SECURE ATM BY IMAGE PROCESSING

A Seminar report submitted in partial fulfillment of the requirementsfor the award of the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

by

S.AKHILA (20S41A05A2)

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

Accredited by NAAC with A+ Grade

(Affiliated to JNTU Hyderabad &Approved by AICTE New Delhi)

Ramakrishna colony, Karimnagar-505527

December 2023

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

Accredited by NAAC with A+ Grade

(Affiliated to JNTU Hyderabad &Approved by AICTE New Delhi)

Ramakrishna colony, Karimnagar-505527

CERTIFICATE

This is to certify that the seminar report entitled **"SECURE ATM BY IMAGE PROCESSING"** submitted by the following students in partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology in CSE and is a bonafide record of the work performed by.

S.AKHILA **(20S41A05A2)**

Head of the Department

Dr. N. CHANDRAMOULI
Associate Professor

Principal

Dr.CH.SRINIVAS

ACKNOWLEDGEMENT

We wish to pay our sincere thanks to **Dr.Ch. Srinivas**, Principal, Vaageswari College of Engineering, Karimnagar, for providing all required facilities and his support during the Seminar.

We would like to thank **Dr. N.Chandramouli,** Associate. Professor and HOD of the Computer Science and Engineering Department for his valuable suggestions during the seminar.

We are also conveying our heartfelt thanks to the Institute authority, Department, Library, and Laboratory staff of Vaageswari College of Engineering for their co-operation during our seminar. We thank our beloved friends for their help and encouragement regarding the concepts and presentation.

S.AKHILA

(20S41A05A2)

ABSTRACT

This system generally used for bank security. Picture Processing structure contains finger inspect,picture check. The image planning is progressively balanced system. Secure Automated Teller Machine by picture taking care of is assume control over a huge segment of the ATM.The multimodal biometric system is the much more secure system that is ensuring the more than the one check.

This system involves the finger scanning along with the voice scan and hand geometry scam and even a image scan. The image scans by image processing is the highly modified system. Secure ATM by the image processing is adopted by the most of the bank ATMs both in the private and government sectors. The image processing is the complex method system interwoven processes.

Analysis of the image is also done by taking out the image features, qualifying the shapes and also registering them along with recognizing them. The various process makes the Bank ATMs secure.

CONTENTS

PAGE NO

LIST OF FIGURES

INTRODUCTION

The rise of technology has brought into force several types of tools that aspire at more customer pleasure. ATM is a machine which has made money transactions effortless for customers. But it has both advantages and disadvantages. Current ATMs make use of not more than an access card and PIN for uniqueness confirmation. This exposes ATMs to a lot of fake attempts to use them by means of card theft, PIN theft, stealing and hacking of customer's account details. Using Face Recognition System in ATMs can show the way to deal with such cases. Biometrics innovation permits persistence and demonstrate of onece personality through physical qualities. It transforms your body into your secret key. We talked about different biometric procedures. That is all are retina filter, finger examine, facial output, hand check and so on there are two calculations have been configuration by taking biometric systems to verification an ATM account holder or the record client, empowering a safe ATM by picture handling. Biometrics is currently accessible in any resembled in different open and private segments moreover. No more issues if passwords and I'd codes have been overlooked, biometrics is the innovation that deals with it, making your body your secret key. Typically To make your mystery word assurance and advancement controls logically exhaustive, the more problematic it will be for customers to review their passwords. Unfortunately, to stop essential software engineer strikes on the framework, serious mystery key rules are required. The current accessible age security issue is viewed as the fundamental TCP/IP encryptions and different variables that are given.

Nowadays ATM Machines are one of the most important and useful thing. Millions of transactions take place on regular basis, ATM not just make our daily work easy but also provide safe, efficient and better service. They help in saving our valuable time, it is better to use ATM instead of directly reaching to bank for withdrawing money which is a total waste of time and resource. So, It is important to take care of ATMs by providing the security to the machine is our responsibility, protecting it from unauthorized access, tampering or any kind of robbery. Advance ATM security system the surveillance of ATM. These days research is going in field of crime avoidance and detection in ATM.But till now there is no good technology has came in the field of ATM that can avoid these crimes. So the idea of making this project has comed from my observation of life incidents happening in the world. So to provide some security measures for ATM transactions is what is the purpose of project.In this project, I will analyze various facial & emotional features using various algorithms.The machine will only work if the expression and emotions are normal and there is no other sign of the forced usage or any of the other illicit activities.

