Published online: 13 September 2024 DOI: 10.54254/2977-3903/11/2024110

Which factors most strongly influence the popularity of facial recognition software on mobile device?

Dongheng Zhu

Suzhou No. 1 High School, Jiangsu Province, Gongyuan Road, Gusu District (230 meters' walk from Exit 1 of Lindun Road Subway Station)

1413741069@qq.com

Abstract. Facial scanning is becoming more common as the commercial use of facial recognition technology expands. Face recognition technology, can be widely used in public security, finance, subway, airport and other important fields of natural identification. Now, the technology has also been applied to the routine outbreak control and prevention, through the form of "face recognition" to bring more convenient, safer and more accurate experience. However, with the development of technology, the drawbacks of facial recognition are gradually revealed, and people's opinions on the technology are mixed. As facial recognition is widely used in the market, protecting users' privacy information and data is becoming an increasingly important issue. In this article, this paper will discuss the different factors contributing to the popularity of facial recognition among people from five aspects, respectively from the aspects of devices and people. This paper was covered a number of parts in this article to explore what factors influence the popularity of facial recognition, racially biased, Accuracy of identification, public acceptance, Personal experience with technology, public perception of face recognition technology and Alternatives to FRS. The conclusion is that the factors which most strongly impact on FR is accuracy.

Keywords: facial recognition, mobile device, facial scanning

1. Introduction

Face recognition is a biometric identification technology based on information about a person's facial features. Portrait recognition typically refers to a series of technologies related to the use of cameras or camcorders to collect images or video streams containing faces, automatically detect and track faces in the images, and then perform face recognition on the detected faces.

This article mainly discusses whether the popularity of facial recognition will be changed under the influence of different factors. Because facial recognition is a very influential technology today, it has greatly affected people's lives. In this article, they will start with four points, the potential risks of facial recognition, the accuracy of facial recognition, the acceptance of facial recognition by the masses and the alternatives to facial recognition. At present, the racial difference is a major factor affecting the popularity. In today's world, the application error rate of facial recognition technology in countries of color is obviously much higher than that in Europe and America, which will lead some people of color to mistake it as a kind of racial discrimination. While the racial issue was a very serious problem in the last century, and now the world theme is equality for all, it has become a taboo topic. Second, the accuracy of facial recognition is also a very important factor to affect the popularity of facial recognition. Why facial recognition is so widely used today is because of its efficient and convenient use, once there is a problem with the accuracy, it shows that the most basic algorithm of this technology has a problem, which directly determines the upper limit of this technology. Third, the acceptance of the masses directly determines whether this technology can have a good reputation. In today's society, mass public opinion is a double-edged sword, and good use can ensure that this technology can produce huge benefits until it is thoroughly studied. Once there is a problem with public opinion , this technology to a large extent, no great benefits can be obtained. Finally, facial recognition is so widespread that it has competitors. This factor can also affect the popularity of facial recognition, different recognition methods have different advantages, such as fingerprint recognition, voice recognition and so on.

In the end, this paper concluded from four different factors, racial differences in today's society, only a few people will think that this technology has discriminatory meaning; Mass acceptance does not affect the basic advantages of this technology, facial recognition can get so much favor, because its most basic algorithm is very competitive today. Not to mention the alternative to facial recognition, all products other than facial recognition are currently on the market, such as iris recognition. The technology is

more accurate than facial recognition, but the price is far higher. Or fingerprint recognition, which is cheap and easy to use, but far less accurate than facial recognition. Facial recognition has an average advantage in today's market, which has also established its position as the market leader. Facial recognition has an average advantage in today's market, which has also established its position as the market leader. Is accuracy of facial recognition the highest priority factor? Also, if the most basic accuracy is high, there are other factors that we will discuss.

2. Research review

2.1. Facial recognition

Face recognition is a biometric identification technology based on information about a person's facial features [1]. Portrait recognition and face recognition, usually refers to the capture of an image or video stream containing a face by a video camera or camera, the automatic detection and tracking of faces in the image, and then face recognition of the detected faces [2].

In the 1960s, face recognition systems began to be researched, and after the 1980s, they continued to improve with the development of computer technology and optical imaging technology. In the late 1990s, it really entered the stage of primary applications, and was mainly implemented technically in the United States, Germany and Japan [3]. Whether it has a mature core algorithm and whether it can make the recognition results have practical recognition rate and recognition speed is the key to the success or failure of the face recognition system. The Face Recognition System, which integrates the expertise of artificial intelligence, machine recognition, machine learning, model theory, expert systems, video image processing, etc., and which also needs to combine the theory and implementation of intermediate value processing, is the latest application of biometrics. The implementation of its core technology demonstrates the transformation of weak artificial intelligence to strong artificial intelligence.

