PRIVACY PRESERVATION USING MACHINE LEARNING

MAJOR PROJECT

Submitted in the Partial Fulfilment for the Requirement for the Award of the Degree of

Bachelor of Technology

in

Computer Science and Engineering

Submitted by:

Abhishek Panda (2k21/CO/19)

Pranay Avnish Kachhap (2k21/CO/338)

Pritesh Das (2k21/CO/348)

Under the supervision of

Dr. Nipun Bansal

Assistant Professor

Department of Computer Science and Engineering

Delhi Technological University

(Formerly Delhi College of Engineering)

Bawana Road, Delhi-110042

May 2025

Department of Computer Science and Engineering

Delhi Technological University
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

Candidate's Declaration

We, Abhishek Panda (2k21/CO/19), Pranay Avnish Kachhap (2k21/CO/338) and Pritesh Das (2K21/CO/348), students of B. Tech (Computer Science and Engineering), hereby declare that the project Dissertation entitled "Privacy preservation using Machine Learning", is submitted by us to the Department of Computer Science and Engineering, Delhi Technological University, Delhi in partial fulfilment for the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma, Associateship, Fellowship or other similar title or recognition.

Place: New Delhi
Date:

Abhishek Panda (2k21/CO/19)
Pranay Avnish Kachhap (2k21/CO/338)
Pritesh Das (2k21/CO/348)

Department of Computer Science and Engineering

Delhi Technological University
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

Acknowledgement

We thank GOD almighty for guiding us throughout the semester. We would like to thank all those who have contributed to the completion of our major project and helped us with valuable suggestions for improvement. We are grateful to Dr. Nipun Bansal, Assistant Professor, Department of Computer Science and Engineering, and all the staff of Computer Science and Engineering Department for providing us with the best facilities and atmosphere for the creative work, guidance, and encouragement. We have been extremely lucky to have a supervisor who responded to our questions and queries so promptly. Above all we would like to thank our parents without whose blessings we would not have been able to accomplish our goal.

Place: New Delhi
Date:

Abhishek Panda (2k21/CO/19)
Pranay Avnish Kachhap (2k21/CO/338)
Pritesh Das (2k21/CO/348)

Department of Computer Science and Engineering

Delhi Technological University
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

Certificate

I hereby certify that the Project Dissertation titled "Privacy Preservation using Machine Learning" which is submitted by Abhishek Panda (2k21/CO/19), Pranay Avnish Kachhap (2k21/CO/338) and Pritesh Das (2k21/CO/348), Computer science and Engineering, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of the degree of Bachelor of Technology, is a record of the project work carried out by the students under my supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: New Delhi
Date:

Dr. Nipun Bansal
Assistant Professor

TABLE OF CONTENTS

ABSTRACT

Individualised online marketing requires taking a stand regarding legal laws and user privacy. Although laws and regulations have arisen to strengthen individuals' rights to privacy and data control, the subject is still perceived as complex. This study aims to investigate consumers' experiences regarding privacy and personal data for marketing purposes. The aim is to gain an insight into how users assess the value of the positive aspects of internet use, concerning the concerns linked to protecting personal data. Researchers of the study will research which factors impact consumers than they are sharing their personal data. The widening spread of image manipulation technology paves a way for falsification of information in sectors ranging from journalism and forensic analysis to digital media. Spotting those kinds of manipulation is vital to maintaining authenticity of pictures we see. This study aims to resolve one of the major challenges, namely, the detection of image manipulation by developing a new Convolutional Neural Network (CNN) architecture. The implemented CNN model is formed of five convolutional layers which is followed by two fully connected layers. The same model is implemented using DCGAN augmented data and later on the accuracy of both the developed methods is compared. Although our model has less than 4 million parameters, it tends to perform superior to numerous well established CNN networks models.

LIST OF FIGURES

LIST OF ABBREVIATIONS

GDPR: General Data Protection Regulation

EU: European Union

OBA: Online Behavioral Advertising

AI: Artificial Intelligence

ML: Machine Learning

FRT: Facial Recognition Technology

DNA: Deoxyribonucleic Acid

UK: United Kingdom

US: United States

UN: United Nation

DPIA: Data Protection Impact Assessment

CNN: Convolutional Neural Networks

GAN: Generative Adversarial Network

CHAPTER-1

INTRODUCTION

The section presents existing research on personal data and marketing. The problem discussion, purpose and research question are also presented.

1.1 BACKGROUND

The Swedish Personal Data Act (1998:204) was established in 1998 and had the purpose of protecting personal integrity. The purpose of the law was to protect people so that their integrity is not violated when processing personal data. For 20 years, the same legislation applied despite changes regarding the internet and digitalization being in full swing. In 2018, the law was repealed by (2018:218) the Act on Supplementary Provisions to the EU General Data Protection Regulation (GDPR). The law was added so that the user himself would have the opportunity to control and regulate the disclosure of his personal information. GDPR began to impose new requirements where companies needed to inform the user about how they collected and processed personal data. This has led to an increasing number of notifications and consent processes from websites where the user can see how their personal data will be processed [1].

For the 90s generation, digitalization has been a natural part of their upbringing. They had to quickly adapt to the new technology and became familiar with digital tools and platforms in a different way than previous generations.

The generation grew up in a world where everything was about marketing, and not only private companies but also governments and schools have been active in marketing themselves. The digital world opened up new opportunities in marketing and introduced new strategies and methods that were previously not possible. The 90s have had the privilege of being part of this changing marketing world from the beginning, which has meant that they have developed a natural habit and understanding of technology and its use in marketing contexts [2]. Digitalization has dramatically changed the existence of

marketing. Through digitalization, it has enabled personalized marketing through the customer's own behavioural patterns [3].

A study shows that digital assistants such as Siri and Alexa bring high customer satisfaction where apps and Artificial Intelligence are interconnected. According to [4], digital assistants are speech-activated with Artificial Intelligence, which makes the apps dynamic by learning the customer's personal preferences with the help of data collection. The digital services are multifaceted and include complex technology, which means that the functions can be adapted to individuals. Despite high customer satisfaction, the study shows that more and more customers are concerned about their personal data being misused or compromised.

Companies must be transparent and have an understanding that personal data can be misused regardless of whether it is unintentional [4].

Consent standards have been developed to an ever-increasing extent through the progressive digital world. In order for the consumer themselves to have the opportunity to determine and influence the sharing of personal data, consent forms are often used in the form of cookies.

Cookies are an essential function for enabling smooth use of websites. They work by saving information, which means, for example, that the user does not have to log in and out every time they visit a website. In addition, cookies can store information about previous searches or pages viewed. An important aspect is that it should be as easy for a visitor to accept as to waive consent standards. If a person chooses not to give their consent, there should be some form of minimum service that allows the visitor to use certain parts of the website [5].

GDPR has established guidelines for protecting private information that is collected. The goal is to provide clear messages that collection is done through acceptance, allowing consumers to choose for themselves whether they want to allow such collection. A study has shown that several websites limit consumers' choices when it comes to information collection, which means restrictions and disclosure of choices for consumers [6].

1.2 PROBLEM DISCUSSION

There are laws for regulating personal data, which look different for different countries, and the definition of personal data also differs [7]. This project will therefore choose to define the concept based on the European Commission.

“Personal data is any information relating to an identified or identifiable living individual. Various pieces of information which together can lead to a specific person being identified also constitute personal data.” [8]. Examples of personal data are name, home address, e-mail, location information, cookies and advertising identification on the phone. Information that creates an identity such as one’s digital footprints is included in personal data. Location information is a category of personal data, which includes the collection of data about which geographical area an individual is in.

There are personal data that should only be collected through the user’s consent so that people themselves have the opportunity to regulate their own personal data. This is because tracking cookies can target behavioural advertising, create web analytics, third-party cookies and take data for the purpose of conducting marketing studies [8]. There are regulations and laws that are intended to protect the individual’s personal data, on the other hand, there is a problem with the legislation that regulates the processing of personal data.

There is room for interpretation, which has made consent processes difficult and made it difficult for customers to absorb the information [9]. The researchers of this study therefore want to see whether consumers feel that laws and regulations protect their personal data.

Several studies have been conducted on the views and beliefs of customers and private individuals about the collection of data online. A study conducted by Smit [10] shows that 58.9% of respondents had the belief that organizations were not allowed to collect data on OBA (individuals' internet behaviour with the aim of making marketing more efficient), which is false. The study also showed that users were very concerned about their privacy online and, above all, about how their personal data was at risk of being misused by organizations.

At the same time, the same study showed that respondents rarely refused to collect cookies. Despite this being their biggest concern. Similar to this study, researchers [11] conducted a study on how easy it is to get customers to share their personal data with companies. The researchers investigated this by analysing customers' behavioural patterns when faced with a choice between two identical products from different companies.

The first company offered the product at a lower price but required more personal data from the customer compared to the second company that sold the same product at a higher price. The difference in product prices was only one euro. Despite this, 39 out of 42 participants chose the cheaper product, in exchange for sharing more personal data. Digitalization has made personalized marketing possible, which has become a popular marketing strategy, as it is possible to target specific target groups.

Collecting personal data means that consumers are given more choice and competitive prices that they would not otherwise have discovered [12]. [13] describe how general advertising can make the customer feel distant. Therefore, personalized marketing can be a profitable strategy, but the challenge is to understand how willing consumers are to share their personal data. Therefore, it may be relevant to investigate the consumer's own perception of what influences their decision to share their personal data. As well as investigate what attitude consumers have towards personalized marketing in terms of collecting their own personal data.

[14] concluded that consumers still avoid shopping online because they feel that too much personal data is collected about them. Their study thus showed that the collection of personal data through cookies is negative for the development and efficiency of digital online marketing. The researchers also report results that the respondents in the survey considered the collection of cookies to be unethical and that it increases the risk of their identities being stolen.

Despite this, the [15] shows statistics on Swedes' use of social media, and their latest statistics, published in their report, are based on figures collected in 2021. Shows that 96 percent of Swedes born in the 1990s use some social media every day. Social media refers to the digital platforms used to communicate and share material with other users. In addition to social media, they use the internet to read news, play games or as a tool

for daily tasks. An example of how important the internet is to be able to carry out daily tasks in an easy way is BankID, which is a digital identification service when contacting companies or authorities. In total, the report shows that 100 percent of Swedish 90s people use the internet on some type of device, every day.

The Internet Foundation's [15] report presented statistics that 81 percent of the Swedish population limited their internet use because they wanted to protect their privacy, and that 50 percent limited themselves because they felt unsafe with digital internet services. The report also showed that 80 percent of the population did something active to protect their privacy when using internet-based services. Those who acted actively to protect their privacy on the internet were mainly the younger half of the population, where 90s people dominated in percentage terms when it came to limiting their data distribution on e-platforms.

64 percent of the group chose not to share location information, while 54 percent chose not to give apps access to use the microphone and 49 percent chose not to give internet-based platforms access to their contacts. When it came to choosing to share cookies on digital platforms, 39 percent opted out of sharing cookies. [16] described that today's consumers are more informed about what their data is used for than they have been in the past.

The author argued that consumers have not only increased their understanding of data collection but have also become smarter and more involved in sharing their personal data. [16] exemplified that some consumers today are having a dialogue about how they should be able to sell their data and at what price. Based on the studies, there was concern from users that their personal data would be exploited.

Despite this, many approved that their personal data would be shared to gain access to different platforms through social media or to gain access to websites. [7] argued that there are reasons for how consumers choose to view their own personal data. They argued that personal data can be seen as a tradable asset as it creates added value for both consumers and companies. Studies indicate that consumers have a strong sense of integrity but a low level of knowledge about the collection of data online that is then used in marketing [17]. This means that there are factors that influence consumers'

opinions, but it is not clear which factors consumers themselves perceive as driving the decision-making process.

The problem is consistently at a societal level where all internet users are affected. This study is aimed at the target group that wants to understand consumers' reasoning and their attitude regarding the collection of personal data.

This study can contribute to understanding how a young generation that has grown up with the internet and is used to their digital footprints always being part of their personal data. The respondents' perceptions based on their experiences will be able to help companies with their marketing work. Companies will gain insight into what consumers may see as the benefits and risks of personal data and integrity, which means that companies will be able to work proactively with the help of this knowledge. In addition to benefits and risks, consumers' knowledge, trust and perceived control will be sought to map out a perception of how the different factors affect the consumer when making decisions.

Studies have shown that there are concerns related to sharing their personal data, but despite this, consumers continue to share their data. Consumers are aware that personal data is being collected but do not always understand the implications of the collection. Despite this, it is common for consumers to accept sharing their personal data in order to gain access to websites, services or targeted advertising. A privacy problem is that consumers experience that their personal data is being misused, despite this, personal data is shared to a fairly high extent.

Various things are important in the decision-making process for the consumer to be willing to share their own personal data. The collection can entail advantages for the consumer, which means that they choose to share their personal data, but how much does it affect the disadvantages and can the disadvantages make the consumer not want to share their personal data.

This study will also contribute to implement Machine Learning models with high accuracy in order to protect the personal data, so that these models can be used by the companies handling big private data for making their privacy protection system stronger.

1.3 PURPOSE

1. This study aims to gain a broader understanding of consumers' experiences and experiences regarding the sharing of personal data for marketing purposes.

2. The aim is to gain insight into how users assess the value of the positive aspects of internet use, in relation to concerns related to the protection of personal data.

3. To ensure effective privacy protection through machine learning, thematic codes will be developed to guide the design and implementation of six distinct models. These thematic codes will represent key privacy-related concerns.

4. To explore the use of Convolutional Neural Networks (CNNs) as a powerful tool for image manipulation detection. To fulfil this goal, CNN will be used to extract the complex features from the images that will lead to the development of a simple yet effective CNN structure for image manipulation detection.

CHAPTER-2

THEORY

The section presents theory through value words and important themes, which have been developed through the theoretical mapping, which led to a theoretical model.

2.1 KNOWLEDGE

The authors [18] investigated consumers' online behavioural patterns, in relation to their privacy preferences.

The authors believed that consumers' choices about which personal data they want to share should be consistent with the actual results of shared personal data. At the same time, the authors identified that there is a discrepancy where the actual sharing of personal data does not match what the consumer wishes to share.

Acquisti [18] identify the psychological factors that lead to the discrepancy. The authors stated that internet users tend to make decisions about how much and which personal data they will share online, based on what other users choose to share. Acquisti [18] also identified that the human brain tends to settle into an acceptance when it perceives a serious problem as difficult to solve. This acceptance then results in the user overlooking the problem and the possible fear of being offended.