BIOMETRIC

Biomertics are body measurements and calculations related to human characteristics. Biometric (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under survelliance.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological characteristics which are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor/scent, voice, shape of ears and gait. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to mouse movement, behavioral profiling, and voice. Some researchers have coined the term **behaviometrics** to describe the latter class of biometrics.

More traditional means of access control include such as a driver's passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

Many different aspects of human physiology, chemistry or behavior can be used for biometric authenication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain *et al.* identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication. Biometric authentication is based upon biometric recognition which is an advanced method of recognising biological and behavioural characteristics of an Indian.

For a quick biometrics definition: Biometrics are biological measurements — or physical characteristics — that can be used to identify individuals. For example, fingerprint mapping, facial recognition, and retina scans are all forms of biometric technology, but these are just the most recognized options.

Researchers claim the shape of an ear, the way someone sits and walks, unique body odors, the veins in one’s hands, and even facial contortions are other unique identifiers. These traits further define biometrics.

.

TYPES OF BIOMETRICS

Three Types of Biometrics Security

While they can have other applications, biometrics have been often used in security, and you can mostly label biometrics into three groups:

1.Biological biometrics

2.Morphological biometrics

3.Behavioral biometrics

Biological biometrics use traits at a genetic and molecular level. These may include features like DNA or your blood, which might be assessed through a sample of your body's fluids.

Morphological biometrics involve the structure of your body. More physical traits like your eye, fingerprint, or the shape of your face can be mapped for use with security scanners.

Behavioral biometrics are based on patterns unique to each person. How you walk, speak, or even type on a keyboard can be an indication of your identity if these patterns are tracked.

As mentioned before, there are different kinds of biometrics that mainly fall under 2 categories: physiological biometrics and behavioral biometrics. Let us take a deep dive into them:

Physiological Biometrics

Physiological biometrics are taking an individual's physical characteristics as an input to recognize identity.

Fingerprints

This is one of the most commonly used and oldest forms of biometrics and it uses the measurement of your unique finger ridges to identify an individual. Once the print is captured, the image is used to obtain a specific digital biometric template with the help of advanced algorithms.

Finger/hand veins

The blood vessels under the skin of a human finger or hand have a unique pattern (formed by the veins and vessels that take blood to the heart) and this authentication technology works on the unique.

Iris recognition

The color and pattern of the iris vary in individuals. The pattern of the iris and color is different for each individual. It is the colored part of the eye with a circular opening circular in the center. The muscles that shape the pupil of the eye authorize the passage of light into the eye. The identity of an individual can be verified accurately by the biometric devices as they take measurements of the unique muscle folds in the eye.

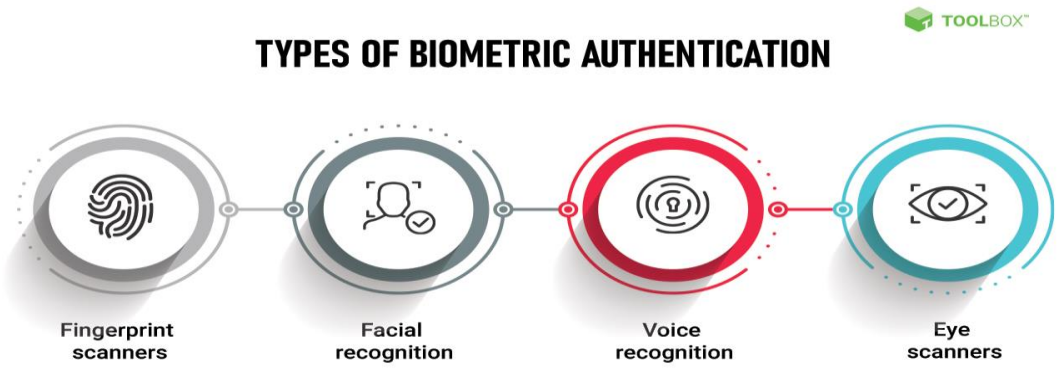

Fig 1.Types of Physiological Biometrics

Facial recognition

Another commonly used and oldest form of biometrics. This technology requires only a digital camera and facial recognition software. Facial recognition software takes measurements of the face like the distance between both eyes, the distance between forehead and cheekbones, etc. Once the data is collected, a sophisticated algorithm converts it into a facial sign that is encrypted. Facial recognition only requires a digital camera and facial recognition software.

