficiently recognize users and match faces in the images. Besides, only a small number of features are needed for training the face recognition model and for face matching algorithm.

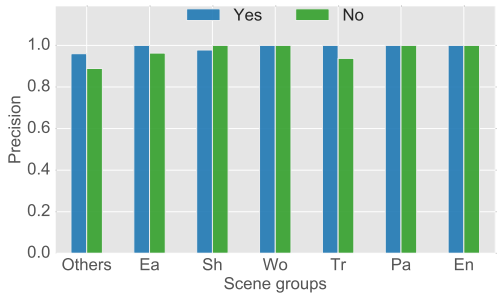
4.4.3 Gesture Recognition

We asked our volunteers to take pictures for each other with different distances, angles, lighting conditions, and backgrounds. We manually annotated all images with hand regions and the scene group it belongs to. In total, we got 338 hand gesture images with 208 "Yes" gestures, 211 "No" gestures, and 363 natural hands. The images covers 6 out of 9 scene groups. For images do not belong to our summarized scene groups, we categorize them into group *Others*.

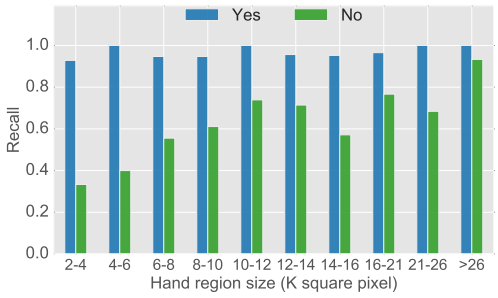
Figure 4.16a and Figure 4.16b show the recall and precision for "Yes" and "No" gestures under different scene groups. The recall and precision of "Yes" gesture, the precision of "No" gesture



(a) Recall for different scenes



(b) Precision for different scenes



(c) Recall for different hand region sizes

Figure 4.16: Hand gesture recognition results.

reach 1.0 for most of the scene groups, while the recall of "No" gesture achieves 0.70 on average. For *Entertainment (En)*, the recall is low, resulting from dim illumination in most of the images we tested. In general, the performance of gesture recognition does not show any marked correlation with different scene groups. Therefore, we further investigated the recall in terms of gesture size, as low recall will greatly threatens user's privacy compared with precision.

Figure 4.16c plots the recall of gestures with varying hand region sizes. Each image will be resized to about 800×600 square pixels, while keeping its aspect ratio. We classify them into 10 size intervals as plotted along the x–axis. The result shows "Yes" gestures can achieve more than 0.9 recall for all sizes of hand region. On the other hand, recall of "No" gestures tends to rise with increasing hand region size in general. It indicates that the performance of "No" gesture recognition can be improved with more training data with smaller sizes.

In summary, the performance of gesture recognition demonstrates the feasibility of integrating gesture interaction in Cardea for flexible privacy preference modification. It performs extremely well for "Yes" gesture recognition, and there is room for improvement of "No" gesture recognition with more training samples.

4.4.4 Overall Performance

After evaluating each vision task separately, we now present Cardea's overall privacy protection performance. Faces in the image taken using Cardea end up being protected (e.g., blurred) or remain unchanged, correctly or incorrectly, depending on protection decisions made based on both

Table 4.4: Cardea's overall privacy protection performance.

Overall accuracy	**86.4%**	Protection accuracy	80.4%
		No protection accuracy	91.0%
Face recognition accuracy	98.5%	"Yes" gesture recall	97.9%
scene classification recall	77.7%	"No" gesture recall	77.3%

user's privacy profile and results from vision tasks. Therefore, we asked 5 volunteers to register as Cardea users and set their privacy profiles. Now the face recognition model is trained using 1100 face feature vectors from 55 people, including 50 people from LFW dataset. We take about 300 images and get processed images. As we focus more on face recognition rather than face detection, we only keep images that faces have been successfully detected. In total we got 224 images for evaluation.

Table 4.4 shows the final privacy protection accuracy, as well as performance of each vision task. The protection accuracy shows 80.4% faces that require protection are actually protected, and 91.0% faces that do not ask for protection remain unchanged. Overall, 86.4% faces are processed correctly, though the scene classification recall and "No" gesture recall do not reach 80%. The reason is that protection decision making process of Cardea sometimes can make up for mistakes happening in the early step. For example, if user's "No" gesture is not detected, his face can still be protected when the predict scene is selected in user's profile.