2.2. Potential risks

Racially biased is one of the most important risks in this area. Facial recognition has become an integral part of today's world, and its impact is huge. It makes people's lives so much easier, including getting around, paying money, entering and leaving their homes or companies [4]. But the boom in product sales also contains problems, more and more people are using this product, but the immaturity of the product is also gradually reflected. Due to the difference of race, some people with faces different from those of the native country are difficult to be identified. National Institute of Technology Standards, NIST, carried out research, which examined whether facial recognition software differed by race, gender and age [11]. 189 algorithms voluntarily submitted by 99 academic institutions, companies and other developers were reviewed in this study. These included the majority of the industry-leading systems from major technology contractors and companies such as Idemia, Intel, Microsoft, Panasonic, Sensetime and Vigilant Solutions. Amazon did not submit to the test, and CNN Business has learned from NIST that Amazon believes its software is incompatible with the test [11]. Amazon's facial recognition software, Rekognition, was sold to the Oregon State police to track suspects [11].

2.3. Detection result

In one-on-one matching, Asians and African-Americans are 10 to 100 times more likely to be the victim of make facial recognition errors than Caucasians (Different algorithms vary.) [5].

Native Americans experienced the largest rate of false positives of any ethnic group; For one-to-many matches, the false positive rate was higher in African American women [5].

Age and gender factors. Compared with men, women were more likely to be misidentified, and older people and children were tend to be misidentified as well. Middle-aged whites had the highest accuracy [5].

Algorithms developed by different countries have different performance. Algorithms developed in Asia, Africa, and the United States have high margins of error. Smaller differences in error rates between whites and Asians in algorithms developed in Asia [5].

2.4. Accuracy of identification

The accuracy of face recognition is especially restricted by the three factors of skin color, illumination and posture, resulting in the lack of stability of accurate recognition [9]. However, such stability will magnify the color bias of the system, leading to greater uncertainty in the accuracy of recognition. A test found that darker skin was responsible for a 39 per cent error rate, with darker skin becoming less accurate [6]. Secondly, under the influence of illumination, the accuracy of recognition will also decrease. Because the face gray features include "face contour features, face gray distribution features, organ features and template features", and as a three-dimensional object face is inevitably affected by light shadow, irradiation intensity and other external factors. When exposed to external illumination, it will change the relative distribution of face image gray, and then affect the contours of face

head, mouth, eyes and nose and other core areas, resulting in facial image changes. Such changes are even higher than those caused by individual differences [7]. Finally, attitude factors also affect the recognition accuracy. Face pose includes front and side (pitch, profile, rotation), and face is a "3D flexible skin surface with strong prosecutions". Different orientation pose shooting angles will produce different recognition accuracy for people of different ages, resulting in the reduction of the accuracy of recognition system performance [10].

2.5. Public acceptance

The research found that China has the highest acceptance of face recognition technology, Germany the lowest, and the UK and the US somewhere in between [12]. The four countries differed markedly in terms of socio-demographic factors and perceptions of the usefulness, reliability and consequences of face recognition technology. While previous studies have noted that face recognition technology is a tool for surveillance and control, this study suggests that people in the four countries priorities convenience and security rather than the surveillance and control that face recognition technology brings. Previous research has preliminarily discussed the influence of sociodemographic factors on the facial recognition technology acceptance [12]. A survey of biometric security technology in the United States found that acceptance increases with income and education. A telephone survey in Germany showed that less educated respondents and women were more receptive to surveillance policies. Acceptance of facial recognition technology increases with age, according to the Pew Research Center, which also found race to be a significant influencing factor. There is also data showing that where you live affects attitudes, with city dwellers having a stronger preference for extra security measures [12].

2.6. Personal experience with technology

Only the German public's acceptance was positively correlated with the frequency of exposure to different functions of the technology; Only in China and the United States, people who use face recognition technology more frequently have higher acceptance of face recognition technology; In Germany, the acceptance of face recognition technology in public places was low among people who were regularly exposed to face recognition technology applications, while there was no significant correlation in the other three countries[12].

2.7. Public perception of face recognition

In terms of the perception of the benefits of technology, except Germany, Chinese, British and American people's cognition of the convenience of face recognition technology is positively and significantly correlated with its acceptance; In all four countries, perception of the efficiency and security that face recognition technology brings had a significant impact on its acceptance [12]. In terms of technology risk perception, there is a significant negative correlation between the perception of privacy invasion and increased discrimination and the acceptance of face recognition technology in all four countries. It should be noted that there is a negative correlation between Chinese people's perception and acceptance of surveillance, while in Germany there is a positive correlation [12]. In terms of usefulness, the British and American people who think the technology is useful in a variety of occasions are more accepting. In terms of reliability, the reliability perception of face recognition technology has a significant impact on its acceptance in all four countries [12].