Voice recognition

Voice Reconition Techinque under both types of biometric authentication – behavioral and physiological. Physiologically, the sound emitted by an individual helps in identifying the shape of the vocal tract, such as the nose, mouth, and trachea. When it comes to the biological side, the pronunciation, variations in tone, movement, etc. are taken into account. After combining data from both biometric types, a precise vocal signature is created.

Behavioral biometrics

Behavioral biometrics studies and measures behavior patterns or body functions. Here are some of the behavioral biometric forms:

Signature recognition

This biometric measures factors such as pressure exerted on the pen, spatial dimensions, and pen stroke in applications (offline and online). The measurements are tracked by a digital tablet.

Fig 2.Types of Behavioral Biometrics

Keystroke

Keystroke patterns improve security and take basic passwords to another level. Keystroke Dynamics records the rhythm while entering a password. It measures the time taken to click each key, the delay between keys, and the number of characters typed in minutes.

Gait

Gait refers to a mix of cyclical and coordinated movements that cause a person to Human gait is considered a unique feature to recognize a familiar person. move.

Facial Recognition for Secure ATM Access

Face recognition technology helps the machine to identify each and every user uniquely thus making face as a key. This completely eliminates the chances of fraud due to theft and duplicity of the ATM cards. Moreover, the randomly generated OTP frees the user from remembering PINs as it itself acts as a PIN.

Fig 3.Facial Recognition

Each person has a unique facial structure. Facial recognition technology allows automatic identification of the ATM user. In this article we will tell you about the features of this technology. You will learn about the principle of its operation, advantages and disadvantages.

The algorithm for facial recognition technology consists of two steps:

1. Identification (who is this person?)
2. Verification (is this the person pretends to be?

Key factors include the distance between your eyes, the depth of your eye sockets, the distance from forehead to chin, the shape of your cheekbones, and the contour of the lips, ears, and chin. The aim is to identify the facial landmarks that are key to distinguishing your face.

Security doors or gates are yet another use case of facial recognition software technology. Facial recognition technology can be applied to ticket counters at railway stations, the entry to the residential area, or even the main gate of the company.

Stages of the facial recognition system

1.Face detection

This step involves highlighting the person's face in the image.

2.Facial features detection

Determining anthropometric points reveals individual characteristics.

Important: The recognition algorithm and calculating facial characteristics is constantly being improved. Previously, the main point for the algorithms was the eyes. Currently, the algorithms take into account a minimum of 68 points on the face. The contour of the face, the shape of the chin, eyes, nose and mouth, as well as the distance between them are taken into account.

3.Face normalization

Eliminating head tilt, facial color correction, and other image transformations allows to get the clearest frontal image possible.

4.Feature extraction and descriptor computation

Descriptor computation makes it possible to identify features characteristic of a face regardless of the user's age, hairstyle, makeup, or other factors. Comparison of different descriptors allows one to evaluate whether the two obtained face images refer to the same person.

5. Face verification

In the end, the resulting digital template is compared with the available faces in the database.

Iris Scanning for Enhanced ATM Security

The iris scanner being the primary security check lets the system access the further steps for transaction. Fingerprint scanner embedded in the ATM card acts as the secondary security check for the system. The transaction procedure is successful only if the input data by the card holder match.it is widely being adopted leaving behind the old biometric system.

Iris scanning raises significant civil liberties and privacy concerns. It may be possible to scan irises from a distance or even on the move, which means that data could be collected surreptitiously, without individuals' knowledge, let alone consent. There are security concerns as well: if a database of biometric information is stolen or compromised, it is not possible to get a new set of eyes like one would get a reissued credit card number. And iris biometrics are often collected and stored by third-party vendors, which greatly expands this security problem.

