International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 4 Ver. I || April 2018 || PP 59-65

Degraded Ocular Image Recognition in Enrollment System

P.Sathiyapriya [1] , R.Vincy Rooth [2]
Asst.Professor/Department Of CSE
PG Scholar/Department Of CSE Sir Isaac Newton College Of Engineering And Technology
Nagapattinam, Tamil Nadu, India.
Corresponding auther: P.Sathiyapriya

Abstract: *Biometric Identification Is A Unique Factor For Each Individual, To Recognize Iris For Authentication Purpose. Biometrics Such As Signatures, Photographs, Fingerprints, Voiceprints And Retinal Blood Vessel Patterns All Have Noteworthy Drawbacks. Iris Recognition Is An Automated Method Of Biometric Identification That Uses Mathematical Pattern-Recognition Techniques On Images Of The Irises Of An Individual's Eyes, Whose Complex Random Patterns Are Unique. Work It Is Proposed To Implement An Iris Recognition System, Where HAAR And Curvlet Transform Is Used To Segment The Iris Region. A Template Of The Detected Region Is Created Using Template Matching For Recognition Is Based On Iris Features. The Results Shows That The Proposed Method Is Efficient For Iris Based Biometric Recognition.*

Keywords*—Biometric Authentication, Curvlet Transform, Degrade Ocular, Human Iris, HAAR Cascade*

Date of Submission: 24-03-2018 Date of acceptance: 09-04-2018

I. Introduction

Biometrics Refers To Metrics Related To Human Characteristics. Biometrics 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 Surveillance. Biometric Identifiers Are Then Distinctive, Measurable Characteristics Used To Label And Describe Individuals. Biometric Identifiers Are Often Categorized As Physiological Versus Behavioral Characteristics. Physiological Characteristics 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 And Odour/Scent. Behavioral Characteristics Are Related To The Pattern Of Behavior Of A Person, Including But Not Limited To Typing Rhythm, Gait, And Voice. Some Researchers Have Coined The Term Behavior-Metrics To Describe The Latter Class Of Biometrics. Fig 1 Shows The Block Diagram Illustrates The

Two Basic Modes Of A Biometric System. First, In Verification Mode The System Performs A One-To-One Comparison Of A Captured Biometric With A Specific Template Stored In A Biometric Database In Order To Verify The Individual Is The Person They Claim To Be.

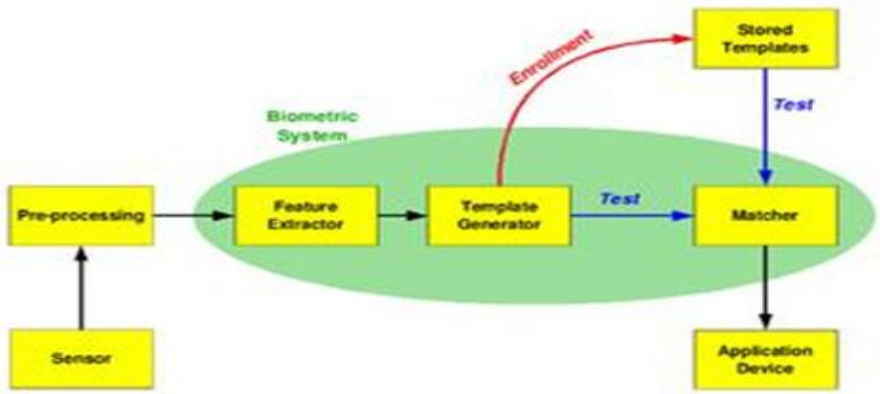

Fig 1: Block Diagram Of Biometric System

Three Steps Are Involved In The Verification Of A Person. In The First Step, Reference Models For All The Users Are Generated And Stored In The Model Database. In The Second Step, Some Samples Are Matched With Reference Models To Generate The Genuine And Impostor Scores And Calculate The Threshold. Third Step Is The Testing Step. This Process May Use A Smart Card, Username Or ID Number To Indicate

Which Template Should Be Used For Comparison. 'Positive Recognition' Is A Common Use Of The Verification Mode.