A well-established term for personalized marketing on the internet is the term Online Behavioural Advertising (OBA), which is an umbrella term for the data that is collected on internet-based platforms and is used to target marketing to specific individuals and not general groups of people.

Boerman [19] suggested that there are two main problems that stand between consumer knowledge and the impact on the consumer of personalized marketing. The first was that there is no research on how OBA affects the consumer's understanding and that there is no research on how knowledge from consumers could affect the results of OBA.

That consumers do not have good knowledge about the meaning of collecting personal data and OBT is a consistent finding in several studies.

The concept of OBT was defined by [17] as a method that creates an opportunity for marketers to design individual marketing for consumers. A study by [17] showed that consumers answered approximately 50 percent of the questions regarding the meaning of OBT correctly. The questions that were answered correctly by less than half were whether personal data collection differs between traditional mail and email, whether it is possible to influence the browser's collection of flash cookies, and what privacy policy means.

Turow [54] showed results that people with an educational level of a college degree or higher tended to have a broader knowledge of the meaning of the concept of privacy. The same was true for consumers who had an income of, or more than, $100,000, who also tended to have broader knowledge than those who earned less than $100,000 annually.

Turow [54] continued to describe that there was a distinct difference between how women and men related to privacy policies on the internet, where men tended to have a greater knowledge of the meaning of the concept. At the same time, there were conclusions that women were more proactive and protective when it came to disclosing personal data on the internet.

According to Tikkinen-Piri [9], GDPR is an EU regulation that needs to be followed, but in parallel with that, national legislation must also be followed. Companies that collect, use and process personal data are obliged to comply with the legislation. When GDPR was to be implemented, companies were faced with several challenges, one challenge was understanding and awareness of what the law would entail.

Knowledge of privacy and personal data was also a major basis for being able to implement data protection measures in a safe way. This meant that both companies and consumers needed to gain increased knowledge in the area. If GDPR is not followed, sanctions are imposed for violations, which entails financial consequences but also legal and reputational risks for companies [9].

[17] investigated in a study whether there was a potential willingness among young adults to sell or trade their data. The group of young adults was selected because the researchers wanted to study the group that uses the internet the most of all generations and has grown up with the internet. The average age of the participants was 25 years, 51 percent were men and 49 percent were women, and the average income was 21,000 USD per year.

The survey consisted of two scenarios, the first of which involved a trade between monetary funds and personal data between the consumer (respondent) and a hypothetical website. The answer options aimed to investigate what amount a consumer would demand to sell their personal data, and the amount that consumers were willing to pay to not have to disclose their personal data, for marketing purposes. The results of the survey by [17], showed that consumers were willing to sell their personal data for data collection for marketing purposes, and that consumers were willing to install software that tracks their purchases and use of websites, in exchange for a monetary sum.

The study reported results on two groups, which were (a) a group that had higher knowledge of OBT and (b) a lower knowledge of OBT. The results showed that the group that had a greater knowledge of OBT tended to demand a smaller amount to sell their personal data, and that the same group was willing to pay a higher amount to not have to share their digital traces of personal data. Group (b) demanded a higher price to sell their personal data, while the group was willing to pay a smaller amount to not have to share their personal data.

Li [17] identified that the respondents' answers to the questions were not about the level of privacy they had, but that there is a clear connection between the level of knowledge about the meaning of the concepts of privacy policy and OBT and willingness to share their data.

In a study conducted by [12], consumers were first asked to sell their personal data for a monetary sum and then trade the same personal data in exchange for goods or services. The study showed a result that consumers demanded a smaller sum for the personal data when the sum was a service or good, compared to the monetary sum.

The human behavioural pattern in relation to communicative AI services has been studied by [25], who identified the difference between communication between people, and between people and AI services.

The authors argued that humans as individuals experience that when they share knowledge with other people, an exchange of information occurs. They then use this behavioural pattern when communicating with AI services. What is lacking in the transfer is that the individual tends to misunderstand the communication with the AI service. The authors argued that in this communication, the AI service is not a service adapted to the individual's preferences, but in the communication, it is the user, that is, the individual, who is the product.

The authors concluded that the individual interprets the service as temporary, just as humans interpret the exchange of information between people. The authors exemplified the reasoning by saying that when an individual asks a stranger on the street for directions, the stranger will only have knowledge of where you are right now and where you are going, while an AI service will know everything about you, even things that are not related to the question. It will also share all the information with other services, and someone will probably make money from it [25].

2.2 TRUST

Turow [54] conducted a study over 6 years, between 2009 and 2015, which aimed to investigate the understanding of American consumers regarding the collection of personal data. The study showed that there was a consistent relationship between consumers who have a strong trust in the legal laws and regulations that are supposed to protect their personal data online. Compared to those who misunderstand the privacy policies that are available on websites. Furthermore, the study noted that consumers who experienced a stronger sense of security on the internet tended to share more personal data. [54] argued that young adults who grew up with the internet tended to share more personal data on the internet than older generations.

The conclusion that the authors drew was that the problem was not in the knowledge of technology. The authors concluded that this was because the younger generation was raised with technology and did not perceive it as something difficult to handle. Rather, the problem was that the younger generation had a stronger and partly incorrect trust in the legal laws.

Brill [4] conducted a study in which they examined customer satisfaction with AI technology linked to digital assistants. The study examined how expectations underlie customer satisfaction. They described how customer satisfaction is a benchmark for good marketing, which needs to meet the customer's needs. Trust was the basis for how willing consumers are to value risk or uncertainty. Perceived trust was part of the trust process and influences the consumer in deciding how much the customer dares to get involved. The authors also stated that there was an expectation that companies work to secure personal data, which should be in line with laws and conditions. They stated that the user should have control over which personal data is stored and shared.

In order for individuals to have the opportunity to feel trust in a secure process of data collection, the authors [20] believe that there is a so-called “secure cookie system, which has the task of providing four different services that include Authentication, Anti-replay, confidentiality, and integrity.”

This is done by the cookie system working to verify the user and ensure that the owner of the website is real, so that it is not possible to communicate with fake cookies. At the same time, the system is responsible for detecting if cookies have been modified. To achieve confidentiality, the system works to prevent parties other than the server from having access to the cookies about the user's personal data [20]. Lavin [21] believed that it was important for companies to be clearer with consumers about why it is important that they collect cookies, as this can help the consumer receive more relevant marketing. When the consumer feels that companies are collecting data and risking abusing it, the companies lose the consumer's trust.

Kim [13] described that advertisements have been a form of marketing for several decades, with the help of the internet, advertisements gained a new place. Advertisers can target individuals with precision, which makes marketing work more efficient. Personalized online advertising can potentially make the internet more appealing to

consumers because what is displayed is more likely to be relevant when it is based on the individual's preferences. When advertising is displayed on the internet that is not relevant to the consumer, it can create an annoyance with an abundance of information and advertising that the consumer feels distant from.

Marketers can collect personal data and integrate with the consumer to create personalized advertising. Personalized advertising can be done by tracking or collecting the consumer's personal preferences. Another effective way is to advertise a product that the consumer has searched for or viewed. This can lead to a conviction towards the customer and acts as an exposure tool. Targeted ads that are personalized can be more relevant to the consumer, which can therefore meet the consumer's needs.

The authors highlighted that it can, however, give double messages, a consumer may experience the fact that the ads are personally targeted as a privacy problem, which can therefore reduce the effectiveness of the ad. For the process to work, it may require trust from the consumer to be willing to share their personal information [13].

2.3 BENEFITS

Why personal information is stored in the browser today is based on Lou Montulli's solution in 1994 on a recurring problem for internet users. When the website could only register and keep an item in the digital shopping cart to place an order. To overcome this problem, Montulli created digital cookies, as he was working with the Netscape web development team during this period. The reason was to solve the problem that arose in online shopping and enable benefits for the customer [22]. Personal information is stored in a database that forms the basis for creating a shopping cart and purchasing multiple items at the same time on the internet.

This has enabled marketing benefits for both companies and consumers. Based on this, cookies have been developed and today, in principle, every website is connected to a “third-party” website, which assists in storing and changing cookies, in order to be able to track and map the individual’s behavioural patterns. This is a tool for companies, where they constantly have knowledge of the user’s behavioural patterns and based on this, marketing can be targeted at the individual [23].

Behaviourally targeted advertising can provide advantages because consumers rarely appreciate advertising that the consumer feels distant from. However, Kim [13] described that the collection of personal information can be problematic.

Regardless of whether the collection is demographic, expressed preferences or whether it is tracking behavioural choices. Marketers must evaluate how willing the consumer is to reveal personal information in exchange for customized advertising. A further aspect the authors highlighted was how companies and consumers approach getting consumers to share their personal data. If companies encourage consumers to share their personal data, this can be a privacy issue in itself [13].

The authors further described that consumers are now demanding a higher degree of advertising transparency, as they are aware that their personal data is being collected to a greater extent than was previously the case. Most people experience personalized ads, but the reasons may vary. Companies that tailor their ads for marketing purposes have begun to inform users about why they are being exposed to the ad.

The “youradchoices” feature is a blue icon that can be used on certain ads and websites where the company justifies and explains why the advertisement is shown. In cases where this feature is not available, it can instead say “why am I seeing this ad?”. In social media, it can depend on which groups the user has chosen to belong to, which posts are liked or whether the user has purchased products through the company at an earlier time. In this way, companies meant that they were transparent about their use of personal data, which could lead to higher trust, which generates benefits.

Consumer demand for more can put more pressure on companies to become more transparent, which could be an advantage for consumers. Although more and more companies are using the feature, there are others who are opposed, as there is a concern that the methods that emerge may be offensive and minimize the effectiveness of the advertisement [13].

Spiekermann [7] argued that personal data is increasingly seen as a tradable asset. Personal data can be seen as an asset for companies because the data creates added value. It enables services for both companies and consumers that would otherwise not be possible. They further discussed how companies can use personal data for several

different purposes, it enables personalized offers, performs risk analyses on customers, targets advertisements to people and creates filtering using the data.

Personal data can be seen as a product in itself, since it can create user-generated content, which is common in social media. Personal data can also be a strategic choice for companies by improving their operations with solid marketing information about their customers. Companies improving their operations can in turn provide advantages to the customer. The fact that personal data can be seen as a product in itself is a way for the individual to try to decide for themselves. The authors Spiekermann [7] further explained that personal data can, on the other hand, become a burden, since the requirements for the handling of personal data have been tightened. One problem that arises may be the processing of personal data by a third party.

Since the collection of personal data carries both advantages and disadvantages, [24] examined a possible solution to continue to benefit from the advantages and avoid the disadvantages. The author argued that the ultimate system would be for individuals to disclose their personal data preferences to an authority, which is responsible for distributing the personal data to services that can contribute to the public good. Oyserman [25] also discussed possible solutions that involve the involvement of politicians.

The authors described the importance of government campaigns that educate the population in the area because they estimated, like other mentioned researchers, that knowledge is too low. The authors used the English proverb to emphasize their position, “If you’re not paying for it, you are the product”, although they emphasized that the individual is still, in this case, the product even in cases where the user pays for the service.

2.4 RISK

Kim [13] described what could be the reasons why advertisements appear in the individual’s feed. The authors described how consumers have become more cautious as it is now common knowledge that online behaviour is being tracked. They highlighted previous examples where it was revealed how a department store tracked customers'

movements using the customer's mobile data. The department store Target chose to make a special offer with coupons for pregnant women and was able to contact the customer using the customer's purchases. The authors also highlighted that there was extensive sharing of personal data and consumer information with other companies. Facebook chose to purchase data from 70 million American households to tailor marketing based on the receiving individual and potential consumer.

When this information was leaked, the company was criticized. This shows that there is a risk for the company when this type of data emerges and creates rumours [13].

The author Lavin [21] stated that consumers' protection of their privacy had increased their knowledge of cookies, which led to more users frequently deleting their cookies in their web history. The author argued that this creates a problem for companies that use cookies to market themselves on the Internet. In an article [26], the authors describe cookies that are not well known to users, so-called flash cookies, which users may perceive as violating privacy.

These cookies are essential for web functions and are stored and shared between websites; they are often not selectable or removable, which interferes with consumers' privacy because they are unaware of these cookies. The authors also argued that there have been cases where this personal data is sold without the consumer’s knowledge and consent. If consumer trust is lacking, it can lead to risks for companies, as consumers’ lack of trust can mean that they are unwilling to share their personal data [26].

Brill [4] described how privacy can be a challenge for companies. Digital services that are AI-based collect a digital footprint about individuals, resulting in a wealth of behavioural and personal information. A lot of data is collected, especially when users use digital assistants.

Digital preferences emerge and are registered in the various digital services. However, there is a risk that the data will be misused. Users have an expectation that protected and confidential information about individuals will be handled in a way that is approved, but despite this, it is possible to find how consumers are concerned about the risks [4]. Mulligan [27] identified that when asked about privacy issues on the internet, people tended to think mostly about theft of, for example, bank details or social security numbers. The authors argued that this is a minor problem, as this type of theft is

relatively uncommon and easy to avoid. The authors expressed that knowledge of how and what personal data was collected for other purposes was, in relation to the previously mentioned, more problematic.

Oyserman [25] defined the human behavioural pattern of prioritizing their goal, where users enter websites with a goal and are interrupted by a form that wants the individual to take a position on the collection of personal data. In turn, the authors argued that there is a risk that the user does not have the time or that it is not in their interest to explore the approach to avoiding collection. The result of this is that the individual tends to experience a sense of failure.

2.5 CONTROL

[9] describe that the GDPR began to develop in 2009 and an official proposal came in 2012, the vote in the European Parliament took place in 2016 where the decision was made that the law would come into force two years later. GDPR came into force in May 2018 and meant a change for both large and small companies. All organizations were given new challenges to protect personal data. The aim was that there would be a consistent way to process personal data where privacy rights would be strengthened. Individuals should be given the opportunity to manage and control their own personal data.

Due to the Data Protection Regulation, companies should allow consumers to choose which personal data should be collected in order to be able to control their privacy. The advantage of the Data Protection Regulation is that the consumer's privacy should be protected and that companies should have clearer guidelines regarding the processing of personal data [9].

In line with [9], [28] also demonstrated how GDPR would have meant better control over personal data and that consumers themselves are given the opportunity to make choices. Kollnig [28] examined how third-party tracking is shared. As consumers themselves would have the opportunity to decide over their personal data, consent standards have been developed. Enforcing the law can be difficult for companies

because GDPR provides room for interpretation. This can mean, in some cases, that it leads to redundant information that the consumer has difficulty absorbing.