Fig 4.Iris Recogintion

Iris scanning measures the unique patterns in irises, the colored circles in people's eyes. Biometric iris recognition scanners work by illuminating the iris with invisible infrared light to pick up unique patterns that are not visible to the naked eye. Iris scanners detect and exclude eyelashes, eyelids, and specular reflections that typically block parts of the iris. The final result is a set of pixels containing only the iris. Next, the pattern of the eye's lines and colors are analyzed to extract a bit pattern that encodes the information in the iris. This bit pattern is digitized and compared to stored templates in a database for verification.

Iris scanners collect around 240 biometric features, the amalgamation of which are unique to every eye. The scanners then create a digital representation of that data. That numeric representation of information extracted from the iris image is stored in a computer database.

The U.S. military has used iris scanning devices to identify detainees in Iraq and Afghanistan. For example, the handheld biometrics recorder SEEK II allows military personnel to take iris scans, fingerprints, and face scans and port the data back to an FBI database in West Virginia in seconds, even

in areas with low connectivity. As is often the case with cutting-edge surveillance technologies developed for use in foreign battlefields, similar iris scanning technology has since been deployed by police departments across the U.S.

The New York City Police Department was among the first police departments to begin using iris recognition. The department installed BI2 Technologies' mobile MORIS (Mobile Offender Recognition and Information System) in the fall of 2010. Although New York City's use of iris scanning in jails was supposed to be voluntary, there have been reports of arrestees being held longer for declining iris photographs. Prisons, such as the Rhode Island Department of Corrections, have also begun using the technology. An EFF survey of California law enforcement agencies in 2015 found that sheriff offices in Orange County and Los Angeles County had plans to implement iris scanning technology

This type of system uses a person's unique eye pattern as their personal key allowing them access to their funds without the need for cards or passwords. The increased popularity of iris scanning technology, also known as "eye-recognition" has grown exponentially in recent years with many banks offering this new service. The biometric authentication methods, such as fingerprint recognition, facial recognition, and iris scanning, have gained widespread recognition for their accuracy and difficulty to forge. Among these, iris scan biometric technology stands out as one of the most secure and reliable methods for verifying an individual's identity. The unique patterns in the iris of the human eye remain stable throughout a person's life and offer a vast number of distinctive features, making it an ideal candidate for securing sensitive transactions. Advantages include improved accuracy compared to other biometric methods (such as fingerprint recognition), heightened security features that reduces identity theft, cost saving from reduced card management fees and less time spent on authentication process. In addition, automated teller machine operators can offer customers greater privacy than other forms of identification such as fingerprints since no physical contact or records exist after the transaction is complete.

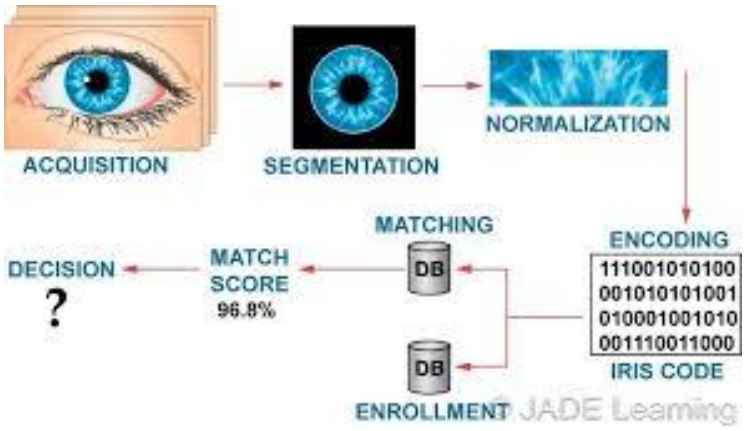

Fig 5.Process of Iris Recognition

The iris is a thin membrane on the interior of the eyeball. Iris patterns are extremely complex.Patterns are individual (even in fraternal or identical twins).Patterns are formed by six months

