

## Enhancing Iris Security by Detection of Fake Iris

Vijay Kumar Sinha<sup>1</sup>, Dr. Anuj Gupta<sup>2</sup>

### Abstract

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on still / video images of the irises of an individual's eyes, whose complex random patterns are unique and can be seen and recognized from some distance. Now days, Iris is being used widely by several organizations, including governments, for identification and authentication purposes. Aadhar, India's UID project uses Iris scan along with fingerprints to uniquely identify people and allocate a Unique Identification Number.

Most of the work done in the area of Iris pattern recognition systems emphasizes only on matching of the patterns with the stored templates. Security aspects of the system are still unexplored. The available security algorithms provide only some cryptographic solutions that keep the template database in a secret cryptographic form. Some recent works on fake Iris detection has done but they still lacking of efficiently detect whether an iris is really of a live person or it is just an scanned image or iris of a unconscious or dead person.

We successfully worked on these security issues of present iris recognition system and enhanced the detection capabilities of fake iris images .We use motion detection algorithm for detection of natural eye movement and flash reflection detection algorithm to detect and This enhanced significantly the performance of the system in terms of security and reliability. We use Flash and motion detection of natural eye. We successfully attained 99.98% accuracy at 5.2% threshold value at 10.5 cm distance from the Iris scanner.

Iris acknowledgment is a computerized strategy for biometric distinguishing proof that uses numerical example acknowledgment procedures on video pictures of the irises of a singular's eyes, whose perplexing irregular examples are novel and can be seen from some separation. Presently days, Iris is being utilized generally by a few associations, including governments, for recognizable proof and verification purposes. Aadhar, India's UID task utilizes Iris filter alongside fingerprints to extraordinarily recognize individuals and apportion a Unique Identification Number.

The greater part of the work done in the region of Iris example acknowledgment frameworks stresses just on coordinating of the examples with the put away layouts. Security parts of the framework are still unexplored. The accessible security calculations give just some cryptographic arrangements that keeps the format database in a mystery cryptographic structure.

We effectively improved the discovery of fake iris pictures and include the procurement of identification of false of examined iris pictures as format. This improved fundamentally the execution of the framework as far as security and unwavering quality. We utilize movement location of normal eye within the sclera part of eye which is not seen in the fake iris images. We effectively achieved 98.87% exactness at 6.3% limit esteem at 10.5 cm separation from the Iris scanner.

## 1. INTRODUCTION

In today's general public, security is a noteworthy concern and is turning out to be progressively vital. Cryptography has ended up a standout amongst the best ways and has been perceived as the most mainstream innovation for security purposes. History demonstrates that people can recall just short passwords; most clients even have a tendency to pick secret word that can be effectively speculated utilizing lexicon or animal power systems. This confinement has set off the utilization of biometrics to create solid cryptographic key[1]. Biometrics is interesting to every person and it is solid. For a considerable length of time, information/individual security in the business world has been generally taking into account passwords, PINs, or a security question, for example, mother's last name by birth or singular's date of conception and so on. This security/ID highlight is effectively overlooked, stolen, shared or split. Biometrics is an estimation of the human body natural or physical qualities to decide the human character[2]. There are diverse sorts of biometric advances accessible today which incorporate fingerprints, face, iris/retina, hand geometry, signature, DNA, keystroke and tongue and so forth. Biometrics offered an inseparable connection from the authenticator to its proprietor, which can't be overcome by passwords or tokens, since it can't be loaned or stolen. Biometrics is utilized to improve the protection and security shortcomings that exist in the present security innovation, for example, straightforward watchword or PIN validation. Another favorable position of biometrics is that it can distinguish and keep different IDs[3]. Despite the fact that biometrics is one of a kind among all people, it is unrealistic to utilize biometrics as an immediate cryptography key for the framework because of the distinction bits that happen in the format amid each verification[4]. At the end of the day, every time the filtered biometric picture varies in minor extent. Biometric pictures or layouts are variable by nature which implies each new biometric test is constantly distinctive. Clamors and blunders may happen in the caught picture because of burst or foundation mistake and subsequently the produced format is diverse amid each confirmation[5]. There is additionally mindfulness concerning the protection and the security of individual data because of the stockpiling of the biometric layouts. The misfortune or trade off of biometric layouts may wind up in unusable biometric. Iris acknowledgment biometric frameworks apply scientific example acknowledgment procedures to pictures of the irises of a singular's eyes[6].

## 2. THE PRINCIPLE

The structure of the human eye is appeared in Fig 1. Iris is the external dull segment (chestnut, dark, blue or green) encompassing the focal part called the understudy behind which lies the lens. The white segment (called sclera) encompasses the iris[7].

Fig. 2 demonstrates the point of interest of the iris (alongside focal understudy). The examples of the iris are unmistakably obvious in Fig 2. These examples are special in each human and are additionally exceptional in every eye i.e. left and right eye of the same person. These novel examples of the individual's eyes can be utilized to recognize the individual[8].

In iris acknowledgment framework a singular's eyes are filtered by a high determination scanner (Fig. 3) and after that these pictures are handled by the PC to make secure and dependable advanced formats and put away in the information base[9].

For confirmation, the pictures of the objective individual's iris are contrasted and the formats put away in the databank. In the event that the match happens, the check procedure is fruitful generally not[10].