Second, In Identification Mode The System Perform A One-To-Many Comparison Against A Biometric Database In An Attempt To Establish The Identity Of An Unknown Individual. The System Will Succeed In Identifying The Individual If The Comparison Of The Biometric Sample To A Template In The Database Falls Within A Previously Set Threshold. Identification Mode Can Be Used Either For The Latter Function Can Only Be Achieved Through Biometrics Since Other Methods Of Personal Recognition Such As Passwords, Pins Or Keys Are Ineffective

The First Time An Individual Uses A Biometric System Is Called Enrollment. During The Enrollment, Biometric Information From An Individual Is Captured And Stored. In Subsequent Uses, Biometric Information Is Detected And Compared With The Information Stored At The Time Of Enrollment. Note That It Is Crucial That Storage And Retrieval Of Such Systems Themselves Be Secure If The Biometric System Is To Be Robust. The First Block Is The Interface Between The Real World And The System; It Has To Acquire All The Necessary Data. Most Of The Times It Is An Image Acquisition System, But It Can Change According To The Characteristics Desired Block Necessary Features Are Extracted. This Step Is An Important Step As The Correct Features Need To Be Extracted In The Optimal Way. A Vector Of Numbers Or An Image With Particular Properties Is Used To Create A Template. A Template Is A Synthesis Of The Relevant Characteristics Extracted From The Source. Elements Of The Biometric Measurement That Are Not Used In The Comparison Algorithm Are

Discarded In The Template To Reduce The File Size And To Protect The Identity Of The Enrollee.

During The Enrollment Phase, The Template Is Simply Stored Somewhere. During The Matching Phase, The Obtained Template Is Passed To A Matcher That Compares It With Other Existing Templates, Estimating The Distance Between Them Using Any Algorithm. The Matching Program Will Analyze The Template With The Input. This Will Then Be Output For Any Specified Use Or Purpose. Selection Of Biometrics In Any Practical Application Depending Upon The Characteristic Measurements And User Requirements. In Selecting A Particular Biometric, Factors To Consider Include, Performance, Social Acceptability, Ease Of Circumvention And/Or Spoofing, Robustness, Population Coverage, Size Of Equipment Needed And Identity Theft Deterrence. Selection Of A Biometric Based On User Requirements Considers Sensor And Device Availability, Computational Time And Reliability, Cost, Sensor Size And Power Consumption

1.1 Multimodal Biometric:

Multimodal Biometric Systems Use Multiple Sensors Or Biometrics To Overcome The Limitations Of Unimodal Biometric Systems. For Instance Iris Recognition Systems Can Be Compromised By Aging Irises And Finger Scanning Systems By Worn-Out Or Cut Fingerprints. While Unimodal Biometric Systems Are Limited By The Integrity Of Their Identifier, It Is Unlikely That Several Unimodal Systems Will Suffer From Identical Limitations. Multimodal Biometric Systems Can Obtain Sets Of Information From The Same Marker . Multimodal Biometric Systems Can Fuse These Unimodal Systems Sequentially, Simultaneously, A Combination Thereof, Or In Series, Which Refer To Sequential, Parallel, Hierarchical And Serial Integration Modes, Respectively. Fusion Of The Biometrics Information Can Occur At Different Stages Of A Recognition System. In Case Of Feature Level Fusion, The Data Itself Or The Features Extracted From Multiple Biometrics Are Fused. Matching-Score Level Fusion Consolidates The Scores Generated By Multiple Classifiers Pertaining To Different Modalities. Finally, In Case Of Decision Level Fusion The Final Results Of Multiple Classifiers Are Combined Via Techniques Such As Majority Voting. Feature Level Fusion Is Believed To Be More Effective Than The Other Levels Of Fusion Because The Feature Set Contains Richer Information About The Input Biometric Data Than The Matching Score Or The Output Decision Of A Classifier. Therefore, Fusion At The Feature Level Is Expected To Provide Better Recognition Results.