after birth, stable after a year. They remain the same for life.Imitation is almost impossible.Patterns are easy to capture and encode. Biometrics is the automated recognition of individuals based on behavioural and biological characteristics. The technology is designed to automatically take a picture from person and match it to the digitized image stored in the biometric passport. In the field of financial services, biometric technology has shown a great potential in offering more comfort to customers while increasing their security. Applications due to information protection issues, it is believed that the technology will find its way to be widely used in many different applications. Biometrics such as signatures, photographs, fingerprints, voiceprints, DNA and retinal blood vessel patterns all have significant drawbacks. Face Recognition: Changes with Age, Expression, Viewing angle, Illumination. Finger Print Recognition: Fingerprints or handprints require physical contact, and they also can be

counterfeited and marred by artifacts. IRIS recognition is one among the biometric systems the tool used for this recognition is MATLAB. To determine the uniqueness of iris patterns in terms of hamming distance distribution by comparing template generated from different eyes. The iris consists of a number of layers the lowest is the epithelium layer, which contains dense pigmentation cells. The stromal layer lies above the epithelium layer, and contains blood vessels, pigment cells and the two iris muscles. The density of stromal pigmentation determines. The color of the iris. The externally visible surface of the

multi-layered iris contains two zones, which often differ in color. An outer ciliary zone and an inner pupillary zone, and these two zones are divided by the collarets which appears as a zigzag pattern.

2.1Success rate:Failure rate using IRIS technology in just 1 in 1.2 million. When compared to other technology systems.

Iris scanners detect and exclude eyelashes, eyelids, and specular reflections that typically block parts of the iris. The final result is a set of pixels containing only the iris. Next, the pattern of the eye's lines and colors are analyzed to extract a bit pattern that encodes the information in the iris. This bit pattern is digitized and compared to stored templates in a database for verification.

Iris scanners collect around 240 biometric features, the amalgamation of which are unique to every eye. The scanners then create a digital representation of that data. That numeric representation of information extracted from the iris image is stored in a computer database.

Fingerprint Authentication

Fingerprint authentication, also called fingerprint biometrics, uses the unique characteristics of the human fingerprint. The human fingerprint is composed of ridges and lines that represent a pattern wholly unique to the person when taken as a whole.

Fig 6. Fingerprint Authentication

Fingerprint Authentication is the act of verifying an individual's identity based on one or more of their fingerprints. The concept has been leveraged for decades across various efforts including digital identity, criminal justice, financial services, and border protections.

Fingerprint authentication or scanning is a form of biometric technology enables users to access online services using images of their fingerprint. The biometric scan commonly relies on mobile and other device native sensing technology, as this has all but eclipsed software, third-party biometric algorithms. Some fingerprint scan solutions are architected in a decentralized model such as FIDO that ensures a user's fingerprint template is secured on the user's device. Here, a user's fingerprint scan is verified locally against itself, a token is sent to the service provider, and access is granted. The biometric authentication takes place locally, and the biometric data itself is not stored at the service provider (true secret).

Other fingerprint scan solutions are architected in a legacy centralized scheme in which user templates are stored at the service provider, and matching is done against a library of all other users' national security settings. Lastly, some fingerprint scan systems (e.g. in government) rely on specialized hardware found at the point of care, access, or sale.

Fingerprint Biometric Authentication Use Cases

Healthcare

Hospitals mainly use biometric authentication to accurately track patients and prevent any mix-ups. Clinics and doctors offices tend to implement biometric authentication to keep their patients' information secure. By using biometric authentication, hospitals and clinics can store and access patients' medical history at any time.Thus Hospitals mainly use biometric authentication to accurately track patients and prevent any mix-ups.

Travel

An electronic passport contains a microchip that stores the same biometric information as a conventional passport. The chip stores a digital image of the passport holder's photo which is linked to their name and other information that identifies them. The e-passport is issued electronically by a country-issuing authority, which checks the identity of the applicant through fingerprints or other biometric information and confirms the data in the chip with the information provided by the applicant before issuing the passport. An electronic passport contains a microchip that stores the same biometric information as a conventional passport.

