Voice biometric

By

Charoenkeith Wan. 5455213
Palod Patimavirujh 5612602
Kritanu Singhavorawuti 5616813
Daran Sae-lim 5618624

Submitted to

Asst.Prof.Dr. Adtha Lawanna

IT4363 Information System Security and Auditting
1/2016
Preface

Table of contents

Figure

Table

Chapter1: Introduction of voice biometric in Citibank

Introduction

In the present, there are many things need a security system for protecting from action which it is without authorization. Many developer try to develop a security system but it didn't have a good enough and convenience one for using. In the present, the one security system which we know that is good and convenience for using is Voice biometric.

Voice biometric or you can have called Voice recognition is a type of security measure use to identify a person in a unique way which uses the voice of the identifier. This can be done as voice is a personal characteristic which cannot be replicate easily and the voice itself contains a lot of information when creating.

In the present, Voice biometric is very new in Thailand. The one and only commercial bank use the voice biometric verification is Citibank Thailand.

Citibank, a commercial bank was originated in United States of America and expand its branches throughout the world in more than 160 countries including Thailand. In Early 2016, Citibank Asia has introduced voice biometric authentication technology and become the first commercial bank across Asia Pacific to use this technology. In Thailand, Citibank was introduced voice biometric verification technology to Thai's customer on November 9, 2016.

Fig 1.1 Press Conference by Citibank Thailand, Introducing Voice Biometric Authentication Technology on November 9,2016

Current Problems & Solutions
(base on phone banking contact in commercial bank)

Phase 1 : Lack of verification

When customer contact to a bank and ask about some information such as credit card outstanding balance or assign to change the address for billing is sure that customer tells the credit card number but is really that the owner of credit card contact for ask to do? Without the verification, there is no privacy for customer information. This problem was solved by let a customer set a pin code or password which it will discuss on **Phase 2**.

Phase 2: Set PIN Code

The first security system of this problem is let a customer to create a pin code. A pin code is having 4-digit or 6-digit of number, sometime it can be an alphabet or mix together. For example, "aa3456" is the 6-digit of mixing with number and alphabet pin code. Pin code is still not a good security system at all, the disadvantage of pin code is when a customer cannot remember their code, an assistant will not allow a customer to know an information which is a security purpose from using pin code to protect customer's privacy. Ask Personal Information is a verification that without using any PIN, which it solves problem from using

PIN code, it will be discuss on **Phase 3**.

Phase 3: Ask Personal Information

From the disadvantage of using PIN Code, asking personal information is one of verification system and become popular in security verification in commercial bank. A questions for verification are what is your citizen identification number? what is your phone number? have you ever withdraw a money on ATM? and more. However, this type of verification is still had a disadvantage. The disadvantage is waste a time for service to

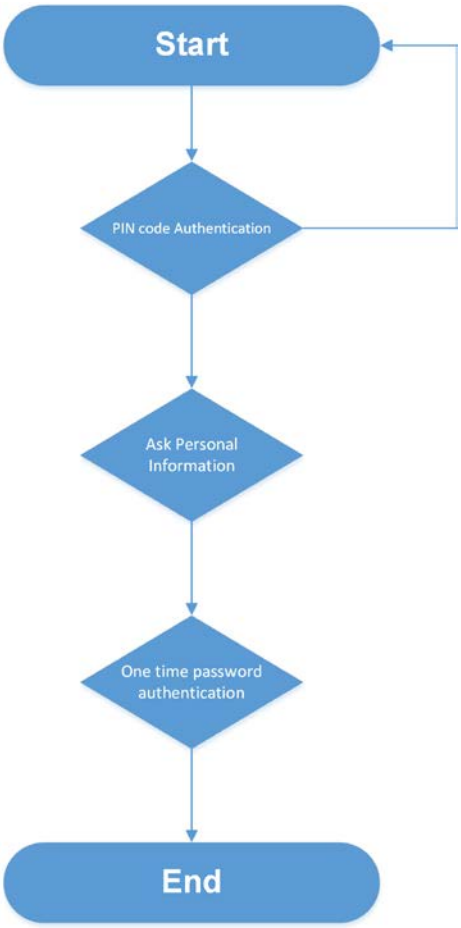
customer, these types of question might take up to 5 minutes to finish a verification. Customer might not free to answer of these questions because of time of processing, customer might not have a time too much to answer these questions from their duty in daily life. One-time password is a solution from this problem, see more detail on **Phase 4**.

Phase 4: One-Time Password via SMS or E-Mail

Some commercial bank use one-time password for verification. The process of one-time password is send a password to only mobile number or e-mail address which customer give an information to a bank. The disadvantage of this type of verification is when a customer have a problem with their phone number or e-mail address for receive the password, one-time password verification will not work for this case and back to use asking information verification to verify a customer.

Moreover, one of disadvantage which it on every phase (except phase 1 which it's not have a verification) is cannot ensure a truly customer's identity. From a type of verification of each phase, they are still cannot make sure that this person is really this person because when some person fake to be that customer and call to a bank and he/she know a pin, a personal information or have a phone or e-mail which it registers to a bank for one-time password verification, An assistant cannot really know that he/she fake to be that customer. Voice biometric is a solution of these problems and how? It will be discussing on each topics below.

Flowchart of the current technology



(Fig 1.2 Flowchart of current technology)

Chapter 2

In this security measure use to prevent unauthorized person accessing to the organization there are several ways to defend this situation from happening and the biometrics is a useful and effective counter-measure to solve the authentication of the bank's firm.

Nowadays, security system is the most important thing to provide a protection to your assets from the outsiders especially with the increasing of crime rate incident will make people or organization feel unsafe about their important assets from inside or outsiders.

The following system shows the point of view of the current biometrics technologies in order to restrict the user to access the system. It allows only the authorized people to access the system and denied those who do not have the permission to access. The complex security system is difficult to attack. Moreover, each biometric technology are suitable in different use and there also have different interference that obstruct the process of biometrics. Biometrics is more secure in any other counter measure against the threat of accessing without permission as biometrics determine the person base on what they are born with like eyes or fingerprint which cannot be replicate easily by others.

Out of many biometrics theory and system we have chosen 3 type to explain how and what is required in this system.