Mulligan [27] considered that the legal and political laws and regulations that are added to protect the privacy of individuals are downright offensive as the authors concluded that the laws and regulations are not capable of fulfilling their duty. Especially since the authors considered that users are confused by interface design and data collection policies.

According to [28] the consent process became more complicated than it needed to be. Within the GDPR there is a transparency principle, but despite this, it is possible to see terms and conditions from websites that include meaningless and misleading information. According to the authors, this can demonstrate that the transparency principle is not being followed. The authors also described a problem with third-party tracking. Although the GDPR is supposed to regulate third-party tracking, it is not guaranteed that it will be followed.

There are also no obvious methods to be able to review whether the GDPR is being followed or not [28]. In line with [9] and [28], [12] agreed that the role of the GDPR is to protect personal privacy. [12] also described that reduced personal data not only has an impact on companies but also leads to fewer choices for consumers. The author based this assumption on the fact that companies cannot share and control private data about consumers' actions and behaviour on the internet.

This in turn negatively affects the consumer, as companies do not have data about consumers' online behaviour and thus cannot offer competitive prices in the same way.

[29] highlighted the importance for marketers to collaborate with third-party data collectors. This is because these data brokers effectively address consumers' privacy preferences and their interest in sharing personal data, while collecting the necessary data. In their study, [29] investigated consumers' willingness to share their personal data with data brokers, through a quantitative survey conducted on French consumers.

In line with authors [17], [29] also investigated whether there was a potential incentive for consumers to sell their personal data, and in this case to specific data brokers. The authors concluded that the willingness to share personal data with a third party is

generally low among consumers and that offering a higher monetary amount to increase the willingness to share personal data has the opposite effect. This means that the result is not only unchanged, but it tends to make the consumer even more negative about wanting to share their personal data with a data broker.

Furthermore, the results of the study showed that the personal data that consumers value as more sensitive, consumers are less willing to share. What the study by [29] found as the key to getting consumers to want to share their personal data was to create a feeling among consumers where they experienced control. Offering control over data sharing increases consumers' willingness to share personal data, while this willingness still decreases the more sensitive personal data that is requested. In practice, the study showed that by informing the consumer about personal data collection and offering choices about what information the website is allowed to collect, a perception of control was created for the consumer. This also tended to make the consumer feel safe sharing more information [29].

Jagadish [24] discussed how the handling of personal data could affect the individual who had not given their consent for their personal data to be shared, but the data was shared anyway. The author refers to the Cambridge Analytica scandal, which involved personal data being shared without individuals using the app. This had happened because personal data from non-users was retrieved through users who had consented to the sharing of personal data. [24] clarified that just because the information is part of a user's personal data and is defined as their personal data, it does not necessarily mean that they have the right to share the information.

2.6 THE SURVEY MODEL

Figure 1 presents the theoretical model with themes that the researchers developed when processing scientific articles. The model was created based on the theoretical framework and was named the survey model.

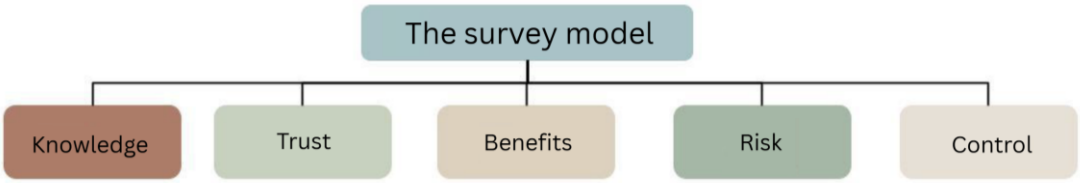

Figure 1: The survey model

2.7 CONVOLUTIONAL NEURAL NETWORKS (CNN)

Convolutional Neural Networks (CNNs) are a revolutionary approach in computer vision due to their self-directed high-dimensional feature extraction capabilities. Particularly designed for visual learning, CNNs yield competitive results in areas like image classification, object detection, segmentation, etc. Underlying basic blocks of the CNN architecture are convolutional layers that work as main feature extractors. The layer contains learnable filters (kernels) to detect local patterns like edges, textures, or other features across an input image.

Figure 2: Images without filter

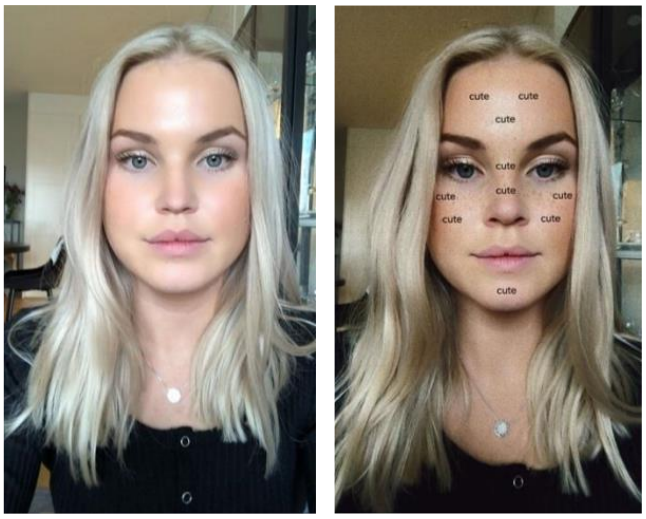

Figure 3: Images with filter

CHAPTER-3

LITERATURE SURVEY

The section discusses the qualitative research method according to which the study is designed and also presents the selection and analysis of data.

3.1 RESEARCH STRATEGY

Bryman [30] believed that the qualitative method is partly difficult to define because researchers do not completely agree on the definition. In general terms, the authors [30] believed that a qualitative research strategy is what does not fall within the framework of a quantitative research strategy. Despite the broad definition, [30] provided some more specific definitions of a qualitative strategy. For example, the authors believed that in qualitative research, the information is analysed based on words and not quantification of numbers. A central part of qualitative research is social reality. Making individuals' experiences and interpretations of reality visible is the focus area.

The authors of this study chose the research strategy qualitative research study because it appropriately enables the study to fulfil the purpose of the study.

The theoretical framework was obtained through scientific articles and published literature, which was used as a basis for the research work.

The study was founded on an interest of the researchers in understanding how Artificial Intelligence affects people's behaviour on the internet. An interest in ethics and the demarcation between personal data and the management of personal data laid the foundation for the subject.

Research into the subjects at the beginning of the process resulted in the author’s focusing on the collection of personal data collected online for marketing purposes. When reviewing scientific articles, the researchers observed that there was a concern that personal data would be misused if it was collected for marketing purposes. The researchers observed that there were both positive and negative attitudes towards the

collection of personal data. On the other hand, the researchers considered that there was a clear research gap in that it had not been identified what influences consumers when deciding to share their personal data.

In addition, there was a lack of research on consumers' self-perceived experiences within the subject, which constituted a possible area of research. The researchers therefore considered it important to understand how consumers feel about sharing their personal data with companies in order for them to be able to produce effective marketing. The research therefore aims to understand the users and highlight which factors are important when sharing, as well as to consider their views on the advantages and disadvantages of sharing personal data.

Here we present related research regarding four areas that we have identified as central given the topic of our study. These are AI, facial recognition, privacy and biometrics.

We have chosen to study related research to expand knowledge within the areas that the study contains and to get a better overview of which parts have already been explored. The knowledge learned from the related research will be used as a basis when the work with the qualitative study is then carried out [30].

The purpose of related research is to gain a deeper understanding of the respective phenomena discussed in the report. Previous studies on how facial recognition affects personal integrity using AI give us insight into the subject and which questions have been answered previously. Since facial recognition is a relatively broad area, we chose to read literature items that have similarities and are considered relevant to our question. Facial recognition in public places and facial recognition in police operations are examples of studies that were read during this part, as we believe that these issues have a close relationship to the main question of this report. The keywords used are shown in the table below.

Keywords: Integrity, Personal Integrity, Privacy, Facial Recognition, FRT, Facial Recognition Technology, Artificial Intelligence, AI, AI FRT Biometrics

3.1.1 AI

In this section, we will review what Artificial Intelligence is and follow its history to its current functions. Artificial Intelligence (AI) is in practice a relatively new field that deals with creating intelligent software that can perform tasks that traditionally only humans have been able to do.

Dignum [31] describes in her book that there is no easy way to briefly describe what Artificial Intelligence actually is, however, the closest definition she came up with was "A computational algorithm that is built through human intervention that thinks or acts like humans, or how we expect humans to think or act" [31].

3.1.2 HISTORY BEHIND AI

The foundations of AI go as far back as Aristotle (384–322 B.C). Aristotle formulated a group of laws about the rational mind; he also created an informal system of correct reasoning which largely allowed people to produce conclusions mechanically with the right initial premises. Leonardo da Vinci designed a mechanical calculator as early as 1500, he never created the calculator itself but in recent years it has been proven that his design was functional [32].

The first work that is generally classified as AI today was created by Warren McCulloch and Walter Pitts in 1943. They proposed a model of artificial neurons where each neuron had two states, off and on. If the surrounding neurons were stimulated, the state of the neuron changed to on and otherwise they were off. This showed that all computable functions could be calculated by a network of connected neurons and that logical connections could be implemented by relatively simple network structures [32].

In 1950, two students at Harvard created the first computer based on the proposal developed by Warren McCulloch and Walter Pitts. It was named SNARC and used 3,000 vacuum tubes and an automatic pilot mechanism previously used in a B-24 bomber to simulate a network consisting of 40 neurons [32].

Alan Turing was a mathematician who is known for being an early pioneer in AI and computer science. In 1950, he created “The Turing test”, which is a thought experiment that is intended to answer whether a machine can think like a human. The test involves a person sitting in a locked room with two terminals, one of the terminals is connected to a machine, the other is connected to a human. The person sitting in the locked room can ask questions to both terminals and must decide after a few minutes which of the terminals is a machine. The machine passes the test if it is not identified as a machine in 30% of the cases. This test is not as relevant today as AI is most often used to perform certain specific functions [33].

3.1.3 AREAS OF APPLICATION IN AI

There are several different areas of application for AI, for example, it can be used to drive a vehicle without a human needing to control the vehicle, it can also be used for more specific functions such as playing chess and producing visual art [31]. The academic field that Artificial Intelligence covers is very large and covers several categories such as psychology, philosophy, cognitive science, but above all mathematics and computer science.

The systems that help humans in situations like these are called artificial agents and include flexible decision-making. The flexibility of the agents has three characteristics as the basis for the system, reactivity, proactivity and social ability. The first is reactivity and means that the agent has the ability to find its way in the environment it is in and then adapt to any changes that occur. The second characteristic is proactivity (or prevention) and is briefly explained as the agent's ability to perform specific actions in order to achieve its own goals. The last characteristic of an agent is social ability and means exactly as it sounds, the knowledge to be able to interact and collaborate with other robots and humans [31].

Today, Machine Learning (ML) is often used to develop AI systems, ML uses a learning algorithm to learn from the data that is available. The algorithms usually use statistical or stochastic methods to be able to analyse and find patterns in the available data. It requires a large amount of data and takes a long time to be able to train these algorithms

to identify different patterns and then apply the learned knowledge in other situations [31].

ML is used to create trained models that can generalize without humans being involved, the result must be correct not only for the data that the system is trained on but also for future situations that the algorithm has not encountered before. When applying Machine Learning, the developer starts with an existing set of data that is divided into two different sets, one for training and one for testing. The developer also chooses a structure with adjustable parameters that the algorithm uses.

The system automatically adjusts these parameters by comparing the results the system gets with the expected results in the training data. Once the system is fully trained, the test data is used to evaluate how accurate and effective the system is [31].

Recently, so-called deep learning has become very popular in the development of Artificial Intelligence, deep learning uses Machine Learning with multiple layers of simple and adjustable programming elements. Experiments with deep learning were already carried out in the 1970s in the form of Convolutional Neural Networks, but it was not until 2011 that deep learning methods became popular in areas such as voice recognition and image recognition [32]. Thus, it was only at this stage that various forms of AI-based facial recognition became available.

3.2 BIOMETRICS

Biometrics is a term that refers to the measurement of physical characteristics, such as a face, fingerprint or iris pattern (i.e. the iris of the eye). Biometric data that is stored falls under a special category within the GDPR that includes personal data, where strict rules and conditions apply to the use of biometric data [35].

Biometric data can be divided into two different categories, physiological and behavioural. These are so-called biometric identifiers. The most common identifiers used in society today within the physiological aspect are face, fingerprint, hand geometry and iris. In addition to these, there are other identifiers that are in an early stage of development and are therefore not used at all to the same extent.

These are DNA, the shape of the ears, scent, the retina, the skin's reflection and thermograms within the physiological part [36].

Within the behavioural part, name signature and voice recognition are used. In this part there are also identifiers that are used much less, which are walking style, type of keystroke and lip movement [36].

3.3 FACIAL RECOGNITION

Facial Recognition Technology (FRT), or facial recognition, is a technology that is used more and more in today's society, for example to unlock private mobile phones. The technology is used to verify an identity or identify a person by linking the face to existing data. If the face matches data or images stored in the database, then the face has undergone successful verification. The process behind this work is intensive and requires high-performance hardware and software. The technology contributes to higher efficiency for end users, such as individuals who want to quickly unlock their mobile phone or airport employees who want to verify themselves in a smooth way [37].

The faces stored in databases are not digital images of individuals' faces and therefore ease the tension of people who feel that it violates their privacy. The main purpose of the technology is for organizations to be able to offer secure and reliable biometric identification systems that reduce or even eliminate existing visual copies of individuals, such as images [37].

In order for a face to be recognized, the system must have knowledge that an actual face is in front of the camera. This function is called “EigenFaces”, which translates from German to “characteristic”. In short, this means that the system extracts relevant information from an image and then compares the image with an existing face that is already in the database.

There, a mathematical algorithm is created that analyses four variables that determine whether a face is in front of the camera or not. This leads to programs that perform these facial analyses based on algorithms that handle the different details and patterns of the face. This algorithm undergoes two processes. The first is face detection, which means that a face must be detected before further processing can continue. Once the face has

been detected, facial recognition is introduced that identifies the face and links the data to a person [37].