2.8. Alternatives to facial recognition

The former typically uses anthropometric data, such as fingerprint recognition, facial recognition, iris recognition, retina recognition and hand recognition. On the other hand, the latter typically uses measurements derived from human behavior, such as speech recognition, signature recognition, gait patterns, and keystroke dynamics. In recent years, with the swift development of touchscreen mobile phones, touch dynamics have increasingly been a hot topic in the field of biometric authentication [13].

2.8.1. Physiological biometric authentication

Physiological biometrics on the basis of physical characteristics of a person that are considered comparatively unchangeable, like fingerprints, face, iris/retina, and hand/palm [13].

(1) Fingerprint recognition: This is probably the most widely known authentication technology for successfully identifying individuals and has actually been used in mobile phones. For example, the 2000 Sagem MC959 mobile phone has a fingerprint identification system on the back panel [15].

(2) Face recognition: Face (or face) recognition system is a kind of application that uses facial features to identify or verify people from digital images or video frames. It is a popular biometric identification technology. Due to its extensive interdisciplinary nature, it has received wide attention from academia and industry [15].

(3) Iris recognition: The iris is an elastic, pigmentary, and connective tissue that governs the pupil, and it has a distinct form in the eye and between people. In the middle of the 1980s, the iris was regarded as a great biometric technology since no two irises are the same. Therefore, identifying a person by mathematical analysis of random patterns within the iris of an eye visible from a certain distance away is the main goal of iris recognition.

(4) Retinal Recognition: This authentication technique is used. A distinctive pattern on a person's retina for recognition. The human retina is a thin tissue made of nerve cells. Located in the eyes and behind each person's eyes. The retina is unique [18].

(5) Hand and palm recognition: Generally speaking, a person's hands do not change significantly after a certain age, however, human hands are not uniquely suited. Under such circumstances, the precision of hand recognition can be enhanced by combining other individual characteristics. In contrast, palmar veins are unique to each person, even among identical twins. The palm usually has a broad and complex pattern of blood vessels and therefore contains a wealth of distinguishing features for personal identification. For some research articles on palmprint verification, see [19, 20].

One of the major concerns that authors have relating to FNS (File Nesting System) is the lack of privacy. One solution is to take a ‘snapshot’ of a video rather than the full video itself, which can then be encrypted and only accessed through legal channels. In particular, an approach which relies on machine learning from data is especially promising as a viable alternative. However, the authors were not able to run an image processing program in real time and concede that the energy consumption required is not small [14].

Additionally, alternatives to FRS (Facial Recognition System) exist from the not-too-distant past. The Samsung SPH-S2300 makes use of iris recognition with an equal error rate of 0.05%, which is much smaller than the equivalent values for facial recognition software [13]. The authors also note that iris scanning achieves a success rate of 98.5% when glasses or contact lenses are worn whereas retina scanning requires the user to remove their glasses.

3. Discussion/ Development

Since the 1960s, there have been efforts to program computers to ‘see’ faces - to develop automated systems that can recognise faces and distinguish them - often referred to as face recognition technology. Computer scientists are pursuing FRTS (Fast Return to Sender) to devise smarter, more interactive machines, businesses and state government agencies see the technology as well-suited to "smart" surveillance systems - automating surveillance work to improve its efficiency and expand its reach. In tracking this technological quest, biometric future sees FRTS as typical examples of a failure of the technocratic approaches to governance, in which novel technologies are being courted as short-sighted resolutions to complicated society's issues. Sifting through news stories, press releases, policy statements, PR materials and other materials, Kelly Gates offers proof that the pursuit of FRTS is not about providing more security for more people, but rather is motivated by the priorities of businesses, law enforcement and national security agencies who all believe in the need for the technology [8], And unimpeded by its complex and potentially destructive social outcomes. By focusing on the politics of developing and deploying these technologies, "Our Biometric Future" does not argue that a particular technological future is inevitable, but that it is deeply contingent and debatable [21].

TABLE I
EXISTING USER AUTHENTICATION METHODOLOGIES.

Method	Instances	Properties
What you know	ID, Password, PINs, etc.	Can be shared and forgotten
What you have	Cards, Keys, Badges, ect.	Can be shared and duplicated
What you are	Fingerprint, Face, Iris, etc.	Not possible to share and repudiate

Figure 1. Existing User Authentication Methodologies [21]