1. Retina scanning

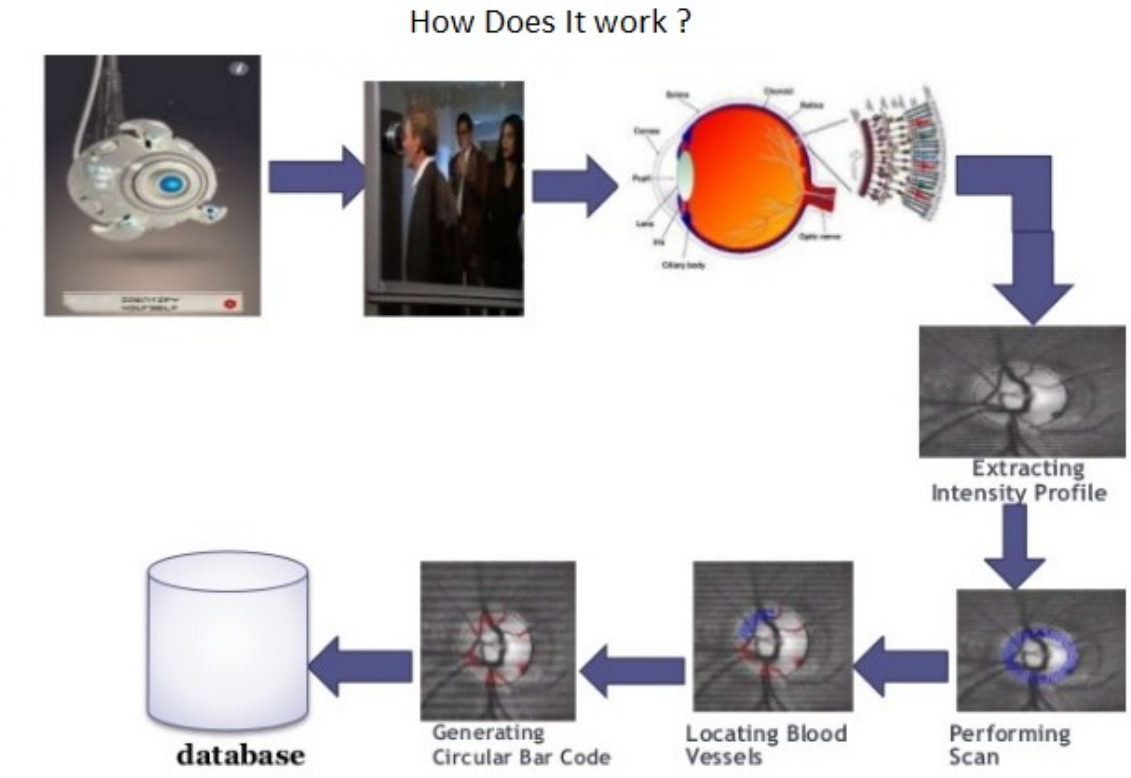
Retina scanning is a form of biometric which uses the pattern of the person's retina blood vessels which is unique in different people. So it can be used as an identifier or verification to many authentication systems in the modern days.

So how does this retina scanning work is as follow:

There are several steps in order to identify and verify the person on who has the permission to access .Firstly, once the system is set in the place for only authorized people can access it is the starting of the system whereby the person who intended to access need to pass the verification of the retina scan which involve the person to come contact to the retina scanning machine which scan the blood vessels of that person.

When the system scan the retina, it will extract the intensity profile of that person which then leads to the performing the actual scan that scan through-out the retina in order to locate the blood vessels of that person can find the pattern of the whole blood vessels where these blood vessel pattern is unique in every person. Then this blood vessel pattern will go through further algorithm that will generate circular Bar code that is a form of a digital data to use for verification. This process will use the data obtain in the process and extract the database to find whether the data gather from the blood vessel pattern match any of the database that include only those who have the right permission to access which if the comparison is not match the system will denial the access to that intended person. On the

other hand if the circular Bar code matches the information in the database, it will grant permission and authorization for that intended person.



(Fig 2.1 How retina scanning work)

Advantages

- This biometric have high accuracy and as you know every people have different retina that can be used to identify their identity.
- The retina scanning can differentiate the eyes from dead people or animals

Disadvantages

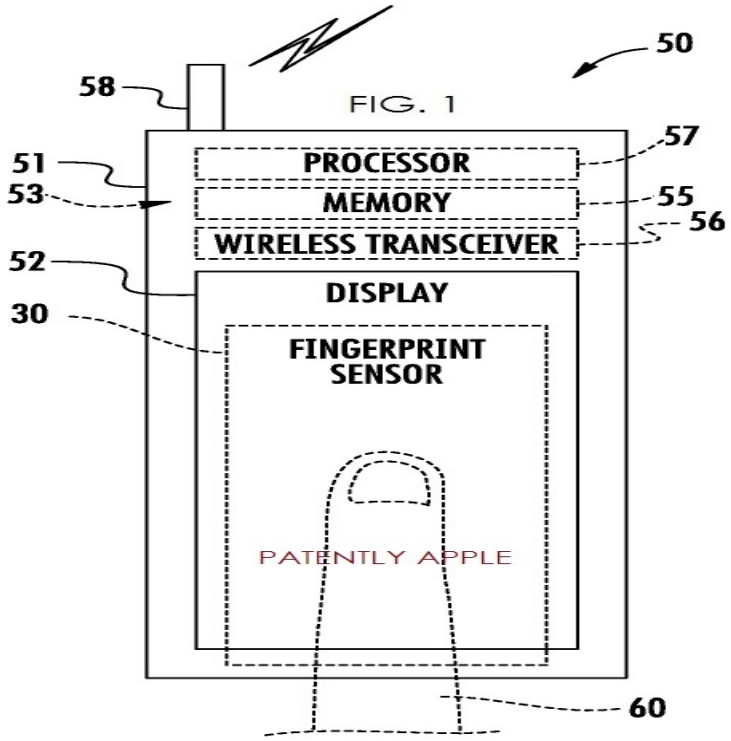
- Frequently use of retina scanning may be harm to the eyes of the person
- This biometric is very expensive and not accept in general use. It will be use in the secret or important project such as nuclear installation
- The data after recorded need a lot of memory for storing.

2. Fingerprint

Another type of the biometrics used for security system is the fingerprint which identify the fingerprint pattern which is identical to only one person that is use to authenticate the right to access.

There are various advantages about the use of fingerprint biometric. First, these biometrics have high accuracy and ease of use. Also, it is the one of most developed and

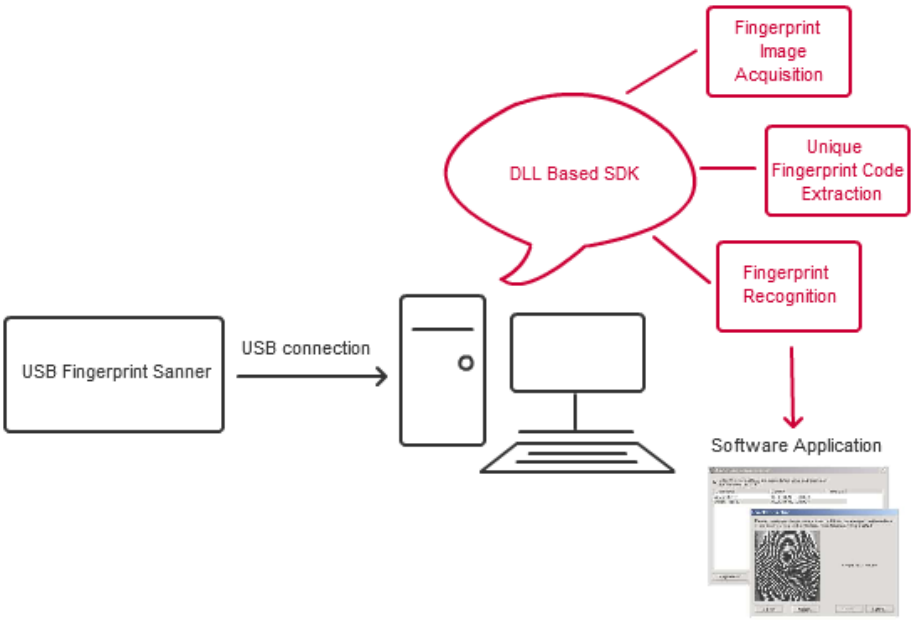
mostly use or standardized in user's authentication. Moreover, the recorded data require small storage space in database.