The algorithm's identification is done using a camera that looks at several aspects of a face. Examples of this are the shape of the face and how far the person's eyes, mouth, chin and nose are from the centre of the face. It is this type of data that is processed and stored in the database that is then linked to people, which is why these systems offer protection against personal privacy, although to a certain degree [37].

A study by [38] was conducted to investigate the difference in the accuracy of face recognition that was controlled by 2D and 3D algorithms. What could be seen was that the different approaches outperformed each other under different circumstances. For example, three-dimensional image analysis is more accurate when it comes to positioning the face, the lighting of the face and the background, and facial expressions.

The two-dimensional image analysis was instead better at recognizing a face that has beard growth or the like. What gave the best results was to combine both techniques into one and the same image analysis, which then outperforms both individual techniques. The conclusion that was drawn was that none of the image analysis techniques can deal with all the types of changes that a face can undergo [38].

When discussing the phenomenon, the question of privacy and how facial recognition affects it often comes up. A company called SenseNets, which develops a facial recognition program, had a data breach from an unprotected database. This resulted in the biometric data of a million people being leaked into the public domain, for anyone to see and use. The consequences of this are that this type of data is almost unchangeable over a lifetime, as a person's face rarely changes. The security of using biometric data, especially one's face, can come with current consequences. This is due to the development of various software and applications that change one's face.

Face-Swap and Deepfake are techniques that replace your face with another, which can potentially be used to deceive systems that contain facial recognition. Therefore, facial recognition systems cannot be classified as completely reliable in terms of security [39].

In addition to using facial patterns to locate characteristic features in real time, there is another method for facial recognition, namely holistic images. [40] explains that these can be divided into two parts, the statistical approach and the Artificial Intelligence approach.

The former uses two-dimensional images that compare a face with all images of faces in the existing database. This appears to work to some extent as other aspects can affect a successful or unsuccessful identification, such as backlighting in the image, how close the face is to the camera when the image was taken, and the position of the face. The second part of the holistic approach is controlled by AI and instead uses Machine Learning to locate and identify faces. The system divides the face into three parts; mouth, eyes and nose, which are then assigned to the neural network. This led to this approach having a succession rate of 96 percent, which was higher than the statistical method [40].

Face recognition is thus a reliable technology for identifying people by linking faces to names. However, the ethical issues of the technology are sensitive due to the data management, as faces rarely change significantly. The saved data does not illustrate a physical image of a face but instead is displayed as numbers where the numbers represent a pattern on the face. Because of this, it is almost impossible for a human to interpret what a face actually looks like, without the right tool to translate the data points.

3.4 PRIVACY

Personal privacy is a concept that is difficult to define, the meaning of privacy can be perceived as a collection of different meanings, however, it briefly means “the value and dignity of the individual”. Laws and reforms are divided on the subject, and protection for the privacy of individuals is therefore not always complete. This is because the interest of society clashes with personal privacy through, for example, freedom of expression and the pursuit of a secure legal society [41].

The concept of personal privacy can be defined as the ability of each individual to control under what conditions their personal data is collected and used. It can also be generally defined as the right to a private life where it is possible to separate oneself from others anonymously and not be observed. The need for privacy arises from society, people from different social relationships with each other, companies and the government. Privacy is not just a right that the specific individual possesses but a form of freedom that is built into the social structure [42].

If you choose to perform on stage or be in a large crowd, there is a risk that you will be photographed or filmed, in public scenarios like these you renounce part of your personal privacy. On the other hand, if you are standing in the shower at home, you have a moral right not to be photographed, even if it would be possible with a long-range camera where the photographer does not even have to be on the person's property [43].

Your face is a large part of your personal identity; it can therefore be seen as a moral right to control images of your own face. Conversely, one could argue that one's face is always present when one is around other people and that it is therefore impossible to control all the images that one's face ends up in and therefore one has no rights over these images. One's face is an important part of how one communicates and expresses oneself, but this in itself does not mean that one does not have the right to control images of one's face [43].

Logically, one could control the images even if one cannot control who sees one's face in reality. One can exercise a great deal of control over which contexts one chooses to be in and in this way one can exercise control over who sees one's face. One can also decide for oneself how one chooses to present oneself when in the company of others, one can hide or pretend to show one's emotions using one's facial expressions.

When one is in the company of others, everyone's face is visible to everyone in the company, unlike a picture of a face where it is specifically one person's face that one is looking at [43]. People’s right to privacy is not absolute and can be overridden, and the exact boundaries are also quite unclear. A person has no right not to be observed when in a public place but has a right not to have their face photographed in a public place. The right not to have their face photographed can also be overridden in certain circumstances [43].

Privacy has long been a concern for social scientists, philosophers, and lawyers. The United Nations (UN) has recognized privacy as a fundamental human right [44].

3.5 PRIVACY AND FACIAL RECOGNITION

Cameras that incorporate facial recognition are a sensitive area that contains diverse opinions. This section will review relevant studies on facial recognition both in the public sector and in the private sector.

3.5.1 PUBLIC SECTOR

A study by Genia Kostka was conducted in four countries asking the public what they think about facial recognition linked to surveillance and how it affects personal privacy. These countries were China, Germany, the UK and the US. The survey in China, which consisted of 6,100 respondents, showed that 75% of respondents wanted to introduce traditional identification methods instead of facial recognition, and a full 85% said they wanted more control over their personal information and data. The survey in Germany consisted mainly of the question about facial recognition linked to surveillance technologies. Since the development of the technology is minimal and close to non-existent, this survey of the country did not provide any directly conclusive answers.

However, the UK and the US gave informative answers regarding the question and the survey showed that out of 4,109 respondents in the UK, 77% of respondents feel uncomfortable with companies using facial recognition. At the same time, almost half (49%) of respondents support the use of the technology for police purposes. The same survey conducted in the US gave similar responses from respondents. More than half (59%) support the technology if it is used for security purposes, such as law enforcement. When it comes to the use of the technology by companies and advertisers, respondents showed trust in the technology of only 36% and 18%, respectively [45].

Why are people so worried and negative about the use of facial recognition? [46] gives examples of six possible risks that may accompany the constant development of Artificial Intelligence, most of which are related to personal privacy. One risk that is

already implemented is the constant surveillance that is taking place in China, which is the basis of their social credit system [46].

[47] also continues on this path, explaining that systems that include the technology are most often used in public places such as airports and large squares, places where anyone can be. The system sees your face, saves it and can reuse it later for further identification. The information retrieved can be sold or shared to social networks or public databases that anyone can access. All of this is usually done without the consent of individuals.

The data that is saved contains sensitive information that can later be used against their will in either good faith or abuse. The right to anonymity of individuals is eliminated and the idea of constant surveillance characterizes personal integrity. [47] describes an example where an otherwise anonymous person participating in a protest can be linked to a name and personal information.

Andrejevic [48] discuss that regardless of whether Facial Recognition Technology works as promised, the technology is increasingly being implemented in schools. The important thing is not whether the technology actually works as promised, but that people believe that it works as promised and act accordingly. They believe that against this background, there is a need to treat the continued implementation of facial recognition as a serious and worrying proposal. They also address the fact that with all new technology, it is important to think about what is not being talked about and what has stopped being talked about, and to consider the most undesirable consequences that may result from its implementation.

Andrejevic [48] also argue that there is a great need to discuss the fundamental question of whether facial recognition has a place in schools at all. The values and effects achieved by the implementation may outweigh the possible consequences such as automatic sorting and classification of students.

Facial recognition can also be used in police work as a tool to quickly and effectively identify criminals. A study of YouTube comments on the police use of facial recognition has been conducted by [49]. In this study, they came up with several different negative and positive concerns that people had about facial recognition in the justice system. One of the points is the technology itself, where 33.15% of the negative comments were

about the technology's precision, bias, and its advancement, and not about how the judiciary used it. At the same time, 23.66% of the positive comments expressed support for the technology and its rapid development and precision.

Another main point from the data in the study by [49] was about rights and freedom. 26.26% of the negative comments were about where people expressed concerns about how facial recognition would change or affect people's rights and freedoms, and how it could be used to track the population at large.

3.5.2 PRIVATE SECTOR

Facial recognition has recently become popular for use in hotel check-in, especially in China.

Wang [50] conducted a study to investigate how hotel guests' use of facial recognition for hotel check-in is affected by security, privacy and customer experience. The study shows that hotel guests perceived security, privacy and trust in facial recognition systems significantly affect their willingness to use them for hotel check-in. The survey also showed that hotel guests considered privacy to be a very important issue, even more important than the security of the system. Wang [50] believe that this is because the systems used in hotels are maintained by the Chinese Ministry of Public Security and that the technology comes from companies authorized by the Chinese regime. They therefore believe that it is important for system providers and authorities to improve consumers' perceptions of privacy and security in order to gain their trust.

The hotel industry contains a large number of bankruptcies and in order to achieve market leadership, such an organization should consider two fundamental aspects. To protect consumer privacy and security, and to offer services that result in loyalty and satisfaction for the customer.

A study was conducted by Morosan [51] in this area where they investigate how willing consumers are to create a profile using biometrics, mainly facial recognition. A brief summary of the respondents is as follows; the number of respondents who participated in the survey was 421 people, of which 63% were women and 37% were men. Of these, 76% of respondents had an annual salary of less than $100,000 per year. Most of the

respondents visited hotels three to ten times per year. The results of the study showed that disclosure of personal information was beneficial due to social rewards.

The willingness to disclose information is strongly linked to the willingness to create a profile with biometrics [51]. Consumers receive an assurance of future benefits within the hotel, for example by receiving rewards from the organization. Morosan [51] describes that consumers who have chosen to offer their biometric data are strongly motivated to remain engaged with the hotel in the future.

Another study similar to the above was conducted on patients in the healthcare sector. 4,048 respondents were asked whether their privacy is affected by the storage of biometric data for medical purposes and research. The results gave varying answers, but the item that emerged most clearly was the storage of video footage of patients, where 71% of respondents thought this would be “very” or “somewhat” concerning. The item that was most “acceptable” was imaging-based data, where 47% of respondents indicated that the storage was “very” or “somewhat” concerning [52].

The General Data Protection Regulation (GDPR) is a relatively new concept and its impact on data security and privacy is significant. A study was conducted on EU countries on their views on GDPR and the use of facial recognition from a non-police perspective. The question the study aims to answer is “To what extent is the use of Facial Recognition Technology for non-law enforcement purposes compatible with the current EU legal framework?” The study and the question contain sub-questions that should clarify the answer to the main question, and the question that is most relevant to us in this report is “To what extent does GDPR legitimize the use of FRT for non-law enforcement purposes in public and private spaces?”

Identifying a person using biometric data must circumvent several strict laws and regulations under the GDPR, however, there are several exceptions that make this possible. The study mentions three of the most relevant which are; If the person in question gives explicit consent for the use and registration, if the data is made public in an obvious way, and if FRT is of significant public interest for the society or organization in which facial recognition is to be applied. These exceptions also include some issues that fall under the Data Protection Impact Assessment (DPIA). If the DPIA considers that the subject or subjects are exposed to a high risk of security breach or

privacy violation, the system owner should consult with the respective authority before implementing the system [53].

CHAPTER-4

MODEL IMPLEMEMNTATION

4.1 USE OF CNN IN DETECTING IMAGE FORGERIES

This section concentrated on a few of the earlier studies using Convolutional Neural Networks (CNNs) to detect image forgeries. [19] created the first CNN architecture for handwritten digit training in the 1980s. The MNIST handwritten number dataset from 1988 makes use of the similar design. However, because of a lack of technological developments in hardware and the creation of techniques like Support Vector Machines [20] and Bayesian networks [21]. After emerging victorious from the ImageNet Large Scale Visual Recognition Challenge [22] (ILSVRC), CNN has recently made a resurgence. CNN's new path was made possible by AlexNet's victory in the ILSRVC [23]. Subsequently, major corporations like Google, IBM, Microsoft, and others created their own CNN-based Deep learning models called ResNet [24], which are employed for tasks including feature extraction and categorization.

CNNs are also capable of handling tasks related to fraud detection, such as visual forgery localization [25], deepfake detection [26], and image forgery detection [27]. A novel Convolutional layer was presented by [28] to identify features in images that have been modified through various means, like scaling, blurring, or noising. Numerous real and altered photos are used to train their algorithm. [29] presented a CNN-based media filter-based forgery detection method in 2015.

The suggested model could recognise copy-paste type and median filtering manipulation. Afterwards, the authors also released a paper that illustrates how various CNN architectures affect picture forensics [30]. [31] identify manipulated areas in an image by combining CNN and Long Short-Term Memory (LSTM) networks. To prevent vanishing gradient issues in the deeper networks, the model employs residual propagation to recall input features. On datasets like COLUMB [32] and CASIA [33], their trials yield encouraging findings. [24] subsequently put forth an end-to-end network that executes detection and localization functions without any further pre- or post-processing.

The idea of visual chirality holds that objects differ from their mirror images, for example. Using this idea, [34] demonstrate how reflection alters the statistics of visual data. Their method can be used in visual forensics, self-supervised learning, and data augmentation. A few CNN-based models have attained state-of-the-art performance for image forgery detection [35]. These models include [36], [37], and [38].

4.2 CNN ARCHITECTURE

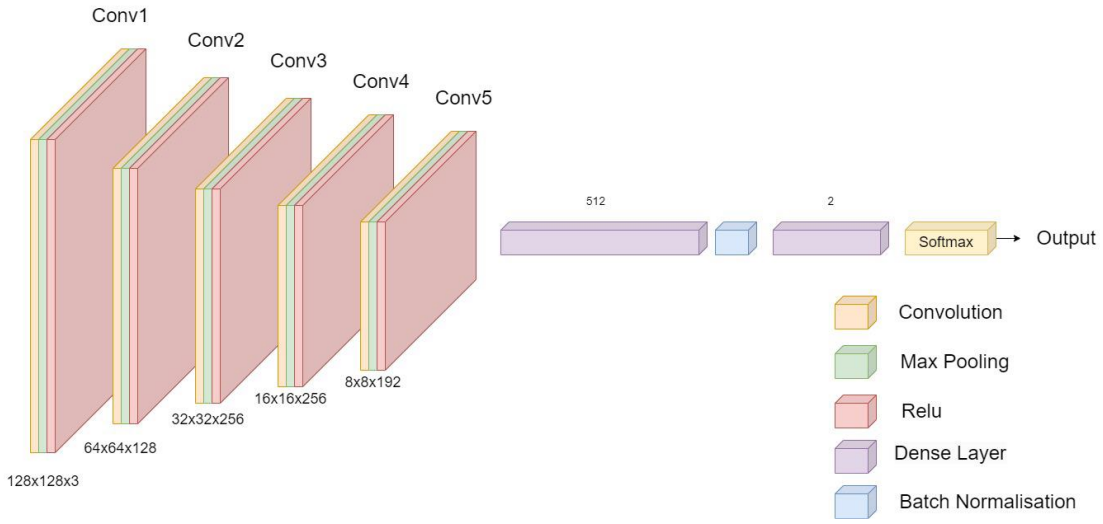

Figure 4: Architecture of the proposed methodology

Underlying basic blocks of the CNN architecture are convolutional layers that work as main feature extractors. The layer contains learnable filters (kernels) to detect local patterns like edges, textures, or other features across an input image. This is essential for understanding complex visual data since the network can depict the spatial hierarchies of the captured features, which are of paramount importance. The pooling operations (max pooling or average pooling) do not only down sample the feature maps, but they also help in abstraction of the features, which is important for the representation of the objects of interest.

