**PROJECT SYNOPSIS**

**ON**

**“RETINA BASED BIOMETRIC RECOGNITION SYSTEM”**

|  |  |  |
| --- | --- | --- |
| **Batch. No : A9** | | |
| **Sl.No** | **USN** | **NAME** |
| **1** | **3VC15CS053** | **Meghana K** |
| **2** | **3VC15CS050** | **Manjula G P** |
| **3** | **3VC15CS027** | **G. Ramya** |
| **4** | **3VC14CS112** | **Veluru Eshwari** |

**Submitted to:**

|  |
| --- |
| **PUNEETH GJ** |
| **Assistant Professor,**  **Computer Science and Engg. Dept.,**  **R.Y.M.E.C,**  **Ballari – 583104** |

**Submitted by:**

CONTENTS

1. Introduction 1
2. Problem Statement 2
3. Improvement Over The Existing Implementation 3
   1. Present State and its drawbacks 4
   2. Advantages of proposed system 5
4. Scope of the project 6
5. Tools and Technologies 7
6. Project Cost Estimation(Use COCOMO Model) 8

References

**1. Introduction:**

In today’s world, among various biometric modalities, iris, arguably, is one of the most reliable, universal, measurable, accurate and inimitable. Over the years, it has been established that every iris is unique, particularly in the detailed structure of the front or anterior layer. Not only are the irises of identical twins different, but the iris of the two eyes of the same person are also different. Although specific details of the appearance of an iris vary depending on the level and direction of illumination, it has been claimed that the basic and significant features of iris remain stable and do not change over a long time. Generally, covariates in iris recognition are image quality (i.e. noise, blur), illumination (specular reflection), off angle, occlusion, and resolution. In recent years, several approaches have been developed to advance the state of- art in iris recognition and address these covariates. However, there can be potentially many other covariates in iris recognition which have not yet been identified.

A biometric system is a pattern recognition system that checks the authenticity of a person using biometric measures. There are two types of authentication: - verification (checking the validity of a given identity) and identification (checking if a given pattern is associated with any of the enrolled identities stored in the database).

The retina is an internal protected organ of the body. The human retina consists of blood vessels that form a unique pattern and the pattern does not change through the individual’s life. So it is impossible to forge that pattern. Retina based security system works by tracking an image of an individual's retinal blood vessel network and comparing it to a previously authenticated scan of the same individual. The uniqueness and stability of retina guarantees a strong biometric authentication. Also, it is less vulnerable to identity theft.

The primary application for retinal pattern recognition till date has been for physical access entry for high-security facilities such as military installations, nuclear facilities, sophisticated laboratories, etc. It is also used in access control systems at high-security facilities. There are many advantages of retina biometry:- it has a low occurrence of false positives, also offer extremely low (almost 0%) error rates, since no two people have a same retinal pattern it is highly reliable and it can provide speedy results that are identity of a person can be verified very quickly.

**2. Problem Statement:**

Biometric Security has become more important because of the increasing activities of terrorism and hackers. Retina recognition technology is continuously growing over years, this technology can resolve Biometric security has become more important because of the increasing activities of terrorism the identification of a person’s identity, the main purpose of this project is to develop a retina based biometric recognition system for authenticating individual’s.

**3. An improvement over the Existing Implementation:**

**3.1. Present State and its drawbacks:**

1. Although there are some authentic systems based on different biometrics all of these can easily be forged.

2. However, several spoof attacks can also be carried against many types of biometrics, like fingerprint, face, and iris. Under spoof attacks replica of the genuine user’s fingers are created using some artificial material like silicon or wood glue, etc. to circumvent a system.

3. Sometimes the attackers use an artificial finger, a mask over a face or a contact lens on an eye.

4. As one’s signature may alter over a period and it is not as unique as Iris, Face, and Fingerprint.

5. In voice recognition, the main obstacle is speech features that are sensitive to background noise. Gait biometrics also may vary due to changes in body weights. It may not remain fixed for a long period of time, owing to major injuries involving leg or brain or due to inebriety.

**3.2. Advantages of the proposed system:**

1. Low occurrence of false positivies.

2. Extremely low (almost 0%) false negative rates.

3. Highly reliable because no two people have the same retinal pattern.

4. Speedy results:Identity of the subject is verified very quickly.

5. Security system are mainly used to authenticate a person. Hence our project can be used to authenticate a valid personal for process like bank transactions, personal security.