(Fig 2.2 How fingerprint is recorded)

On the figure above shows how the fingerprint is recorded and the hardware involve in doing so which record the fingerprint of the person and wirelessly transmit to the computer to match and compare with the database on who will have the right to access according to the database.

Once the fingerprint is scan it will send to the computer that is being process and extract the fingerprint image out from the scanner.After this process is done the system will extract the image to find the unique code which is then pass through the finger recognition to be either compare with the database or to be save in the database for those authorize person in the database and then it will be process in the software application.



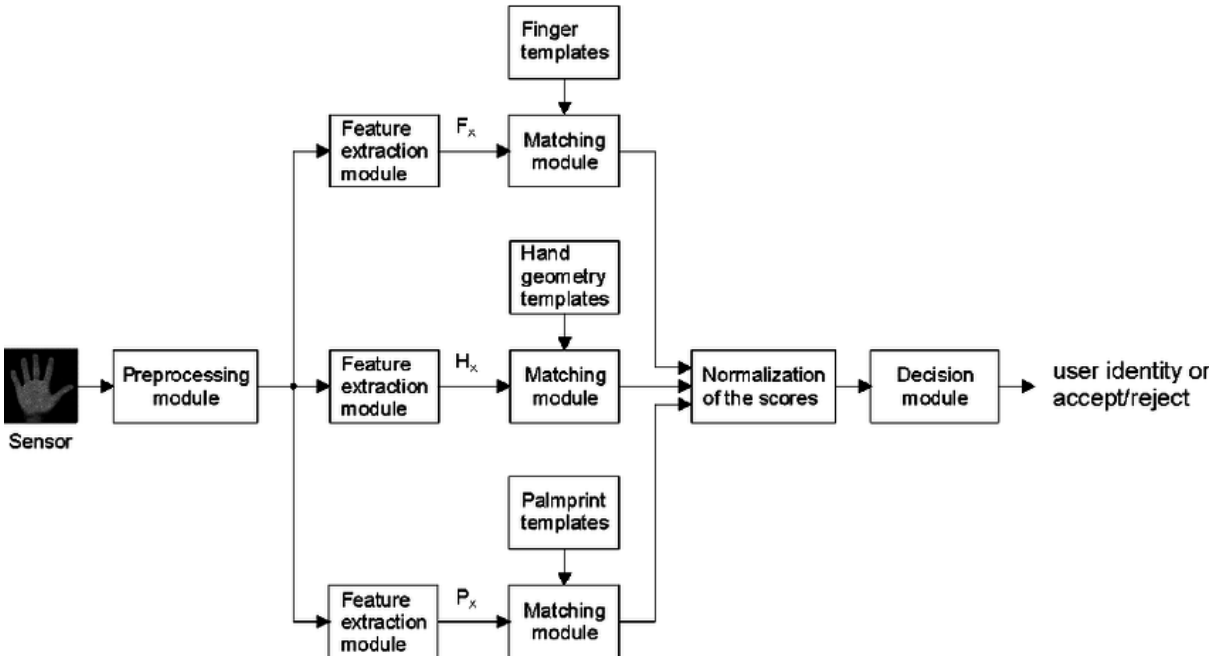
(Fig 2.3 How fingerprint system work)

On the other hand, there are several disadvantages of fingerprint biometric. First, for some people is intrusive to their privacy that why the acceptance to people are not popular as expected. Second, the system accuracy may have an error in detection and authentication when the skin of the finger is dry and dirty. Third, this biometric system is not suitable to the children because the size of their fingerprint has changed quickly.

3. Hand geometry

Hand geometry is one kind of biometric that identifies the user identity by the shape and dimension of user hands and stores it in a file. Therefore, there are several advantages of using hand geometry. First, this biometric use special hardware to process the user identity. so, it can be integrated with other system more easily. Second, the acceptance of this biometric is high because it most commonly used for access authorization.

How the hand geometry actually works is that first off, the intended person need to place the hand to the sensor for recording and scan the shape and dimension of that person's hand.Then the system will process to extract the information from those dimensions in to a form of templates or information .There are 3 information that is extracted during the scanning which includes extracting the finger templates, hand geometry template and palm print templates once it is being scanned.During the extraction other process is running simultaneously by retrieving each template from the database and compared those template with the extracted information and find the comparison scores.If it is matched or unmatched it will send to the decision module to give the final outcome whether that person is accepted or rejected.



(Fig 2.4 How hand geometry work)

In contrast, these biometrics is very expensive and the size of machine is quiet big. Moreover, it is not appropriate for the disables or people that have arthritic problems or the problem with their joint. So, they cannot put their hands in the scanner properly. Even though it might be effective in using the hand geometry but compared to other biometrics it does not view as a detailed scanning devices meaning that it is not as unique as fingerprints, palm veins etc. This type of biometrics is better if used with other security measure such as the use of other identification like identification cards or personal number that is given to them.

Furthermore, for the reason why voices biometric are appropriate for the user in term of security, cost and convenience as following:

1. Voice biometric has more unique than fingerprint: Voice biometrics authentication uses the unique tone, resonance, pitch, and physical characteristics of a person's voice. Also, there are less vulnerability for attackers
2. It is a natural way to measure someone's identity and saving people time and effort.
3. Convenient and portable for the mobile device because nowadays most portable devices are supported the voice record. It can adapt to in term of security.
4. Nowadays password is a problem for someone who has a different style of complicated password. As a result, they will be forgot and your security may be leak to the bad guys. Therefore, when changing to use voice biometric. Customers no need to remember their complicated password or answer all of security question.
5. The cost of implementation is lower than other biometric such as fingerprint or retina scan

Chapter 3

3.1 What is Voice biometrics and history?

Voice biometrics, voice print or voice recognition is a type of security measure use to identify a person in a unique way which uses the voice of the identifier. This can be done as voice is a personal characteristic which cannot be replicate easily and the voice itself contains a lot of information when creating. So, in voice biometrics it is the use of technology which can extract the voice and verify by the voice pattern to determine whether the voice match with the person or not.

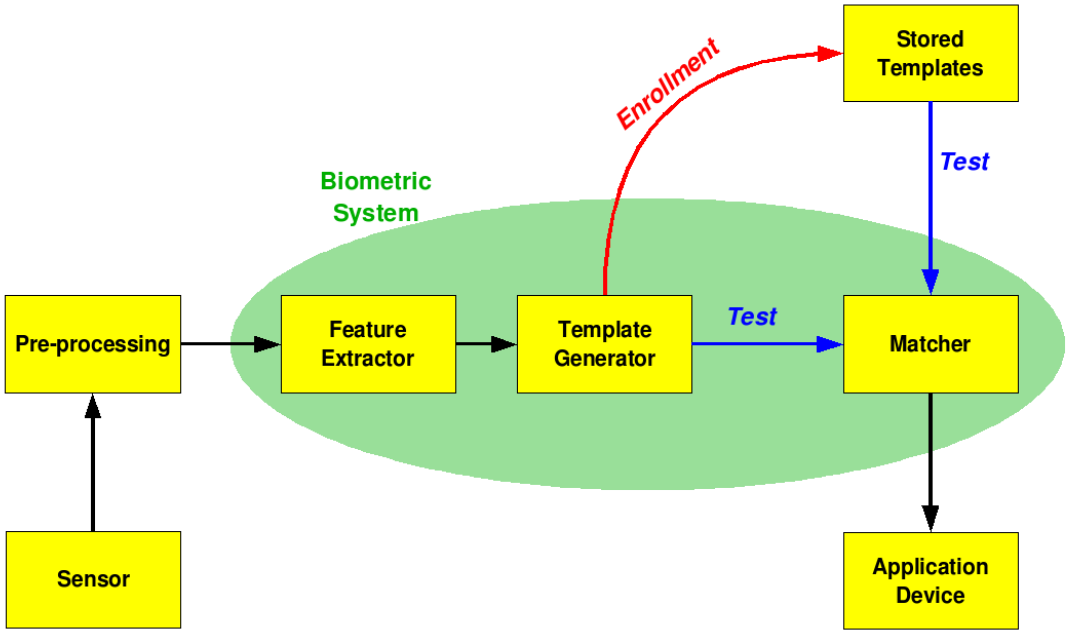
Voice biometrics is often mistaken for speech recognition and behavioral speech recognition which is totally different to voice biometrics as the speech recognition recognizes only words that is coming out but cannot identify the speaker . As for the behavioral speech recognition recognizes characteristic of the voice like accent, emotion, etc. but not the speaker. In voice biometrics, will track and find the information carried with the voice pattern of the speaker which is embedded in the speaker's sound wave this information is hardly replicate by others and is captured by the voice biometrics technologies.