In summary, Cardea achieves over 85% accuracy for users in the real world. Improvements of each vision part will directly benefit Cardea's overall performance in the future.

4.4.5 Runtime and Energy Consumption

We validate the client side implementations on Samsung Galaxy Note 4[1], with 4×2.7 GHz Krait 450 CPU, Qualcomm Snapdragon 805 Chipset, 3GB RAM, and 16 MP, f/2.2 Camera. The server side is configured with Intel i7–5820K CPU, 16GB RAM, GeForce 980Ti Graphic Card (6GB RAM). The client and server communicate via a TCP over Wi–Fi connection.

Figure 4.17 plots the time taken for Cardea to complete different vision tasks. We take images

[1] http://www.gsmarena.com/samsung_galaxy_note_4-6434.php

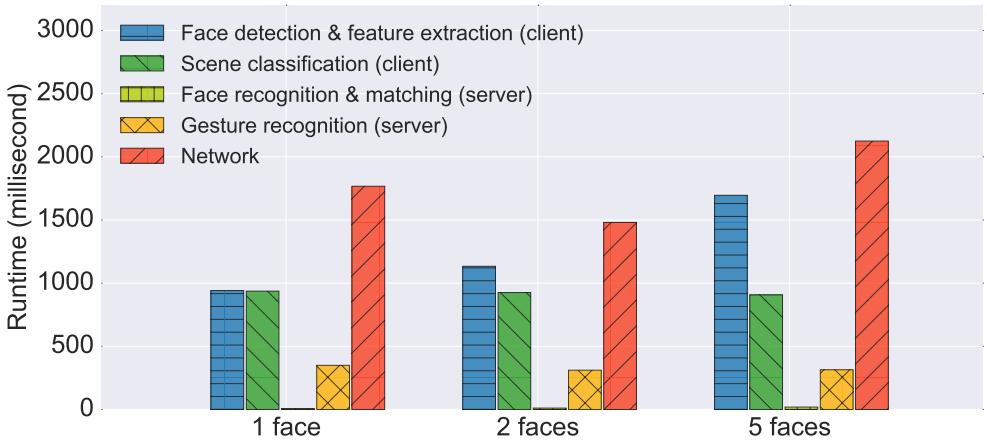


Figure 4.17: Task level runtime of Cardea.

with 1 face, 2 faces, and 5 faces, in the size of 1920×1080. The images will be compressed in JPEG format. On average, the data sent is about 950 KB. Note that some vision tasks will not be triggered in some situations according to the decision workflow shown in Fig 4.12. For example, if no user is recognized in the image, all other tasks will not start. For the purpose of measurement, we still activate all tasks to illustrate the runtime difference of images captured with varying number of faces.

Among all vision tasks, face processing (i.e., face detection and feature extraction) and scene classification are performed on the smartphone. The face processing takes about 900 milliseconds for 1 face, and increases about 200 milliseconds per additional face. Therefore, it reaches about 1100 and 1700 milliseconds for 2 faces and 5 faces respectively. This is the most fundamental step that runs on the smartphone locally due to privacy considerations. Owing to the real–time OpenCV face detection implementation and lightened CNN feature extraction model, it takes less then $1/3$ overall runtime. The scene classification takes around 900 milliseconds per image, as it only performs once, independent of number of people in the image. The face recognition and matching tasks on the server side take less than 30 milliseconds for five people. Though the time grows with increasing number of people, compared with other tasks they barely affect the overall runtime. The gesture recognition also runs on the server, and it takes about 330 milliseconds. Similar to scene recognition, it performs on the whole image once regardless the number of faces. According to the measurement, we find the network transmission accounts for a majority of the

Table 4.5: Energy consumption of Cardea with different number of faces.

	Face recognition	Whole process (uAh)	# of images
1 face	217.2 (std 3.4)	1134.5 (std 45.9)	~ 2800
2 faces	344.1 (std 13.1)	1276.7 (std 113.8)	~ 2500
5 faces	692.6 (std 36.5)	1641.1 (std 66.0)	~ 2000

overall runtime due to the unstable network environment.