Law Enforcement

Law enforcement uses different kinds of biometric data for identification purposes. State and federal agencies use fingerprints, facial features, iris patterns, voice samples, and DNA. This makes it quicker and easier for them to access confidential information. Normally law enforcement uses a trained human examiner to compare a fingerprint image to the prints on file. Today, AFIS (Automated Fingerprint for identification).

Voice Recognition for secure ATM Transactions

Biometric ATMs can identify users through their vocal characteristics and patterns, captured via integrated microphones. This method not only ensures security but also aids users with physical disabilities, offering an alternative mode of authentication.

Fig 7.Voice Recognition

Voice-activated automatic teller machines were designed to help people with visual impairments, including some elderly people, make financial transactions. Not every blind person can read Braille, and so ATM's equipped with Braille keypads don't always suffice. In addition, Braille keypads may allow blind people to enter the information they need to, but they don't provide a means of delivering directions to visuallyimpaired customers. So unless a blind person were to walk into a bank already knowing exactly how to use the ATM, it might not be possible for him or her to make transactions without assistance from a bank employee. Indeed, in the past, some visually-impaired people tended to avoid ATM's altogether.

The main focus of this project, was the novel interaction embraced by the ATM concept. To demonstrate an alternative, humanlike interaction, speech synthesis and speech recognition were used for the interaction rather than a standard keypad or touch screen. In this scenario user speaks into the microphone. microphone capture sound waves and generates electrical impulses and sound card converts voice signal into digital signal.

The system has the following phases:

- Training phase
- Testing (operational)

Training phase:

Training enrolment as shown, the persons are registered and their voices are recorded. The recorded voices are then extracted. Features extracted from the recorded voices are used to d envelop models of persons.

Testing (operational) Phase :

Testing or operational phase in this phase a person who wants to access the ATM is required to enter the claimed identity and his/her voice. The entered voice is processed and compared with the claimed person model to verify his/her claim. At this point system decides whether the feature extracted from the given voice matches with the model of claimed person. Threshold is set in order to give a definite answer of access acceptance or rejection. When degree of similarity between a given voice and model is greater than threshold the system will accept the access, otherwise the system will reject the person to access the ATM.

This focuses on the implementation of voice recognition in ATM machine. The main aim is to make the disabled people use the ATM in an effective manner. This method is one of the safe recognition and cost effective system which is appropriate for the current scenario. The implementation of this system depends on three algorithm includes: Hidden state algorithm for speech rate and frequency evaluation, Pitch identification algorithm for pitch estimation of voiceprints and accent analysis algorithm for accent calculation. These proposed algorithms make the system much more secured, efficient and accurate than the other system. The advantages in the proposed voice recognition system are: The background noises and distortion in voice is reduced and the insecurity in the system is overcome.

Fig 8.Voice Payment process

Security is an essential part of human life. In this era security is a huge issue that is reliable and efficient if it is unique by any mean. Voice recognition is one of the security measures that are used to provide protection to human's computerized and electronic belongings by his voice. In this paper voice sample is observed with MFCC for extracting acoustic features and then used to trained HMM parameters through forward backward algorithm which lies under HMM and finally the computed log likelihood from training is stored to database. It will recognize the speaker by comparing the log value from the database against the PIN code. It is implemented in Matlab 7.0 environment and showing 86.67% results as correct acceptance and correct rejections with the error rate of 13.33%.

Regardless of how you use it, there are both advantages and disadvantages that come from using voice activation technology. Some of the biggest advantages include:

- **Accessibility:** Voice activation allows a greater number of people to access digital technology, connected devices, and the internet more easily. It improves accessibility for people with disabilities, especially for individuals who have impaired vision or motor functions.
- **Connection:** Voice activation can easily work with other connected technologies and devices in your home, such as smart appliances and speakers. This connection makes it that much simpler and faster to accomplish different tasks in your home.
- **Convenience:** Using voice activation can be significantly more convenient than typing something out on a keyboard or smartphone or manually completing a task.