3.1. Potential risks of facial recognition

3.1.1. Racially biased

With economic globalization, the whole world is advancing with the times. Face recognition is a hot topic, and every country is scrambling for more advanced technology. It is also hoped that people in their own country can use this technology as soon as possible. However, the speedy advancement of science and technology has also exposed a lot of problems, the racial difference is a big problem. A team of researchers from Japan found that black people tended to be less accurate than white people when facing a camera for facial recognition in the dark. The accuracy difference between white and black authentication is up to 2.1 times under dark conditions. Facial recognition systems have been accused of racial bias in people other than white people. Although this may

not affect the popularity of the software in predominately light-skinned countries and parts of the world (e.g., Europe, Japan, and other parts of Asia), it likely limits its mass adoption in the African continent. This result will help to develop a fair and more accurate certification system. Racial differences have a great impact on the perception of people who use facial recognition technology. There are about 200 countries in the world today, and the skin color of people in each place is different, for example, white people in Europe, fair-skinned people in Asia, black people in Africa, etc. Currently, the immaturity of facial recognition makes it harder to identify dark faces, especially in the dark. This can lead to doubts about the utility of the technology and whether it is worth the high price. Again, there may be a political dimension to this, where some people may see the difficulty in recognizing the faces of dark people as a sign of discrimination, given the history of efforts to discriminate against those with darker skin.

National Institute of Technology Standards, NIST examined whether the usefulness of facial recognition software differed by race, gender and age [11]. 189 algorithms voluntarily submitted by 99 academic institutions, companies and other developers were reviewed. These included a majority of the industry-leading systems from major technology companies and contractors including Idemia, Intel, Microsoft, Panasonic, Sensetime and Vigilant Solutions. Amazon did not submit to the test, and CNN Business has learned from NIST that Amazon believes its software is incompatible with the test. Amazon's facial recognition software, Rekognition, was sold to the Oregon State police to track suspects [11].

This are countered against by geography and security firms. Because technology in Asia focuses on Asian face-types. Computers also can be programmed as they see far more colors than the human eye. These strategies help to reduce issues based on race.

3.2. Accuracy of the identification

With the development of The Times, facial recognition is very common. Among them, the accuracy of recognition greatly affects the application of facial recognition products and their popularity among people. I think facial recognition today is mainly influenced by skin color, posture, and environmental lighting. The influence of skin color is weak, and the environment is the most influential factor. The environment can change anytime and anywhere, which will greatly affect the current immature facial recognition technology. For example, the dark environment or bumpy environment will affect the accuracy of recognition. This could also lead to lower consumer ratings of the technology. One test found that people with darker skin had a 39 percent inaccuracy rate, and those with darker skin had a lower rate [7]. Secondly, under the influence of illumination, the accuracy of recognition will also be reduced [7]. Because the gray features of face include "face contour features, face gray distribution features, organ features and template features", and face as a three-dimensional object, inevitably will be affected by light, irradiation intensity and other external factors. When exposed to external light, it will change the relative distribution of the gray scale of the face image, and then affect the contours of the face head, mouth, eyes and nose and other core areas, resulting in the change of the face image [7]. The variation is even greater than that caused by individual differences [6]. Finally, attitude factors also affect the recognition accuracy. The face poses both front and side (pitch, side, rotation), and the face is a "3D flexible skin surface with intense changes". Different azimuth and pose shooting angles will produce different recognition accuracy for people of different ages, resulting in lower accuracy of recognition system performance [6].

But the poor accuracy of facial recognition may have a big impact on people's lives. It can make things happen to people who do not know what they are supposed to do. Police arrested Steve Talley in 2014 after a series of bank robberies in the United States. He was severely beaten during his arrest and held under maximum security for nearly two months. His estranged ex-wife identified him as the robber from closed-circuit television footage, and an FBI facial examiner later corroborated her story. Turns out Talley wasn't a criminal. Unfortunately, the arrest took a toll on him, cost him his job and led to a period of homelessness. Talley is now a poster child for facial recognition gone wrong.

Just as Australia is launching a national facial recognition scheme. This will allow police agencies to search large databases of images using facial recognition software.

Importantly, the application of face recognition technology is not automatic, as is the case with autonomous boundary control systems. Instead, the technology generates a "candidate list" as follows. In order for the system to function fully, humans must review these candidate lists to determine if the target identity exists. In a 2015 study, my colleagues and I found that when reviewing a list of candidates, the average person makes a mistake in every two decisions and chooses the wrong person 40 percent of the time. 60% success rate is still lower than what a computer could achieve. Perhaps society does not realize that computers are still more accurate.

3.3. Public acceptance

The public are the most important part of our society at the same time, the acceptance of the masses to a large extent determines the development prospects of a product or technology, once the technology makes a great response to the masses, the technology will absolutely become a phenomenon of technology frenzy, moreover, once the masses of its evaluation is not high or poor, no matter how expensive the technology is, it will lose its chance. As a major development trend in today's world, facial recognition can have today's prosperity, and the acceptance of the public accounts for a large part. Although with the rapid development of information

technology, information leakage has become a major problem of information technology, facial recognition is no exception. Public acceptance will also be affected.