In general, photographers using Cardea to take pictures can get one processed image within 5 seconds in the most heavy case (i.e., there is registered user who enables gestures, and scene classification will be triggered on the smartphone). Compared with existing image capture platforms that also provide privacy protection such as I-pic [20], Cardea offers more efficient image processing functionality.

Next, we measure the energy consumption of taking pictures with Cardea on Galaxy Note 4 phone using the Monsoon Power Monitor [112]. The images are also taken in size of 1920×1080 square pixels. The first two columns of Table 4.5 show the energy consumption for the face processing part only, and for the whole process (i.e., from taking a picture to getting the processed image) with 1 face, 2 faces, and 5 faces respectively. The screen stays on during the whole process, therefore a large portion of the energy consumption is due to the always–on screen. Moreover, we can observe that face processing energy is linear to face numbers. All the other parts including scene classification, sending and receiving data are independent of the number of faces in the image, which is consistent with runtime measurements.

Using energy measurements, we also show Cardea's capacity on Galaxy Note 4 in the last column of Table 4.5. This device has a 3220 mAh battery, therefore can capture about 2000 high quality images with 5 faces using Cardea.

CHAPTER 5

CONCLUSION AND FUTURE WORK

In this thesis we present Cardea, a visual privacy control service framework that aims to address individual's visual privacy issues caused by pervasive cameras. Users can express their privacy preferences in terms of location, scenes, and presence of others. Furthermore, "Yes" and "No" gestures can be used to temporarily modify users' privacy settings. The combination of context-dependent privacy profiles and interactive instructions provides a flexible and convenient way for individuals to control their visual privacy. We demonstrate performances of different vision tasks with pictures "in the wild", and overall it can achieve about 86% accuracy on users' requests. The evaluation of runtime and energy consumption with Cardea prototype proves the feasibility of using Cardea for taking pictures while respecting bystanders' privacy preferences.

Privacy itself is an abstract concept hence can not be hard coded if we are aiming at a smart and general control framework. We believe deep learning methods will be applied more and more on privacy control area, towards the direction of learning visual privacy concerns automatically using bigger and higher quality dataset available in the future. Based on Cardea's current design, implementation and evaluation, we propose the following future works for improvement:

- Recently there are many research works about neural network model compression [113], which points us a straight way to decrease the resources consumption, especially for Android client apps. Managing to deploy neural networks on mobile's GPU will save resources both in terms of RAM usage and computation, this requires Cuda or OpenCL implementation of related layers. Also during the forwarding time, activations of all layers are unnecessarily kept in memory for backpropagation which is not needed in deployment time, an implementation of forwarding phase that only keep previous layer's activation will largely reduce memory consumption, which is very important to mobile devices.

- The requirement of connection to the server makes Cardea easily hackable. An ad hoc approach that mobile devices broadcast owners' facial features as well as privacy preferences to nearby devices is possible if the RPN layer is implemented in C++, making gesture recognition runs locally. Another advantage of ad hoc solution is there will be no large scale face recognition problem, instead it becomes a small scale face matching/verification problem. We also consider using siamese network for better performance of face matching.

- Preparing larger and more comprehensive dataset for each task is definitely needed. Both scene classification model and gesture recognition model can benefit a lot if we are able to collect more daily life images with better labels or annotations. How to get supervised signals about visual privacy concerns from the design of user interactions is an interesting topic, integration of these interactions in life logging devices will provide high quality training dataset.

- As in [23], it is preferable to integrate Cardea within camera subsystems of different mobile platforms.

Bibliography

[1] *Number of surveillance cameras per thousand people by country*. URL: http://www.statista.com/statistics/484956/number-of-surveillance-cameras-per-thousand-people-by-country/.

[2] Heather Kelly. *iPhone photography is cool, eyeball photography is cooler*. URL: http://money.cnn.com/2016/05/12/technology/eyeball-camera-contact-sony.

[3] Tara Seals. *Popular Android Camera App Leaks Sensitive Data*. URL: http://www.infosecurity-magazine.com/news/popular-android-camera-app-leaks/.

