International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Anti-spoofing detection based on eyeblink liveness testing for iris recognition

Isaack Adidas Kamanga * and Johanson Miserigodiasi Lyimo

Department of Electronic and telecommunications engineering, Dar es Salaam Institute of Technology (DIT), Dar es Salaam, Tanzania.

International Journal of Science and Research Archive, 2022, 07(01), 053–067

Publication history: Received on 30 June 2022; revised on 08 September 2022; accepted on 10 September 2022

Article DOI: https://doi.org/10.30574/ijsra.2022.7.1.0186

Abstract

Iris pattern is the most stable biometric trait for personal identification. It is the only traits that can't be used after a person death. Despite its stability and difficulty to spoof, it has found that presenting a high quality image of an iris one can spoof and gain an access. Furthermore, the use of video frames of an authorized personnel and the use of 3D models can cheat the system. This study aimed at presenting a solution to this problem by testing the liveness of an eye being scanned by an access control device. The algorithm works by additional process of detecting an eyeblink and background subtraction and correlation to assume liveness. For one to gain access, first an iris is scanned and identified, secondly if this iris is in the database before providing an access, an eyeblink is also sensed. If eyeblink is sensed an access is granted otherwise access is denied. An algorithm has been developed in MATLAB adopting an adaptive Canny method for edge detection. The proposed algorithm validates the user being scanned by two stages which are; Eyeblink detection, background subtraction and correlation. Testing on standard datasets of ZJU Eyeblink, ACASIA v3 and the TalkingFace databases showed show 96.47% accuracy.

Keywords: Biometric ID; Iris recognition; Hamming distance; Eyeblink; Iris Code

1. Introduction

The rapid change in technology especially mobile industry growth demands more secure and viable and more secured authentication techniques [1- 4, 11]. Traditional authentication methods such as using passwords, pins, tokens, and bar codes. can, be forgotten, stolen, or duplicated easily. Biometric-based access control systems are playing a celebrated able role in accuracy and reliability. Biometric security systems use biometric traits such as face, voice, signature, DNA, retina, Iris, fingerprint, hand geometry, and ear structure to identify a person [2, 13] also see [14]. Iris recognition is the most secure and accurate method for authentication [3-5]. Daugman found that the chance of iris patterns from two individuals to be similar is almost impossible therefore iris pattern is an ideal label for authentication, it actually supersedes fingerprint of the fact that even a fingerprint can be used to authenticate whilst it has been found that immediately after death the structure of the iris pattern changes and therefore impossible to authenticate [13].

The bio-metric trait is a distinctive, measurable characteristic that can be used to label and describe the uniqueness of an individual such as iris patterns, fingerprints, and facial recognition [17]. There are two main types of biometric identifiers [17]. There are physiological characteristics (The shape or composition of the body such as DNA, face, fingerprints, hand geometry, retina or Iris patterns) and behavioral characteristics (The behavior of a person such as typing rhythm, gait, gestures and voice) [17]. Other areas that are being researched in the quest to improve biometric authentication include brainwave signals, and a password pill that contains a microchip powered by the acid present in the stomach [21]. Once swallowed, it creates a unique ID radio signal that can be sensed from outside the skin, turning the entire body into a password. Authentication by biometric verification is becoming increasingly common in corporate

* Corresponding author: Isaack Adidas Kamanga
Department of Electronic and telecommunications engineering, Dar es Salaam Institute of Technology (DIT), Dar es Salaam, Tanzania.

and public security systems, consumer electronics, and point-of-sale applications [3-5]. In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry [3-5, 17].

The key reason to as why we need Biometric identification is because the ID cannot be forgotten, is not easily copied, is versatile, and reduce the burden of carrying along, things like security/bank cards, and passports which can easily be forgotten at home [5].