The survey data was analysed through a comparative statistical model in SPSS (Statistical Package for the Social Sciences), which substantiated the low level of awareness of face recognition technology among public transport users in the UAE compared to iris recognition and fingerprint authentication.[8]. The results show that Chinese citizens are more accepting of facial recognition technology than other countries, whether for public or private purposes.

In both China and Germany, gender and income were correlated with technological acceptance of face recognition, but in opposite directions. In China, women's acceptance is higher than men's, and high income is positively correlated with high acceptance; In Germany, men are more accepting than women, and higher income is negatively correlated with higher acceptance. As for the US and UK, gender and income were not significant correlation factors for acceptance [10]. The effect of education on acceptance was only found in Germany. In Germany, this effect is the second most important factor after safety. Ethnic factors were not significantly associated with acceptance in any of the four countries.

Previous experience has had mixed effects on public acceptance across the four countries, but overall, these effects are generally small, if any. Outcome perception plays an important role in the acceptance of technology. Perceived convenience, efficiency and security all have a positive effect on receptivity (but in Germany, convenience has nothing to do with receptivity), while privacy invasion and discrimination are negatively correlated with receptivity. The relationship between perceived monitoring and receptivity is negative in China. Positive in Germany; In Britain and America it is not. [10].

Perceived usefulness can enhance public acceptance in both Britain and America. For Germans, only the usefulness of the scene of airport customs and security increased its acceptability; On the other hand, Chinese people are more conservative, and their usefulness in the three scenarios of public street, financial identity verification and private house will reduce their acceptance, while usefulness in the other scenarios has no significant correlation with their acceptance. Perceived reliability is positively correlated with the acceptance of face recognition technology in all four countries. [10].

So, in this paper 's views, there are many aspects of acceptance that can influence the popularity of facial recognition. Gender, income, education level, previous experience or ethnic factors are only a small part of the factors. The only way to get people to accept this technology is to make them feel fast, convenient and safe.

3.4. Alternatives to facial recognition

With the rapid development of facial recognition technology, many well-known technology companies have realized the benefits of this technology and produced a number of derivative products, such as iris recognition, fingerprint recognition and so on. These technologies all show their special advantages and ways. Under the influence of these technologies, the face recognition market is facing unprecedented challenges.

3.4.1. Physiological biometric authentication

1) Fingerprint recognition: This is probably the most widely known authentication technique for successfully identifying individuals and has actually been used in mobile phones. For example, the 2000 Sagem MC959 mobile phone has a fingerprint recognition system on the back panel [11]. However, obtaining high quality fingerprint ridges and fingerprint details is a complex task as fingerprints can be affected by cuts, dirt and even wear and tear.

2) Face recognition: A face (or facial) recognition system would identify or verify a person from a digital image or video frame by using facial features and is a popular biometric technology. It has received a lot of attention from both academia and industry due to its wide range of interdisciplinary interests [12]. However, face (or facial) recognition systems have difficulty functioning under certain conditions (e.g., angle, pose); it may also fail to work properly in low light, when wearing sunglasses, long hair or other objects that obscure the face, and with low-resolution images.

3) Iris recognition: Iris is an elastic, pigmented and connective tissue that controls the pupil and it has a distinct pattern for each eye and each individual. In the middle of the 1980s, the iris was considered to be a good biometric identification technology because no two irises are the same. Therefore, identifying a person from a certain distance by mathematically analysing random patterns within the iris of the eye is the main goal of iris recognition [9]. The iris has been used as a means of personal identification since some of the early work, like [12, 13]. For example, the mathematical algorithms required to digitally encode the iris image were provided by Daugman to enable the comparison with real-time images. However, the main drawbacks of these biometrics are that they are expensive and time-consuming (i.e., the user must remain motionless while being scanned). The high cost is a limiting factor, although these biometrics are feasible on touch phones.

4) Retina recognition: This is an identity verification technology that uses the unique pattern on the human retina for identification. The human retina is a thin layer of tissue made up of nerve cells located at the back of the eye and is unique to each individual [14]. For the above reasons, this chart mainly talks about the performance of iris recognition, facial recognition and fingerprint recognition in recent years.

5) Hand and Palm recognition: Generally, human hands do not change noticeably after a certain age, but human hands are not uniquely suited. In these circumstances, combining other individual characteristics can improve the accuracy of hand recognition.

By comparison, palm veins are distinctive to each individual, even identical twins. The palm of the hand usually has an extensive and complex pattern of blood vessels and therefore contains a large number of features used to identify an individual. Several investigative articles about palm print verification can be found at [15, 16]. But its main disadvantage is that its performance is unstable and its accuracy is easily affected by human body and ambient temperature.

TABLE II
THE RESULTS OF PHYSIOLOGICAL BIOMETRIC AUTHENTICATION ON MOBILE PHONES WHICH CLAIMED BY RELATED WORKS.

