ATM ACCESS USING IRIS RECOGNITION

[1]Ms. P. Sabitha, [2] Sourabh Kumar Mishra, [3] Akriti, [4] Chanchal Matania, [5]Anirjit Roy
[1]1Asst. Professor in CSE Department, SRM IST, [2] UG Scholar CSE Department, SRM IST, [3] UG Scholar CSE Department, SRM IST, [4] UG Scholar CSE Department, SRM IST, [5] UG Scholar CSE Department, SRM IST
[1], CSE Department,
[1] SRM IST RAMAPURAM, Chennai, India

***Abstract*:** ATM access using iris recognition is a Multi-Banking Transaction System. It is one of the most secured systems these days. People have multiple bank accounts and hence they need to carry many ATM cards leading to many different PIN numbers for various accounts which is not much secured because anyone can misuse it. In the case of forgetting of the PIN numbers or losing the card can lead to various problems. To provide a better security system this has been introduced i.e. the iris recognition technique where the system recognizes the iris of a person and displays all his accounts in various banks. Unauthorized access is wholly restricted since it makes "iris recognition" unique for every individual. Hence, the proposed system has no risk overhead in managing multiple accounts and provides way more security than the previous traditional ATMs.

I. INTRODUCTION

An automatic teller machine is used to conduct several bank activities such as cash withdrawal, money transfer, checking account balance etc. ATM provides customers with a quick and convenient way to access their bank accounts and to conduct financial transactions. Personal Identification Number (PIN) is one of the critical aspects of the ATM system which is used to protect the financial information of customers from unauthorized access. Since many ATM cards and PIN numbers are not very safe to keep and remember, we've introduced the new iris recognition system in ATM. After the registration and authentication the user can have access to all his accounts and can proceed with transactions. The iris recognition system allows for maximum privacy and security. There is no risk of theft and fraud as no ATM card is required and no PIN number is to be remembered. After the iris is recognized, an OTP will be sent to the customer's mobile number to verify.

II. EXISTING SYSTEM:

ATM access using biometric is a one-touch Multi-banking Transaction system using biometric and Iris recognition technique. This technique is highly secure and reliable.

Nowadays every individual has multiple accounts in different banks hence people need to carry multiple ATM cards for transactions, leading to different PIN numbers for each account. In the traditional system, if the cards get lost or the passwords are forgotten, then it's a significant issue to be solved. It can take days to get a new card. The work gets hampered and time is wasted. Hence this One-Touch ATM access system is promoted.

In this existing system, unauthorized access cannot be restricted. Hackers can hack into your account details and can do the needed damage.

III. PROPOSED SYSTEM:

Eye image acquisition:

An important and complex step of iris recognition system is image acquisition. Especially for Indians, the iris is small in size and dark in color. It is difficult to acquire clear images. The image acquisition means the first step of any vision system.

After the image has been obtained, various processing methods can be applied to it. The image enhancement and the iris recognition techniques can be henceforth carried. The image acquisition consists of three steps:

1. The energy reflected from the object of interest.
2. An optical system focusing on the energy.
3. Sensor to measure the amount of energy.

Challenge-response test:

Biometric features may be counterfeited and criminally used. This is a crucial weakness of the biometric system. This module aims to ensure that an input image actually originates from a person instead of iris photographs, phony eyes, or other artificial sources. This is called the challenge-response test.

The Challenge-response test is crucial for the determination whether the ongoing process is justified or not. It helps us to fix any error, if occurred.

This method verifies the response of the pupil diameter by varying illumination levels at the same distance from the eye. The algorithm of this method is elaborated as follows:

Step 1: Capture the same person's eye images under different lighting levels

Step 2: Measure the pupil diameter from the captured eye images. If these values are divergent then the image is actually from a real source (human), otherwise artificial sources may have been used. The diameter of the pupil is calculated by satisfying (1). Equations (2) and (3) describe the challenge-response process.