Iris Recognition- This is the process of recognizing a person by taking a picture of an eye analyzing the random patterns of the iris [18], 20]. The automated method of iris recognition is relatively modern, existing in the patent only since 1990s [18]. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle [17], the iris of human eye is the annular part between the black pupil and white sclera. It is located behind the cornea, iris is the only internal organ that is usually externally visible, the diameter of iris is only 12mm but it has a highly complex structure. Under infrared illumination, iris displays rich texture determined by many distinctive minutes. Such iris texture is distinctive between persons and stable over individual's life time, which makes iris particularly useful for personal identification [3].

2. Proposed Model with anti-spoof

2.1. Image Acquisition

The iris recognition system works by first a scanner taking a picture of an eye when an eye is illuminated with near-infrared light in the 700–900-nm band [3]. During scanning even dark brown irises reveal rich texture [19], the existing system is able to take the picture from a printed still picture with high resolution like 1200x1200 dpi, providing a window for bypassing a security check by presenting the image of another person, the proposed model comprises the additional hardware but utilizing the same infra-red radiation to confirm whether the image being taken is the living eye of from a picture or dead person. Once image of the eye is taken the software convert it to gray scale locates the iris within the image then the image is enhanced for further processing. Segmentation and later normalization follows. The normalized and dimensionless iris mapping is encoded into an IrisCode through a process of demodulation that extracts phase sequences, Gabor wavelets transform is used in order to extract the spatial frequency range that contains a good best signal-to noise ratio considering the focus quality of available cameras. The result is a set of complex numbers that carry local amplitude and phase information for the iris image called the IrisCode [19].

Before any further processing of the acquired iris image, this model works by first employing an algorithm to verify that there is no a spoof attempt.

2.1.1. Anti-spoof algorithm design

The combined effect of this algorithm is the ability to detect eyeblink, detecting high background correlation between stored background and current acquired one from a video frame and finally the ability to find border edge line which is the sign of photograph spoofing.

2.1.2. Detecting eyeblink

Blinking is a semi-autonomic rapid closing of the eyelid [2, 5]. A single blink is determined by the forceful closing of the eyelid or inactivation of the *levator palpebrae superioris* and the activation of the palpebral portion of the orbicularis oculi, not the full open and close [16]. A blink lasts about a 10th of a second, and most people blink about 15 times a minute or every 4 seconds [3]. Eyeblink in general lasts from 150 to 300ms [16]. To achieve eyeblink detection, a flowchart in Figure 1 is engaged.

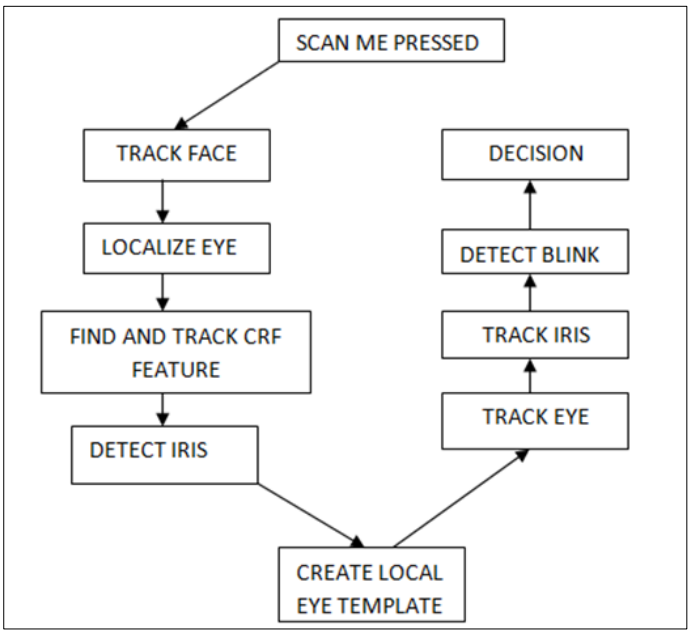

Figure 1 Blink detection flowchart

The Viola-Jones face detector is employed which uses Haar feature-based cascade classifiers with two stages as in Figure 1[20]. In face detection initially, the algorithm needs a lot of positive images (images of faces) and negative images (images without faces) to train the classifier as detailed in [8, 9, 21]. After detecting the face, CRT features are used to track the face [20]. The proposed anti-spoofing algorithm's block diagram is indicated in Figure 2.