The uses of voice biometrics vary in many different fields and as of the present moment, it is widely use as of surveillance and a caller authentication. Another area which is forensics used to identify the caller in the police department as evidence, criminal databases and for fraud detection purposes.

The history of this voice biometrics is relatively new in the market area which the first time this it emerges during the late 1990s where application is made and voice biometrics is usable in areas of a voice authentication. Whereas the concepts and analyses of the voice biometrics started way back during the late 1800s where Alexander Melville Bell who is the father of telephone inventor Alexander Graham Bell, has laid the groundwork for future voice biometrics research by inventing a language called Universal Alphabetic which is the replication of the position of the mouth when speaking certain speech pattern, it's possible to transcribe not only what a person is saying, but how they are saying it.

The foundation is plant there in the late 1800s but it is used before during the World War II as a voice, biometric identity verification to intercept voice transmission and track enemy movement. But due to the limitation of technology in that era which it does not provide substantial information and does not have precise accuracy but then in 1976 that the first modern voice biometrics engine is created which is capable of accurately registering and determine the speaker. Since then this technology is being developed and used in the various filed for security technologies?

1st diagram

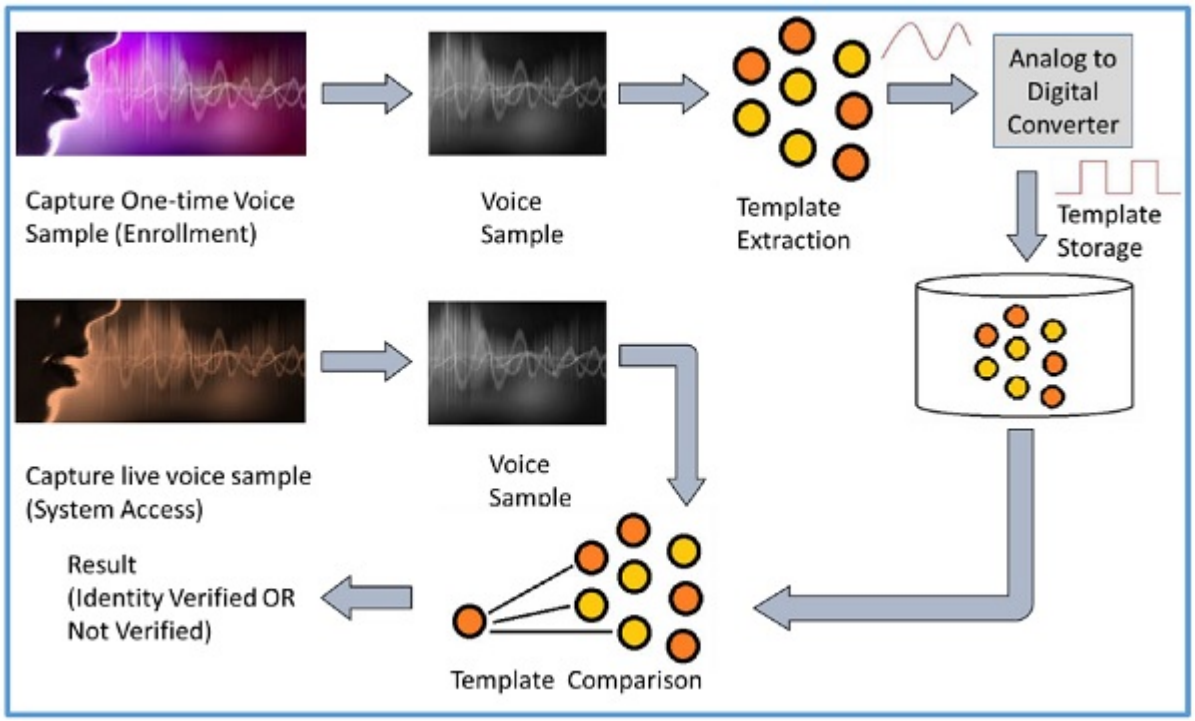


(Image source: https://en.wikipedia.org/wiki/Biometrics)

(Fig 3.1 How voice biometric function work in sequence)

The diagram above shows how the voice biometric function in a step-by step sequence which depends on what application or platform the system is used. The sensor records the spoken words from the speaker and then does a pre-processing to capture the characteristic of the voice. Then that characteristic is being process further to extract the necessary information of these characteristic in a form of a sound wave, pitch, tone, etc. After being extracted it will create a template that is like a sample to compare this template with the stored template in the database and the pass through the process of the matching meaning that both the extracted template and store template is being test to see whether the extracted template is match with the store temple or not If either one whether match or not matched it will be forwarded to the application devices to tell the person that they have permission or not.

2nd diagram



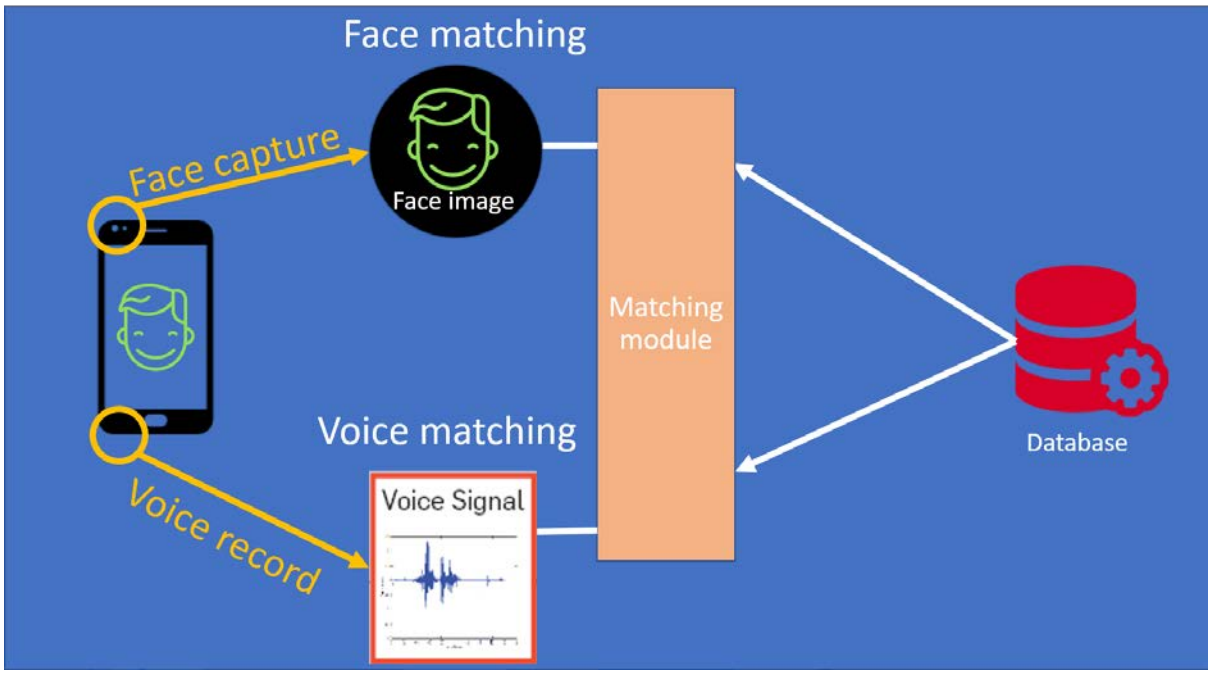
(Fig 3.2 How voice biometric work 2)