(x - x1)(x - x2) + (y - y1) (y - y2) = 0,

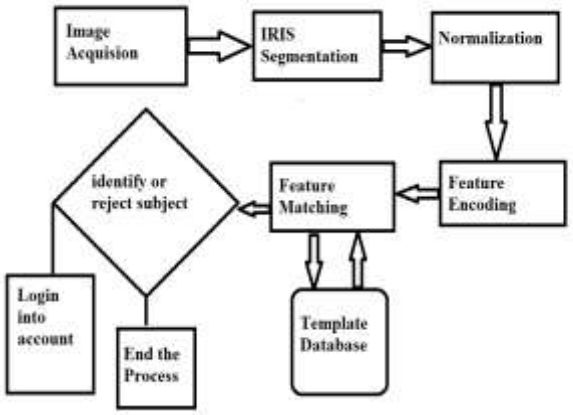
Td =n-1_i=0 |_i - _i+1|, CRT = _True, if Td _= 0, False, otherwise

Where:

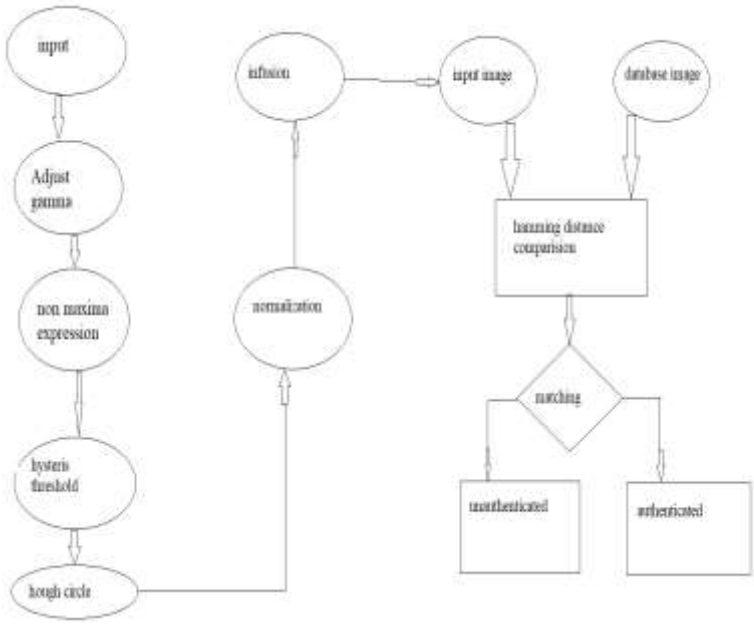
- Td is total diameter of the pupil in the capturing sequences,
- CRT is a challenge-response test parameter,
- n is number of eye images,
- i and i+1 are diameters of the pupil under different illuminations.

This method assures that an input is coming from a real sequence and not from photographs or other artificial sources. The biometrics-capturing device needs to be capable of ensuring that they are inspecting genuine user features (as opposed to a photograph or recording) and that the output signal is not substituted. This is used to prevent replay attacks lifted from video-signals. The Challenge-response test is crucial to determine the productivity and efficiency of the technique being used. It ensures that we are inspecting genuine user features and that the output signal got is hereby not substituted. Overall it helps in the proper functionality of the system.

A.SYSTEM ARCHITECTURE



B.FLOW DIAGRAM



C. ALGORITHM

[1] A high definition image is captured using a digital camera then the image is enhanced by removing the white spots obtained due to light reflection Steps to enhance:

1. The morphological operation using MATLAB tool 'infill'
2. Thresholding
3. Identifying local minimum point in 3x3 neighborhood 4. Cutting off those circles that do not fit inside the image.

[2] Iris segmentation is done using Daugman's operator

$$ma(r,xp,yo) \mid G\sigma * d\ dx\ I(x, y)\ (r,x0,yo)\ 2\pi r\ ds\mid$$

I(x, y) is the intensity of the pixel at coordinates (x, y) in the image of an iris. r denotes the radius of various circular regions with the center coordinates at (x0, y0). σ is the standard deviation of the Gaussian distribution. Gσ(r) denotes a Gaussian filter of scale sigma (σ). (x0, y0) is the assumed center coordinates of the iris. s is the contour of the circle given by the parameters (r, x0, y0)

[3] It is done using Daugman's Rubber sheet model.

The center of the pupil was considered as the reference point, and radial vectors pass through the iris region. Many data points are selected along each radial line defined as the radial resolution. The number of radial lines going around the iris region is defined as the angular resolution.

[4] Feature is encoded and saved in the database. This is done by calculating the ratio between the number of non-zero pixels which are in the foreground mask (the moving objects) and the total pixels in the foreground mask. The calculation done is – Density = cv2.countNonZero (mask)/fgmask.size

The fgmask stands for the foreground mask. Thus now the variable "Density" holds the traffic density of the roads. This can be further fine-tuned to ignore moving objects other than vehicles to get more accurate density count.