On the other hand, there are also disadvantages and barriers to using voice-activated technology that can affect consumers' ability to engage with it. Some of the biggest concerns about it include:

- **Cost:** Different devices that make use of voice activation, including speakers and smart appliances, can be costly for some people. They may only be able to afford one piece of voice-activated technology, such as a smartphone, and miss out on the benefits of connecting and using multiple devices.
- **Inaccuracy:** Although the accuracy of voice-activated technology has increased dramatically in the last several years, it still isn't perfect. You'll likely still encounter some minor inaccuracies or errors when using voice activation.
- **Limitations:** Voice-activated technology is currently capable of only doing so much. There are limitations to how it can be used, and it will take more time to discover more applications and uses of voice recognition.
- **Multi-tasking:** You may think that using voice recognition helps you multitask, but it may actually just be disruptive. For example, a growing body of research especially when it doesn't work accurately.

Advantages

This system generally used for bank security. Picture Processing structure contains finger inspect, picture check. The image planning is progressively balanced system. Secure Automated Teller Machine by picture taking care of is assume control over a huge segment of the bank ATMs,

Modern ATMs are implemented with high-security protection measures. They work under complex systems and networks to perform transactions. The data processed by ATMs are usually encrypted, but hackers can employ discreet hacking devices to hack accounts and withdraw the account's balance.

Some of the advantages of ATM include:

- Saves time.
- Increased security.
- Wide range of banking services.
- Easy accessibility.

Scalable Performance- ATM can send data across network quickly and accurately, regardless of the size of the network. ATM works well on both very low and very high-speed media. Flexible, guaranteed Quality of Service- ATM allows the accuracy and speed of data transfer to be specified by the client.

There are several advantages to the use of small, fixed-size cells. First, the use of small cells may reduce queuing delay for a high-priority cell, because it waits less if it arrives slightly behind a lower-priority cell that has gained access to a resource.

The biggest advantage of ATM machines is that they allow access to cash at any time. In addition to having a limited amount of time to obtain cash, there was only one way of accessing it before 1967, through visiting the nearest bank.

There are many advantages to using biometrics as a form of identification for access, including that biometrics:

– Cannot be lost: You can always forget your key, access card or password, but you can’t forget your fingerprints or your eyes. If biometrics are the only means of authentication, a user can never be locked out

if they're entitled to access. If you use multi-factor identification, a biometric factor is one less thing that users need to remember.

– Cannot be transferred or stolen: It is easy and not uncommon for people to leave access cards or notepads containing passwords lying around where unwanted personnel could get hands on them. You cannot lose your biometrics due to carelessness, and they cannot be transferred or stolen without causing physical trauma to the user.

– Are person-specific: Unless a user is colluding with an unauthorized person, you can be confident that the person who is using biometrics to gain access is who they purport to be.

– Are intuitive: Most users should have little difficulty figuring out how to press their finger onto a fingerprint scanner or look into an eye scanner. This process can be much faster and more convenient than hunting around for another password or trying to find the right way to insert an access card.

Your company's management will have to decide which biometric factors are most appropriate for your business. Some may prefer behavioral biometrics because you can often use existing hardware to collect the information with just the installation of new software to analyze the data. Some may prefer fingerprint identification because it's more recognizable and user-friendly than certain other methods.

While you can use multiple biometrics for identification, in most cases currently, a single biometric when paired with some other authentication factor — like a key card, push notification or password — is sufficient for secure access. While some companies with special security issues may require further measures, it's often not cost-effective for a standard company to use more than one biometric authentication factor.

- They are linked to a single individual (unlike a password, which can be used without authorisation),
- They are very convenient since there is no need to remember or carry anything,
- The security, they are highly fraud resistant.

Disadvantages

This system generally used for bank security. Picture Processing structure contains finger inspect, picture check. The **ATM machines can be targeted by criminals, robbers and hackers**

One of the disadvantages of ATM machines is that they are both physically and electronically vulnerable. This makes them an easy target for criminals. Malware can be used to access people's cash. Skimming devices and small cameras can be fitted onto Automated Teller Machines. Other criminals can physically destroy an ATM in order to access cash. People risk being robbed using ATM machines especially in isolated areas. This is a huge disadvantage of ATM Machines.

