International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 8, ISSN No. 2455-2143, Pages 85-89
Published Online December 2017 in IJEAST (http://www.ijeast.com)

UNLOCKING SMART PHONE VIA WEARABLES THROUGH IRIS SCANNER

Avinash Arunachalam
Department of CSE
Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India

Sai Aravindhan. C. P
Department of CSE
SNS College of Technology, Coimbatore, Tamil Nadu, India

Abstract-- iris scanner is evolving for the futuristic security purpose electronic device. It is the most accurate device in the current scenario. IRIS scanner scans the retina with the help of CCD (Charge Coupled Device) camera. CCD is a device which scan the retina and converts the image to a compactable language which can be understood by the device (for example the image is converted to a digital value). This working of CCD is achieved by 'shifting'. This shifting performs the data to be transferred from one device to another in a single instance of time. The working of IRIS scanner is simpler than any of the device. It just scans the colored ring of muscle that opens and shuts the pupil of the eye like a camera shutter.

There are two stages involved while scanning. The first stage is Enrollment, enrollment is nothing but the process of scanning the pupil of the eye for the first time and storing it in a database. The data which is stored is the one used for the authorization purpose when the people scans their eye for the next time.

The second stage is Verification; verification is the process which will check for the data in database and then authorize the personnel if the data is available in the storage are. If the data is not present it will not authorize the personnel or it will again ask the personnel for Enrollment process or will show an error log.

IRIS scanner is used in many fields but it is used enormously in the security field. The IRIS Scanner can be built in the smart watches (here after referred Wearable) which is used to unlock the smart phone to which the watch is connected. This implementation is used to ease of access for unlocking the smart phone via an external device and also by locking the smart phone via an external device, this implements the overall security of a device to a next level. This implementation does not stop only with the locking and unlocking system in a smart phone it can be authorized to send a SMS (voice or text) and can be able to make a call in the smart phone through wearable.

Keywords: **CCD digital camera, shifting, wearable.**

I. INTRODUCTION

Iris Recognition Immigration System (IRIS) is an initiative, launched in 2004. The IRIS Scanner is a biometric technique that use reads the human retina and store the details in a machine understandable form (for e.g. in Binary form or in Digital form). The Human eye is made up of thin tissue of neural cells that is in the posterior part of the eye.

A common question will arise, what will happen when identical twins tries to unlock the system. It is simple according to study the network of blood vessels in the retina is not genetically determined so that even an identical twin do not share the same pattern.

From birth the pattern in retina remains unchanged till your death, so the IRIS biometric is one of the most secure access control in terms of security. In case of fingerprint biometric, the fingerprint scanner can easily lead to false acceptance. A person's finger can change its size/form over the time, so does the the fingerprint may also get varied and that change is not accepted in the finger print scanner. These serious disadvantage is not occurred in terms of IRIS Scanner.

As already mentioned, the human retina remains unchanged from birth to death, so the possibility of lead to false acceptance of the scanned data is very less. Another major advantage is that is cannot be easily false matched with another data to crack the access.

A. Working of IRIS Scanner-

The IRIS Scanner scans the pupil which is located in the center of the eyeball, it dilates on exposure to light and contracts in dark, so the size of the pupil varies in respect to light emitted it is exposed to from the device. The thin ring located between the sclera and pupil boundary is known as IRIS and contains a lot of minute data in it. It has a data rich physical structure and it is unique to each person. IRIS Scanner scans this detail and store it

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 8, ISSN No. 2455-2143, Pages 85-89
Published Online December 2017 in IJEAST (http://www.ijeast.com)

in the database or in the cloud or in the device, so that the validation for accessing can be verified.

B. Steps involved in IRIS Scanning-

Before proceeding to the steps, the basic process is to capture the image of the IRIS in rich texture, so that only the IRIS can be scanned and processed. This is achieved by using a CCD digital camera, It uses both visible and near-infrared light to take a clear, high-contrast picture of a person's iris. With near-infrared light, a person's pupil is very black, making it easy for the computer to isolate the pupil and iris.