## 2. LITERATURE SURVEY :

It has been long realized that our iris examples (like retina examples and fingerprints) are one of a kind and these can be utilized for individual recognizable proof[11]. Notwithstanding, this could be misused just in late 1980s when fitting innovation was accessible for executing such a framework[12]. The beginning of a dependable iris acknowledgment framework can be followed to 1987 when two ophthalmology educators , Leonard Flom (MD, New York University) and AranSafir (MD, University of Connecticut) were issued a first of its kind wide patent # 4,641,349 entitled " Iris Recognition Technology"[13]. Along these lines, Dr John Daugman (Harvard Computer Science workforce) was asked by the two eye specialists to compose a calculation for their idea based upon a broad arrangement of high determination iris photographs supplied to him by Dr. Flom from his volunteer private patients[14]. Quite a long while later, Daugman got a technique patent for the calculation[15]. The three people then established "Iridian Technologies Inc." for further adding to the idea[16]. This strategy in view of Daugman calculation was authorized to a few partnerships for commercializing the framework [17].

Upon the termination of the Flom/Safir patent in 2008, different calculations were protected; some of them were better than Daugman's. Some of these are as a rule further created/ marketed by US Govt. organizations [18].

On account of Daugman calculation, a Gabor wavelet change [19] is utilized on the pixels of the human iris. This outcomes in a progression of complex numbers which convey the adequacy and stage data about the iris design[20]. Most abundancy data is disposed of[21]. This guarantees the layout remains to a great extent unaffected by changes in enlightenment or camera pick up and adds to the long haul ease of use of the biometric format. This format can then used to look at the sweeps of the iris from diverse persons for recognizable proof[22].

From that point forward, a ton of innovative work has been done in this field[23]. The anxiety has been on security and distinguishing proof of the iris picture when contrasted and the put away layout. Utilization of Error Correcting Codes (ECC) has been utilized to sift through clamors and mistakes which may happen in the caught pictures because of burst or foundation blunders which can creep-in in each new iris filter. Sim HieuMoi et al [24] have utilized Error Correcting Codes to dispense with these commotions and burst blunders in the distinguishing proof of the iris filters. They have utilized two distinctive separation metric capacities in the format coordinating procedure.

The Chinese Academy of Sciences (CASIA) have built up an Iris Database (form 1.0) of 756 iris tests taken from 108 persons ( with seven unique pictures for every individual) These pictures are 8-bit dark level JPEG documents [25]. Iris formats are made by iris division, standardization and highlight extraction procedure to deliver the iris twofold code which is then encoded utilizing Reed Solomon Code. This RS Code is then encoded utilizing a secret word to frame a Cipher content which is then put away in the database as a format. (Fig. 4) With the utilization of division and propelled elements of cryptography, the system gives higher unwavering quality and security in Iris acknowledgment. (Fig. 5)

Gaganpreet et al [26] have proposed an improved iris acknowledgment technique which overcomes issues like reducing so as to expand the rate the multifaceted nature of the system. For the most part, three stages are taken after while working with the iris acknowledgment framework viz pre-preparing, highlight extraction and acknowledgment stage. This paper introduces a robotized and novel iris acknowledgment framework where general computational match velocity is lessened while as yet having a precision of 99.38 % and low FAR.

IfeanyiUgbagaNKole et al [27] have proposed another technique for division of the iris picture by utilizing 8-neighborhood administrators. This picture is then bolstered into a circle Hough Transform to upgrade iris division which is the most challenged issue in the iris acknowledgment framework. For this examination 320 iris pictures from CASIA standard dataset were utilized. The dispatch demonstrates a higher exactness rate.

P. Lorrentz et al [13] have explored how human distinguishing proof and personality confirmation can be performed by the use of FPAG based weightless neural system to the iris biometric methodology. The human iris is handled for highlight vectors which are utilized for arrangement of availability amid learning and resulting acknowledgment.

Nithyanaudam.S et al [14] utilize a Canny Edge Detection Scheme and a Circular Hough Transform to recognize iris limits in the eye's advanced picture.

In any case, to the best of our insight, the utilization of Flash location (of normal eyes) and utilization of double iris rather than a solitary iris (i.e. whether the specific iris picture is from the left or right side eye of the individual) have not been utilized till now for location/confirmation of the individual under thought.

#### **4. PROPOSED WORK:**

For template making, the high resolution scanned images of the iris are processed by various computer subroutines.

First, an iris recognition algorithm (subroutine) is used to localize the inner and outer boundaries of the iris. Parts of eyelids, eye lashes and specular reflections which often occlude parts of the iris are detected and excluded from the images scanned.

The set of pixels containing only the iris are then normalized to compensate for pupil dilation or constriction. The information stored in each pixel is then encoded to obtain a set of complex numbers that carry the amplitude and phase information about iris patterns. The amplitude information thus stored may be discarded to ensure that the template remains largely unaffected by changes in illumination or camera gain (contrast). This contributes to the long term usability of the biometric template.

Various transformations and encoding techniques are used in this process of template making to ensure security and longevity of the template [1].

For format making, the high determination filtered pictures of the iris are handled by different PC subroutines.

Initial, an iris acknowledgment calculation (subroutine) is utilized to restrict the internal and external limits of the iris. Parts of eyelids, eye lashes and secular reflections which frequently block parts of the iris are distinguished and avoided from the pictures filtered.

The arrangement of pixels containing just the iris is then standardized to make up for student expansion or tightening. The data put away in every pixel is then encoded to get an arrangement of complex numbers that convey the plentifulness and stage data about iris designs. The sufficiency data subsequently put away may be disposed of to guarantee that the format remains generally unaffected by changes in enlightenment or camera addition (contrast). This adds to the long haul ease of use of the biometric layout.

Different changes and encoding systems are utilized as a part of this procedure of format making to guarantee security and life span of the layout [1].

#### **5. PROCESS OF IDENTIFICATION / VERIFICATION:**

For identification (one to many template matching) or verification (one to one template matching), a template created by imaging an iris is compared with stored template(s) in a database.