Voice biometric is types of biometric that identify or authenticate a person base on the characteristic of the voice. In this case user's voice is use to authenticate and grant access to service or certain database. To use this biometric user is required to give sample voice to the system then sample voice will be converting from analog to digital and send to storage to be a template for comparison with next access. When the next permission come, system will require use to capture live voice sample then that voice sample will be used to compare with template in storage to determine whenever user will be verifying to system or not.

Voice biometric is a type of biometric that is started to be use in banking nowadays even some company has start using it too. This is mainly because of ease for user to do authentication. The process can be done within 5 seconds so that user can saves their precious time to do other activity that they want to without wasting time to answer question or finding passcode that will be forgotten in a month.

For security side voice biometric can be very secure for user because of voice are hard to duplicate and hack. Because a voiceprint is a hashed string of numbers and characters, a compromised voiceprint has no value to a hacker and if they try to spoke to call center or mobile app they will leave behind their own voiceprint that can be used to proactively keep them out of the system and even alert law enforcement.

3rd diagram



(Fig 3.3 Multi-model of biometric)

Multi-model of biometric to enhance portable device security and authentication

As mention earlier, voice biometrics is a type of biometric that identifies or authenticates a person base on the characteristic of the voice but this technology can have a serious weakness in term of the disruption or interference of the input device while capturing the speaker personal voice characteristic. In addition, someone might place a jammer while doing this authentication that can result in inaccurate to match the person wrongly. Other disruption may involve with someone having a flu which make the sound of the speaker change in pitch, pattern or tone that reduce the effectiveness of the system or somewhere with strong wind or climate change that can affect the sound capture by the system.

In the present, mobile phone is widespread through everyone around the world so why don't we use something that people have and make the voice biometric further since the voice biometric is now apply on mobile phone directly. Face recognition is another area where it is effective in terms of identify the person through facial scan and that some mobile phone have this function equip why don't we use as another solution if the voice biometric does not work.

In order further enhance the voice biometric further , we think that combining both the voice biometric and also the face recognition is a way to improve the voice biometrics as in 1 mobile phone it consist of a camera that can capture the face and also the microphone that capture the sound of the speaker.By doing both of this will allow like a double protection with both voice and face at the same time and is much more secure and effective way to identify a person than the previous stand-alone voice biometric.

3.2 Use of voice biometric

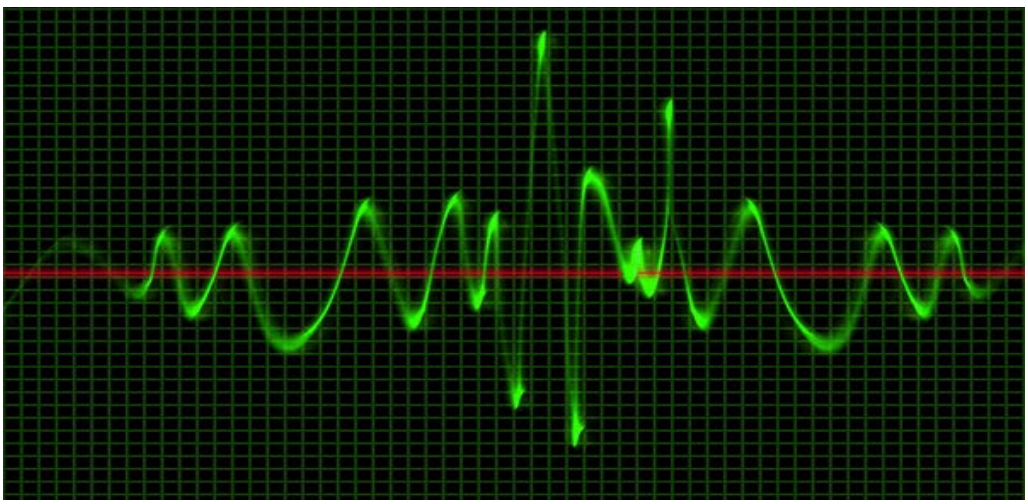
Voice biometric can be used in various fields. First, voice biometric can be used in term of security such as financial transactions like accounts access, funds transfer, credit card processing and etc. Second, use voice biometric for authentication like citizen facilities by combining with id card to let the residents access in their apartment. Moreover, for the future cellphones and laptops will be a device that adapt of biometric in term of security concept like use voice to unlock your phone or personal laptops.

Nowadays, most organization especially banks are turning to use voice biometrics as a security in term of client's authentication rather than using passwords or answer for the security question. In contrast, this technology is not widely trusted or understood by the organization that why this biometric technology was not grow as expected.