[4] Ian Goodfellow Yoshua Bengio and Aaron Courville. "Deep Learning". Book in preparation for MIT Press. 2016. URL: http://www.deeplearningbook.org.

[5] Jiwon Kim. *Awesome Deep Vision*. URL: http://github.com/kjw0612/awesome-deep-vision.

[6] Yaniv Taigman et al. "Deepface: Closing the gap to human-level performance in face verification". In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2014, pp. 1701–1708.

[7] Yi Sun et al. "Deepid3: Face recognition with very deep neural networks". In: *arXiv preprint arXiv:1502.00873* (2015).

[8] Florian Schroff, Dmitry Kalenichenko, and James Philbin. "Facenet: A unified embedding for face recognition and clustering". In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2015, pp. 815–823.

[9] Tobias Weyand, Ilya Kostrikov, and James Philbin. "Planet-photo geolocation with convolutional neural networks". In: *arXiv preprint arXiv:1602.05314* (2016).

[10] Olga Russakovsky et al. "Imagenet large scale visual recognition challenge". In: *International Journal of Computer Vision* 115.3 (2015), pp. 211–252.

[11] Alessandro Acquisti, Ralph Gross, and Fred Stutzman. "Face recognition and privacy in the age of augmented reality". In: *Journal of Privacy and Confidentiality* 6.2 (2014), p. 1.

[12] Alison Spiegel. *Lost Lake Cafe, Seattle Restaurant, Kicks Out Patron For Wearing Google Glass*. URL: http://www.huffingtonpost.com/2013/11/27/lost-lake-cafe-google-glass_n_4350039.html.

[13] Jeremy Schiff et al. "Respectful cameras: Detecting visual markers in real-time to address privacy concerns". In: *Protecting Privacy in Video Surveillance*. Springer, 2009, pp. 65–89.

[14] Cheng Bo et al. "Privacy. tag: Privacy concern expressed and respected". In: *Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems*. ACM. 2014, pp. 163–176.

[15] Franziska Roesner et al. "World-driven access control for continuous sensing". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2014, pp. 1169–1181.

[16] Yann LeCun et al. "Gradient-based learning applied to document recognition". In: *Proceedings of the IEEE* 86.11 (1998), pp. 2278–2324.

[17] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. "In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies". In: *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM. 2014, pp. 2377–2386.

[18] Roberto Hoyle et al. "Privacy behaviors of lifeloggers using wearable cameras". In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM. 2014, pp. 571–582.

[19] Roberto Hoyle et al. "Sensitive lifelogs: A privacy analysis of photos from wearable cameras". In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM. 2015, pp. 1645–1648.

[20] Paarijaat Aditya et al. "I-pic: A platform for privacy-compliant image capture". In: *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (New York, NY, USA, 2016), MobiSys*. Vol. 16. 2016.

[21] Kenta Chinomi et al. "PriSurv: privacy protected video surveillance system using adaptive visual abstraction". In: *International Conference on Multimedia Modeling*. Springer. 2008, pp. 144–154.

[22] Jaeyeon Jung and Matthai Philipose. "Courteous glass". In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. ACM. 2014, pp. 1307–1312.

[23] Nisarg Raval et al. “What You Mark is What Apps See”. In: *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (New York, NY, USA, 2016), MobiSys*. Vol. 16. 2016.

[24] Mohammed Korayem et al. “Screenavoider: Protecting computer screens from ubiquitous cameras”. In: *arXiv preprint arXiv:1412.0008* (2014).

[25] Robert Templeman et al. “PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces.” In: *NDSS*. 2014.

[26] Suman Jana, Arvind Narayanan, and Vitaly Shmatikov. “A Scanner Darkly: Protecting user privacy from perceptual applications”. In: *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE. 2013, pp. 349–363.

[27] Suman Jana et al. “Enabling fine-grained permissions for augmented reality applications with recognizers”. In: *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*. 2013, pp. 415–430.

[28] J Alex Halderman, Brent Waters, and Edward W Felten. “Privacy management for portable recording devices”. In: *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*. ACM. 2004, pp. 16–24.

[29] *Tegra Processors*. URL: `http://www.nvidia.com/object/tegra.html`.