In this process, the steps in template making are repeated and this digital image (template of the person to be identified / verified) is then compared with the stored template in the database. Various criterions may be employed for comparison purposes. In one commonly used method, if the Hamming distance is below the decision threshold, a positive identification is made. [2] Like everything else, this system has advantages and drawbacks.

## 6. ADVANTAGES OF IRIS IDENTIFICATION / VERIFICATION:

The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons:

It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labor.

The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae) that control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face.

The iris has a fine texture that—like fingerprints—is determined randomly during embryonic gestation. Like the fingerprints, it is very hard (if not impossible) to prove that the iris is unique. However, there are so many factors that go into the formation of these textures (the iris and fingerprint) that the chance of false matches for either is extremely low. Even genetically identical individuals have completely independent iris textures.

An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the person being identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures against fingerprint scanners, where a finger has to touch a surface, or retinal scanning, where the eye must be brought very close to an eyepiece (like looking into a microscope).

The commercially deployed iris-recognition algorithm, John Daugman's Iris Code, has an unprecedented false match rate (better than  $10^{-11}$  if a Hamming distance threshold of 0.26 is used, meaning that up to 26% of the bits in two Iris Codes are allowed to disagree due to imaging noise, reflections, etc., while still declaring them to be a match). [ 3]

While there are some medical and surgical procedures that can affect the colour and overall shape of the iris, the fine texture remains remarkably stable over many decades. Some iris identifications have succeeded over a period of about 30 years.

## 7. PROBLEM STATEMENT:

Many commercial Iris scanners can be easily fooled by a high quality image of an iris or face in place of the real thing.

The scanners are often tough to adjust and can become bothersome for multiple people of different heights to use in succession.

The accuracy of scanners can be affected by changes in lighting.

Iris scanners are significantly more expensive than some other forms of biometrics, password or proxy card security systems.

Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made into fingerprint recognition.

Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera. However, several academic institutions and biometric vendors are developing products that claim to be able to identify subjects at distances of up to 10 meters ("standoff iris" or "iris at a distance" as well as "iris on the move" for persons walking at speeds up to 1 meter/sec). [4]

As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates.

As with other identification infrastructure (national residents databases, ID cards, etc.), civil rights activists have voiced concerns that iris-recognition technology might help governments to track individuals beyond their will. As with most other biometric identification technology, a still not satisfactorily solved problem with iris recognition is the problem of live-tissue verification. The reliability of any biometric identification depends on ensuring that the signal acquired and compared has actually been recorded from a live body part of the person to be identified and is not a manufactured template. Many commercially available iris-recognition systems are easily fooled by presenting a high-quality photograph of a face instead of a real face, which makes such devices unsuitable for unsupervised applications, such as door access-control systems. The problem of live-tissue verification is less of a concern in supervised applications (e.g., immigration control), where a human operator supervises the process of taking the picture.

Methods that have been suggested to provide some defense against the use of fake eyes and irises. These include:

Changing ambient lighting during the identification (switching on a bright lamp), such that the pupillary reflex can be verified and the iris image be recorded at several different pupil diameters.

Analyzing the 2D spatial frequency spectrum of the iris image for the peaks caused by the printer dither patterns found on commercially available fake-iris contact lenses.

Analyzing the temporal frequency spectrum of the image for the peaks caused by computer displays.

Using spectral analysis instead of merely monochromatic cameras to distinguish iris tissue from other material.

Observing the characteristic natural movement of an eyeball, measuring nystagmus (voluntary or involuntary eye movement) tracking eye while text is read, etc [5].

Testing for retinal retro reflection (red-eye effect).

Testing for reflections from the eye's four optical surfaces (front and back of both cornea and lens) to verify their presence, position and shape.

Using 3D imaging (e.g., stereo cameras) to verify the position and shape of the iris relative to other eye features.

## **9. PROPOSED RESEARCH WORK:**

The present research is made to improve the reliability and security of the iris detection

System by detect and distinguish fake scanned iris images with real human iris images. As Iris scanners can be made fool by presenting a scanned high resolution scanned iris image to make scams.

### **9.1 OBJECTIVES OF RESEARCH:**

The main aim & objectives of current research work are to enhance the security and intelligence of existing Iris recognition system which includes following objectives:

To study the existing available iris recognition system.

To improve the security level of existing iris recognition system by taking both iris together.

To test and evaluate the proposed system for efficiency with existing techniques.

#### **9.1.1 Research Methodology & Tools:**

We used MATLAB for result analysis and algorithm implementations. Statistical tools are used for data analysis.

#### **9.1.2 Iris Enrolment Process (Template making):**

Following steps will be used in template making.

Take images of both the irises of the volunteers at five different angles viz.  
in the frontal normal position.

at 45° angle (Left and Right)in the horizontal plane.

at 45° angle( Up and Down) in the vertical plane .