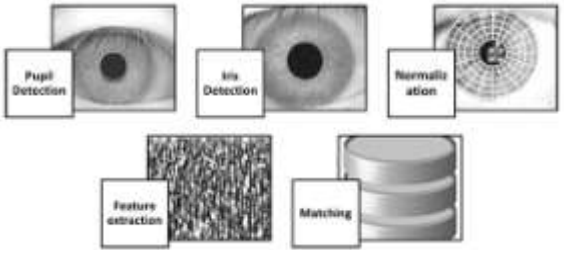

Fig. 1. Steps in IRIS Scanning.

C. Pupil detection-

The first step after capturing the image of human retina is to separate the pupil from the captured eye image so that the iris pattern can be used for matching purpose. The pupil is the darkest portion of the eye and has very low intensity, so that the edges can be easily found out. Once the edges are found it will be easy to find the center of the pupil by using the Euclidean distance between non-zero points and the spectrum image can be obtained from that. From the spectrum image the center of the pupil can be obtained and the nearest non zero pixel is the radius of the pupil.

D. IRIS detection-

By using intensity variation approach the outer boundary of the IRIS is detected and concentric circles are drawn with different radius to show different intensity of the circle drawn. The intensity are marked as a rectangular strips for identification of the data in the pupil.

E. Normalization-

The IRIS image taken from pupil boundary are composed of points, which is to be normalized to ensure the size of the strips to remain constant for different image. So that when user tries to access with different types of images the points remains the same and the access can be granted, i.e., the size of the iris on the strip is constant in spite of the expansion and dilation of pupil.

F. Feature Extraction-

Haar Wavelet Decomposition process is used here to derive the unique characteristics of the iris. This process decomposes the image into four co-efficient,

- Horizontal
- Diagonal
- Vertical and
- Approximation

This process is continued for five level. The co-efficient of the last level is combined to form a vector and converted into binary form. This allows the IRIS Scanner to compare the data in the database and query image, and grant the access by passing the binary value.

G. Matching-

The hamming distance approach is used to compare the iris code that are generated for the database and query image. The difference between two codes is counted and the number is divided by the count. This matching score is provided as input that generates final matching score.

H. Advantages of using Iris Scanner-

- The biggest advantage of using the IRIS Scanner is its accuracy and reliability.
- Patterns apparently stable throughout life
- Externally visible; patterns imaged from a distance

I. Disadvantages if Iris scanner-

- The distance between the scanner and the human eye is minimum. i.e., it cannot scan the retina when the distance is high.
- Located behind a curved, wet, reflecting surface
- Obscured by eyelashes, lenses, reflections
- Illumination should not be visible or bright
- Some negative (Orwellian) connotations

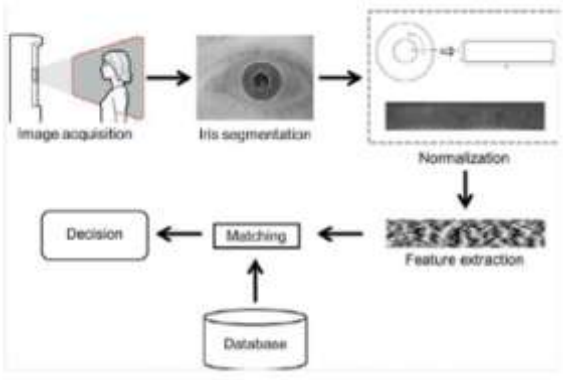

Fig 2. Block diagram of IRIS Recognition System.

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 8, ISSN No. 2455-2143, Pages 85-89
Published Online December 2017 in IJEAST (http://www.ijeast.com)

II. LITERATURE REVIEW

A. Technology overview-

Smart watches are digital watches that do more a lot more that your old analog time tracking device. These are full-fledged digital tools.

The technology for connecting the wearable devices and the smart phones through internet falls under the Internet networking of things i.e., the IOT. As seen in many areas IOT is a wide application domain for things to be connected in a network and make them work.

Wearable devices like smart watch has the specification to view contacts, music, photos, our health data which is synced with our phone, this feature of syncing the smart watches with smart phones help us to easily access the data in easy way.

The process behind this technique is simple one. All the data are either stored in cloud, so that other devices can log into the cloud account and can be synced, or the smart watch is connected directly to the phone with Bluetooth so that there is no need of internet connectivity to sync the data. Here, we can implement the work by using the IOT domain, and not by the Bluetooth technology to connect the devices. So we can think about what if the implement is done in both ways. The simple thing relying behind this will help the user for accessing the smart phone via wearable's in case if there is no ISP. But in case if ISP fails, the user cannot access the smart phone via smart watch. That's because Bluetooth can't be connected to cloud, but ISP can, so the method can be implemented only there is an strong internet connectivity in both the devices.