[30] *Tegra X1 Processor*. URL: `http://en.wikipedia.org/wiki/Tegra#Tegra_X1`.

[31] *Snapdragon 820 Processor*. URL: `http://en.wikipedia.org/wiki/List_of_Qualcomm_Snapdragon_devices#Snapdragon_820_and_821`.

[32] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton. “Deep learning”. In: *Nature* 521.7553 (2015), pp. 436–444.

[33] Feng-Hsiung Hsu. *Behind Deep Blue: Building the computer that defeated the world chess champion*. Princeton University Press, 2002.

[34] Donald Olding Hebb. *The organization of behavior: A neuropsychological theory*. Psychology Press, 2005.

[35] Frank Rosenblatt. “The perceptron: a probabilistic model for information storage and organization in the brain.” In: *Psychological review* 65.6 (1958), p. 386.

[36] David E Rumelhart, Geoffrey E Hinton, and Ronald J Williams. *Learning internal representations by error propagation*. Tech. rep. DTIC Document, 1985.

[37] Geoffrey E. Hinton, Simon Osindero, and Yee-Whye Teh. “A Fast Learning Algorithm for Deep Belief Nets”. In: *Neural Comput.* 18.7 (July 2006), pp. 1527–1554.

[38] Geoffrey E Hinton and Ruslan R Salakhutdinov. “Reducing the dimensionality of data with neural networks”. In: *Science* 313.5786 (2006), pp. 504–507.

[39] Yoshua Bengio et al. “Greedy layer-wise training of deep networks”. In: *NIPS*. 2007.

[40] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. “Imagenet classification with deep convolutional neural networks”. In: *Advances in neural information processing systems*. 2012, pp. 1097–1105.

[41] Karen Simonyan and Andrew Zisserman. “Very Deep Convolutional Networks for Large-Scale Image Recognition”. In: *CoRR* abs/1409.1556 (2014).

[42] Christian Szegedy et al. “Going deeper with convolutions”. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2015, pp. 1–9.

[43] Kaiming He et al. “Deep Residual Learning for Image Recognition”. In: *CoRR* abs/1512.03385 (2015).

[44] Pierre Sermanet et al. “Pedestrian detection with unsupervised multi-stage feature learning”. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2013, pp. 3626–3633.

[45] Clement Farabet et al. “Learning hierarchical features for scene labeling”. In: *IEEE transactions on pattern analysis and machine intelligence* 35.8 (2013), pp. 1915–1929.

[46] Camille Couprie et al. “Indoor semantic segmentation using depth information”. In: *arXiv preprint arXiv:1301.3572* (2013).

[47] Dan CireAn et al. “Multi-column deep neural network for traffic sign classification”. In: *Neural Networks* 32 (2012), pp. 333–338.

[48] David Silver et al. “Mastering the game of Go with deep neural networks and tree search”. In: *Nature* 529.7587 (2016), pp. 484–489.

[49] *AlphaGo versus Lee Sedol*. URL: `http://en.wikipedia.org/wiki/AlphaGo_versus_Lee_Sedol`.

[50] Volodymyr Mnih et al. “Playing atari with deep reinforcement learning”. In: *arXiv preprint arXiv:1312.5602* (2013).

[51] George Dahl, Abdel-rahman Mohamed, Geoffrey E Hinton, et al. “Phone recognition with the mean-covariance restricted Boltzmann machine”. In: *Advances in neural information processing systems*. 2010, pp. 469–477.

[52] Li Deng et al. “Binary coding of speech spectrograms using a deep auto-encoder.” In: Citeseer. 2010.

[53] Geoffrey Hinton et al. “Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups”. In: *IEEE Signal Processing Magazine* 29.6 (2012), pp. 82–97.

[54] Ilya Sutskever, Oriol Vinyals, and Quoc V Le. “Sequence to sequence learning with neural networks”. In: *Advances in neural information processing systems*. 2014, pp. 3104–3112.

[55] Dzmitry Bahdanau, Kyunghyun Cho, and Yoshua Bengio. “Neural machine translation by jointly learning to align and translate”. In: *arXiv preprint arXiv:1409.0473* (2014).