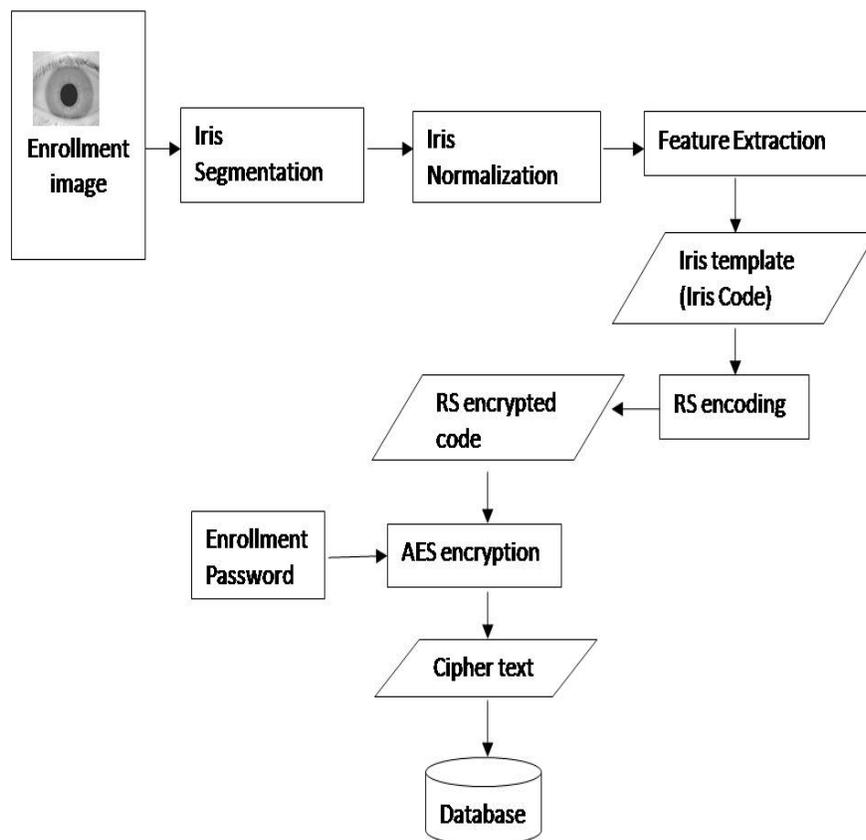
The enrollment steps are described below [15] :

**Step1:**Iris extracted through iris Segmentation by using thresholding [16], Iris Normalization by using normalization algorithms [17]and Feature Extraction process by RGB (Colour) to Grey conversion , Thinning, Smoothing, etc. to generate the iristemplate andto produce the iris binary code.[18].**Step2:**Thebinary code for the iris image will then undergo the Reed Solomon Code Encoding Process i.e. Grey to binary conversion [19].

**Step3:**The RS Code is then encrypted with the enrolment password using Advanced Encryption Standard Cryptography Algorithm to generate a cipher text.[20]

**Step 4:** The generated cipher text is then stored in the database as a template.

The final extracted Iris pattern templates are encrypted by using AES encryption algorithm.



**Fig. 4 The Iris Enrollment Process**

### 9.1.1 Research Methodology & Tools:

We used MATLAB for result analysis and algorithm implementations. Statistical tools are used for data analysis. Distance metrics is used to calculate the Iris distance within the sclera.

### 9.1.2 Iris Movement Detection Algorithm:

Following steps will be used in Iris natural movement detection process.

Take images of both the irises of the volunteers at five different angles viz.  
 in the frontal normal position.

at 45° angle (Left and Right)in the horizontal plane.

at 45° angle( Up and Down) in the vertical plane .

The enrollment steps are described below :

## **Iris Flash& Movement Detection Algorithm**

### **Start Iris movement detection**

#### **Step 1: Capture the both Iris Images**

**Step 2: Turn head at 45° angle left then capture the Iris image including the whole eye area .**

Step 3 : Turn head at 45° angle right direction then capture the iris image including whole eye area

Step 4 : Turn the head down at 45° angle down and capture the iris position for the both in the eye.

Step 5 : Turn the head upward at 45° angle and then capture the iris position for the both eye .

Step 6: Compare the iris position in the sclera.

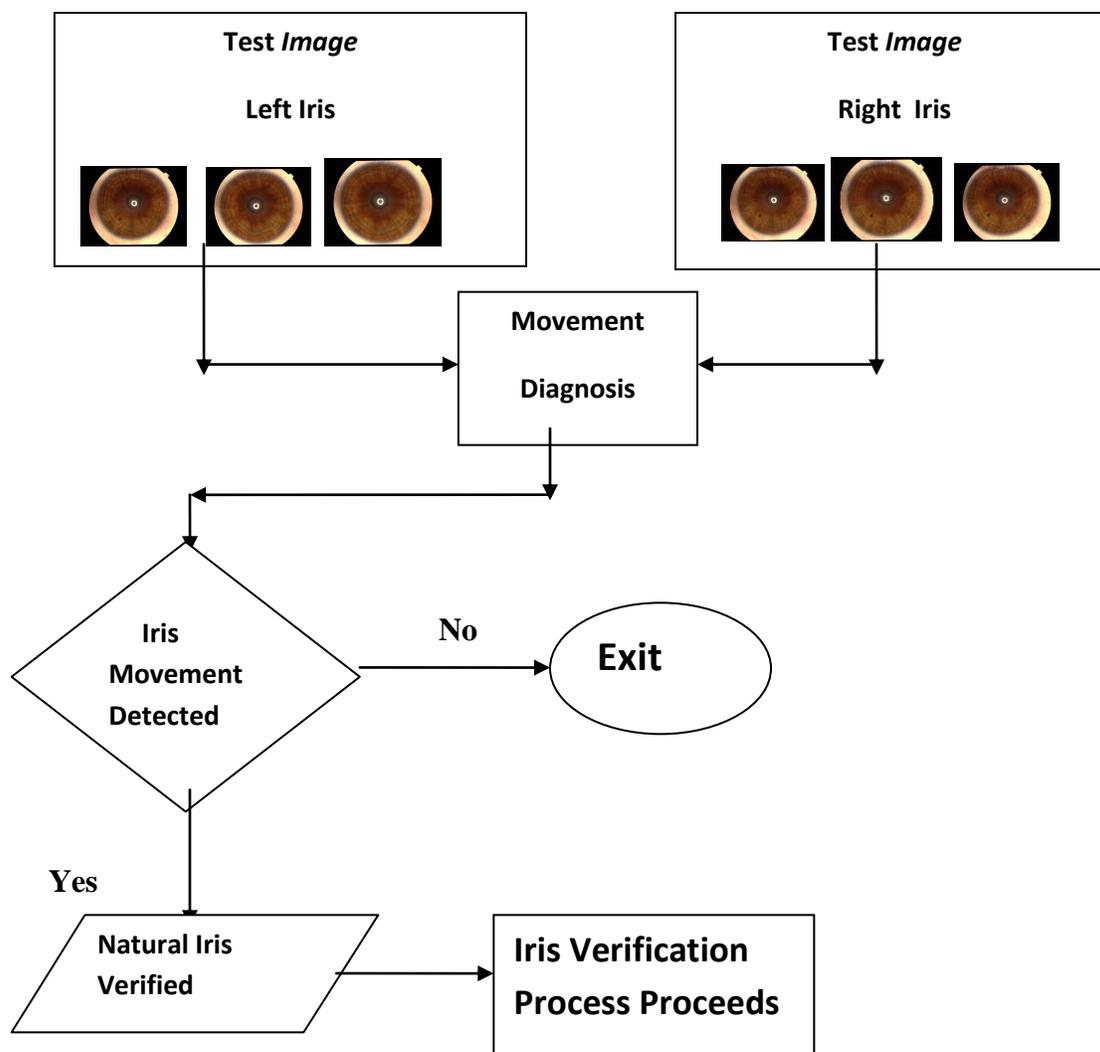
Step 7: Calculate the iris distance from the sclera for both iris