Method	Works	Platform	Performance (%)		
			FAR	FRR	EER
Fingerprint recognition	[34] in 2005	BIRD smart phone E868	-	-	4.16
	[65] in 2012	Nokia N95 and HTC Desire	-	-	4.66 (Nokia N95) 14.65 (HTC Desire)
	[199] in 2012	Simulated dataset	0.03	3.23	2.0
Iris recognition	[163] in 2008	Samsung SPH-S2300	-	-	0.05
Face recognition	[1] in 2006	Nokia 6680	-	-	3.95
	[87] in 2007	Nokia N90	4 (Average authentication error rate)		
	[222] in 2012	Nokia Series 60 (S60) emulator and Nokia N73	-	-	3.58 (expected)
	[35] in 2014	Samsung Galaxy Nexus	2-3 (Average false alarm rate)		

Figure 2. Results of Physiological Biometric Authentication on Mobile Phones Which Claimed by Related Works [21]

3.4.2. Behavioral biometric authentication

1) Voice recognition: This is biometric technology that attempts to recognise the person speaking by their voice characteristics. The point is that everyone's voice characteristics are different, so the same words may have different meanings if spoken in a different tone or in a different context [17]. But there's also a big problem with voice recognition. If people have an injury to their vocal cords, or have a different voice for some other reason, it can lead to a high rate of mismatches.

2) Signature recognition: It measures and analyses the physical activity of signing, with behavioural recognition at its core. Traditionally, there are two approaches to signature recognition: static (i.e., signing on paper) and dynamic (i.e., signing on a digitising tablet). In mobile telephony, signature recognition is assumed to be dynamic and the user should write the signature in real time on a digitised tablet [13]. But the error rate for signature recognition has been high, because people can't keep their handwriting the same from moment to moment as they do at any given moment. Although the technology is still used on touch phones, it is not widely used.

3) Gait recognition: This is an emerging biometric technology that identifies people purely by analysing the way they walk. Currently, this biometric technology is still under development, but since most mobile phones (e.g., iPhone) now provide accelerometers in three main axes (X, Y, Z), it is feasible to deploy this technology on mobile phones [18]. Gait recognition has many influences on its accuracy, such as terrain, injuries, footwear, fatigue, personal quirks, etc.

4) Behavior Profiling: It aims to identify users based on how they interact with the mobile device service. During the authentication process, the current user's activities (e.g., dialing a phone number) are compared with an existing profile (created based on historical usage), which will, by means of a machine-learning method [19]. However, the main drawback of this technology is that the two phones do not behave in the same way when users interact with other phones in an unusual way.

5) Keystroke Dynamics: It will authenticate the user on a mobile device using the way and rhythm of the individual when typing characters on a keyboard or keypad, a method that has been known and studied for a long time. For example, Clarke et al. [20]. A feasibility study was first conducted in 2003 to use keystroke dynamics to verify the identity of mobile phone users based on their input method. They showed that 9.8% FRR and 11% FAR could be achieved using a neural network classifier. Subsequently, Buchoux and Clarke [20] carried out research and found that keystroke analysis is technically possible on mobile phones and that users are willing to adopt this method. But a major drawback is that recognition systems based on keystroke dynamics are difficult to accomplish consistently if the user performs an abnormal action.

6) Touch Dynamics: As mobile platforms have rapidly evolved, touchscreens have become a major input method in recent years. They are electronic visual displays that users can control through simple or multi-touch gestures by touching the screen. Global shipments of touchscreens are expected to reach 1.75 billion in 2013, with mobile phone shipments accounting for 73% of the total at about 1.28 billion, up 14.2% year-on-year.[21]. Thus, touch dynamics refers to the collection of detailed information about a single touch, such as touch duration and touch direction. It is very popular in the mobile market and an emerging topic in the literature. The downside of this technique is similar to keystroke dynamics in that it doesn't always complete the task once something is wrong. This chart mainly talks about the advantages and disadvantages of the mainstream recognition methods in the market today.

TABLE III
THE RESULTS OF BEHAVIORAL BIOMETRIC AUTHENTICATION ON MOBILE PHONES WHICH CLAIMED BY RELATED WORKS.