6. Biometric security system are the reliable source of security for highly sensitive area such as airport, military base etc.

**4. Scope of the project:**

The process of recognition mainly includes pre-processing, feature extraction and then features matching. The features generally used in this process are either blood vessel features or non-blood vessel feature.

**5. Tools and Technologies:**

**Software Requirements:**

Minimum software configuration in order to work with the proposed methodology is

Operating system : - Windows OS7

Front End : - MATLAB

TOOL : - MATLAB R2009

**Hardware Requirements:**

Minimum hardware configuration in order to work with the proposed methodology is

Hard Disk : 500 GB

RAM : 8 GB

CORE : i5

**6. Project Cost Estimation (Use COCOMO Model):**

For this project we apply basic cocomo model which has three categories:

1. Organic

2. Semi-detached

3. Embedded

Our project comes under the organic model which is the first level; **Basic COCOMO** can be used for quick and slightly rough calculations of Software Costs. Its accuracy is somewhat restricted due to the absence of sufficient factor considerations.

According to this,

**Estimation of Effort: Calculations –**

**1. Basic Model –**

**E= a (KLOC) b**

The above formula is used for the cost estimation of the basic **COCOMO** model, and also is used in the subsequent models. The constant values a and b for the Basic Model for the different categories of the system:

| **SOFTWARE PROJECTS** | **A** | **B** |
| --- | --- | --- |
| Organic | 2.4 | 1.05 |
| Semi Detached | 3.0 | 1.12 |
| Embedded | 3.6 | 1.20 |

The effort is measured in Person-Months and as evident from the formula is dependent on Kilo-Lines of code. These formulas are used as such in the Basic Model calculations, as not much consideration of different factors such as reliability, expertise is taken into account, henceforth the estimate is rough.

Our project roughly contains 2500 lines of code. Hence substituting the values in the above formula we get:

**E = 2.4 (2500)1.05**

**E = 8872.54**

**7. Reference:**

[1] Robust Vessel Segmentation in Fundus Images, A. Budai, R. Bock, A. Maier, J. Honegger, and G.Michelson. Hindawi Publishing Corporation International Journal of Biomedical Imaging Volume 2013, Article ID 154860, 11 pages <http://dx.doi.org/10.1155/2013/154860>

[2] A Combined Method to Detect Retinal Fundus Features V. Bevilacqua S. Cambo L. Cariello G. Mastronardi, Politecnico Di Bari (Italy)

[3] Retinal Verification Using a Feature Points-Based Biometric Pattern, M. Ortega, M. G. Penedo, J. Rouco, N. Barreira, and M. J. Carreira, Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2009, Article ID 235746, 13 pages DOI:10.1155/2009/235746.

[4] Alejandro F. Frangi, Wiro J.Niessen, et al. “Multiscale vessel enhancement filtering,” Medical Image Computing and computer-Assisted Intervention-MICCAI’98. 1998,1496:130:137.

[5] Digital image processing, third edition, Rafael C Gonzales and Richard E Woods.

[6] Retinal Fundus Biometric Analysis for Personal Identifications, Vitoantonio Bevilacqua, Lucia Cariello, Donatello Columbo, Domenico Daleno, Massimiliano Dellisanti Fabiano, Marco Giannini, Giuseppe Mastronardi, and Marcello Castellano, D.-S. Huang et al. (Eds.): ICIC 2008, LNAI 5227, pp. 1229–1237, 2008.

[7] Retinal Fundus Features Hybrid Detection based on a Genetic Algorithm, Vitoantonio Bevilacqua, Lucia Cariello, Simona Cambo, Domenico Daleno, Giuseppe Mastronardi, DEE Polytechnic of Bari, Via Orabona 4, 70125 Bari, Italy

[8] J. Daugman, “How iris recognition works,” *IEEE Trans. Circuits Syst.Video Technol.*, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[9] J. Daugman, “Probing the uniqueness and randomness of IrisCodes:Results from 200 billion iris pair comparisons,” *Proc. IEEE*, vol. 94,no. 11, pp. 1927–1935, Nov. 2006.

[10] *Unique Identification Authority of India*. [Online]. Available:http://uidai.gov.in, accessed Nov. 1, 2015.