Step 8: calculate the direction of movement for both the iris

Step 9 : Is iris is moving with sclera if no then declare fake iris and exit else go to step 10

Step 10 : Is the both iris moving in the same direction if yes then declare real human and proceed for template matching process else declare fake and exit

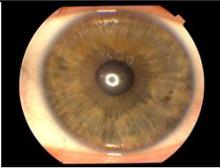
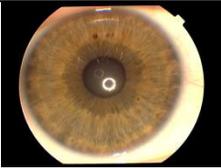
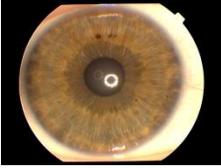
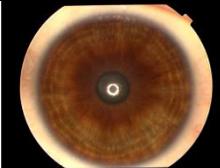
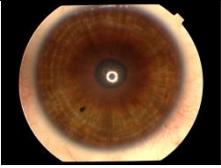
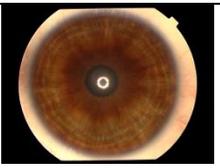
Step 11: End movement detection

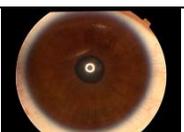
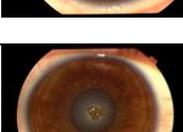
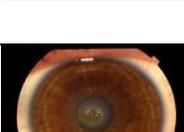
**Iris Movement Detection Process****Image 5: Iris Movement Detection Process****9.2 Result and Discussions**

The above algorithm is tested and analyzed on various iris templates.

Testing of Real vs Fake scanned Iris detection accuracy:

**Table-I : Real Iris Images**

Sl No.	Persons	Iris Images (Left Eye )	Iris image (Right Eye )	Distance from iris scanner	Threshold value	Natural Moveme nt of Iris	Result
1	1 <sup>st</sup>			11.6 cm	6.3	Yes	Real Human Iris
2				11.2 cm	6.3	Yes	Real Human Iris
3				10.3 cm	6.3	Yes	Real Human Iris
4	2 <sup>nd</sup>			11.5 cm	6.3	Yes	Real Human Iris
5				10.8cm	6.3	No	Fake Human Iris
6				10.7 cm	6.3	Yes	Real Human Iris
7	3 <sup>rd</sup>			12.5 cm	6.3	Yes	Real Human Iris

8				11.6 cm	6.3	Yes	Real Human Iris
9				10.9 cm	6.3	Yes	Real Human Iris
10	4 <sup>th</sup>			10.2 cm	6.3	Yes	Real Human Iris
11				10.0 cm	6.3	Yes	Real Human Iris
				10.7 cm	6.3	No	Fake Iris Image

From the above both tables of Real and Fake scanned Iris Images we can conclude that the security algorithm introduced for Flash detection and natural movement detection are robust enough to detect and protect the system from scammers of fake users .