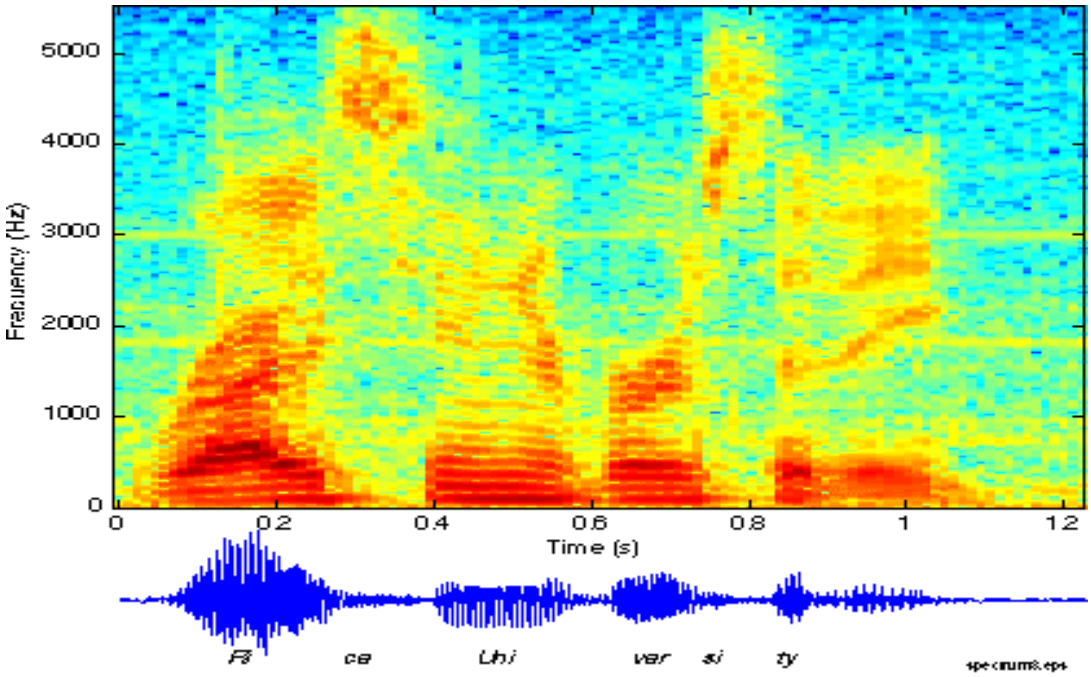
How voice biometric work

Our voice is unique because of the shape of our vocal cavities and the way we move our mouth when we speak. It has distinctive feature that can be used to identifying ourselves. To enroll in a voiceprint system, we either say the exact words or phrases that it requires, or give an extended sample of our speech so that the computer can identify you no matter which words we say.

When people think of voiceprints, they often think of the wave pattern they would see on an oscilloscope. But the data used in a voiceprint is a sound spectrogram, not a wave form. A spectrogram is basically a graph that shows a sound's frequency on the vertical axis and time on the horizontal axis. Different speech sounds create different shapes within the graph. Spectrograms also use colors or shades of grey to represent the acoustical qualities of sound.



Oscilloscope



Spectrogram

When our voice registered by the system next time we wanted access our pre-record voice can act as the pass code to gain access to data we needed. The system will request us to say a specific words or phrases and it will use our voice that was pre-record to compare similarity of voice and decide to gain us access or not depend on how similar the voices are.

In conclusion, how voice biometric or voice recognition work is system will require us to said specific words or phrases to register as sample. When we require access to any task that needed to be confirm security pass code we can use our voice to act as pass code and gain access like when we use pass code itself.

When we call most large companies, a person doesn't usually answer the phone. Instead, an automated voice recording answers and instructs you to press buttons to move through option menus. Many companies have moved beyond requiring you to press buttons, though. Often you can just speak certain words (again, as instructed by a recording) to get what you need. The system that makes this possible is a type of speech recognition program an automated phone system.

You can also use speech recognition software in homes and businesses. A range of software products allows users to dictate to their computer and have their words converted to text in a word processing or e-mail document. You can access function commands, such as opening files and accessing menus, with voice instructions. Some programs are for specific business settings, such as medical or legal transcription.

People with disabilities that prevent them from typing have also adopted speech-recognition systems. If a user has lost the use of his hands, or for visually impaired users when it is not possible or convenient to use a Braille keyboard, the systems allow personal expression through dictation as well as control of many computer tasks. Some programs save users' speech data after every session, allowing people with progressive speech deterioration to continue to dictate to their computers.

Current programs fall into two categories:

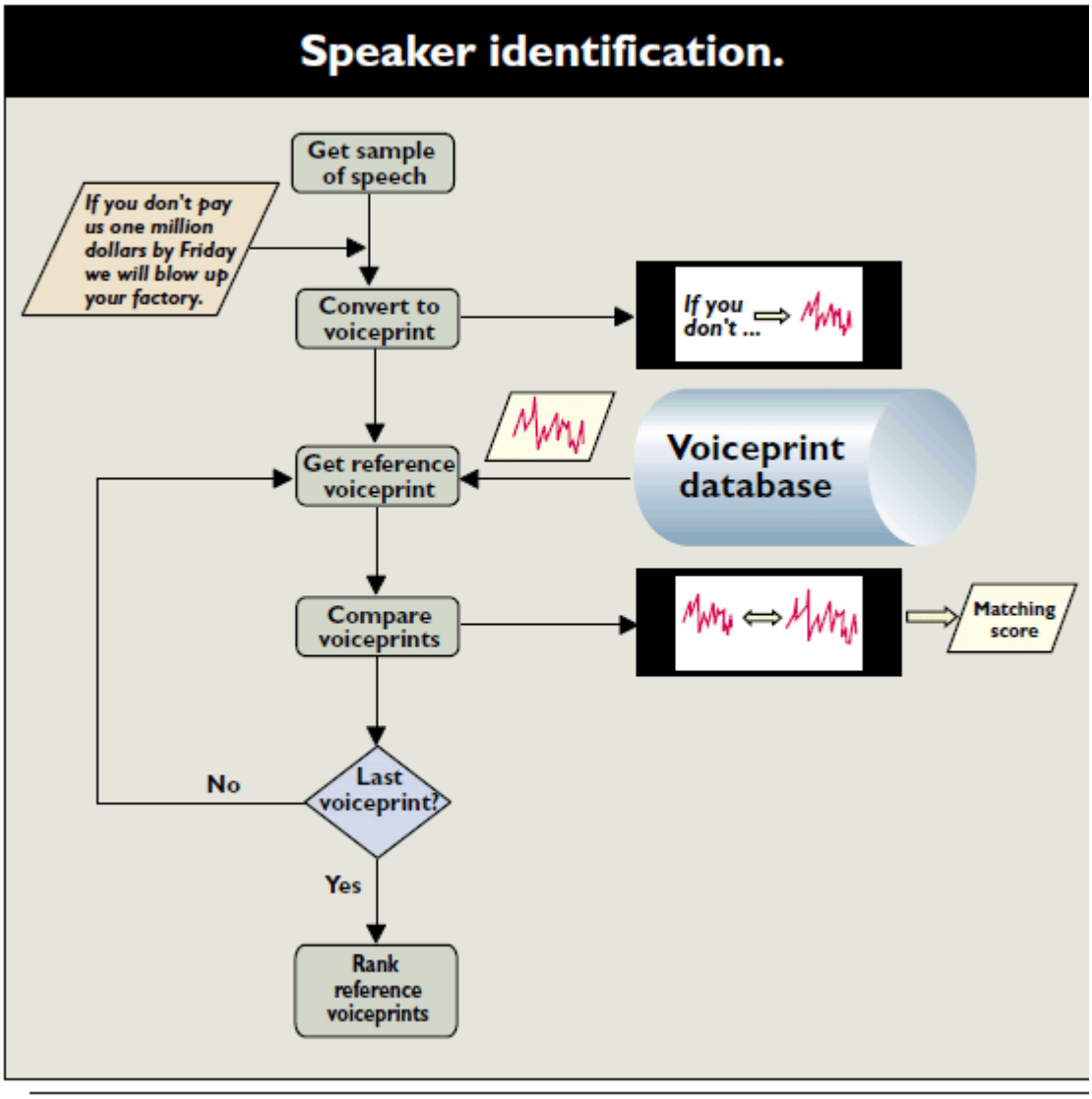
Small-vocabulary/many-users

These systems are ideal for automated telephone answering. The users can speak with a great deal of variation in accent and speech patterns, and the system will still understand them most of the time. However, usage is limited to a small number of predetermined commands and inputs, such as basic menu options or numbers.