B. Overview of connecting wearable devices to smartphones-

Since the evolution of smart watches, the innovation of making is smarter has come up at its best. At the beginning the smart watches are connected to Bluetooth, and here also this is going to be done in the same way. But the connection at first innovation of smart watch was at its best.

Soon after the smart watches have come up with a cellular connectivity. It took up to the next level for the user, it made them not to carry their smart phones all the time and all the way out.

The smart watch was in existence from 1994 started from a simple data transfer from a PC to doing all the thing that a smart phone can do.

The smart watches should have a Bluetooth and Wi-Fi enabled inside it so that the user can be connected to their phones in any of their desired wish. Coming to the method of accessing the phone by the watch will be implemented by unlocking the phone through watch by Iris scanner in the watch.

III. PROPOSED METHOD

As illustrated above, the smart phone can be accessed through wearable devices by unlocking it using the Iris scanner in the smart watch. This can be implemented by placing the supportive camera in the smart watches rather than ordinary camera. The camera thus should support the iris scanning facility thus it can be used to unlock the smart watch as well as the smart phone.

Once the user gets initialized the watch the iris will be detected and the data is encrypted and will be saved in cloud. The need of encryption is to ensure that the data will be stored securely in the cloud, so that the user is in no need to worry about the data in the cloud. The data which is stored in the cloud can be accessed anywhere with the help of internet connectivity in any smart devices, so here comes the key to our proposed method. The data is stored in a centralized storage, once the user scans through the smart watch the data in the cloud will be compared with the scanned data and thus can unlock the smart watch as well as smart phone by automatically entering the passcode in the smart phone.

This is similar to unlocking the smart phone through Iris scanner, which is in existence in many of the smart phone now, once the smart watch is unlocked, simultaneously the smart phone will also be unlocked if it is connected in the Internet and to the same cloud account.

The main reason for developing this access security is to give the user a whole new tech feature for integrating the smart watch and the phone via a cloud. Thus, it will face a very serious challenge and can face a lot a technical development in the future. By implementing this method, the security throughout the devices which is used now will be further more improved to preserve the user data and privacy on it, and also the user is of no need to use his/her smart phone all the time to do all the stuffs, it can be all bought to the wrist end and can be make it simpler and elegance to use the features.

This work can be a real-time existence and is possible to make that once there is a possible way to scan the iris in the smart watches. Once the Iris is scanned and the scanned data is encrypted using any algorithm to ensure the security in the cloud. Then the data stored in the cloud will be useful to unlock the smart phone by allowing the permission to enter the passcode automatically once the verification is successful in the smart watch.

Fig 3.1 shows an overall view about how the connection between the smart watch and the

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 8, ISSN No. 2455-2143, Pages 85-89
Published Online December 2017 in IJEAST (http://www.ijeast.com)

smart phone is carried out. This model will explain how securely the data will be stored in the cloud. Thus, maintaining data integrity and privacy of the user so that the any chance of misusing the data can be prevented.

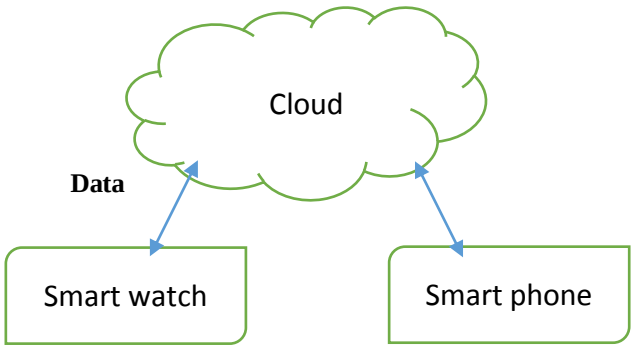

Fig. 3. Communication of device via cloud

A. Working concept-

To make this idea into a real-time scenario it should be started with smart watch as stated above. The watch should have the facility to scan the iris and should also have to connected to the internet so that it can transfer the data to the cloud. Once after the data is transferred it is then encrypted to ensure the privacy of the user data so that no one can peek into it and then the verification is done to unlock the phone if the scanning is successful.