Method	Works	Platform	Performance (%)		
			FAR	FRR	EER
Voice recognition	[56] in 2008	Database	-	-	0.47
	[124] in 2011	Simulated Dataset	-	-	15
	[16] in 2012	Simulated Dataset	-	-	0.83
Signature recognition	[140] in 2008	Simulated Dataset	-	-	4
	[15] in 2012	Samsung Galaxy Note	-	-	0.17 (Stylus) 0.29 (Finger)
Gait recognition	[138] in 2005	Portable device	-	-	7
	[64] in 2010	Google G1 phone	-	-	20
Behavior Profiling	[132] in 2013	MIT Dataset [71], [72]	4.17	11.45	-
	[50]in 2013	iPhone	< 1 (Average AER)		
Keystroke dynamics	[40] in 2003	Simulated Mobile Phone	11	9.8	-
	[172] in 2005	Pentium IV microcomputer	-	-	3.6
	[42] in 2007	Nokia 5110	-	-	12.8
	[33] in 2009	Nokia 6680	-	-	13
	[95] in 209	Samsung SCH-V740	-	-	4
	[233] in 2009	Symbian mobile phone	2.07	1.73	-
	[141] in 2010	Simulated Platform	-	-	1.45 (under constraints)
	[137] in 2011	Nokia 6680	-	-	13.59
	[86] in 2014	Samsung Nexus S	-	-	0.08
Touch dynamics	[75] in 2012	HTC Android smartphone	4.66	0.13	-
	[143] in 2012	Google/HTC Nexus One	2.5	3.34	-
	[79] in 2013	Android phones (e.g., Droid Incredible phones, Nexus One)	-	-	< 4 (related to scenarios)
	[130] in 2013	Motorola Droid smartphone	4	4	-
	[144] in 2014	Google/HTC Nexus One	2.55	2.37	-

Figure 3. Results of Behavioral Biometric Authentication on Mobile Phones Which Claimed by Related Works [21]

TABLE V
EMPIRICAL EVALUATION OF DIFFERENT BIOMETRICS BASED ON THE SEVEN CHARACTERISTICS IN COMMON SCENARIOS.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Fingerprint	Medium	High	Medium	Medium	High	High	Medium
Face recognition	High	Low	Medium	High	Low	High	Low
Iris/retina recognition	High	High	High/Medium	Medium/Low	High	Low	High
Hand recognition	Medium	Medium	Medium	High	Medium	Medium	Medium
Palm vein recognition	Medium	High	High	Medium	High	Low	High
Voice recognition	Medium	Low	Low	High	Low	High	Low
Signature recognition	Low	Low	Low	High	Low	High	Low
Gait recognition	Medium	Medium	Low	Medium	Low	Low	Medium
Behavior profiling	High	Low	Low	High	Low	Medium	Medium
Keystroke dynamics	High	Medium	Low	High	Low	High	Medium
Touch dynamics	High	Medium	Low	High	Low	Medium	Medium

Figure 4. Empirical Evaluation of Different Biometric Based on The Seven Characteristics in Common Scenarios [21]

4. Conclusion

In conclusion, facial recognition is a highly competitive technology in today's society. The fast growth of computer, optical imaging and other related technologies, the application of face recognition in various fields continues to expand, and the market size of the face recognition industry continues to grow. At the same time, this is also used for various technology-concentric products, such as automated robots. Once there is a problem with the core technology, the widespread publicity will be empty talk. At the same time, the face information is mostly unmodified and unique biometric information, easy to manufacture synthesis, crack the verification process of face recognition, violation of privacy, reputation and property, resulting in more than a few cases, security issues are increasingly causing public concern, such as China, face recognition related legislation and regulatory measures have been introduced. In July 2021, the Supreme People's Court issued the Provisions on Several Issues Concerning the Application of Law in Civil Cases Involving the Processing of Personal Information by Facial Recognition Technology; The Personal Information Protection Law of the People's Republic of China was officially implemented in November 2021.

Meanwhile, the strong competitiveness of facial recognition has led others to use other technologies. Gradually losing money, which leads to information recognition in this area of the industry competitive pressure is very large. As the most basic requirement of high-tech information recognition, precision is very important. All additional derivatives, such as packaging, price, etc. Only when the algorithm based on this technical background is unique and convenient enough will there be other problems for everyone to discuss.

This paper thinks accuracy is one of the biggest factors affecting the popularity of face recognition, and this result will not be broken in the next few decades, after all, accuracy determines the reliability of the most basic algorithms of this technology until new technologies surpass it. In the future, facial recognition technology will become more and more mature, which also means that the technology will be saturated.

With the increasing growth and optimization of facial recognition technology, the recognition speed and accuracy of facial recognition have been very high. However, there are still some shortcomings in intelligence and self-learning. In the future, face recognition technology will be upgraded to enhance its intelligence level. The use of deep learning, neural network and other technologies, so that face recognition technology with independent analysis, independent expansion and other functions.