Large-vocabulary/limited-users

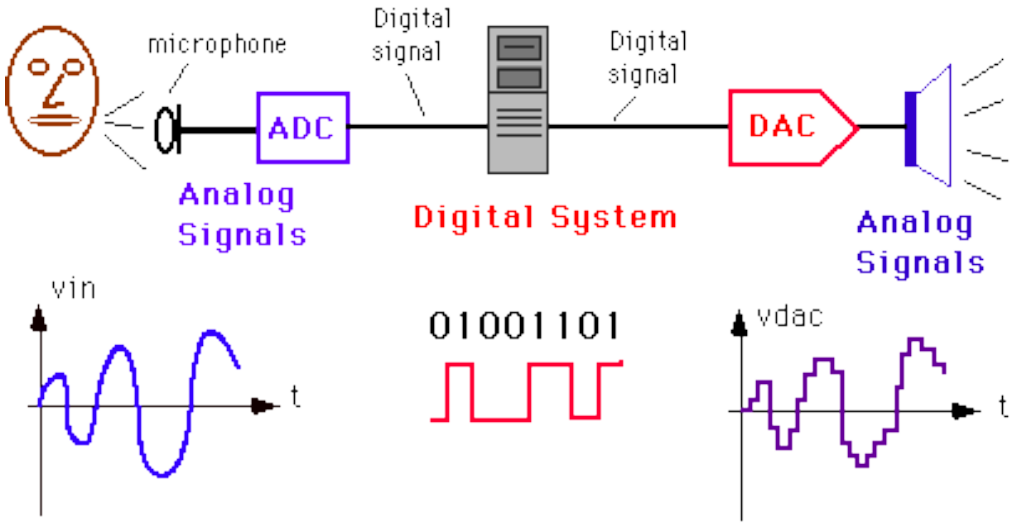
These systems work best in a business environment where a small number of users will work with the program. While these systems work with a good degree of accuracy (85 percent or higher with an expert user) and have vocabularies in the tens of thousands, you must train them to work best with a small number of primary users. The accuracy rate will fall drastically with any other user.

Speech recognition systems made more than 10 years ago also faced a choice between discrete and continuous speech. It is much easier for the program to understand words when we speak them separately, with a distinct pause between each one. However, most users prefer to speak in a normal, conversational speed. Almost all modern systems are capable of understanding continuous speech.



(Fig 3.4 Speaker identification)

To convert speech to on-screen text or a computer command, a computer has to go through several complex steps. When you speak, you create vibrations in the air. The analog-to-digital converter (ADC) translates this analog wave into digital data that the computer can understand. To do this, it samples, or digitizes, the sound by taking precise measurements of the wave at frequent intervals. The system filters the digitized sound to remove unwanted noise, and sometimes to separate it into different bands of frequency (frequency is the wavelength of the sound waves, heard by humans as differences in pitch).



It also normalizes the sound, or adjusts it to a constant volume level. It may also have to be temporally aligned. People don't always speak at the same speed, so the sound must be adjusted to match the speed of the template sound samples already stored in the system's memory.

Next the signal is divided into small segments as short as a few hundredths of a second, or even thousandths in the case of plosive consonant sounds. Consonant stops produced by obstructing airflow in the vocal tract like "p" or "t." The program then matches these segments to known phonemes in the appropriate language. A phoneme is the smallest element of a language, a representation of the sounds we make and put together to form meaningful expressions. There are roughly 40 phonemes in the English language (different linguists have different opinions on the exact number), while other languages have more or fewer phonemes.

Consonant phonemes, with sample words		Vowel phonemes, with sample words	
1. /b/ – bat	13. /s/ – sun	1. /a/ – ant	13. /oi/ – coin
2. /k/ – cat	14. /t/ – tap	2. /e/ – egg	14. /ar/ – farm
3. /d/ – dog	15. /v/ – van	3. /i/ – in	15. /or/ – for
4. /f/ – fan	16. /w/ – wig	4. /o/ – on	16. /ur/ – hurt
5. /g/ – go	17. /y/ – yes	5. /u/ – up	17. /air/ – fair
6. /h/ – hen	18. /z/ – zip	6. /ai/ – rain	18. /ear/ – dear
7. /j/ – jet	19. /sh/ – shop	7. /ee/ – feet	19. /ure/[4] – sure
8. /l/ – leg	20. /ch/ – chip	8. /igh/ – night	20. /ə/ – corner (the 'schwa' – an unstressed vowel sound which is close to /u/)
9. /m/ – map	21. /th/ – thin	9. /oa/ – boat	
10. /n/ – net	22. /**th**/ – then	10. /**oo**/ – boot	
11. /p/ – pen	23. /ng/ – ring	11. /oo/ – look	
12. /r/ – rat	24. /zh/[3] – vision	12. /ow/ – cow	

(Table 1: Phonemes)

The next step seems simple, but it is actually the most difficult to accomplish and is the main focus of speech recognition research. The program examines phonemes in the context of the other phonemes around them. It runs the contextual phoneme plot through a complex statistical model and compares them to a large library of known words, phrases and sentences. The program then determines what the user was probably saying and either outputs it as text or issues a computer command.

Early speech recognition systems tried to apply a set of grammatical and syntactical rules to speech. If the words spoken fit into a certain set of rules, the program could determine what the words were. However, human language has numerous exceptions to its own rules, even when it's spoken consistently. Accents, dialects and mannerisms can vastly change the way certain words or phrases are spoken. Imagine someone from Boston saying the word "barn." He wouldn't pronounce the "r" at all, and the word comes out rhyming with "John." Or consider the sentence, "I'm going to see the ocean." Most people don't enunciate their words very carefully. The result might come out as "I'm goin' da see tha ocean." They run several of the words together with no noticeable break, such as "I'm goin'" and "the ocean." Rules-based systems were unsuccessful because they couldn't handle these variations. This also explains why earlier systems could not handle continuous speech -- you had to speak each word separately, with a brief pause in between them.

But today's speech recognition systems use powerful and complicated statistical modeling systems. These systems use probability and mathematical functions to determine the most likely outcome. According to John Garofolo, Speech Group Manager at the Information Technology Laboratory of the National Institute of Standards and Technology, the two models that dominate the field today are the Hidden Markov Model and neural networks. These methods involve complex mathematical functions, but essentially, they take the information known to the system to figure out the information hidden from it.

The Hidden Markov Model is the most common, so we'll take a closer look at that process. In this model, each phoneme is like a link in a chain, and the completed chain is a word. However, the chain branches off in different directions as the program attempts to match the digital sound with the phoneme that's most likely to come next. During this process, the program assigns a probability score to each phoneme, based on its built-in dictionary and user training.

This process is even more complicated for phrases and sentences -- the system has to figure out where each word stops and starts. The classic example is the phrase "recognize speech," which sounds a lot like "wreck a nice beach" when you say it very quickly. The

program has to analyze the phonemes using the phrase that came before it in order to get it right. Here's a breakdown of the two phrases:

r eh k ao g n ay z s p iy ch

"recognize speech"

r eh k ay n ay s b iy ch

"wreck a nice beach"

These statistical systems need lots of exemplary training data to reach their optimal performance sometimes on the order of thousands of hours of human-transcribed speech and hundreds of megabytes of text. These training data are used to create acoustic models of words, word lists, and multi-word probability networks. There is some art into how one selects, compiles and prepares this training data for "digestion" by the system and how the system models are "tuned" to a particular application. These details can make the difference between a well-performing system and a poorly-performing system -- even when using the same basic algorithm.