[5] Normalization It is done using Daugman's Rubber sheet model. The center of the pupil was considered as the reference point, and radial vectors pass through the iris region. A number of data points are selected along each radial line is defined as the radial resolution. The number of radial lines going around the iris region is defined as the angular resolution.

The process undergoes many steps. The registration procedure is done. Then, the required data is stored in the database. The next step is the scanning process. After the scanning process, we check if the templates are being matched or not. If the templates do not match, the process goes back to the start point. It then undergoes the whole process again till the time the matching occurs.

[6] The final process is the generation of the iris code. For this, the most discriminating feature in the iris pattern is extracted. The resulting phasor lies using the wavelet.

H Re,Im sgn Re,Im I ρ,Ø ρ,Øe−iω θ0−Ø .e− r0−ρ 2 α2 e− θ0−Ø 2 β2 ρdρdØ Where, h Re, Im has the real and imaginary part, each having the value 1 or 0, depending on which quadrant it lies in The frequency response of a Log-Gabor filter is given as.

(f)= exp − (log (f f0)) 2(log (σ f0)) 2

[7] The template capture and template present in the database is matched if the template gets matched system gets login or else

FUTURE WORKS:

In the future, a more progressive approach of the system will be developed. This technique can be used in the banking system, in shopping malls to keep a security check on any suspected activities. It can also be used for the safety of the general public.

The future model holds more promises to serve better and has a more reliable mechanism.

In the future, the model will be developed with high accuracy.

RESULT:

The result obtained from the technique leads to a well developed and progressive technology aiming at providing more security than the traditional system. It's a comprehensive and straightforward approach that's very accurate. This has no risk overhead of the problem of managing multiple bank accounts and losing information and money if the system fails or is hacked. This approach is welcomed by many with open hands. It solves the problem of the common public and provides a hassle-free use of technology.

VI. CONCLUSION

The new model of ATM system that has been proposed shall be of immense help and benefit for the society. Money has and shall be a valuable resource and asset for us. Financial security is very essential these days and is a case of concern. The iris access ATM system paves a smooth path towards financial security. The iris scanning method is beneficial as it is unique and cannot be tampered easily unlike the conventional fingerprints. The proposed system is accurate to the best of our knowledge and is subjected to future enhancements.

VII.REFERENCES

1. A study of liveness detection in fingerprint and iris recognition using image quality assessment.
By: Karuna. R. and Prof. S.K. Kumaresan (Dept. of CSE Government College Of Technology, Coimbatore)
2. A self-banking biometric machine with fake detection applied to iris along with GSM Technology for OTP
By: Joyce Soares, A.N. Gaikwad
3. Iris recognition based authentication System in ATM
By: P. Nagarajan (PG Scholar ECE Dept.) and Dr. Ramesh S.M. (Asst. Professor ECE Dept.) of Bannari Amman Institute Of Technology.
4. Recognition technique for ATM-based on Iris Technology (An article published on September 2012.)
5. ATM Transaction: A new time-based approach research paper.
By: Sunny Nahar(Asst. Professor) Dhanush J. Nair (Student) of Vivekananda Education Institute Of Technology, Chembur, Mumbai.
6. Fingerprint verification of ATM security system by using biometric and hybridization.
By: Pramila D. Kamble, Dr. Bharti W. Gawali
7. Enhanced security system using biometrics.
By: Prof Selina Oko and Jane Oruh (Dept of CSE, Ebonyi State University Abakaliki, Nigeria)
8. Fingerprint and iris biometric controlled smart banking machine embedded with GSM Technology for OTP.
By: Joyce Soares and A.N. Gaikwad of ECE Dept.,Zeal College Of Engineering & Research, Nahr, Pune.
9. Score level fusion based biometric identification using Thepade's sorted ternary block truncation coding.
By: Ms. Manisha S. Madane and Dr. Sudeep Thepade,
IT Dept., Pimpri Chinchwad College of Engineering, Pune.
10. Enhanced security for ATM with OTP and facial recognition features.
By: Mohsin Karavaliya, Saifali Karedia, Sharad Oza, Dr. D.R. Kalbande of CSE dept. , Sardar Patel Institute of Technology, Mumbai.