II. Related Work

Ajaykumar,Et.Al,…[1] Focuses On The Comparative Performance Evaluation From The Phase Encoding Of Iris Patterns Using Four Approaches; Haar Wavelet, Gabor Filter, Discrete Cosine Transform , And Fast Fourier Transform Based Feature Extraction. The Resulting Combination Of The Best Performing Approaches Is Used To Investigate The Further Performance Improvement. The Experimental Results Illustrated In This Paper Suggest That The Performance From The Haar Wavelet And Log Gabor Filter Based Phase Encoding Is The Most Promising Among All The Four Approaches Considered In This Work. Therefore The Simultaneously Extracted Matching Scores From These Two Matches Are Combined For Further Performance Improvement. The Difference In The Magnitude Of Adjacent Blocks Is Computed And A Binary Feature Vector Is Formed From The Zero Crossings Of Each Difference. The Size Of The Blocks Was Chosen To Be 8 × 12 With An Overlapping Of 4 Pixels In The Vertical Direction And 6 Pixels In The Horizontal

Direction. The Size Of The Resulting Feature Vector Was 8160 Bits And Hamming Distance Was Used To Measure The Difference Between The Feature Vectors. The Feature Extraction Using The Four Level Haar Wavelet Decomposition Of The Enhanced Image Was Firstly Investigated.

Yingzi Du, Et.Al,…[2] Proposed To Use Fourier-Based Trigonometry To Estimate The Two Spherical Components Of Angle Of Gaze And Used An Affine Transformation To ―Correct‖ The Image And Center The Gaze. Schuckers Et Al. Proposed Two Methods To Calculate Angle Of Gaze: Using Operator And Also An Angular Deformation Calibration Model. It Is Assumed That An Estimate Of The Degree Of Off-Angle Is Available For The Algorithms And Subjects Are Required To Place Their Heads On A Chin Rest Looking Front. Both Methods Are Limited Because ―The Affine Transformation Assumes The Iris Is Planar, Whereas In Fact It Has Some Curvature‖. Recently, We Proposed The Regional Scale Invariant Feature Transform Approach For Noncooperative Iris Recognition Which Works For Off-Angle Iris Images. Iris Features Are Described Without A Polar Or Affine Transformation And The Feature Point Descriptors Are Scale And Rotation Invariant. However, The Iris Region Consists Of Both Noise And Patterns, And Regional SIFT Describes The Area Around A Feature Point Using Gradient Information, Which Is Not Best Suited For Feature Extraction. Most Importantly, Regional SIFT Would Not Work Well With Local Pattern Deformation. If The Strengths Of SIFT And Gabor Wavelets Can Be Combined For Feature Extraction, It May Improve The Recognition Accuracy For Off-Angle Iris Images. A Simple Combination Of SIFT And Gabor Wavelet Method Would Not Work, And It Is Challenging To Design A Method That Can Take Advantage Of The SIFT And Gabor Wavelet. The SIFT Method May Select Many Feature Points In A Small Region. This Increases The Computational Complexity.

Ying Chen, Et.Al… [3] Proposed An Efficient Iris Recognition System Based On Optimal Sub Feature Selection Strategies And Sub Region Fusion Method. This Recognition System Is Composed Of Two Parts. The First Part Is Discriminative Sub Feature Selection Based On Finite-Delete-Sorting Multistage Strategy, And The Second One Is Fusion Sub Region Of Segmented Annular Iris Area. The Goal Of Discriminative Sub Feature Selection Is To Discard The Redundant SIFT Key Point's Feature; The Feature Selection Strategies Include (1) Feature Selection Based On Key Point's Orientation, (2) Feature Selection Based On Key Point's Neighborhood Magnitude, And (3) Compounded Feature Selection..Major Drawback Of Standard SIFT Technology. First Divide Segment Iris Annular Area Into Three Equally Sized Partitions In A Non Overlapping Way. Second ,Weighted Coefficients Of Sub-Region Are Obtained Via Training With Particle Swarm Optimization PSO Recognition Algorithm.