References

[1] Devue, C., Wride, A., & Grimshaw, G. M. (2019). New insights on real-world human face recognition. *Journal of Experimental Psychology: General, 148*(6), 994-1007. https://doi.org/10.1037/xge0000493

[2] Martinez-Martin, N. (2019). What are important ethical implications of using facial recognition technology in health care? *Proceedings of IEEE, 107*(2), 318-326. https://doi.org/10.1109/JPROC.2019.2890038

[3] Ishii, H., Fukumi, M., & Akamatsu, N. (1996). Face detection based on skin color information in visual scenes by neural networks. *Proceedings of IEEE International Conference on Image Processing (ICIP), 3*, 112-115. https://doi.org/10.1109/ICIP.1996.559612

[4] Braje, W. L., Kersten, D., Tarr, M. J., & Troje, N. F. (2010). Illumination effects in face recognition. *Attention, Perception, & Psychophysics, 72*(8), 1954-1963. https://doi.org/10.3758/BF03330623

[5] Anwarul, S., & Dahiya, S. (2018). A comprehensive review on face recognition methods and factors affecting facial recognition accuracy. *Proceedings of the 8th International Conference on Pattern Recognition Systems*, 379-388. https://doi.org/10.1007/978-3-030-29407-6_36

[6] Zhang, S. (2014). Research on face recognition algorithm under different posture. *Journal of Chengdu Electromechanical College, 25*(1), 25-29. Retrieved from http://www.cdmd.cnki.com.cn

[7] Tom, S. (2019). The best algorithms struggle to recognize Black faces equally. *Wired*. Retrieved from https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/

[8] Gates, K. A. (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York, NY: NYU Press. https://www.jstor.org/stable/j.ctt9qg8xd

[9] Riaz, A. M., & Ibrar, H. (2022). Analyzing and comparing public perception of facial recognition, iris verification, and fingerprints-based authentication systems. *2022 8th International Conference on Control, Decision and Information Technologies (CoDIT)*, 641-646. https://doi.org/10.1109/CoDIT55151.2022.9803965

[10] Lewis, P. G. (2019). Moral foundations in the 2015-16 U.S. presidential primary debates: The positive and negative moral vocabulary of partisan elites. *Social Sciences, 8*(8), 233. https://doi.org/10.3390/socsci8080233

[11] Baumann, J. (2000). SAGEM points a finger at GSM. Retrieved from https://www.sagem.com

[12] Peng, S., Yu, S., & Yang, A. (2014). Smartphone malware and its propagation modeling: A survey. *IEEE Communications Surveys and Tutorials, 16*(2), 925-941. https://doi.org/10.1109/SURV.2013.070813.00214

[13] Daugman, J. G. (1993). High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 15*(11), 1148-1161. https://doi.org/10.1109/34.244676

[14] Daugman, J. (2004). How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 21-30. https://doi.org/10.1109/TCSVT.2003.818350

[15] Kong, A., Zhang, D., & Kamel, M. (2009). A survey of palmprint recognition. *Pattern Recognition, 42*(7), 1408-1418. https://doi.org/10.1016/j.patcog.2008.10.011

[16] Zhang, D., Zuo, W., & Yue, F. (2011). A comparative study of palmprint recognition algorithms. *ACM Computing Surveys, 44*(1), Article 2. https://doi.org/10.1145/2071389.2071391

[17] Baumann, J. Voice recognition. Retrieved from http://www.hitl.washington.edu/scivw/EVE/I.D.2.d.VoiceRecognition.htm

[18] Clarke, N. L., Furnell, S. M., Lines, B. M., & Reynolds, P. L. (2003). Keystroke dynamics on a mobile handset: A feasibility study. *Information Management and Computer Security, 11*(4), 161-166. https://doi.org/10.1108/09685220310489526

[19] Buchoux, A., & Clarke, N. L. (2008). Deployment of keystroke analysis on a smartphone. *Proceedings of the 6th Australian Information Security Management Conference*, 1-7. https://doi.org/10.4225/75/57b55a56b876a

[20] Yang, J. (2012). Trends and forecast for 2013 touch panel market. *DigiTimes*. Retrieved from http://www.digitimes.com/news/a20121228RS401.html

[21] Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys & Tutorials, 17*(3), 1268-1293. https://doi.org/10.1109/COMST.2014.2386915

[22] Beranek, B. (2013). Voice biometrics: Success stories, success factors and what's next. *Biometric Technology Today, 7*(10), 9-11. https://doi.org/10.1016/S0969-4765(13)70128-0

[23] Cai, Z., Shen, C., Wang, M., Song, Y., & Wang, J. (2012). Mobile authentication through touch-behavior features. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 386-393.

[24] Chen, X., Tian, J., Su, Q., Yang, X., & Wang, F.-Y. (2005). A secured mobile phone based on embedded fingerprint recognition systems. *Proceedings of the IEEE International Conference on Intelligent Systems and Informatics (SISY)*, 549-553. https://doi.org/10.1007/11427995_57

[25] Clarke, N. L., & Furnell, S. M. (2007). Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security, 6*(1), 1-14. https://doi.org/10.1007/s10207-006-0006-6