While the software developers who set up the system's initial vocabulary perform much of this training, the end user must also spend some time training it. In a business setting, the primary users of the program must spend some time (sometimes as little as 10 minutes) speaking into the system to train it on their particular speech patterns. They must also train the system to recognize terms and acronyms particular to the company. Special editions of speech recognition programs for medical or legal offices have terms commonly used in those fields already trained into them.

Chapter4: Result and discussion

4.1 Point of view and Comparison to biometric method

Biometric Technology	Accuracy	Cost	Devices required	Social acceptability
ADN	High	High	Test equipment	Low
Iris recognition	High	High	Camera	Medium-low
Retinal Scan	High	High	Camera	Low
Facial recognition	Medium-low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature recognition	Low	Medium	Optic pen, touch panel	High

Table 2: Point of view of accuracy, cost, devices required and social acceptability.

Source:

http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies

4.2 Comparison to other biometric method

	Eye-Iris	**EyeRetina**	**Fingerprint**	**Hand geometry**	**Signature recognition**	**Voice**
Reliability	Very high	Very high	High	High	High	High
Ease of use	Medium	Low	High	High	High	High
Acceptance	Medium-Low	Low	Medium	High	High	High
Stability	High	High	High	Medium	Medium	Medium
Identification & Authentication	Both	Both	Both	Authen.	Both	Authen.
Interference	Glasses	Irritation	Dirty Injury Roughness	Rheumatism	Changeable, Easy signature	Disease Weather
Use	Nuclear installation -Medical service	- Nuclear installation -Medical service	-Police industrial	-General use	-Industry	Access in bank or database

(Table3:. Comparison of biometric method)

Source:
http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies

4.1.1 Comparison of current system to old three system

Voice Biometric VS. Eye-Iris Biometric

In this modern day, the use of biometrics has been increasingly widespread in term of identification and authentication in security concept such as medical service, access in bank or database, etc. Therefore, when compare voice biometric to the others. there has some strengths and weakness in difference fields.

First of all, voice biometric has high accuracy same as the fingerprint, hand geometry and signature recognition. In case of using it to access in the bank, it is sure that a bank will use voice biometric because customer can access to their own personal information via voice only which does not involve the need to tell the number of the card and other information for verification.

On the other hand, voice biometric still have a weakness in term of accuracy when compare to other biometrics such as eyes iris and eyes retina.This is because the voice of a human being can be disrupt when speaking or the voice of that person changes in contact with sickness like cold or sore throat which makes it hard to verify that person identify and these factors can be an interference or obstacles in authentication. Voice biometric also has average stability when compare to eye iris, eye retina and fingerprint and it can only be used in user authentication

In this present, this technology is not widely trusted or understood by the organization that why this biometric technology was not grow as expected. It can be used in some fields that have a sensitive information that required a stricter protection such as Bank and database authorization. In the future, voice biometrics will have a significantly grow because voice is a part of human. So, it will be convenient to adapt to use in part of security. Voice biometric may have high possibility to use or adapt on smartphones or laptops such as the use voice to unlock your smartphone or laptop rather than entering pin code or complex password that may forgot easily. Another reason of adapting because it is portable device that people use in everyday life, if it can add some function that can help them reduce their tasks that why people does not choose to use it.

5. Analysis

In this rapidly growing world where the use of technology has been spreading significantly and in many different field makes people working smarter and more efficient than ever before. Although it makes things easier and faster this does open up to new threat as the value of information is one of the major asset of a person which is valuable. So, cybercrime is increase as the ease of accessing information increases. In order to prevent cybercrime like those hacking personal information and trick others to gain benefit from them, there are a need in improving the security system to compensate the increasing of cybercrime. The most common security that is used is the authentication that will identify the person identity but in this present moment, the technology use for authentication is like a PIN code that the person only know , a card that identify that they can access certain facility which both of these authenticating method is accurate but there are still some flaw in it as well.

Firstly the flaw of using the PIN code ,if that person forget the PIN code they need to ask that certain department to retrieved but before they can do that they must authenticate you first by asking personal information to see whether you are the owner of that certain thing or the right person to use it.

Second flaw is the use of a thing that will identify that person usually is in the form of a card or a tag to verify with another system or machine which can be quite princely. This thing the person has might be lost in any way like dropping or that person can't remember where they put it which once lost the card or tag they have no real authentication except for turning to the people in charge of that system for verification only.

How will the world be like with this growing technology?

Technologies has been growing continuously from big machine into a portable device so in the future there will be less and less bulky device that a person need to carry and have you ever ask, how will the world move towards the future with these growing technologies. The answer can be vary but there are a chance that the need of carry things around is troublesome and that in this present moment things has been moving towards the future by reducing the need to carry things around, everything is in the form of a digital device that combine everything like bank account through mobile application and it works. Like the use to identify a person without having anything just by their voice only so the person does not need to carry any bulky or useless information around as they can access their information though purely by using what are they born with or the biometrics in this case by voice to get information with just saying a phrase which is more convenient in many ways that the person does not need to remember any long password or PIN they set or having a problem with losing thing or carrying a lot of information to identify themselves in other firm.

Satisfy Expectation from User

Voice biometric authentication technology is can solve a problem of security purposes and give a benefit to a user from using their voice identity. As mention from a process of authentication, voice biometric is take a short time to authentication but it did not make the quality of authentication is low, voice biometric is classify the reliability is high in the field of security system. From a fact of voice biometric, there are no need to set any pin or password, ask any personal information or using one-time password or OTP, we expect that a user will satisfy with voice biometric in high level.

The future of voice biometric

Before coming of the biometrics technologies. People still use of many complex passwords to protect their personal profile because they have use to online activities that someday it may be hacked or steal by someone and if you set a very complex password or security question, someday you will probably forgot it.

Nowadays, security breach is very common and it can lead to the major risk in organizations operation if they does not have a security system that have enough performance to handle with the external factors like threats.

Future security systems are coming like voice biometrics which identify personal identity by their voice tone. It looks like a natural way to measure identity and it can be used as a password that become more secured than the current technology like OTP or password. Also, you can get rid of about the remember of your passwords. Voice biometric may have high possibility to use or adapt on smartphones or laptops such as the use voice to unlock your smartphone or laptop rather than entering pin code or complex password that may forgot easily. Another reason of adapting because it is portable device that people use in everyday life, if it can add some function that can help them reduce their tasks that why people will not choose to use it ?. In another word, using your voice to control your personal information like when you want to know information from your bank account, you no need to answer the question to get your correct personal information. You just say and the system will recognize it and return information back to you. It looks convenient and easy when compares to the current security technologies

Furthermore, voice biometric can combine with artificial intelligence or AI like in the iron man movie which called J.A.R.V.I.S it is an advanced computerized system that command by the voice of specific person (Tony Stark) to perform the tasks like accessing to the unlimited resources, data, device and program in global network and it use hologram as a interface to communicate with the owner.

6. Conclusion

Base on the current technologies and the usage of the voice biometric , there a many benefit in using this biometrics which have several advantages over other biometric technologies.In the present this technologies are used mainly in big security company like a bank firm or other government unit and it does not cover every country.However the ease of use of this system is spectacular which is very easy and convenient to use through remote authentication with only a wireless device.So this technology have a lot of potential in the future with this ease of access and the security is rather very safe which will be quite popular in the near future like every bank firm that user can access to their bank account wirelessly and effortless by just saying the password or the phrase recorded. Other unit can use this voice biometric in the police department as well to identify the caller or to track drug or human trafficking which create a fast and efficient way to identify the person.