Chapter 2

2.1 Introduction

In this chapter, an in-depth discussion on the current strides reached in the world of E- Commerce and facial recognition system for payments would be made. A discussion of existing literature on already implemented facial recognition payment systems would also be presented with much emphasis on their strengths and weaknesses. This chapter will also touch on the general disadvantages of a facial recognition system, which clearly are privacy issues. This chapter will also consider the technologies that an efficient facial recognition system is built on.

Chapter 2.1 will discuss existing literature on the work others have done on or by using facial recognition technology.

Chapter 2.2 will highlight on Deep Learning and its algorithms, which is basically the baseline technology for bio-metric systems such as facial recognition and detection systems.

In Chapter 2.3, will present a summary of this chapter, in addition to evaluation of the pros and cons of the reviewed works.

2.2 Review Of Related Works

2.2.1 FACIAL RECOGNTION IN CHINA

China is one country that has made a broad headway into the advancement, execution and practice

of facial recognition technology.

FRT development is a major part of “Face++” which is used to make payments on one of the most used Ecommerce websites “Alibaba”. Some of the advances of Facial Recognition in China are as follows: On September 1, 2017, Alipay rolls out world’s first ‘Smile to Pay’ facial recognition system at KFC restaurant outlet in Hangzhou successfully used FRT to pay for meals that are being bought at the restaurant without the use of physical cash or credit card[2]; also, in an agreed upon experiment has extended its “Smile-to-Pay” facial recognition payment system to more than 300 KFC locations across the country, as it continues to roll out digital technologies to improve customer experiences, growth, and operational efficiency.[3] The joint venture between **China Duty Free Group (CDFG)** and **Lagardère Travel Retail** – **CDF-Lagardère** – has introduced facial recognition payment into its Duty Zero by CDF stores at **Hong Kong International Airport (HKIA)**.

The Dragonfly POS devices, self-developed biometric technology from **Alipay**, started operating at the airport on 2 April after the software was previously introduced at more than 300 cities in mainland China.

The Duty Zero by CDF liquor and tobacco stores are the first in Hong Kong to feature the software, which is designed to enhance the consumer shopping experience for Chinese consumers. The Dragonfly POS devices are placed next to the checkout, customers input their phone number and face towards the camera; the software then completes the transaction in just a few seconds.[4].Chinese multi-purpose messaging app WeChat introduced a new payment [device](https://pay.weixin.qq.com/wiki/doc/wxfacepay/product/qingwa.html#%E4%BA%A7%E5%93%81%E6%A6%82%E8%BF%B0) on August 27 named the “Frog Pro” at the Chongqing Smart China Expo in an effort to upgrade its offline payments. The new point-of-sale (POS) machine allows customers to pay using facial recognition .By rolling out a device equipped with more advanced facial recognition technology, users can enjoy an even more convenient method of paying for goods and services without using smartphones. According to Tencent, the developer of WeChat, the advanced facial recognition technology used will be safer, quicker and more convenient overall.[5]

Chinese facial recognition companies have taken the lead in helping this growing international market not least because of the advantage they have over peers in other countries: a massive domestic market and an authoritarian system where privacy often takes a back seat. According to IHS Markit, China accounted for nearly half of the global facial recognition business in 2018. The widespread use of facial recognition in China is in part a reflection of how many activities already require real-name identification. Face scans have replaced or augmented human identity checks in hotels, boarding flights and trains, and at banks and hospitals. Regulations, which came into effect this week, require telecom carriers to scan the faces of users registering for mobile phone services. But facial recognition is also being used to extend surveillance in new ways, such as tracking the classroom behavior of students. The country’s rapidly expanding network of facial-recognition cameras means many people are now subject to mass identification. China’s police force already holds the world’s biggest national database of over 1bn faces, captured for the national ID card system. Depending on the quality of these photos, they can be matched to people posing for a face scan.[1]

**2.2.2** **Facial Recognition Technology In Anti-Spoofing Attacks**

It is clear that face recognition systems based on 2D and 3D images can be exposed to spoofing attacks. Researches have proved that they are analyzing these attacks in terms of descriptors and classifiers. Descriptors were categorized as texture, motion, frequency, color, shape or reflectance and classifiers are organized as a discriminant, regression, distance metric or heuristic.[6] Counter-spoofing methods addressing such attacks go under the general term of **liveness detection**. The purpose of liveness detection is to detect whether a face is “alive” or just a fraudulent reproduction. There are two main approaches to liveness detection – active and passive. The active approach requires users to prove their “liveness” by interacting with the system. Passive liveness detection is invisible to the end user because it requires no action on their side.[7] Active face liveness detection is interactive. The system asks the person in front of the camera to perform a few simple actions. For example, they could be asked to blink, smile, nod, etc. Those actions are randomized for additional security. The person must complete all actions successfully – only then are they “recognized”.[7] Active face detection provides strong protection against spoofing but it requires interaction from the user so it might not be a good fit for some use cases. For example, you probably wouldn’t be too happy if you had to perform a set of actions each time you wanted to unlock your smartphone. To ensure a faster and more convenient protection against spoofing, passive liveness detection is used.[7]

**2.2.3 FACIAL RECOGNITION TECHNOLOGY FOR PAYMENT**