Dimensionality reduction of spatial dimensions coupled with preservation of emblematic features through pooling layers enables a computational efficiency advancement and improves network's translation invariance. Non-linear functions used, for example ReLU, sigmoid or tanh, follow the convolution, averaging and max-pooling operations. Nonlinearity is used to train the network through these activation functions,

thus allowing for the capturing of complex relations and relationships that are nonlinear in nature and are present in the images data.

Convolutional and pooling layers are mostly followed by dense fully connected layers which takes over the process of spatial information aggregation and eventually perform the classification or regression tasks with help of the extracted features. These dense layers leverage the extracted hierarchical features to make predictions.

The proposed model has 5 convolutional layers from L1 to L5. After every layer there is max pooling layer with a pool size of (2,2) down sampling the feature maps by taking the maximum value within each 2x2 region, reducing spatial dimensions by half. A constant stride of 1 is present for all the convolutional filters.

– The first convolutional layer (L1) has 128 filters (output channels) and a kernel size of (5,5). The input is of size 128 * 128 * 3. It outputs an image of size 128 * 128 * 128 which after going through the max pooling layer gives an output of 64 * 64 * 128.

– The second convolutional layer (L2) has 256 filters (output channels) and a kernel size of (5,5). The input is of size 64 * 64 * 128. It outputs an image of size 64 * 64 * 256 which after going through the max pooling layer gives an output of 32 * 32 * 256.

– The third convolutional layer (L3) has 256 filters (output channels) and a kernel size of (3,3). The input is of size 32 * 32 * 256.It outputs an image of size 32 * 32 * 256 which after going through the max pooling layer gives an output of 16 * 16 * 256.

– The fourth convolutional layer (L4) has 192 filters (output channels) and a kernel size of (4,4). The input is of size 16 * 16 * 256. It outputs an image of size 16 * 16 * 192 which after going through the max pooling layer gives an output of 8 * 8 * 192.

– The last convolutional layer (L5) has 192 filters (output channels) and a kernel size of (3,3). The input is of size 8 * 8 * 192. It outputs an image of size 8 * 8 * 192, which after going through the max pooling layer gives an output of 4 * 4 * 192.

Rectified linear unit (ReLu) activation function is used alongside these layers. ReLU (Rectified Linear Unit) is an elementary activation element in neural networks, which is responsible for non-linearization by applying a threshold operation with a single step. The function is defined as the following equation:

$$f(x) = \max(0, x)$$

Where,

x: is the input to the function.

The working principle of ReLU is that if the input is negative then the output is zero else the output is same as input. One important feature of ReLU is its computational simplicity - the procedure is made up only of simple perceptron and additions. The ReLU has yet another benefit since it helps eliminate the vanishing gradient problem in the positive region by not saturating like *sigmoid* or *tanh* functions in such a way. This is followed by a dense layer with 512 neurons followed be a Batch Normalisation layer which is aimed for the normalization of the activations of that layer helps in the improvement of the network stability speed by reducing instability in the training phase.

Additionally, a Dropout layer with a dropout rate of 0.5 is utilized to introduce regularization by randomly setting a fraction of input units to zero during training. The last layer which is the output one contains two neurons and has SoftMax activation as the activation function.

This part assigns the final classes' probabilities for the two categories, authentic versus manipulated. The SoftMax activation allows output values to confirm to the valid probabilities' numbers, which provides a foundation for the accurate and effective selection of the highest probability class.

4.3 PROPOSED METHODOLOGY

The purpose of the framed model is to create an image forgery detection system and to emphasize the significance of detecting image forgery in numerous applications (e.g., journalism, law enforcement, social media).

4.3.1 ERROR LEVEL ANALYSIS (ELA)

Error Level Analysis (ELA) is primarily a digital image forensics technique, not a conventional feature extraction method used in general-purpose Machine Learning. However, it *can* be used as a preprocessing or feature extraction step in tasks involving image tampering detection or other computer vision applications.

ELA is a technique used to detect areas within a JPEG image that may have been altered. It works on the premise that when a JPEG image is saved, compression artifacts are introduced. If an image is edited and resaved, the modified areas will have different compression errors compared to the rest of the image.

4.3.2 WORKING OF ELA

1. Input Image: Start with a JPEG image.
2. Resave the Image: Save the image again at a known quality level (e.g., 90%).
3. Difference Map: Subtract the recompressed image from the original. This highlights areas with differing compression artifacts.
4. Result: The difference image is often enhanced (e.g., brightness increased) to visually identify inconsistencies.

4.3.3 GAN

Using Generative Adversarial Networks (GANs) as a data augmentation method is a powerful strategy to enhance the performance of a Convolutional Neural Network (CNN) classifier, especially when you have limited training data.

GANs consist of two neural networks:

- Generator (G): Creates fake data samples (e.g., images).
- Discriminator (D): Attempts to distinguish between real and generated (fake) samples.

They are trained in an adversarial process:

- The generator tries to fool the discriminator.
- The discriminator tries not to be fooled.

Over time, the generator learns to produce realistic-looking data.

4.3.4 WORKING OF GAN

When used for augmentation:

1. Train a GAN on your dataset.
2. Use the trained generator to create new, realistic synthetic images.
3. Add the generated images to your training set to improve the diversity and robustness of your CNN.

Example: GAN-Augmented CNN Classification

1. Train a DCGAN on MNIST.
2. Generate 5000 handwritten digits.

3. Train a CNN with:
    - Only original MNIST images.
    - Original + GAN-generated images.

Compare test accuracy (typically, model with augmented data performs better).

4.4 PROJECT STEPS AND METHODOLOGY

4.4.1 DATASET INFORMATION

Our proposed model is trained on openly available and famous open-source dataset. The training, validation and testing split is 60%, 20%, 20%. We have trained the model on the training set so that the model can generalize better on new data.

– CASIA V2 : There are a total of 1721 cut-paste manipulated photos in the v1.0 dataset, compared to 12,614 cut-paste and copy-move altered images in the v2.0 dataset. The JPEG format of the pictures is supported. The images are either of size 240 * 160 or 900 * 600.

Figure 5: Image from Kaggle dataset 5 (1)

Figure 6: Image from Kaggle dataset (2)

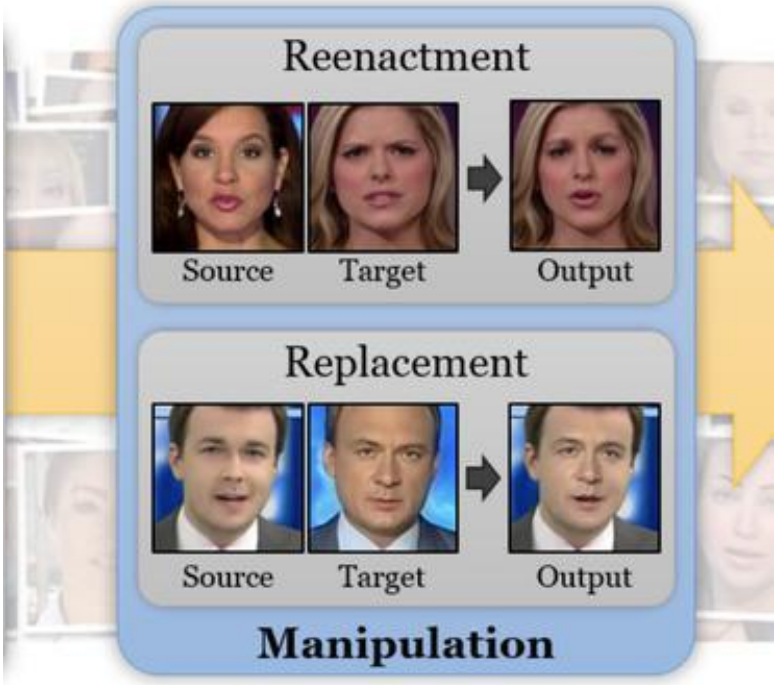

Figure 7: Example of image manipulation

The project utilizes the CASIA Image Tampering Detection Evaluation Database (CASIA v2.0), a publicly available dataset widely used in image forgery detection research. The CASIA v2.0 dataset is structured into two primary categories:

- Authentic Images (Au): This category contains original, unmanipulated images. These images serve as the "real" examples for training our detection model. The dataset includes a variety of scenes and subjects within this authentic category.
- Tampered Images (Tp): This category comprises images that have been digitally manipulated or forged. The forgeries in CASIA v2.0 involve various tampering techniques, such as copy-move forgery (where parts of an image are copied and pasted within the same image) and splicing (where parts of different images are seamlessly combined).
- Dataset Link: https://www.kaggle.com/datasets/sophatvathana/casia-dataset

4.4.2 METHODOLOGY

1. Due to computational limitations encountered in the Google Colaboratory environment, particularly memory constraints when attempting to process the entire dataset, a limit was imposed on the number of samples loaded per class using the `MAX_SAMPLES_PER_CLASS = 3000` parameter. This was a necessary step to prevent the Colab environment from crashing during the data processing and model training phases, given the specifications of approximately 12.9 GB RAM and 110 GB storage.

2. The `load_data` function manages the data loading. It initializes two empty lists, `X` to store the ELA-converted images and `Y` to store their corresponding labels (1 for real, 0 for fake). The function then processes the authentic images located in the `/content/casia-dataset/CASIA2/Au/` directory. For each image file found within this directory, the `convert_to_ela_image` function is called.

3. The `convert_to_ela_image` function is crucial as it performs the Error Level Analysis. This technique works on the principle that when a JPEG image is saved, it undergoes a lossy compression process. If an image has been tampered with and parts

have been re-saved at different quality levels, these inconsistencies in compression artifacts can be highlighted by comparing the original image with a version saved at a specific quality (here, 90). The function saves the input image at a specified lower quality, then calculates the pixel-wise absolute difference between the original and the re-saved image. This difference is then enhanced to make subtle compression differences more visible. The resulting ELA image serves as the input feature for our models.

4. After obtaining the ELA image, it is resized to the specified `image_size = (128, 128)` and normalized by dividing pixel values by 255.0 to scale them to the range [0, 1]. The processed ELA image is appended to the `X` list, and label 1 (indicating a real image) is appended to the `Y` list. This process continues until `MAX_SAMPLES_PER_CLASS` authentic images have been processed.

5. A similar process is then followed for the tampered images located in the `/content/casia-dataset/CASIA2/Tp/` directory. The same `convert_to_ela_image`, resizing, and normalization steps are applied. However, for tampered images, label 0 is appended to the `Y` list. Again, the loading is limited to `MAX_SAMPLES_PER_CLASS` tampered images.

6. Finally, the `X` list (containing the ELA images) is converted to a NumPy array, and the `Y` list (containing the labels) is converted to a NumPy array of categorical labels using `to_categorical` for the binary classification task (real or fake). The data is then split into training and validation sets using `train_test_split` with a `test_size` of 0.2 and a `random_state` of 5 for reproducibility.

4.4.3 TRAINING SETTINGS

The Model is implemented using Python 3.11.Several open-source libraries such as Numpy 1.26.0, Pandas 2.2.2, Tensorflow 2.8.1, Keras 3.3.3, and etc are used. The Network is trained and validated on 8 GB of memory and 160 GB space as part of Kaggle's free compute support. Kaggle's Tesla P100 GPU was used.

For binary classification problems, the model is created using the Adam optimizer with a learning rate of 1e-4 using binary entropy as the loss function. Binary cross entropy calculates the average cross-entropy loss across all samples, penalizing the model more heavily for confidently incorrect predictions. A batch size of 100 samples is employed during training, and validation data is supplied to assess the model's performance.

Ten epochs of training are done, and multiple callbacks are used to track training progress and avoid overfitting. These callbacks include ReduceLROnPlateau, which lowers learning rate if validation loss plateaus for three consecutive epochs, EarlyStopping, which stops training if validation loss doesn't improve for five consecutive epochs, and ModelCheckpoint, which saves the optimal model weights based on validation loss.

4.5 GENERATIVE ADVERSARIAL NETWORK (GAN) FOR DATA AUGMENTATION

To augment the training data with synthetic tampered images, a DCGAN-inspired Generative Adversarial Network (GAN) was implemented. This architecture, known for its effectiveness in image generation, comprises two main components: a Generator and a Discriminator.

The Generator is designed to create synthetic images from a random noise vector. It begins with a dense layer to project the noise into a higher-dimensional space, followed by reshaping into a foundational feature map. Subsequently, a stack of deconvolutional layers (Conv2DTranspose) are used to progressively up sample this feature map, increasing its spatial dimensions and learning to generate image-like structures. Batch normalization is applied after each deconvolutional layer for training stability, and LeakyReLU activation introduces non-linearity. The final layer uses tanh activation to output the synthetic image with pixel values ranging from -1 to 1.

The Discriminator acts as a binary classifier, tasked with distinguishing between real ELA-processed images from the dataset and the synthetic images produced by the Generator. Its architecture consists of a series of convolutional layers (Conv2D) that extract features and down sample the input image using a stride. LeakyReLU activation

is applied after each convolutional layer. The extracted features are then flattened, and a final dense layer with a sigmoid activation outputs the probability that the input image is real.

The Generator and Discriminator are trained in an adversarial manner for 40 epochs. The Discriminator is trained to maximize its accuracy in identifying real and fake images, while the Generator is trained to produce images that the Discriminator misclassifies as real. Both networks are optimized using the Adam optimizer with a learning rate of 1e-4 and the binary cross-entropy loss function. After training, the Generator was used to generate 1500 synthetic tampered images, which were then rescaled to the 0-1 range to align with the original image data.