[56] Ian Goodfellow et al. “Generative adversarial nets”. In: *Advances in Neural Information Processing Systems*. 2014, pp. 2672–2680.

[57] Alec Radford, Luke Metz, and Soumith Chintala. “Unsupervised representation learning with deep convolutional generative adversarial networks”. In: *arXiv preprint arXiv:1511.06434* (2015).

[58] Alex Graves, Greg Wayne, and Ivo Danihelka. “Neural turing machines”. In: *arXiv preprint arXiv:1410.5401* (2014).

[59] Kelvin Xu et al. “Show, Attend and Tell: Neural Image Caption Generation with Visual Attention”. In: *Proceedings of The 32nd International Conference on Machine Learning*. 2015, pp. 2048–2057.

[60] Chris Olah and Shan Carter. *Attention and Augmented Recurrent Neural Networks*. 2016. URL: http://distill.pub/2016/augmented-rnns/.

[61] *CS231n: Convolutional Neural Networks for Visual Recognition.* 2015. URL: http://cs231n.github.io/.

[62] Kaiming He et al. “Delving deep into rectifiers: Surpassing human-level performance on imagenet classification”. In: *Proceedings of the IEEE International Conference on Computer Vision*. 2015, pp. 1026–1034.

[63] Ian J Goodfellow et al. “Maxout networks.” In: *ICML (3)* 28 (2013), pp. 1319–1327.

[64] *Neural Network Playground*. URL: http://playground.tensorflow.org/.

[65] Michael Nielson. *Neural Networks and Deep Learning*. 2016. URL: http://neuralnetworksandde
com/index.html.

[66] *PCA whitening*. URL: http://ufldl.stanford.edu/tutorial/unsupervised/
PCAWhitening/.

[67] Sergey Ioffe and Christian Szegedy. "Batch normalization: Accelerating deep network training by reducing internal covariate shift". In: *arXiv preprint arXiv:1502.03167* (2015).

[68] Nitish Srivastava et al. "Dropout: a simple way to prevent neural networks from overfitting." In: *Journal of Machine Learning Research* 15.1 (2014), pp. 1929–1958.

[69] Sebastian Ruder. *An overview of gradient descent optimization algorithms*. 2016. URL: http://ufldl.stanford.edu/tutorial/unsupervised/PCAWhitening/.

[70] James Bergstra and Yoshua Bengio. "Random search for hyper-parameter optimization". In: *Journal of Machine Learning Research* 13.Feb (2012), pp. 281–305.

[71] Jasper RR Uijlings et al. "Selective search for object recognition". In: *International journal of computer vision* 104.2 (2013), pp. 154–171.

[72] Dumitru Erhan et al. "Scalable object detection using deep neural networks". In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2014, pp. 2147–2154.

[73] C Lawrence Zitnick and Piotr Dollr. "Edge boxes: Locating object proposals from edges". In: *European Conference on Computer Vision*. Springer. 2014, pp. 391–405.

[74] Ross Girshick et al. "Rich feature hierarchies for accurate object detection and semantic segmentation". In: *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2014, pp. 580–587.

[75] Kaiming He et al. "Spatial pyramid pooling in deep convolutional networks for visual recognition". In: *European Conference on Computer Vision*. Springer. 2014, pp. 346–361.

[76] Ross Girshick. "Fast r-cnn". In: *Proceedings of the IEEE International Conference on Computer Vision*. 2015, pp. 1440–1448.

[77] Shaoqing Ren et al. "Faster R-CNN: Towards real-time object detection with region proposal networks". In: *Advances in neural information processing systems*. 2015, pp. 91–99.

[78] *Places2 Dataset Project*. URL: http://places2.csail.mit.edu/index.html.

[79] *Release of Places365-CNN*. URL: http://github.com/metalbubble/places365.

[80] Ali Sharif Razavian et al. “CNN features off-the-shelf: an astounding baseline for recognition”. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*. 2014, pp. 806–813.

[81] Jason Yosinski et al. “How transferable are features in deep neural networks?” In: *Advances in neural information processing systems*. 2014, pp. 3320–3328.

[82] *Caffe*. URL: `http://caffe.berkeleyvision.org/`.

[83] Yangqing Jia et al. “Caffe: Convolutional Architecture for Fast Feature Embedding”. In: *arXiv preprint arXiv:1408.5093* (2014).

