**Select one engineering topic that is of interest to you, and show how one version of the technology is an improvement over a previous iteration of that same technology.**

Ever since the dawn of civilization, vision system has fascinated human beings and it was developed into biometric system in 1990s, coinciding with the development of computer systems. Biometrics is defined as the systems that identifying individuals through acquiring and analyzing biological or behavioral characteristics automatically.[1] This technology has evolved so rapidly that many unimaginable high-performance technologies appear in public within a decade such as fingerprint, speaker, blood vascular, and iris recognitions. This research paper aims to show iris recognition is more developed than other biometrics in terms of accuracy, security and privacy, so it can be significantly used as a reliable tool that helps us in this even more complicated world; and the applications of the iris recognition will be much broader in the future.

As a matter of fact, iris recognition is more reliable and robust in terms of accuracy than other biometrics like fingerprint recognition. For fingerprint-based system, all data is analyzed based on the image of fingers. Therefore, despite of high functional analyzing procedure, if the usage conditions are not satisfying, there is a chance that the results are inaccurate. For instance, dirt, grease, scars and even sweat to some extent can influence the results. Furthermore, some concerns include the effect of professional impact. The large amount usage of hands in touching with chemicals by engineers or rough materials by workers on site may seriously change the original condition of fingerprint which will interfere with the reader. On the contrary,

iris-based systems have the lowest false match rates among all currently available biometric methods. It works by identifying details like corona, crypts filaments, striations and rings which with a fairly conventional charge coupled device (CCD) camera. [2, pp. 21-22]It works well with eyeglasses and non-patterned contact lenses, as well as with different human races with various irises' colors. Besides, without any injuries or disease, iris is hard to be changed in a life time.

Like other technologies, biometrics has been questioned in the way of security since it is used in public because biological characteristics can be duplicated easily. For instance, fingerprint systems are particularly susceptible to spoofing. Without any technological equipment, fingerprint can be copied with a tape or inkpad. Some verification devices are not capable of distinguishing 2D from 3D. Thus, sometimes, a secure biometric system will accept non-legitimate presentation of the biometric identifiers with fake 2D fingerprints. Nonetheless, iris duplication is not as simple as copying fingerprint. The device is able to tell 2D and 3D images, and it is designed to scan irises and translate every single detail into a very complicated 512-byte template called "IrisCode"[3]. Fooling it with a 2D iris image requires high functional software and hardware at the same time. Therefore, iris authentication is more safety than regular fingerprint authentication.

A reliable biometric system will provide precise information in order to identify an individual; consequently, the users may have multiple concerns, especially about privacy, which has been a major problem for decades. When someone is using the fingerprint scanner, some traces will be left on the glass of the scanner, which will

makes stealing personal information much easier. On the other hand, sometimes good intentions will lead to inevitable embarrassment or even personal loss such as in career and family. For instance, when justice department tries to figure out the act of crime at a crime scene with fingerprint readers available, the first thing they will do is gathering the fingerprint traces that left on the scanners. Innocent people will be questioned; and thus, this might affect their reputations in their jobs or activities within their families to some extent, even though it is not intentionally. However, unlike fingerprint-based system, scanning iris will not provide a shortcut for stealing iris pattern, because it will not leave any trace on the screen. At the same time, scientific researches prove that information of iris is incapable of revealing personal secrets such as medical condition and disease which fingerprints might. Thus privacy can be well protected through applying this technology.

After 9/11 terrorism attack, governments are giving increasing weight to enhance security in public places especially venues for large-scale events and airports. As a result, the identification verification systems are mostly improved by replacing fingerprint-based systems with iris-based systems. Due to its high accuracy in matching with database and well-functioning in security and privacy matters, many governments and private firms consider iris recognition system as capable and reliable in conducting classified or sensitive missions. Compared with fingerprints recognition and other forms of biometric, iris recognition is better in fields that demand rapid identification of individuals in a dynamic environment. Furthermore, not like fingerprint recognition, iris recognition is used as a high-tech recognition system by

some governments and large scale state-owned or multinational enterprises. However, even though it is the most advanced biometric nowadays, it still has some drawbacks. Iris recognition device requires users to stop for a few seconds and look directly into the camera so that irises will be illuminated for identification. This poses a challenge for subjects who are blind or have cataracts, since it is difficult for them to stand at the right place and find where the camera is. Therefore, although iris recognition has a brighter future than others, more researches need to be conducted and more factors need to be considered in order to improve it and finally make it public.

After the new word “biometric” has bounced out for several decades from 1960s, the technology in this area grows in an unimaginable rate and tremendous scale. Fingerprint is the signature of it which is also meant as maturity and popularity. Nowadays the highly acceptance rate by people indicates the success in the process of evolving. However, the more complicated and dangerous future need a more advanced tool to make it stay in the right track, iris recognition fits the requirement. With eliminating some disadvantages in accuracy, security and privacy that fingerprint recognition cannot overlap, iris recognition has its own capability and reliability that has already been accepted by government and large private firms. Even though there are some factors that still need to be covered, the future of iris recognition is bright; and there is a belief that it will finally become public enough to be used among the society.

Reference

[1] Alexander Andreopoulos, John K. Tsotsos. *50 Years of object recognition: Directions forward*. Elesevier, 2012.

[2] *Biometric Technology Application Manual*. National Biometric Security Project,2008.

[3] Simon Liu, M. Silverman, "A practical guide to biometric security technology". *IT Professional.* Volume:3.Issue: 1, pp. 27 – 32, August, 2002.