4.6 CONVOLUTIONAL NEURAL NETWORK (CNN) FOR FORGERY DETECTION

Convolutional Neural Networks (CNNs) are highly effective for image classification due to their ability to automatically learn hierarchical spatial features through convolutional filters. This makes them particularly well-suited for identifying patterns and anomalies indicative of image tampering, especially when used in conjunction with ELA-processed images that highlight subtle compression differences.

The CNN model architecture (build_forgery_detection_model) is implemented as a sequential model, meaning the layers are stacked linearly. This relatively simple architecture is designed for binary classification (real or fake) and consists of the following components:

- Several convolutional blocks, each containing one or more Conv2D layers with ReLU activation for feature extraction. These are followed by MaxPooling2D layers, which down sample the spatial dimensions of the feature maps and increase the receptive field of subsequent convolutional layers.
- A Flatten layer that transforms the 2D feature maps from the convolutional blocks into a 1D vector, preparing the data for the fully connected layers.

- A Dense layer with ReLU activation, followed by a Dropout layer (with a rate of 0.5). Dropout is a regularization technique used to prevent overfitting by randomly setting a fraction of the neurons to zero during training.

- A final Dense layer with SoftMax activation, which outputs a probability distribution over the two classes: "fake" and "real".

The CNN is trained using the Adam optimizer with a learning rate of 0.0001 and the categorical cross-entropy loss function, appropriate for multi-class classification with one-hot encoded labels. The training is conducted for CNN_EPOCHS = 8 epochs under two distinct scenarios:

- Baseline: The CNN is trained exclusively on the original ELA-converted real and fake images from the CASIA dataset.

- Augmented: The CNN is trained on a combined dataset that includes the original ELA-converted images along with the synthetic tampered images generated by the GAN. The labels for these generated fake images are also one-hot encoded to represent the "fake" class.

4.7 SYSTEM REQUIREMENTS

Running this project effectively on Google Colab with adequate computational resources requires a minimum of 13 GB of RAM (recommended), with more being beneficial for handling larger datasets. Storage-wise, at least 110 GB is needed to accommodate the dataset and intermediate files. A dedicated GPU with sufficient memory is highly advisable to significantly accelerate the training of the deep learning models (GAN and CNN).

CHAPTER-5

RESULTS

The proposed model is trained, validated, and tested on the above-mentioned dataset. It performs well on the dataset. The work evaluates the model with accuracy as the benchmark metric.

5.1 ACCURACY vs EPOCH

In training deep learning models, an 'accuracy vs. epoch' graph illustrates how the accuracy of a model changes over training epochs. The accuracy of the model refers to the proportion of correctly classified samples out of the total number of samples in the dataset. This metric is often used to evaluate the performance of classification models. The accuracy is usually calculated on a validation set during training.

An epoch is one complete pass through the entire training dataset. During each epoch, the model iteratively updates its parameters (weights and biases) based on the gradients of the loss function with respect to these parameters. Training typically involves multiple epochs.

The 'accuracy vs. epoch' graph plots the accuracy of the model on the y-axis against the number of epochs on the x-axis. Each point on the graph represents the accuracy of the model after completing a certain number of training epochs.

On observing the 'accuracy vs. epoch' graph, we found that at the beginning of training (early epochs), the accuracy is typically low (initial phase). This is because the model's parameters are randomly initialized, and it has not learned to make accurate predictions yet.

As training progresses, the accuracy is increasing. So, we can say that in the training phase, the model learning from the training data and improving its ability to make correct predictions.

The accuracy is usually computed on a separate validation set (not used for training) after each epoch. The accuracy on the validation set is helping to monitor the generalization performance of the created model. If the accuracy on the validation set starts decreasing while the accuracy on the training set continues to increase, it might indicate overfitting.

Eventually, the accuracy is reaching to a plateau, where further training epochs do not significantly improve performance. This is indicating that the model has converted to a solution.

Analysing the "accuracy vs. epoch" graph helps machine learning practitioners understand how their model is learning and whether adjustments to the learning rate, model architecture, or other hyperparameters are needed to improve performance.

5.1.1 BASELINE MODEL (TRAINED WITHOUT GAN AUGMENTATION)

The CNN trained on the original ELA-converted data achieved a validation accuracy that plateaued around 88% after a few epochs, as seen in the "Model Accuracy Comparison" graph. When evaluated on separate subsets of the original data, the baseline model demonstrated a significant disparity in performance: 100.00% accuracy on real images but 0.00% accuracy on fake images. This indicates that the model, without exposure to a wider variety of tampered image characteristics, became highly specialized in identifying real images but failed to generalize to unseen forgeries present in the evaluation set.

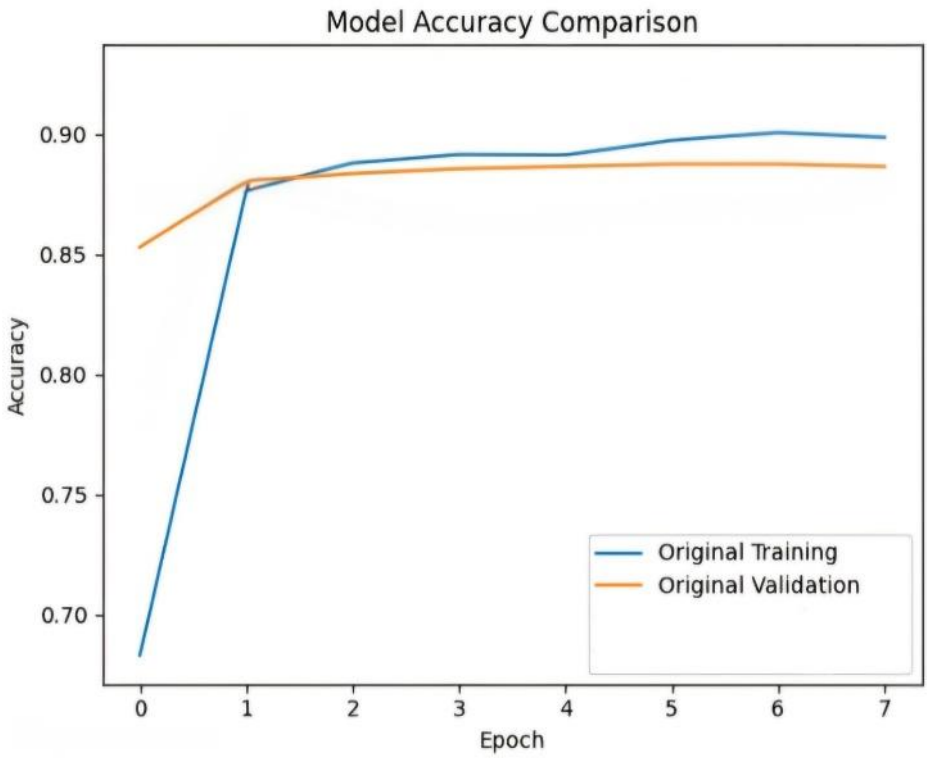

Figure 8: Baseline Model Accuracy Graph

5.1.2 AUGMENTED MODEL (TRAINED WITH GAN AUGMENTATION)

The CNN trained on the augmented dataset (original ELA images + GAN-generated fake images) showed a different training dynamic. The training accuracy reached a higher peak compared to the baseline. However, the validation accuracy, while starting at a reasonable level, fluctuated and plateaued at a similar overall level to the baseline. The evaluation on unseen original data revealed an improved accuracy of 9.00% on fake images, accompanied by a slight decrease to 94.00% on real images. This suggests that the GAN-generated images provided the model with some additional information about potential forgery characteristics, improving its ability to detect fake images it hadn't seen before, although the improvement was modest.

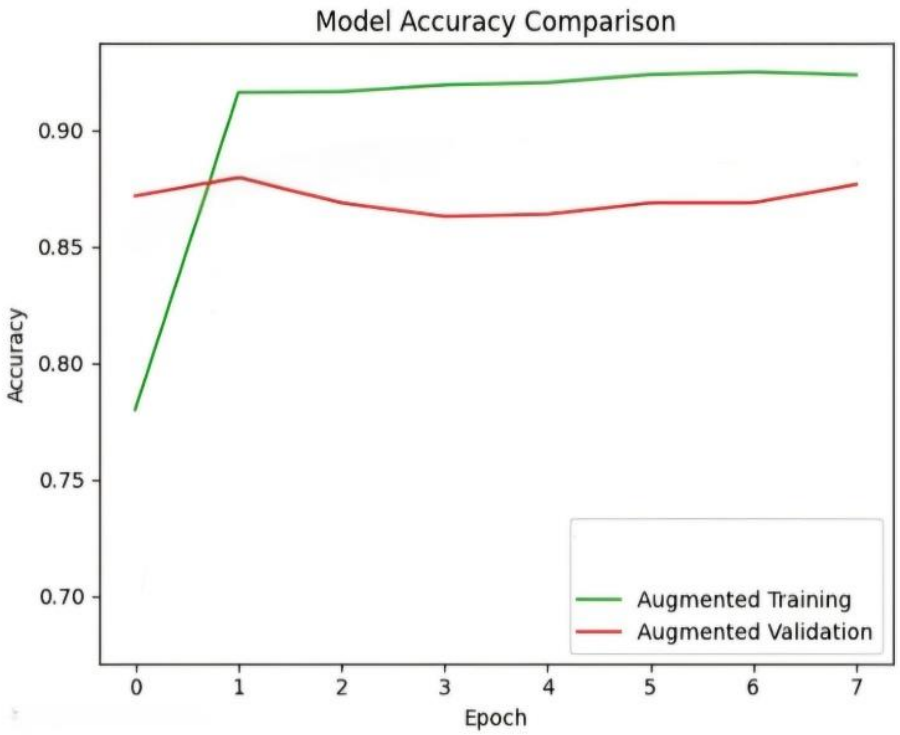

Figure 9: Augmented Model Accuracy Graph

5.2 COMPARISON

The average accuracy across both real and fake image evaluation sets for the baseline model was

(100.00% + 0.00%)/2 = 50.00%.

For the augmented model, the average accuracy was

(94.00% + 9.00%)/2 = 51.50%.

This represents a modest improvement of 1.50% in average accuracy due to the GAN-based data augmentation. While the GAN did contribute to a better detection rate for fake images, the overall impact on the model's generalization ability, as measured by the average accuracy on unseen original data, was limited.

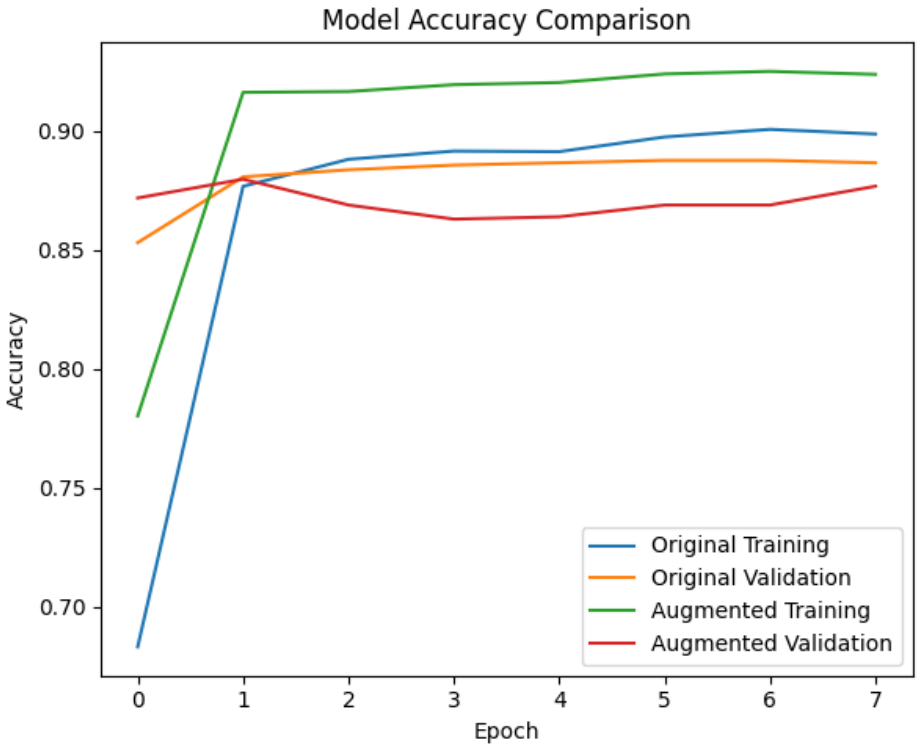

Figure 10: Model Accuracy comparison graph

5.3 TRAINING HISTORY COMPARISON (MODEL LOSS)

The "Model Loss Comparison" graph shows Loss (y-axis) over Epochs (x-axis).

- Original Training Loss (Blue): Starts high, decreases significantly initially, then slows, suggesting approaching learning capacity.
- Original Validation Loss (Orange): Decreases initially, then plateaus and slightly increases, indicating potential overfitting.
- Augmented Training Loss (Green): Starts higher, sharp initial decrease, continues decreasing, ends lower than baseline.
- Augmented Validation Loss (Red): Fluctuates more, decreases initially, then increases and plateaus similarly to baseline, possibly due to GAN image characteristics.

A loss vs. epoch graph is a fundamental visualization used in training machine learning models, including deep learning models. It plots the value of the loss function (typically the training loss) against the number of epochs during the training process.

We can infer many things from the graph plotted.

The x-axis represents the number of training epochs, which are complete passes through the entire training dataset. The y-axis represents the value of the loss function, which measures the difference between the predicted outputs of the model and the true labels in the training data. The shape of the loss curve over epochs provides insight into the training progress and the performance of the model. Initially, the loss is typically high as the model's parameters are randomly initialized, and it hasn't learned to make accurate predictions yet. As training progresses, the loss decreases as the model learns from the data and adjusts its parameters to minimize prediction errors.

Ideally, the loss should decrease steadily over epochs, indicating that the model is improving and converging towards an optimal solution. However, the loss curve may exhibit fluctuations due to factors such as noisy data, model complexity, or learning rate settings. Monitoring the loss curve helps to ensure that the model is making progress and not overfitting or underfitting the data.

Overfitting occurs when the model learns to memorize the training data instead of generalizing well to unseen data, leading to a decrease in training loss but an increase in validation loss. Underfitting, on the other hand, occurs when the model is too simple to capture the underlying patterns in the data, resulting in high training and validation losses. The loss vs. epoch graph can reveal signs of overfitting or underfitting by comparing the training and validation loss curves.