Tieniu Tan, Et.Al,…[4] Present A Novel Iris Segmentation Method, Aiming At Noisy Iris Images In Non-Cooperative Or Less-Cooperative Environments. In This Paper, We Have Presented An Efficient And Robust Algorithm For Noisy Iris Image Segmentation. Iris Recognition Contest. The Main Contributions Are Summarized As Follows. Firstly, A Novel Region Growing Scheme Is Proposed To Cluster The Whole Iris Image Into Different Parts. The Genuine Iris Region Is Then Extracted With The Assistance Of Several Semantic Priors, And The Non Iris Regions. Identified And Excluded As Well, Which Greatly Reduces The Possibility Of Mis Localizations On Non-Iris Regions? Secondly, Anintegro Differential Introduced To Accelerate The Traditional Integrodifferential Operator, And Meanwhile, Enhance Its Global Convergence Ability For Papillary And Limbic Boundary Localization. Thirdly, A Horizontal Rank Filter And An Eyelid Curvature Model Are Adopted To Tackle The Eyelashes And Shape Irregularity, Respectively, During Eyelid Localization. Finally, The Eyelash And Shadow Occlusions Are Detected Via A Learned Prediction Model Based On Intensity Statistics Between Different Iris Regions. Extensive Experiments On The Challenging UBIRIS Iris Image Database Shave Shown That The Proposed Method Achieves State-Of-The-Art Iris Segmentation Accuracy, And Therefore Can Be Well Adapted For Non-Cooperative Iris Recognition.

Chun-Wei Tan, Et A,… [5] Automated Iris Recognition Has Emerged As One Of The Most Promising Biometrics Technologies To Provide Reliable Human Identification. Almost All The Existing Commercial Iris Recognition Systems Acquire Iris Images Using Near Infrared Imaging Within Short Distance And Under Constrained Environment. In Other Words, Significant Cooperation Is Expected From The Users To Provide Their Eye Images While Staring At Imaging Devices Under Such Constrained Environment. Such Imaging Can Generally Achieve Remarkable Matching Accuracy As Iris Texture Is More Clearly Preserved In Such High Quality Iris Images Acquired Using NIR Imaging Under The Constrained Setup. The Superiority Of The Nirbased Iris Recognition Technologies Has Been Practically Engaged In Very Large Scale Applications, Such As In Aadhar Project To Identify Millions Of Citizens, Or In Border-Crossing Control System In UAE. Recent Advancement In The Iris Recognition Technologies Involves Acquisition Of The Iris Images At-A-Distance And Under Less Constrained Environments Using Visible Illumination Imaging. Such Systems Are Essentially Desirable In Meeting The Increasingly Demand For Forensic And High Security Surveillance Applications, For Example, In Providing Critical Early Warning Support To Thwart For Terrorism Related Threats.

Sirlantzis, Y Et.Al,…[6] Exposed We Distinguish Between Three Main Internet Banking Attack Vectors That Can Be Used Alone Or In Combination. Firstly, A Credential Stealing Attack Is Where Fraudsters

Try To Gather Users' Credentials, Either With The Use Of Malicious Software Or Through Phishing. Secondly, A Channel Breaking Attack, Involves Intercepting The Communication Between The Client Side And The Banking Server, By Masquerading As The Server To The Client And Vice Versa. Finally, A Content Manipulation. The Adversary Is Granted With Privileges To Read, Write, Change And Delete Browser's Data On The "Y", Whilst The Legitimate User Is Seamlessly Unaware. A Browser Root Kit, Is A Content Manipulation Technique, Which Is Capable Of Completely Changing The Browser's Display And Behavior. It Is Basically A Malicious Browser Extension, Which Are Used To Extend And/Or Customize The Browser's Functionality. To Control Unauthorized Installation Of Browser Extensions, Modern Browsers Like Firefox, Have Employed Numerous But Weak Security Measures, Which Can Be Easily Bypassed**.** Current Black-Hat Hackers' Software Requires Manual Intervention To Perform Fraudulent Transactions, Limiting The Damage That Can Be Caused.