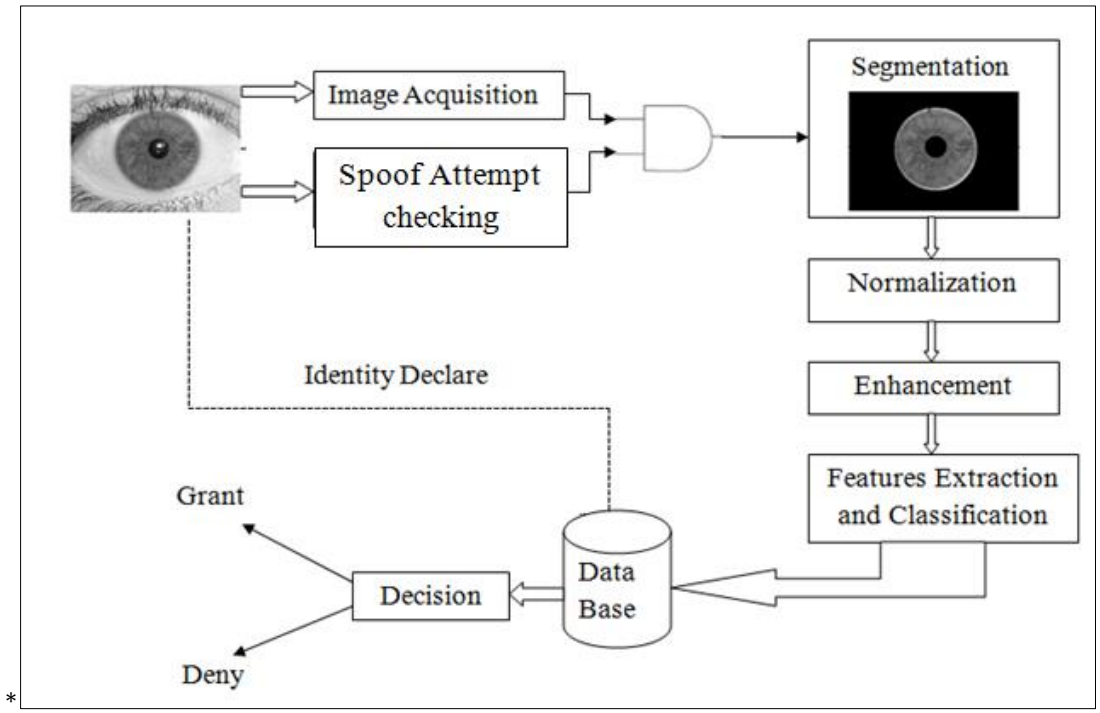

Figure 2 Proposed algorithm block diagram

CRF Feature tracking

Conditional Random Fields shortened as CRF features are classes of statistical modeling methods applied in pattern recognition and machine learning and used for structured prediction [16]. CRFs are type of discriminative undirected probabilistic graphical model [16]. CRFs are used to encode known relationships between observations and construct consistent interpretations, in computer vision; CRFs are often used for object recognition and image segmentation [19].

To super pass the effect that could be brought by slight movement of the head, a feature that is unique and robust should be selected as a reference point for tracking to compensate for minor head movements. The facial features could be point features (eye corners), edge features (lip contours) or texture features (skin color) [8, 9]. In this work I choose CRF features due to their discriminative nature.