Overall, the loss vs. epoch graph is providing valuable feedback on the training dynamics and helping us to monitor and diagnose the performance of the created models during training.

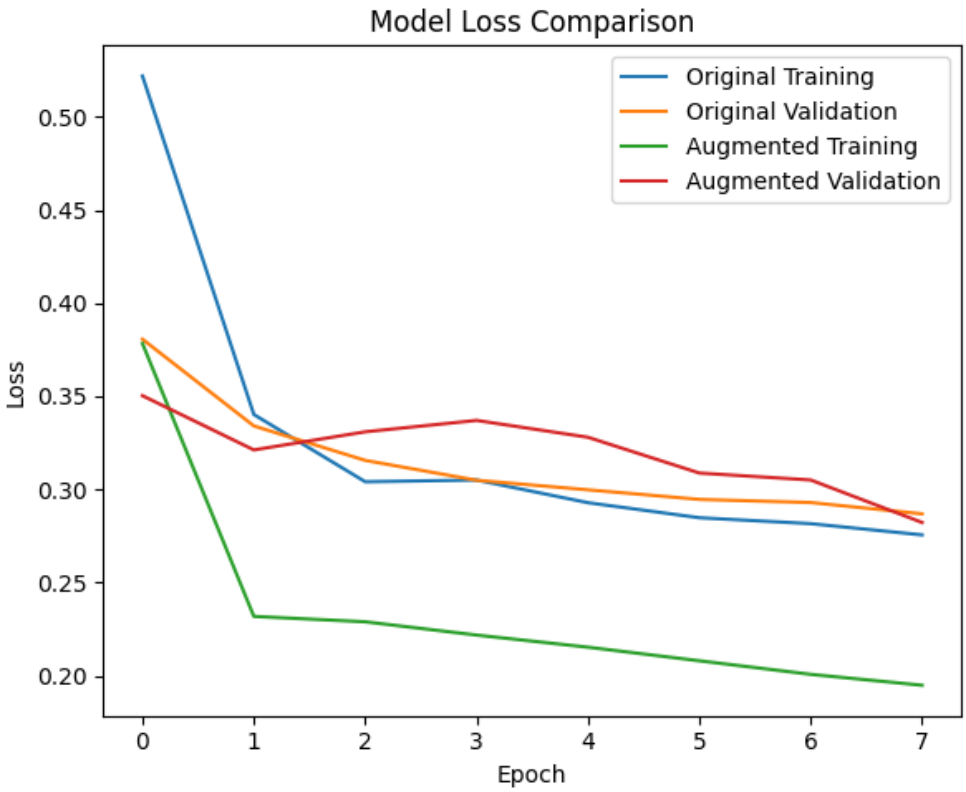

Figure 11: Model Loss comparison graph

Interpretation: Loss curves indicate GAN augmentation influenced training dynamics. Augmented model training loss was smaller, but validation loss did not improve significantly, supporting evaluation metrics of modest fake image detection improvement without extreme overall generalization gain. Plateauing/slight rise in validation loss indicates there is limited improvement with existing setup and possible overfitting. Lower loss is preferable.

5.4 TRAINING HISTORY COMPARISON (MODEL ACCURACY)

The "Model Accuracy Comparison" graph shows Accuracy (y-axis) over Epochs (x-axis).

- Original Training Accuracy (Blue): Starts low, rapid initial increase, continues improving, reaches high accuracy.
- Original Validation Accuracy (Orange): Increases initially, then plateaus with little further improvement, indicating overfitting.
- Augmented Training Accuracy (Green): Starts lower, very sharp initial increase, surpasses baseline, reaches highest training accuracy.
- Augmented Validation Accuracy (Red): Starts higher, fluctuates more, some initial improvement then plateaus/slight decrease, similar final accuracy to baseline.

Interpretation: Accuracy curves indicate GAN augmentation influenced training. Augmented model's training accuracy was greater but final validation accuracy the same as baseline, which means GAN didn't significantly improve generalization to unseen data, even though it may have assisted in learning more features. Plateauing validation accuracy implies there is little further improvement. Greater accuracy is better.

CHAPTER-6

ANALYSIS

The section presents the analysis based on the collected empirical evidence and theory.

6.1 KNOWLEDGE ABOUT COLLECTION

Privacy is a recurring keyword in consent processes between companies and users. According to [29], consumers need to feel their own perceived control over sharing their personal data. They conducted a study to see if consumers were willing to sell their personal data to Data Brokers. [12] discovered in their study that customers demanded a smaller amount if they received services in return for sharing their personal data, while they demanded a higher amount if they only paid money. One problem expressed in the research that [17] showed is that consumers can have strong integrity but low knowledge about what collecting personal data online is, in relation to personalized marketing.

Spiekermann [7] argued that personal data can be seen as a tradable asset. They believed that the data creates added value for companies and can mean an increase in the efficiency of marketing work.

6.2 RULES AND LAWS

Tikkinen-Piri [9] described how GDPR meant changes for companies to adapt to in order to have the privacy of private individuals met. Both companies and private individuals needed to increase their knowledge of the law and gain an increased understanding of what the law would entail.

Individuals should be given the opportunity to control their own personal data and have the opportunity to withdraw their consent if they wish. This view is shared by [9], where they described that the individual should be given the opportunity to control and manage their own data. Kollnig [28] highlighted that the GDPR provides room for

interpretation, which can make the establishment of the law difficult to follow. This meant risks that the process became more complicated than the original purpose.

6.3 THE CONSENT PROCESS

Kollnig [28] described that rules and laws such as the GDPR have meant a change where the storage and processing of personal data needs to take place according to regulations. This has meant higher pressure on consent processes that can be done through cookies. Through cookies, the online user can choose which data to collect, some cookies are necessary according to the companies and cannot be adjusted. but companies need to give the customer the opportunity to control their own consent.

Rules and laws have led to the development of consent standards, but when laws have had room for interpretation, it has been more difficult to handle the law correctly. This has meant an abundance of information, which has made it difficult for consumers to absorb the information. GDPR is intended to provide security for consumers, and the law includes the principle of transparency, but this has not always been followed [28]. Kollnig [28] argued that misleading and meaningless information is included, which then does not enable transparency.

According to [28], a model is rather created for companies to mask their theft of personal data. Bergemann [23] argued that third-party cookies are essential for companies that want to market their products through internet-based advertisements.

Although the GDPR law has the responsibility to inform consumers about this service, this is poorly communicated, as consumers do not know what the service entails.

6.4 PERSONALIZED MARKETING

Wertenbroch [12] described that reducing the collection of personal data means that the consumer cannot be offered as many choices. If the consumer's online behaviour cannot be tracked, it cannot form part of the marketing towards the user. This means that personalized content cannot be maintained, which means that the consumer cannot take advantage of competitive prices or multiple proposals from different companies.

Personalized marketing is not necessarily a positive thing as it can infringe on the individual's privacy.

Most of the people see it as an advantage that alternatives and suggestions come up in the flow and share Wertenbroch's [12] view that the collection of personal data creates multiple choices.

Kim [13] described that consumers rarely appreciate advertising that they can feel a distance from. General advertising can therefore become outdated as behavioural advertising instead leads to higher relevance. However, they described the problem that consumers must also be willing to share their personal preferences. If a company repeatedly encourages sharing their personal information, the consumer may see it as a privacy problem [13]. The authors continued to describe that it is a balance where marketers must evaluate how willing consumers are to share.

According to the authors [13], it is problematic if customers see it as a breach of privacy as it means that customers feel insecure and less willing to share their information.

6.5 SECURITY

Kim [13] described that transparency from companies on how they handle personal data can mean higher trust, which can generate benefits. If customers also expect and demand transparency on how personal data should be handled, it can mean higher pressure on companies, which can lead to change. Lavin [21] described that it is important for companies to be clear to the consumer why they collect personal data through cookies. The purpose is to help consumers to receive more relevant marketing. If customers get the impression that companies collect data and will misuse it, consumer trust disappears [21]. Several people expressed their concern about collected personal data precisely because they believe that companies can misuse the data.

Turow [54] conducted a study in 2018 to investigate the understanding of how American consumers reasoned about data collection. Consumers who showed strong trust in legal laws were more likely to share their personal data. The authors described how young adults who were raised with the internet from the beginning have a different

understanding and acceptance. The authors described how understanding and acceptance is increasing among younger people who have grown up with it [54].

6.6 INCREASED CONSUMPTION

Kim [13] described how personalized marketing enabled companies to contact specific target groups. They integrate with customers using the customer's own behavioural patterns. From a marketing perspective, it is an effective way to convince the customer as it functions as an exposure tool.

6.7 UNCERTAINTY

Kim [13] described the risk that the company faces when they choose to track users' personal data.

What Mulligan [27] defines as offensive when individuals are misled by companies using how they expressed privacy policies on their website, can be identified in several of the customers. They pointed out that they perceive GDPR and the choices of cookies as complex, as they do not understand what information the website collects about them, while at the same time they believe that it is easy to get away with collecting and sharing personal data.

6.8 RISKS

Jagadish [24] pointed out the problem that users risk sharing their digital contacts' personal data by consenting to the sharing of their own. Individuals who have not given consent can be affected by someone else sharing their contact list with other companies or apps. The author refers to a scandal where an app gained access to personal data about people who did not use the app. The reason why this happened was through other people who had approved the collection of personal data. The author argued that it requires personal reflection for the individual to understand that certain personal data that they accept to be shared may mean that it is done at someone else's expense.

6.9 CONCERNS ABOUT THE FUTURE

Oyserman [25] argued that the human relationship that individuals have with AI services results in users tending to be unaware of what personal data they are actually sharing.

Brill [4] state that there is concern about how personal data is processed in AI services and how it will be processed in the future, while users tend to have a certain trust that their personal data is secured. Several people expressed concern about personal data being misused but that they also have an expectation that AI services work to secure personal data.

6.10 LACK OF CONTROL

Acquisti [18] stated that users tend to decide what personal data they should share on the internet based on what other users choose. Acquisti [18] also identify that users who perceive that a problem that they see as serious cannot be solved, there is a risk that the brain will cope by accepting the problem.

Oyserman [25] also identify the behavioural pattern in humans of not being willing to take the time to avoid sharing personal data.

Weydert [29] described that the key to getting customers to share their personal information is for the consumer to experience self-control. If the consumer perceives it as control, the consumer may want to share more of their own information. However, this willingness is reduced if it is sensitive personal information, as fewer people are willing to share that personal information. If choices and information are offered about what information is collected and if the information is easily accessible and manageable for the customer to absorb, it can lead to the consumer feeling more secure.

CHAPTER-7

CONCLUSION

The section presents the conclusion of the study, practical and theoretical contributions, and suggestions for future research.

The purpose of the study was to gain an understanding of how the positive aspects were put in relation to the disadvantages. That there is now a concern linked to sharing one's personal data can be seen in the survey and in accordance with Kim [13]. We agreed with the view held by the authors Acquisti [18] and Oyserman [25], as there are certain problems with the consent process. For example, cookies, but that it ends at a stage where they perceive that they have no opportunity to influence the situation. This means that the choice that remains is to accept the sharing of personal data if it is to maintain the standard expected in society.

In accordance with Kollnig [28] and Tikkinen-Piri [9] would allow consumers to control what information is disclosed, but the process has become more complicated than necessary. Making it more difficult to refuse and lacking laws and regulations that are intended to protect consumers do not help to the extent that could be required. Tikkinen-Piri [9] also described that making it more difficult to refuse creates an adverse effect for the consumer because companies try to circumvent their obligations. In cases where the consumer does not feel protected by rules and laws, the result is that the consumer feels less willing to share their personal data, which is consistent with Kim [13] view. If it is too difficult to say no to sharing personal data, the consumer may perceive it as the company planning to misuse personal data, which makes the consumer more restrictive.

Oyserman [25] described a risk that may be significant in the future. Humans base their experience of human communication patterns when communicating between AI-based services, which may entail risks for the collection of personal data and how it will be handled in the future.

This study has concluded that for consumers to be willing to share their personal data, it is necessary that the service generates positive aspects.

If the consumer does not experience any benefits or positive aspects of sharing personal data, they will not be willing to share their own personal data. If the consumer only sees risks with sharing personal data, it is more likely that they are afraid of misuse of personal data and thus actively choose to prevent sharing. The study has been able to clarify which factors the consumer considers decisive in the decision-making process, which has then been analysed using theory. A consistent aspect is the consumer's experience, which plays a significant role in how the consumer will then act, linked to the various factors.

The meaning of the word privacy as a feeling that the individual's private and personal boundaries are respected and that the choice to share personal data is up to the individual and not the company behind the website. The GDPR is the law that is supposed to protect personal data theft and dissemination, but that the law is complex and the relationship between users and the law is uneasy in several cases. They criticized companies that collect data without it being made clear, since this does not give the consumer the opportunity to decide for themselves over their personal data.

The difficulty of refusing cookies leads to involuntary sharing, which creates frustration and distrust on the part of consumers. The result that can be extracted from this uneasy relationship is that there is a risk of a deteriorating relationship between users and companies, since the lack of trust in the company risks increasing.

The study also identifies a decrease in trust in companies when users feel manipulated and deceived by persecution via digital tracking of personal data. When this trust decreases, the company risks losing consumers and losing valuable personal data that could be used for more effective marketing, in the form of personalized advertising. Lavin [21] described this problem by saying that if the consumer believes that personal data will be misused, the consumer loses trust. Hence, personalized marketing can infringe on the individual's privacy. Despite this, disadvantages emerge, and hence it is an advantage that alternatives and suggestions are presented.

7.1 THEORETICAL CONTRIBUTION

The study aimed to investigate how consumers' perceptions and experiences of privacy and personal data for marketing purposes. The research question was answered by five value words emerging from the theoretical framework. The five value words and factors were developed from the theoretically collected material that the researchers in this study assessed as relevant when deciding on the sharing of personal data.

The five values of knowledge, trust, benefits, risk and control were identified as relevant based on the theoretical framework when consumers choose to make decisions about their privacy and personal data.

What emerged from the analysis was that if consumers do not consider the service exchange to be sufficient, the company loses the individual's personal data. This means that companies do not have the same opportunity to collect data for marketing purposes, which reduces efficiency.

Since the study concludes that the disadvantages and advantages constantly have an impact on which decision the consumer will ultimately make, it was decided that the model would be created in a circular form to demonstrate that the factors are interconnected.