[11] K. R. Nobel, “The state of the art in algorithms, fast identificationsolutions and forensic applications,” MorphoTrust USA,Billerica, MA, USA, Tech. Rep., Jan. 2013. [Online]. Available:http://www.planetbiometrics.com/article-details/i/1446/.

[12] P. E. Peterson *et al.*, “Latent prints: A perspective on the state of thescience,” *Forensic Sci. Commun.*, vol. 11, no. 4, pp. 1–9, 2009.

[13] C. Champod, “Edmond Locard—Numerical standards and ‘probable’ identifications,” *J. Forensic Identificat.*, vol. 45, no. 2, pp. 136–163,1995.

[14] K. McGinn, S. Tarin, and K. W. Bowyer, “Identity verification usingiris images: Performance of human examiners,” in *Proc. IEEE 6thInt. Conf. Biometrics, Theory, Appl., Syst. (BTAS)*, Sep./Oct. 2013,pp. 1–6.

[15] H. Proenca, “Iris recognition: On the segmentation of degraded imagesacquired in the visible wavelength,” *IEEE Trans. Pattern Anal. Mach.Intell.*, vol. 32, no. 8, pp. 1502–1516, Aug. 2010.

[16] H. Proenca, S. Filipe, R. Santos, J. Oliveira, and L. A. Alexandre, “TheUBIRIS.v2: A database of visible wavelength iris images captured onthe-move and at-a-distance,” *IEEE Trans. Pattern Anal. Mach. Intell.*,vol. 32, no. 8, pp. 1529–1535, Aug. 2010.

[17] Z. Sun, L. Wang, and T. Tan, “Ordinal feature selection for iris andpalmprint recognition,” *IEEE Trans. Image Process.*, vol. 23, no. 9,pp. 3922–3934, Sep. 2014.

[18] M. S. Sunder and A. Ross, “Iris image retrieval based onmacro-features,” in *Proc. 20th Int. Conf. Pattern Recognit.*, 2010,pp. 1318–1321.

[19] J. De Mira and J. Mayer, “Image feature extraction for applicationof biometric identification of iris—A morphological approach,”in *Proc. Brazilian Symp. Comput.Graph. Image Process.*, 2003,pp. 391–398.

[20] F. Shen, “A visually interpretable iris recognition system with crypt features,”Ph.D. dissertation, Dept. Comput. Sci. Eng., Univ. Notre Dame,Notre Dame, IN, USA, 2014.

[21] F. Shen and P. J. Flynn, “Using crypts as iris minutiae,” *Proc. SPIE*,vol. 8712, p. 87120B, May 2013.

[22] F. Shen and P. J. Flynn, “Iris matching by crypts and anti-crypts,” in*Proc. IEEE Conf. Technol. Homeland Secur.*, Nov. 2012, pp. 208–213.

[23] F. Shen and P. J. Flynn, “Are iris crypts useful in identity recognition?”in *Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl., Syst.*,Sep./Oct. 2013, pp. 1–6.

[24] F. Shen and P. J. Flynn, “Iris crypts: Multi-scale detection and shapebasedmatching,” in *Proc. IEEE Winter Conf. Appl. Comput. Vis.*,Mar. 2014, pp. 977–983.=

[25] J. Chen, C. W. Harvey, M. S. Alber, and D. Z. Chen, “A matchingmodel based on earth mover’s distance for tracking Myxococcusxanthus,”in *Proc. Med. Image Comput. Comput.-Assist. Intervent.*, 2014,pp. 113–120.

[26] J. Chen, F. Shen, D. Z. Chen, and P. J. Flynn, “Iris recognition based onhuman-interpretable features,” in *Proc. IEEE Int. Conf. Identity, Secur.Behavior Anal. (ISBA)*, Mar. 2015, pp. 1–6.

[27] P. J. Phillips, K. W. Bowyer, P. J. Flynn, X. Liu, and W. T. Scruggs, “Theiris challenge evaluation 2005,” in *Proc. 2nd IEEE Int. Conf. Biometrics,Theory, Appl., Syst.*, Sep./Oct. 2008, pp. 1–8.

[28] *CASIA Iris Image Database*. [Online]. Available: http://biometrics.idealtest.org/, accessed Nov. 14, 2015.

[29] Y. Rubner, C. Tomasi, and L. J. Guibas, “A metric for distributions withapplications to image databases,” in *Proc. IEEE 6th Int. Conf. Comput.Vis.*, Jan. 1998, pp. 59–66.