### **Proposed Algorithm:**

**Step 1: Start iris diagnosis**

**Step 2 :Capture image**

**Step 3 :Test Flash Level**

**Step 4 : If Flash below level detect fake Iris and stop else proceed**

**Step 5: Test natural movement of Eye ball**

**Step 6 : If movement of eye ball is not natural then detect fake iris image and stop else proceed**

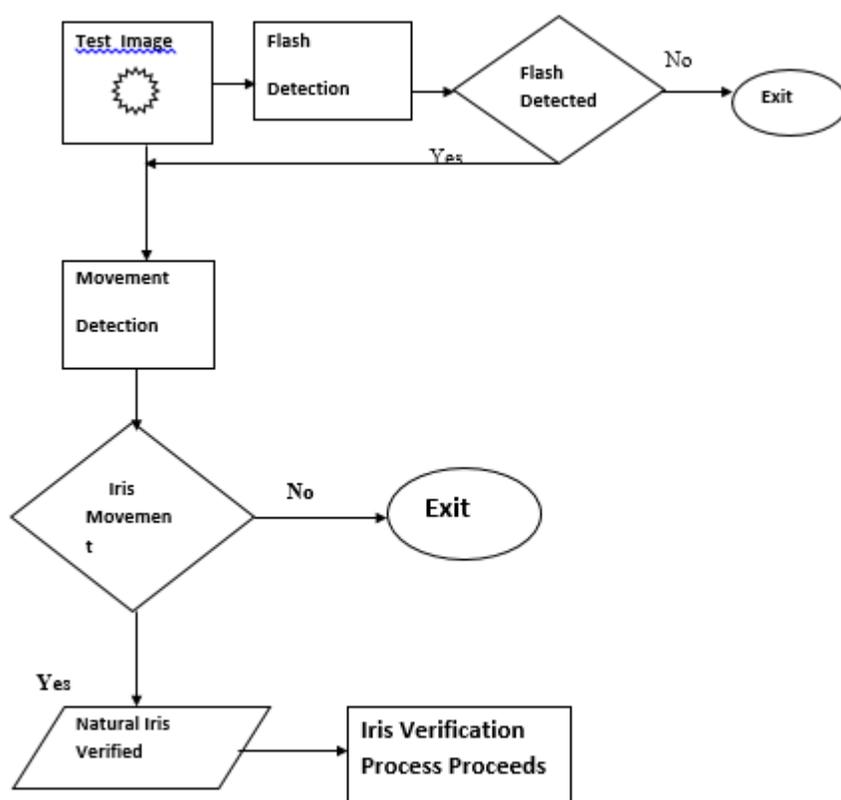
**Step 7 : Conduct Template matching from stored database**

**Step 8 : Match left Iris with left iris template and right iris with right iris template**

**Step 9 : If Iris is matching then declare user identified and authorized else declare unidentified and unauthorized .**

**Step 10 : Exit iris diagnosis**

### Iris Flash & Movement Detection Process



**Image 5: Iris Flash Detection and Movement Detection Process**

### 9.2 Iris Verification Process:

The next stage is the verification / identification process of the target person. After iris verification process will continue. For this, I propose to take iris samples of volunteers (randomly from those whose iris images are stored in the database as well as those whose iris images are not in the database).

Verification is proposed to be carried out in the following steps: (refer to Fig. 5)

Firstly we conduct tests for the natural iris verification . For this we teste for Flash detection using Shine Artifact algorithm. [21]

If iris lecture detected natural then we go for next step i.e. movement detection for a natural iris by using difference algorithm and threshold filters.

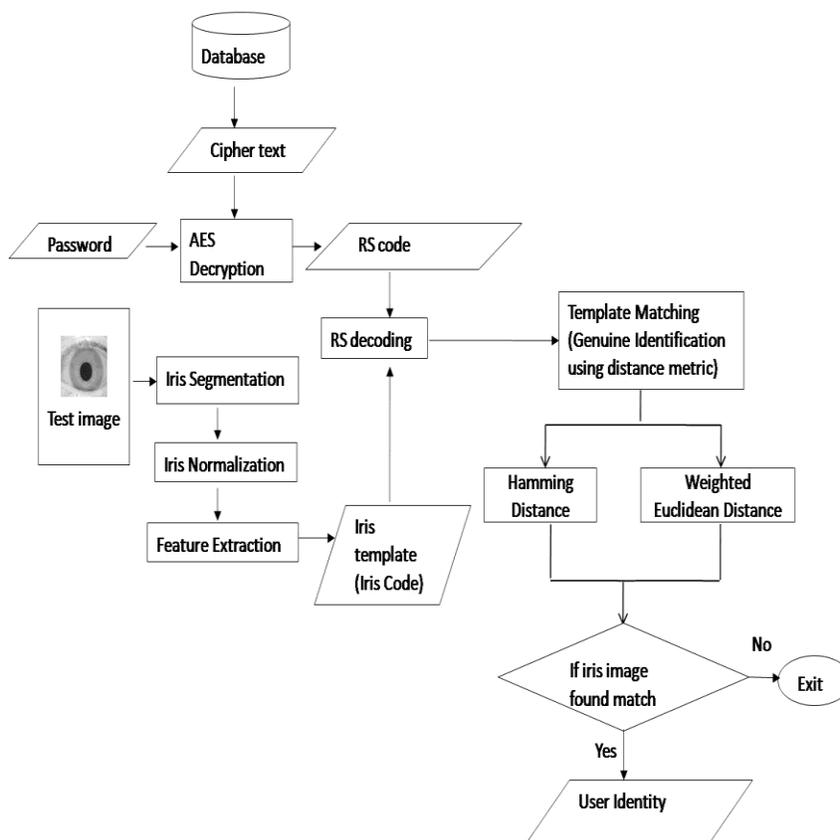
After movement verification process we proceed for the next iris verification process. (Refer to fig. 6 )

For this we repeat all the steps of iris enrollment process as described above i.e. : Iris Segmentation , Iris Normalization , Feature Extraction , Iris Template Generation , RS Decoding , Template Matching by using Hamming Distance and Weighted Euclidian Distance. This would be the template of the target person.

This template of the target person is then matched with the stored template in the database for verification / identification process.

Finally iris is declared matched if all the specified criteria are met otherwise declared not matched or false iris.

### Iris Verification Process



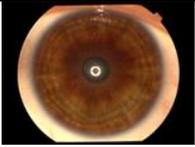
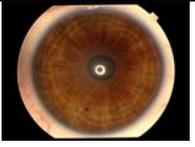
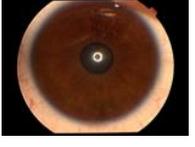
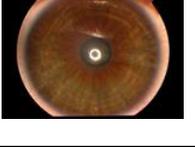
**Fig. 6 The Iris Verification Process Diagram**

### 9.2 Result and Discussions:

The above algorithm is tested and analyzed on various iris templates.