7.2 PRACTICAL CONTRIBUTION

The study results in the decision process model that the researchers consider to be a suitable model to follow in marketing strategies on the internet.

This can, for example, be done by the marketing intermediary investigating how the target group experiences security and functioning processes when using their websites. The result of this will thus contribute to the company gaining an increased understanding of its consumer group and in turn increasing the chance of effective personalized marketing.

The consumers must experience self-control in order to be willing to share their personal data. The practical contribution from this study is that companies and marketing strategies gain insight into how they can build their strategy when collecting personal

data. If personalized marketing is to be directed at individuals, it needs to be done in such a way that consumers do not see it as offensive, which is why third-party cookies should not be the basis for marketing to consumers.

If the consumer feels trust and benefits, the individual is more likely to want to share their personal data. If personal data were to be misused, consumers will become even more restrictive about sharing their data. For the consumer to voluntarily want to share their personal data, the customer must experience an exchange of services. If the consumer does not see a personal benefit in sharing their personal information, individuals will not be willing to share their information, whether it is, for example, location information, telephone number, email or contact list.

Therefore, companies need to work actively to ensure that the consumer voluntarily provides their personal information and does not collect the information without the consumer's knowledge. Companies can therefore build relationships with consumers to demonstrate trust and confidence, which increases the likelihood that the consumer will share their information. If companies give the consumer the choice to refuse to share their personal information, the consumer will become less suspicious.

In this study, we have explored how personal integrity is affected by a check-in and check-out system with AI-supported facial recognition at a company.

The study shows that everyone is accepting a solution with AI-supported facial recognition, even though most people value their personal privacy highly and are critical of the technology itself and what the technology can be used for. As long as the technology is only used in the entrance for check-in and check-out and they have control over what the data is used for and that the system is secure, most people accept the technology. However, if the technology were to be present in more places in the premises, some people would feel monitored.

There is also a fear that personal contact will disappear when a company implements such a system. Many believe that exchanging a few words with the receptionist when you arrive at the office is important, and that those who do not work in the office on a daily basis may need more information than the system can provide.

The technology itself is also not completely flawless, as it requires large amounts of data to correctly learn to identify people and is often better at identifying certain specific groups of people than other groups that it is not as trained on. This can lead to some employees having difficulty being identified correctly and the technology not working as well on them. There is also a risk that the technology will not work if the person has any damage or other markings on their face that the algorithm does not consider the face to be similar enough. There should therefore always be another way for employees to enter the office, for example by using a code or access card.

We believe that the technology must be more developed to be used as a sole solution, the algorithms must be able to identify all employees regardless of ethnic background with great accuracy and also be able to identify employees if they have any damage to their face or something else that makes their points not match completely with what the algorithm has saved.

We also believe that it is very important for the company is open about what the system will the system will be used for and how the collected data is used and saved.

If an employee were to change jobs, it is very important that the biometric information about this is immediately deleted and does not continue to be used by the company.

7.3 CNN MODEL FOR IMAGE MANIPULATION

In conclusion, the research presents a method within a deep learning framework based on a Convolutional Neural Network (CNN) that detects image manipulation.

This project investigated the use of GAN-based data augmentation, combined with Error Level Analysis, to enhance a CNN's ability to detect image forgeries. The results indicated a 1.5% improvement in the average accuracy on the evaluation set after augmenting the training data with GAN-generated synthetic tampered images, suggesting a marginal enhancement in the detection of unseen fake images. However, the overall impact on the model's generalization remained modest. A significant factor potentially limiting the effectiveness of the GAN augmentation was the necessity to use only a subset of the CASIA dataset due to computational constraints. This likely restricted the variety and realism of the generated synthetic forgeries, thus limiting their

ability to significantly improve the CNN's generalization to a broader range of unseen tampered images.

Moving forward, studies can examine the model’s performance on different datasets and look for the expansion and improvements that may lead to the model’s ability to be applicable to image forensics and security problem in the real world. Therefore, further research with more extensive datasets and refined GAN techniques is warranted to fully realize the potential of generative augmentation for image forgery detection.

CHAPTER-8

FUTURE RESEARCH

Sharing one's own personal information involves a consideration, but the protection of the privacy of others also needs to be protected because individuals have the power to share other people's contact information. We believe through this study that the topic of whether individuals value the privacy of others more than their own is a topic for further research. The organizations should prevent the dissemination of others' personal information as it is offensive to act with the personal information of others as it can limit the individual's privacy.

REFERENCES

[1] Van Ooijen, I. & Vrabec, HU. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. Journal of Consumer Policy, 42, p. 91-107. doi:10.1007/s10603-018-9399-7

[2] Affärsstaden. (2016). The 90s is a Consumer at the Fingertips. https://affarsstaden.se/esb-article/90-talisten-ar-en-konsument-ut-i-fingerspetsarna/ [Retrieved 2023-09-26].

[3] Casadesus-Masanell, R. & Hervas-Drane, A. (2015). Competing with privacy. Management Science, 61(1) doi: 10.1287/mnsc.2014.2023

[4] Brill, M.T., Munoz, L. & Miller J.R. (2019). Siri, Alexa, and other digital assistants: a study of customer satisfaction with artificial intelligence applications. Journal of Marketing Management, 35(15–16), pp. 1401–1436. doi:10.1080/0267257X.2019.1687571

[5] European Commission. (2022). Protection of personal data and privacy on the Internet. https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_sv.htm [Retrieved 2023-10-11].

[6] Bornschein, R., Schmidt, L. & Maier, E. (2020). The impact of consumers' perceived power and risk in digital information privacy: The example of cookie notifications. Journal of Public Policy & Marketing, 39(2), pp. 135–154. doi: 10.1177/0743915620902143

[7] Spiekermann, S., Acquisti, A., Böhme, R. & Hui, K.L. (2015). The challenges of personal data markets and privacy. Electron Markets, 25, p. 161–167. doi:10.1007/s12525-015-0191-0

[8] European Commission. (unpublished). What is personal data? https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_sv [Retrieved 2023-10-11].

[9] Tikkinen-Piri, C., Rohunen, A. & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34, p. 134-153. doi: 10.1016/j.clsr.2017.05.015.

[10] Smit, E.G., Van Noort, G. & Voorveld, H.A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. Computers in Human Behaviour, 32, p. 15-22. doi:10.1016/j.chb.2013.11.008

[11] Beresford, A. R., Kübler, D. & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. Economics Letters, 117(1), pp. 25-27. doi: 10.1016/j.econlet.2012.04.07712

[12] Wertenbroch, K. (2021) Marketing Automation: Marketing Utopia or Marketing Dystopia? *NIM Marketing Intelligence Review*. 13 (1), s. 18–23. doi:10.2478/nimmir-2021-0003

[13] Kim, T., Barasz, K. & John, K. L. (2019). Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness. *Journal of Consumer Research,* 45(5), s.906-932.

[14] Kumar, S. & Sharma, R.R. (2015). Empirical analysis of unethical practice of cookies in E-marketing. Abhigyan, 33(3), p. 42.

[15] Internetstiftelsen. (2022). Swedes and the Internet 2022. [Online] Available at: https://svenskarnaochinternet.se/app/uploads/2022/10/internetstiftelsen-svenskarnaoch-internet-2022.pdf [Retrieved 2023-09-28].

[16] Kingsnorth, S. (2022). Digital Marketing Strategy. n.o.:KOGAN PAGE LTD.

[17] Li, H. & Nill, A. (2020) Online Behavioural Targeting: Are Knowledgeable Consumers Willing to Sell Their Privacy? Journal of Consumer Policy, 43(4), p. 723–745. doi:10.1007/s10603-020-09469-7

[18] Acquisti, A. Brandimarte, L. & Loewenstein, G. (2020) Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. Journal of Consumer Psychology, 30(4), pp.736–758. doi: 10.1002/jcpy.1191

[19] Boerman, S.C., Kruikemeier, S. & Zuiderveen Borgesius, F.J. (2017). Online Behavioural advertising: A literature review and research agenda. Journal of Advertising, 46(3), pp. 363–376. doi: 10.1080/00913367.2017.1339368

[20] Gouda, M. G., Kovacs, J. M., Liu, A. X., (2012). A secure cookie scheme. Computer Networks, 56(6), pp. 1723-1730. doi: 10.1016/j.comnet.2012.01.013

[21] Lavin, M. (2006) “Cookies: What Do Consumers Know and What Can They Learn?", Journal of Targeting, 14(4), pp. 279-288. doi: 10.1057/palgrave.jt.5740188

[22] Beauvisage, T. & Mellet, K. (2020). Cookie Monster. Anatomy of a Digital Market Infrastructure. Consumption, Markets and Culture, 23(2), pp. 110-129. doi: 10.1080/10253866.2019.1661246

[23] Bergemann, D. & Bonetti, A. (2015). Selling cookies. American Economic Journal, 7(3), pp. 259-294. doi:10.1257/mic.2014015524]

[24] Jagadish, H. V. (2020) Circles of Privacy. Journal of Consumer Psychology, 30(4), pp. 774–779. doi: 10.1002/jcpy.1188

[25] Oyserman, D. & Schwarz, N. (2020) Identity-Based Motivation and the Logic of Conversations Obfuscate Loss of Online Privacy and What Policy-Makers Can Do About It. Journal of Consumer Psychology, 30(4), p. 759–766. doi:10.1002/jcpy.1189

[26] Sipior, J.C., Ward, B.T. & Mendoza, R.A. (2011). Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons. Journal of Internet Commerce, 10(1), p. 1–16. doi:10.1080/15332861.2011.558454

[27] Mulligan, D. K., Regan, Priscilla M. & King, J. (2020) The Fertile Dark Matter of Privacy takes on the Dark Patterns of Surveillance. Journal of Consumers Psychology, 30(4), p. 767–773. doi:10.1002/jcpy.1190

[28] Kollnig, K., Binns, R., Van Kleek, M., Zhao, J., Lyngs, U., Tinsman, C. & Shadbolt, N. (2021). Before and after GDPR: tracking in mobile apps. Internet Policy Review, 10(4). doi: 10.14763/2021.4.1611

[29] Weydert, V., Pierre, D. & Lancelot-Miltgen, C. (2019) Convincing consumers to share personal data: double-edged effect of offering money. The Journal of Consumer Marketing. 37 (1), p. 1–9. doi:10.1108/JCM-06-2018-2724

[30] Bryman, A. & Bell, E. (2017). Business research methods. 3rd edition ed. Malmö: Liber.

[31] Dignum, V., 2019. Responsible Artificial Intelligence : How to Develop and Use AI in a Responsible Way. 2019. Cham: Springer International Publishing.

[32] Norvig, P and Russel, S., 2021. *Artificial Intelligence: A Modern Approach*, Global Edition. 4th edn. Harlow: Pearson Education Limited

[33] Ertel, W., 2017. Introduction to Artificial Intelligence. 2nd ed. Cham: Springer International Publishing AG.

[34] Schmidt, L., Bornschein, R. & Maier, E. (2020). The effect of privacy choice in cookie notices on consumers' perceived fairness of frequent price changes. Psychology & Marketing, 37(9), p. 1263-1276. doi:10.1002/mar.21356

[35] Romanou, A. 2018. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. Computer law & security review, 34(1), 99-110.

[36] Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K. and Senior, A.W., 2013. Guide to biometrics. Springer Science & Business Media.

[37] Berle, I., 2020, Face Recognition Technology: Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images, Springer Nature Switzerland AG. pp. 9-12.

[38] Abate, A.F., Nappi, M., Riccio, D. and Sabatino, G., 2007. 2D and 3D face recognition: A survey. Pattern recognition letters, 28(14), pp. 1885-1906.

[39] Zeng, Y., Lu, E., Sun, Y. and Tian, R., 2019. Responsible facial recognition and beyond. arXiv preprint arXiv:1909.12935.

[40] Jafri, R. and Arabnia, H.R., 2009. A survey of face recognition techniques. journal of information processing systems, 5(2), pp.41-68.

[41] Bryman, A. and Bell, E., 2019. Social Research Methods. 5th ed. Oxford: Oxford University Press

[42] Karyda, M., Gritzalis, S., Park, J.H. and Kokolakis, S., 2009. Privacy and fair information practices in ubiquitous environments: Research challenges and future directions. Internet Research.

[43] Creswell, J. W. & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5:e upplagan ed. s.l.:SAGE Publications Lt.

[44] Gritzalis, S., 2004. Enhancing web privacy and anonymity in the digital era. Information Management & Computer Security.

[45] Kostka, G., Steinacker, L. and Meckel, M., 2021. Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. Public Understanding of Science, 30(6), pp.671-690.

[46] Marr, B., 2018. Is Artificial Intelligence dangerous? 6 AI risks everyone should know about. Forbes.

[47] Bhandari, V., 2020. Facial Recognition: Why We Should Worry About the Use of Big Tech for Law Enforcement. The Future of Democracy in the Shadow of Big and Emerging Tech (CCG, NLU Delhi/FNF, 2021)

[48] Andrejevic, M. and Selwyn, N., 2020. Facial recognition technology in schools: Critical questions and concerns. Learning, Media and Technology, 45(2), pp.115-128.

[49] Bragias, A., Hine, K. and Fleet, R., 2021. 'Only in our best interest, right? 'Public perceptions of police use of facial recognition technology. Police Practice and Research, 22(6), pp.1637-1654.

[50] Wang, Xijie & Dong, Bin & Wang, Zhiqiang & Ma, Jun. (2021). Wang et al. Respond. American Journal of Public Health. 111. e23-e23. 10.2105/AJPH.2021.306164.

[51] Morosan, C., 2019. Disclosing facial images to create a consumer's profile: A privacy calculus perspective of hotel facial recognition systems, International Journal of Contemporary Hospitality Management, 31(8), pp. 3149-3172.

[52] Katsanis, S.H., Claes, P., Doerr, M., Cook-Deegan, R., Tenenbaum, J.D., Evans, B.J., Lee, M.K., Anderton, J., Weinberg, S.M. and Wagner, J.K., 2021. A survey of US public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. PloS one, 16(10), p.e0257923.

[53] Tangerding, E., 2021. Beyond Data Protection: Applying the GDPR to Facial Recognition Technology (bachelor's thesis, University of Twente).

[54] Turow, J., Hennessy, M. & Draper, N. (2018) Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003-2015. Journal of

Broadcasting & Electronic Media, 62(3), p. 461–478. doi:10.1080/08838151.2018.1451867