Li, P Et.Al,….[7] Proposed One Proposal To Reduce Problems Related To Text Passwords Is To Use Password Managers. These Typically Require That Users Remember Only A Master Password. They Store And Send On Behalf Of The User The Appropriate Passwords To Web Sites Hosting User Accounts. Ideally The Latter Are Generated By The Manager Itself And Are Stronger Than User-Chosen Passwords. However, Implementations Of Password Managers Introduce Their Own Usability Issues That Can Exacerbate Security Problems, And Their Centralized Architecture Introduces A Single Point Of Failure And Attractive Target: Attacker Access To The Master Password Provides Control Over All Of The User's Managed Accounts. When Text Password Users Resort To Unsafe Coping Strategies, Such As Reusing Passwords Across Accounts To Help With Memo Ability, The Decrease In Security Cannot Be Addressed By Simply Strengthening, In Isolation, The Underlying Technical Security Of A System. Usability Issues Often Significantly Impact Its Real-World Security.

Roy, K Et.Al,… [8] Concludes In The Past Decade Our Community Has Recognized A Tension Between Security And Usability: It Is Generally Easy To Provide More Of One By Offering Less Of The Other. But The Situation Is Much More Complex Than Simply A Linear Trade-Off: We Seek To Capture The Multifaceted, Rather Than One-Dimensional, Nature Of Both Usability And Security In Our Benefits. We Further Suggest That "Deploy Ability", For Lack Of A Better Word, Is An Important Third Dimension That Deserves Consideration. Our Usability, Deploy Ability, Security Evaluation Framework And Process May Be Referred To As Semi-Structured Evaluation Of User Authentication Schemes. We Take Inspiration From Inspection Methods For Evaluating User Interface Design, Including Feature Inspections And Nielsen's Heuristic Analysis Based On Usability Principles.

Chan, K Et.Al,[9] Discussed Presents Bod Shapes, A Novel Authentication Method For Smart Phones That Uses The Back Of The Device For Input. We Argue That This Increases The Resistance To Shoulder Surfing While Remaining Reasonably Fast And Easy-To-Use. We Performed A User Comparing. Testing A Front Version Allowed Us To Directly Compare Performance And Security Measures Between Front And Back Authentication. Our Results Show Shapes Is Significantly More Secure Than The Three Other Approaches. While Performance Declined, Our Results Show That Bod Shapes Can Be Very Fast .That Learning Effects Have An Influence On Its Performance. This Indicates That Speed Improvements Can Be Expected In Long-Term Use.

Pereira, M Et.Al,…[10] Security Researchers Have, For Long, Devised Mechanisms To Prevent Adversaries From Conducting Automated Network Attacks, Such As Denial-Of-Service, Which Lead To Significant Wastage Of Resources. On The Other Hand, Several Attempts Have Been Made To Automatically Recognize Generic Images, Make Them Semantically Searchable By Content, Annotate Them, And Associate Them With Linguistic Indexes. In The Course Of These Attempts, The Limitations Of State-Of-The-Art Algorithms In Mimicking Human Vision Have Become Exposed. In This Paper, We Explore The Exploitation Of This Limitation For Potentially Preventing Automated Network Attacks. While Undistorted Natural Images Have Been Shown To Be Algorithmically Recognizable And Searchable By Content To Moderate Levels, Controlled Distortions Of Specific Type And Strength Can Potentially Make Machine Recognition Harder Without Affecting Human Recognition. This Difference In Recognizability Makes It A Promising Candidate For Automated Turing Tests Called Captchas Which Can Differentiate Humans From Machines. We Empirically Study The Application Of Controlled Distortions Of Varying Nature And Strength, And Their Effect On Human And Machine Recognizability.

III. Existing Methodologies

Security Of Data Is Very Important Issue Because Many A Time's Security Lacks In Encryption And Decryption That Way. Use Power Full Techniques Of Visual Cryptography And Provide A Biometric Authentication .Biometric Is A Method Of Identifying The Identity Of Person Based On Physiological Or Behavioral Characteristics'. Many Biometric Technique Are Available Such As Facial, Iris ,Hand, Palm,Voice And Signature Among Those Iris Recognition Is One Of The Most Powerful And Unique

3.1 Texture-Analysis Based

Existing System Proposed Iris Recognition Based On Texture Analysis. High Quality Iris Image Was Captured Using Silicon Intensified Target Camera Coupled With A Standard Frame Grabber And Resolution Of 512*480pixels.