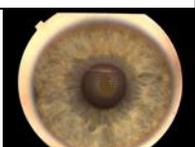
**Fake scanned Iris detection accuracy**

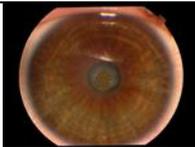
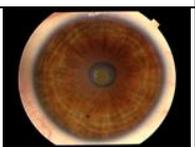
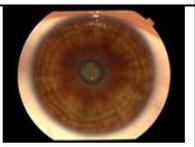
**Table-I : Real Iris Images**

Sl No.	Iris Images	Distance from iris scanner	Threshold value	Flash Detection	Natural Movement of Iris	Result
1		10.5 cm	5.2	Yes	Yes	Real Human Iris
2		10.5 cm	5.2	Yes	Yes	Real Human Iris
3		10.5 cm	5.2	Yes	Yes	Real Human Iris
4		10.5 cm	5.2	Yes	Yes	Real Human Iris
5		10.5 cm	5.2	Yes	Yes	Real Human Iris
6		10.5 cm	5.2	Yes	Yes	Real Human Iris
7		10.5 cm	5.2	Yes	Yes	Real Human Iris

8		10.5 cm	5.2	Yes	Yes	Real Human Iris
9		10.5 cm	5.2	Yes	Yes	Real Human Iris
10		10.5 cm	5.2	Yes	Yes	Real Human Iris
11		10.5 cm	5.2	Yes	Yes	Real Human Iris

Table-II : Fake Scanned Iris Images

Sl No.	Fake Iris Images	Distance from iris scanner	Threshold value	Flash Detection	Natural Movement of Iris	Result
1		10.5 cm	5.2	No	No	Fake Human Iris
2		10.5 cm	5.2	No	No	Fake Human Iris
3		10.5 cm	5.2	No	No	Fake Human Iris

4		10.5 cm	5.2	No	No	Fake Iris	Human
5		10.5 cm	5.2	No	No	Fake Iris	Human
6		10.5 cm	5.2	No	No	Fake Iris	Human
7		10.5 cm	5.2	No	No	Fake Iris	Human
8		10.5 cm	5.2	No	No	Fake Iris	Human
9		10.5 cm	5.2	No	No	Fake Iris	Human
10		10.5 cm	5.2	No	No	Fake Iris	Human
11		10.5 cm	5.2	No	No	Fake Iris	Human

From the above both tables of Real and Fake scanned Iris Images we can conclude that the security algorithm introduced for Flash detection and natural movement detection are robust enough to detect and protect the system from scammers of fake users .

### 9.3 Comparison with Existing Method

Here, we will present a comparison between the current method and Daugman

method and Xiaofu method Described for the purpose of comparison.

we implement his method according to the published paper.

**Table 3: Comparison of proposed system with Xiaofu method**

Sl No.	Features	Xiaofu Method	Security	Fake Detection Accuracy	Proposed Variable Flash Detection System	Security	Fake Detection Accuracy
1	Bright Flash spot detection	Yes	Strong	98.57%	Yes	Strong	99.98%
2	Change of flash color detection	No	Weak		Yes	Strong	
3	Variable Reflection Detection	No	Weak		Yes	Strong	
<b>Improvements over Xiaofu method = 99.98-98.57= 01.41%</b>							
<b>Comparison of proposed system with Xiaofu method</b>							
		Xiaofu Method	Proposed Flash Detection System				
	Fake Detection Accuracy With Printed Clear Iris	98.57%	99.98				
	Fake Detection Accuracy With Printed Non-Clear Iris	98.18	99.24				

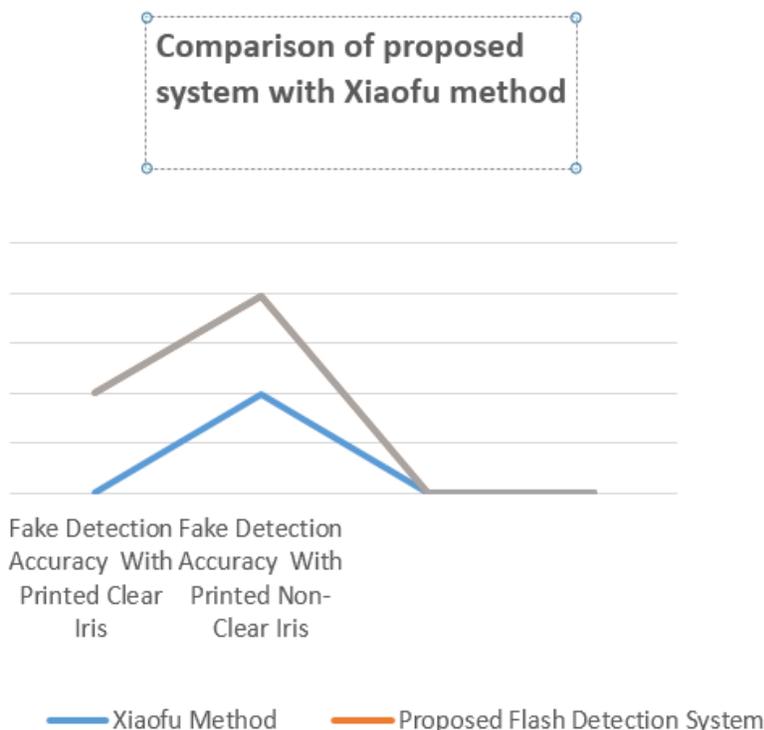


Fig. 7 Comparisons with earlier Algorithms

## 10. CONCLUSIONS & FUTURE SCOPE

We successfully enhanced the detection of fake iris images and add the provision of detection of false of scanned iris images as template. This enhanced significantly the performance of the system in terms of security and reliability. We use Flash and motion detection of natural eye. We successfully attained 98.45% accuracy at 5.2% threshold value at 10.5 cm distance from the Iris scanner.