ATM Machines May Malfunction

An Automated Teller Machine like any other machine is bound to break down, although this is rare. Some machines may fail to recognise bank cards or can run out of cash. At other times the ATM system goes offline. Also, there is a limit to the amount of cash one can withdraw from an ATM which can be an inconvenience if you require more funds. So the other disadvantage of Automated Teller Machines is that they may breakdown.

ATM machines Are Costly For The Users

Setting up ATM machines can be affordable for financial institutions, but it is not the same for the users. Banks and machine owners obtain a lot of revenue from ATM machines in the form of fees that users are charged for using them. The transaction costs are a huge disadvantage of ATM Machines.

Lack of Personal service

Lack of personal service is a disadvantage of ATM Machines. There are no bank assistants to help you or to ask questions to.One of the disadvantages of ATM machines is that they are both physically and electronically vulnerable. This makes them an easy target for criminals. Malware can be used to access people's cash. Skimming devices and small cameras can be fitted onto Automated Teller Machines.

- If you get a problem with your bank card, or forget your pin, you can't withdraw your money
- Cash withdrawal limits on ATM Machines
- If an ATM card is lost, it can be misused

Conclusion

This system generally used for bank security. Picture Processing structure contents finger inspect, picture check .The image planning is progressively balanced system. Secure Automated Teller Machine by picture taking care of is assume control over a huge segment of the bank ATMs.

The banking sector, a cornerstone of our global economy, is in the midst of a transformative era. As we've journeyed through various global implementations, it's evident that biometric ATMs are not just a fleeting trend but a robust response to the growing demands for security and convenience in financial transactions. This evolution is not just about technology; it's about trust. It's about ensuring that every individual, whether withdrawing cash in Tokyo or checking an account balance in Johannesburg, can do so with the confidence that their financial data and assets are protected. It's about recognizing the unique identity of each customer and validating it with impeccable account.

As the demand for secure and user-friendly banking solutions grows, we're committed to delivering cutting-edge biometric solutions that meet the needs of both financial institutions and their customers. If you're a financial institution looking to elevate your ATM services or a business keen on integrating biometric solutions, Aratek Biometrics is here to help you every step of the way. Connect with us today and let's shape the future of secure banking together.

Access card / PIN provide insufficient ATM security. Adding facial verification to the process can greatly decrease fraudulent transactions. Current ATM’s have the power to perform verification locally, given a software change. We have developed a rapid fingerprint enhancement algorithm that can adaptively improve the clarification of ridge and furrow structures based on the estimated local ridge orientation and ridge frequency from the images input. Bank uses fingerprint readers for ATM authorization and becomes more common in grocery stores where they are used to automatically recognize a registry customer and bill their credit card or debit account Enhancement algorithm using the minutiae's goodness index and input fingerprint verification accuracy. The Enhancement algorithm is an input fingerprint verification technique.

References

Arunkumar, Vasanth Kumar, Naveenly King, Aravindan, “ATM Security using Face Recognition”, International Journal of Current Engineering And Scientific Research- Volume- 5, Issue-4, 2018. [2] A S Tolba, A.H. El-Baz, and A.A. El-Harby, “Face Recognition: A Literature Review”, International Journal of Signal Processing, Volume 2 Number 2, 2014. [3] Divyarajsinh N.Parmar1, Brijesh B. Mehta2, “Face Recognition Methods & Applications”, International Journal of Computer Applications in Technology, January 2014. [4] KresimirDelac, Sonja Grgic&MislavGrgic, “Image Compression in Face Recognition” - A Literature Survey, October 2008. [5] Mourad Moussa, MahaHmila& Ali Douik, “A Novel Face Recognition Approach Based on Genetic Algorithm Optimization”, https://doi.org/10.24846/v27i1y201813. [6] Priyanka, Research Scholar, Department of Computer Science and Engineering, “A Study on Facial Feature Extraction and Facial Recognition Approaches”, International Journal of Computer Science and Mobile Computing, May 2015. [7] T.Suganya, T.Nithya,C.Sunita, B.Meena& Preethi, “Securing ATM by Image Processing”– FacialRecognition Authentication, International Journal of Scientific Research Engineering & Technology [8] J. G. Daughman, "How iris recognition works," IEEE Transactions onCircuits and Systems for Video Technology, vol. 14, no. 1, 2004.