3.2 Zero-Crossing Representation

Zero Cross Represents Features Of The Iris At Different Resolution Levels Based On The Wavelet Transform Zero-Crossing.The Algorithm Is Translation, Rotation And Scale Invariant. Input Images Are Processed To Obtain A Set Of ID Signals And Its Zero Crossing Representation Based On Its Dyadic Wavelet Transform.

3.3 Approach Based On Intensity Variations

Intensity Variations Feature Values Are The Mean And The Average Absolute Deviation Of The Magnitude Of Each 8x8 Block In The Filtered Image With The Total Number Of Blocks Being 768. For Dimensionality Reduction, Fisher Linear Discriminate Is Used And For Classification, Nearest Center Classifier Is Used. The Similarity Between The Pair Of Feature Vectors Is Calculated Using The XOR Operation. The Circular Shift-Based Matching Is Performed From Which The Minimum Matching Score Is Considered After Several Circular Shifts.

IV. Proposed Methodology

Biometrics Recognition Is A Common And Reliable Way To Authenticate The Identity Of A Living Person Based On Physiological Or Behavioral Characteristics. It Contains Unique Texture And Is Complex Enough To Be Used As A Biometrics Signature. Compared With Other Biometrics Features Such As Face And Fingerprint, Iris Is A Thin Membrane On The Interior Of The Eyeball. It Is More Stable And Reliable, Imitation Is Almost Impossible. The Iris Is Unique To People And Patterns Of Iris Are Formed By Six Months After Birth, Stable After A Year. They Remain The Same For Life. Furthermore, Iris Recognition Systems Can Be Non-Invasive To Their Users. The Security Has Become A Main Problem Of Concern Among The People. Biometrics Is Robotic Method Of Identifying A Person Based On Physiological Or Behavioral Uniqueness. Threat Starts While A Useless Person Tries To Obtain Access. A Person Verification System Localizes Facial Landmarks And Extracts Biometrical Features For Face Authentication. This Includes Image Acquirement, Segmentation, Normalization, Pattern Generation And Matching. Automatic Iris Recognition System Is Reliable For Automatic Personal Identification. This Research Aims To Recognize And Identify Iris Among Many That Were Stored In Database. It Is Includes, After Entered Iris Image, Image Preprocessing, Feature Extraction Based On Texture Analysis Using Haar Wavelet Transform To Capture Both Local And Global Features Details In An Iris And Iris Identification (Matching Process) Based On The Distance Between The New Input Iris And Templates Stored In The Database Then Choose The Minimum Distance Between Them. So The Score Degree Can Determine The Genuine Or Imposter Person. The Database Can Display Information About Any Processed Iris. The Study Conclusion That Haar Wavelet Transform Was Efficient Distinguished And Noise Sensitive Under Different Conditions. The Basic Cascade Creation Algorithm As Follows:

4.1Algorithm HAAR CASCADE CLASSIFIER

Input: Face Features, Iris Features
Output: IRIS Boundaries
$F_0 = 1$
I=0
While $F_i > T_{arget}$ And I<Stages
I=I=1
Train Classifier For Stage I
Initialize The Weights
Normalize The Weights
Pick The (Next) Best Weak Classifier
Update Weights
Evaluate F_i
If $F_i > F$
Go Back From Normalize The Weights. Combine Weak Classifiers To Form The Strong Stage Classifier
Evaluate F_i

4.2 Iris Image Acquisition

In This Module, Image Of Iris Is First Acquired With The Help Of Web Camera. The Human Iris Image Is Captured Using An Infrared Camera Which Is Fixed Without A Laser Scan System To Get A High Quality Picture From System. There Are Several Metrics Of The Infrared Illuminated Image With Visible

Ranges: Iris Ridges, Nerves, And Crypts Are Being More Evident Here; The Edges And Boundaries Of The Iris Image In Between The Iris And The Pupil More Dealt And Image Is Being Stored In Database To Process The Dataset.

4.3 Iris Feature Extration

Preprocessing Step Is Done To Reduce The Noise Present In The Image. Hence The Correct Lens Aberrations Of The Image Are Processed By Enhancing The Image And Accomplishing He Similar Task For The Authentication Of The Iris Recognition System. The Original Image Interrupted By Median Filter To Remove The Noise In The Image And Histogram Equalization Process Is Held To Get A Perfect Image For Processing The Further Mathematical Patterns Of Technique.