### 10.1 Future Scope:

This research can be further expanded for the detection of fake finger print images and other authentication systems. This research can be expanded for significant distance iris images where camera normally not able to distinguish the level of Flash. This research can be further refined by reducing the level of threshold value by less than 5.2%.

This research can be further expanded for the detection of fake finger print images and other authentication systems. This research can be expanded for significant distance iris images where camera normally not able to distinguish the level of Flash. This research can be further refined by reducing the level of threshold value by less than 6.3%.

## 11. REFERENCES

- [1] Asima Akber , M.N.A. Khan and Sajid Ali Khan , “ A Critical Survey of Iris based Recognition Systems ” ,Middle-East J. Sci. Res., 663-668, 2013
- [2] Rajesh Bodade and sanjay Talbar , “Fake Iris Detection : A Holistic approach, ” IJCA, Vol 19-No. 2 , April 2011.
- [3] B. Thiyaneswaran and S. padma “Iris Recognition Using left and right Iris feature of the Human Eye for Bio-metric Security system” IJCA, vol 50 No. 152, July 2012.
- [4] Ms. P. Revathy and Dr. Sivanthi Aditanar, “Red Eye Detection and Correction”, IJEERT, Vol 2 , issue 2, may 2014 PP 58-63.
- [5] Jayshri Gaud and Prof. Sneha Bohra , “design amd Implementation of Fake Iris detection System Using Image Quality assessment” IJIRCCE, Vol 3, issue 11, Nov 2015
- [6] Mary Dunker , “Don’t Blink: Iris Recognition for Biometric Identification ” , san Security Essentials, July 2013
- [7] Daksha Yadav, james S. Doyle , Richa singh , Kevin W. Bowyer “Unraveling the effect of Textured contact lences on iris Recognition” , IEEE , October 2013
- [8] Swati S. Deshmukh M.E., Dr. A.D. Gawande and Prof. A. B. Deshmukh “ Detection and Correction of red Eye in Digital Photograph”, IJARCET, Vol 2 , issue 6, june 2013
- [9] Gayatri Anand and Sachin Gupta , “A survey of various Iris Recognition Methodologies” , IJARCSE, Vol 4, Issue 5 , May 2014 .
- [10] P. sangeetha Priya and n. Nandhini , S. Sowmiya and Vibith A S “A mathematical Study on Iris code for Security Connotation ”, IJARCSMS , Vol 4 , Issue 3 , March 2016 .
- [11] Adam Czajka , “Pupil Dynamics for Iris Liveness Detection” Vol 10 , No. 4 April 2015.
- [12] Arun Ross “Iris Recognition : The path Forward ” , IEEE , 0018-9162, 2010
- [13] Rashmi Chandra and Rohit Raja , “A Comparative Survey of Automatic Red eye Detection and Correction ” , IJCTEE, Vol 2 , Issue 4 , august 2012 .
- [14] Sandeep Patil , Shreya Gudasalaman and Nalini C. Iyer , “A Survey on Iris Recognition System” , IEEE , 978 , 2016.
- [17] Mayank Vatsa , Richa Singh and Afzel Noore “ Improving Iris Recognition Performance Using Segmentation , Quality Enhancement , Match Score Fusion and Indexing”, IEEE, 1083 , 2008.
- [18] Ajay wakhare , Anil Kardile , Rahul Nikam and Mohit Dighe “Real Time Iris tracking & Blink Detection for hands free Cursor Control”, IJETAE, Vol 3, issue 5 , may 2013.

- [19] James S. Doyle ,and Kevin W. Bowyer “Robust detection of textured contact lenses in iris recognition using BSIF ”, IEEE, Vol 3 , Oct 2015 .
- [20] Lei zhang , yanfeng Sun Mingjing and Hongjiang zhang “Automatic Red Eye detection and Correction in Digital Photographs” , ICIP 2004.
- [21] Eui chul Lee, Kang Ryoung Park and Jaihie Kim “Fake Iris detection by using Purinje Image ” Research Gate , pp. 397-403 , Jan 2006.
- [22]Xiaofu He , Yue Lu amd Prngfei Shi “ A New fake Iris Detection Method” , Springer PP 1132-1139 , 2009.
- [23]Zhang, D.: AutomatedBiometrics: Technologies and Systems. Kluwer, Norwell (2000)
- [24] Prabhakar, S., Kittler, J., Maltoni, D., O’Gorman, L., Tan, T.: Introduction to the Special Issue on Biometrics: Progress and Directions. IEEE Trans. Pattern Anal. Mach. Intell. 29(4), 513–516 (2007)
- [25] Daugman, J.: The importance of being random: Statistical principles of iris recognition. Pattern Recognition 36(2), 279–291 (2003)
- [26] Daugman, J.: How iris recognition works. IEEE Trans. on Circuits and Systems for Video Technology 14(1), 21–30 (2004)
- [27] Wildes, R.P.: Iris recognition: An emerging biometric technology. Proc. IEEE 85(9), 1348–1363 (1997)

### Acknowledgement

*We are thankful for the IKG Punjab Technical University, Kapurthala (India) for the opportunity provided us to conduct current this research work on **Enhancing Iris Security by Detection of Fake Iris**. We also grateful to the Chandigarh Engineering College, Landran , Mohali (Punjab) affiliated to IKG PTU , Kapurthala for supporting and providing environment for our research work . The active and constant support of our department and research supervisors being the main source of inspiration led this research a success. I thanks my supervisors Dr. Ravinder Khanna and Dr. Anuj Gupta for their active support during every steps of this research.*