This simple concept may look a bit tricky to use the camera that has iris scanning facility included in the smart watch.

Another difficult process is to safe guard the data which is stored in the cloud. Then by verification and giving permission.

Thus, all these phases is a simple but need to be implemented carefully a small flaw in the phase will burst out the privacy of the user data.

After all these, the smart phone will allow permission to unlock itself automatically once the smart watch is unlocked. This is done by giving permission in the phone by connecting the smart watch first and then adjusting the setting in the Application of the respective smart watch.

B. Advantages-

- Improved security
- Improved user experience
- Cannot be forgotten or lost

C. Future Work-

The camera which is used for scanning the eye will be updated with enhanced qualities which will speed up the process for scanning the eye. The camera lens will be tweaked in order to work in a dark environment so the users can unlock the phone with iris scanner even in the dark environment.

This can be a path for payment security in smart phones and the payment can be made by just looking at the wearables which will scan and make the transaction with your approval, its much faster than looking at the phone and making the payment.

The cloud security will be enhanced so the information will be stored securely. The encryption algorithm will be updated with more security because the data is very valuable.

IV. CONCLUSION

The unlocking system will be helpful in safeguarding the mobile phone in many ways like secured transaction, unlocking and locking the data from mobile from intruders. This method will also make the unlocking of smart phones security to a next level and can make improved connectivity between the wearable and smart phone.

V. REFERENCES

[1] Donald M. Monro ,Soumyadip Rakshit and Dexin Zhang,"DCT-Based Iris Recognition ", IEEE Transactions On Pattern Analysis And Machine
Intelligence, Vol. 29, No. 4, April 2007.

[2] Dhiraj Kumar Sharma and Prabhjyot Singh ," DCT (Discrete Cosine Transform) Coefficient based Iris Recognition System", International Journal of Bio-Science and Bio-Technology Vol.6, No.5 (2014) , ISSN: 2233-7849.

[3] Ahmad M. Sarhan,"Iris Recognition Using Discrete Cosine Transform and Artificial Neural Networks", Journal of Computer Science 5
(5): 369-373, 2009ISSN 1549-3636.

[4] Iman A. Saad and Loay E. George," Iris Recognition Based On the Low Order Norms of Gradient Components", World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:8, No:8, 2014.

[5] Gonzalez Woods &Eddins, "Digital Image Processing Using Matlab", 2 ndedn. Pearson Education.

[6] Dhananjay Theckedath, "Image Processing", Nandu Publications.

[7] Somdutta Chakraborty, Kavita Chande and Miral Parekh,"IRIS RECOGNITION",Department of Biomedical Engineering, T.S.E.C.,Mumbai.

[8] Rahesha Mulla and Amrita Manjrekar,"Iris Recognition Using DCT",Computational Intelligence and Information Technology Volume 250.

[9] John Daugman, "Iris Recognition", American Scientist vol.89, July-August 2001.

[10] Jain AK, Ross A and Prabhakar S, "An introduction to biometric recognition", IEEE transactions on circuits and systems for video technology, vol.14 (1); 2004.

[11] Su Li, Li Qian and Yuan Xin,"Study on Algorithm of Eyelash Occlusions Detection Based on Endpoint Identification" Supported by Youth Foundation of Heilongjiang Province of China(Grant No.QC07C14, QC08C65) 2011 IEEE.

[12] Khalid A. Darabkh, Raed T. Al-Zubi, and Mariam T. Jaludi "New Recognition Methods for Human Iris Patterns," MIPRO 2014, 26- 30 May 2014, Opatija, Croatia.

[13] Karen P. Hollingsworth, Kevin W. Bowyer"Improved Iris Recognition through Fusion of Hamming Distance and Fragile Bit Distance", Fellow, IEEE, and Patrick J. Flynn, Senior Member, ieee transactions on pattern analysis and machine intelligence, vol. 33, no. 12, december 2011.

[14] R.M. Bolle, S. Pankanti, J.H. Connell, and N. Ratha, "Iris Individuality: A Partial Iris Model," Proc. Int'l Conf. Pattern Recognition, pp. 927-930, 2004.