4.4 Enrollment In Database

Iris Features Are Stored In Database. We Can Store Iris For Improved Authentication. Then We Stored These Features Numerical Values Instead Of Templates. These Featured Are Saved Along With Registered Details Such As Name, Id, Phone Number, Email And So On.

4.5 Authentication

User Can Enter Into The System Using User Name And Password. After That Sensing Eyes Of Same Person With Sub Sequence Press. Eye Features Are Required To Check Whether The Input Image Is Same As That Stored In The Database. If The Curvlet Transform Space Is Maximum Of The Iris Region Than The Threshold Hence No Border Is Fit Into The Region Corresponding To The No Occluding Eyelid Region Which Is Isolated. The Line Are Restricted Both In Exterior And Interior Region Of Pupil. Hence The Thresholding To The Pixels Is Done To Isolate The Eyelashes And Eyelid To Get The Required Part Of The Eye Image To Detect The Perfect Iris. The Steps That Are Taken To Detect The Boundary Of The Iris Are As Follows: The Boundary Is Extracted By Applying The Canny Edge Detected Method. The Curvlet Transform Is Being Applied To Detect The Perfect Hough Circle Of The Iris Image. The Eyelashes And Eyelids Are Being Isolated To Get The Perfect Intermediate Iris Image From The Eye Image Database That Is Being Selected.

4.6 Feature Matching

Feature Matching Phase Identifies Similarities Between Current IRIS Features And Previously Stored Features. Input Images Provided To The System Are Matched With Previously Stored Features Present In Database. Matching Is Entirely Dependent On Whether The System Performs Identification Or Verification. Performs Identification I.E. One-To-Many Matching Approach Is Used, Where IRIS Of An Individual Matches With All Available Templates In Database Otherwise One-To-One Match Is Done For Verification, Where Input Image Of A Person Is Matched With Iris Features.. Works Basically Like This: The Input Pattern On Which The Network Is To Be Trained Is Presented At The Input Layer Of The Net And The Net Is Run Normally To See What Output It Actually Does Produce. The Actual Output Is Compared To The Desired Output For That Input Pattern. The Differences Between Actual And Desired Form An Error Pattern. Extract The Features For Both Fingers At Testing Side. These Features Are Matched With Data Base Using Classification Approach. If There Is Match Found Means, User Can Be Register Into System, Otherwise Rejected.