The typical eye states are *opening* and *closing* suppose that S is a random variable over observation sequences to be labeled and *Y* is a random variable over the corresponding label sequences to be predicted. All of components *yi* of *Y* are assumed to range over a finite label set *Q*. Using the Hamersley and Clifford theorem, the joint distribution over the label sequence *Y* given the observation S can be written as the following form.

$$P_\theta(Y/S) = \frac{1}{Z_\theta(S)} \exp\left(\sum_{t=1}^{T} \Psi_\theta(Y_t, Y_{t-1}, S)\right) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(1)}$$

Given that Zθ (S) is a normalized factor summing over all state sequences and an exponentially large number of terms

$$Z_\theta(S) = \sum_{Y} \exp\left(\sum_{t=1}^{T} \Psi_\theta(Y_t, Y_{t-1}, S)\right) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(2)}$$

The potential function $\Psi_\theta(Y_t, Y_{t-1}, S)$ is the sum of CRF features at time *t:*

$$\Psi_\theta(Y_t, Y_{t-1}, S) = \sum_i \lambda_i f_i(Y_t, Y_{t-1}, S) + \sum_i \mu_j g_j(Y_t, S) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(3)}$$

Where by $\theta = \{\lambda 1, \ldots, \lambda A; \mu 1, \ldots, \mu B\}$, to be estimated from training data.

The *within-label* feature functions *fi* are as:

$$f_i(Y_t, Y_{t-1}, S) = 1\{y_t = l\} 1\{y_{t=1} = l'\}$$

The between-observation-label feature functions gj are as:

$$g_j(Y_t, S) = 1_{\{y_t = l\}} U(I_{t-w})$$

Where; $l \in Q$, $w \in [-W, W]$

U (I) is *eye closity,* measuring the degree of eye's closeness

$$U_M(I) = \sum_{i=1}^{M} \left(\log \frac{1}{\beta_i}\right) h_i(I) - \frac{1}{2} \sum_{i=1}^{M} \log \frac{1}{\beta_i}$$

Where; *βi = _i/(*1 −*_i)* (7)

hi(I) : *R*Dim*(I)* → {0, 1}, *i* = 1, . . . , *M* is a set of binary weak classifiers.

Creating local eye template

The eye region located is fairly larger than the actual eye [7, 10, 12]. Therefore, the users should be allowed limited head motion as long as the eye remains within this region [10]. When the user is required to look at the center of the screen as a part of the training procedure, an eye template is extracted based on the iris position and size [7]. This eye template is typically smaller than the eye region and allows the user some freedom to move around slightly [10, 12]. It serves to restrict the region of the eye image that is searched in order to detect the iris or evaluate a blink, thus reducing errors and unnecessary processing. After localizing the eye, we need to track it and the iris too.

Local eye tracking using normalized cross-correlation. An eye-tracking procedure maintains exact knowledge about the eye's appearance. In order to track the template, the system utilizes the normalized correlation coefficient R proposed by [8, 9] as follows

$$R(x,y) = \frac{\sum_{y'=0}^{h}\sum_{x'=0}^{w} T(x',y')I(x+x',y+y')}{\sqrt{\sum_{y'=0}^{h}\sum_{x'=0}^{w} T(x',y')^2 \sum_{y'=0}^{h}\sum_{x=0}^{w} I(x+x'+y+y')^2}}$$

Where; $T(x',y')=T(x',y')-T^{-}$,
$I(x+x',y+y')=I(x+x',y+y')- I^{-}(x, y)$
T(x,y) and I(x,y)are the brightness of the pixels at (x,y) in the template and source image, respectively, and T^{-} is the average value of the pixels in the template raster and $I^{-}(x, y)$ is the average value of the pixels in the current search window of the image. The coefficient R (x, y) is a measure of the match between the open eye template and all points within the small search region surrounding the location of the eye given from the previous frame

Detect Blink

Now as we have the local template and we are tracking the eye in real time, the next step is to detect an eyeblink. In this work a method proposed by [16], blink detection by motion variant is implemented in MATLAB for blink detection. According to [9] and [19] proposed methods, we focus on detection of an individual eyeblinks before passing the program counter to continue with recognition steps like segmentation normalization etc. Finally, an access is granted or denied to an individual. Partial closed eye is called an incomplete blink [9, 16, 18]. In case of partial blink access is denied. Eyeblink in general lasts from 150 to 300ms [17]. Thus a standard camera with 25 / 30 frames per second like one in our mobile phones is sufficient for eyeblink monitoring. The region of interest is divided into halves to separate individual eye regions. The method runs separately for each eye. A flock of KLT trackers is placed over a regular grid (Figure 3) spaced with 1/15 of the region dimensions (all together around 225 trackers, that count depends on the region size). Next, local motion vectors are extracted and averaged based on their locations. An average variance of vertical components of the 6 upper motion vectors is the input to a state machine, which detects an eyeblink