[84] Erjin Zhou et al. “Extensive facial landmark localization with coarse-to-fine convolutional network cascade”. In: *Proceedings of the IEEE International Conference on Computer Vision Workshops*. 2013, pp. 386–391.

[85] Brandon Amos, Bartosz Ludwiczuk, and Mahadev Satyanarayanan. *OpenFace: A general-purpose face recognition library with mobile applications*. Tech. rep. CMU-CS-16-118, CMU School of Computer Science, 2016.

[86] *Torch7*. URL: `http://torch.ch`.

[87] Omkar M Parkhi, Andrea Vedaldi, and Andrew Zisserman. “Deep face recognition”. In:

[88] Xiang Wu, Ran He, and Zhenan Sun. “A Lightened CNN for Deep Face Representation”. In: *arXiv preprint arXiv:1511.02683* (2015).

[89] Laurens van der Maaten and Geoffrey Hinton. “Visualizing data using t-SNE”. In: *Journal of Machine Learning Research* 9.Nov (2008), pp. 2579–2605.

[90] Mostafa Mehdipour Ghazi and Hazim Kemal Ekenel. “A Comprehensive Analysis of Deep Learning Based Representation for Face Recognition”. In: *arXiv preprint arXiv:1606.02894* (2016).

[91] *OpenCV*. URL: `http://opencv.org`.

[92] Paul Viola and Michael Jones. “Rapid object detection using a boosted cascade of simple features”. In: *Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on*. Vol. 1. IEEE. 2001, pp. I–511.

[93] *Dlib C++ Library*. URL: `http://dlib.net`.

[94] Navneet Dalal and Bill Triggs. “Histograms of oriented gradients for human detection”. In: *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR’05)*. Vol. 1. IEEE. 2005, pp. 886–893.

[95] *Real-Time Face Pose Estimation*. URL: http://blog.dlib.net/2014/08/real-time-face-pose-estimation.html.

[96] *Dlib facial landmarks*. URL: http://openface-api.readthedocs.io/en/latest/openface.html.

[97] *Dlib facial landmark coordinates*. URL: http://openface-api.readthedocs.io/en/latest/_modules/openface/align_dlib.html.

[98] *Face alignment JNI library*. URL: http://github.com/ZhengRui/FaceAlignmentJNI.

[99] Chih-Chung Chang and Chih-Jen Lin. "LIBSVM: a library for support vector machines". In: *ACM Transactions on Intelligent Systems and Technology (TIST)* 2.3 (2011), p. 27.

[100] *ORL face database*. URL: http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html.

[101] Arpit Mittal, Andrew Zisserman, and Philip HS Torr. "Hand detection using multiple proposals." In: Citeseer.

[102] *VGG: Hand dataset*. URL: http://www.robots.ox.ac.uk/~vgg/data/hands/index.html.

[103] *Faster-RCNN (Python Implementation)*. URL: http://github.com/rbgirshick/py-faster-rcnn.

[104] *Image annotation tool*. URL: http://github.com/ZhengRui/ImgAnnotaPyQt4.

[105] *Caffe Android Library*. URL: http://github.com/sh1r0/caffe-android-lib.

[106] *Caffe Android Library (Clone)*. URL: http://github.com/ZhengRui/caffe-android-lib.

[107] *Torch-7 for Android*. URL: https://github.com/soumith/torch-android.

[108] *MXNet on Mobile Device*. URL: http://mxnet.readthedocs.io/en/latest/how_to/smart_device.html.

[109] *Cardea demo video*. URL: http://drive.google.com/file/d/0B4z8qjK8O_uUc0o2RjZWYktiMTg/view.

[110] *Cardea project*. URL: https://github.com/ZhengRui/cardea.

[111] *LFW dataset*. URL: http://vis-www.cs.umass.edu/lfw.

[112] *Monsoon Power Monitor*. URL: http://www.msoon.com/LabEquipment/PowerMonitor.

[113] Song Han, Huizi Mao, and William J Dally. “A deep neural network compression pipeline: Pruning, quantization, huffman encoding”. In: *arXiv preprint arXiv:1510.00149* (2015).