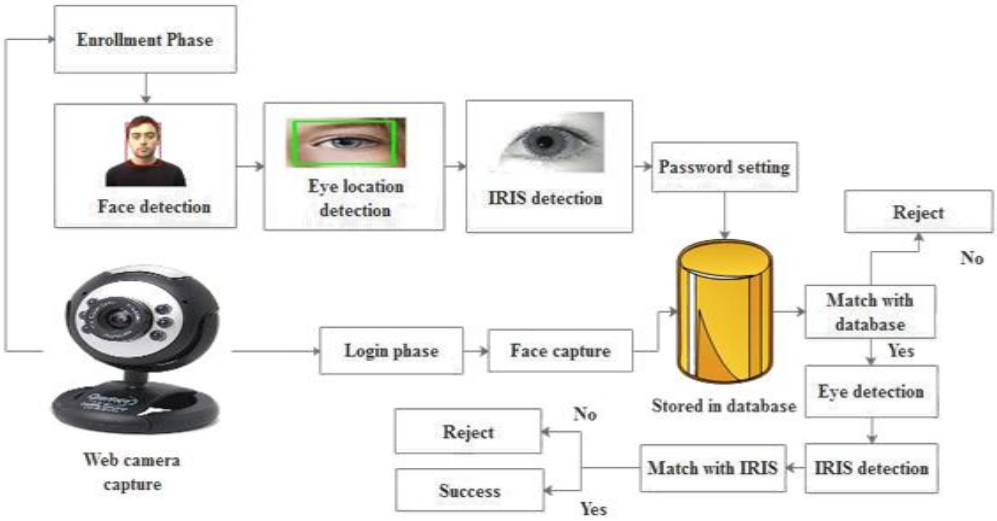

Fig 2: System Architecture

V. Conclusion

Iris Detection For Authentication Using Eye Ball. Biometric Systems Are Commonly Used To Organize Accessing Of Physical Assets Such As Laboratories, Buildings, Cash From Atms, Etc., Or Logical Information Such As Personal Computer Accounts, Secure Electronic Documents, Etc. The Human Biometrics Like Fingerprint, Hand Geometry, Face, Retina, Iris, DNA, Signature And Voice Can Be Effectively Used To Ensure The Network Security. In Biometric Cryptosystems, A Cryptographic Key Is Obtained From The Biometric Template Of A User Stored In The Database In Such A Way That The Key Cannot Be Revealed Without A Successful Biometric Authentication. A Proposal Algorithm For Iris Recognition Has Been Presented. Curve Let Transform Is Useful For Segmentation Of The Iris Because Of Efficient Localization. The HAAR Features Has A Number Of Advantages, It Is Conceptually Simple, Fast, Memory Efficient. In This System, The Concept In The Areas Of Image Processing Technique Is Reused To Extract The Minutiae From Iris Biometric Image. The Preprocessing Techniques Projected In This Project Play An Important Role In Improving The Performance Of The Proposed Biometric Based Network Security System. The Performance Measures Obtained Exposed That The Proposed Method Effectively Provides Network Security. Therefore It Can Be Directly Applied To Strengthen Existing Standard Single-Server Biometric Based Security Applications.

References

[1] A. Kumar And A. Passi, "Comparison And Combination Of Iris Matchers For Reliable Personal Authentication," Pattern Recognition., Vol. 43, Pp. 1016–1026, 2010.

[2] Y. Du, C. Belcher, And Z. Zhou, "Scale Invariant Gab Or Descriptor-Based Noncooperative Iris Recognition," EURASIP J. Adv. Signal Process., Vol. 2010, Pp.1– 13, 2010

[3] Y. Chen, Y. Liu, X. Zhu, F. He, H. Wang, And N. Deng, "Efficient Iris Recognition Based On Optimal Sub Feature Selection And Weighted Sub Region Fusion," Scientific World J., Vol. 2014, Pp. 1–19, 2014.

[4] T. Tan, Z. He, And Z. Sun, "Efficient And Robust Segmentation Of Noisy Iris Images For Non-Cooperative Iris Recognition," Image Vision Compute., Vol. 28, Pp. 223–230, 2010

[5] C. Tan And A. Kumar, "Efficient And Accurate At-A-Distance Iris Recognition Using Geometric Key-Based Iris Encoding," IEEE Trans. Inf. Forensics Security, Vol. 9, Pp.1518–1526, 2014.

[6] Y. Hu, K. Sirlantzis, And G. Howells, "Exploiting Stable And Discriminability Iris Weight Map For Iris Recognition Under Less Constrained Environment," Accepted By IEEE Int. Conf. Biometrics: Theory, Applications And Systems, 2015.

[7] P. Li And G. Wu, "Iris Recognition Using Ordinal Encoding Of Logeuclidean Covariance Matrices," IEEE Int. Conf. Pattern Recognition, Pp. 2420–2423, 2012.

[8] K. Roy And P. Bhattacharya, "Optimal Features Subset Selection And Classification For Iris Recognition," J. Image And Video Processing, Vol. 2008, 2008.

[9] M. Pereira And A. Veiga, "Application Of Genetic Algorithms To Improve The Reliability Of An Iris Recognition System," IEEE Workshop Machine Learning For Signal Processing, 2005.

[10] K. Chen, C. Chou, S. Shih, W. Chen, And D. Chen, "Feature Selection For Iris Recognition With Ad Boost," Int. Conf. Intelligent Information Hiding And Multimedia Signal Processing, 2007.

P.Sathiyapriya "Degraded Ocular Image Recognition In Enrollment System"International Journal of Engineering Science Invention (IJESI), vol. 07, no. 04, 2018, pp 59-65