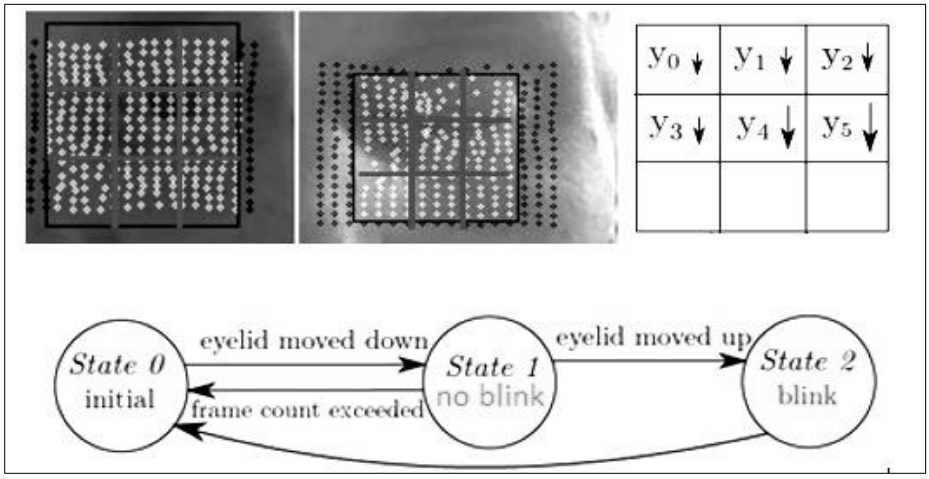

Figure 3 (a) The gray dots representing the trackers used to calculate motion vectors, and (b) shows state machine of eyeblink detection

Kanade–Lucas–Tomasi (KLT) feature tracker is an approach to feature extraction [16, 17, 18]. It is proposed mainly for the purpose of dealing with the problem that traditional image registration techniques are generally costly [16]. KLT makes use of spatial intensity information to direct the search for the position that yields the best match. It is faster than traditional techniques for examining far fewer potential matches between the images [16]. You can find the detail of this algorithm in [14]. The region is divided into 9 cells (Figure 3 (a)). An average cell motion vector is calculated for a cell from the individual local motion vectors belonging to the cell based on their locations. Eyeblink causes a significant vertical move in the cells of the middle row, but only a minor move in the top or bottom row. Motion vectors have different characteristics during head movements or other facial mimics. The vertical components of the middle and top rows are sufficient for further computation. From these 6 (y0-y5) motion vectors the variance var(y) (Equation 4) is calculated

$$Var(y) = \frac{\sum_i (\mu - y_i)^2}{6} \quad \text{..... (4)}$$

Where by $\mu = \frac{\sum_i y_i}{6}$

Statistical variance of the 6 upper cells represents the diversity across moves. If the variance is higher than the variance threshold T_v, it will indicate an eyelid has moved. Variance is invariant to position changes of the person's face, and therefore no head movement compensation is necessary. The variance threshold is evaluated empirically on our dataset as

$$T_v = kx\frac{d}{fps} \quad \text{..... (5)}$$

Where by:

k : is a constant value is 0:018. based on testing.

d : The interocular distance (depends on separation between individual and camera).

fps : The frame rate of the input video from databases used (Talking Face).

I used the publicly available ZJU databases for testing on how many blinks I count and miss, also calculated the efficiency of this approach which is higher than the landmark based approach suggested by [8].

2.1.3. Background Subtraction and comparing

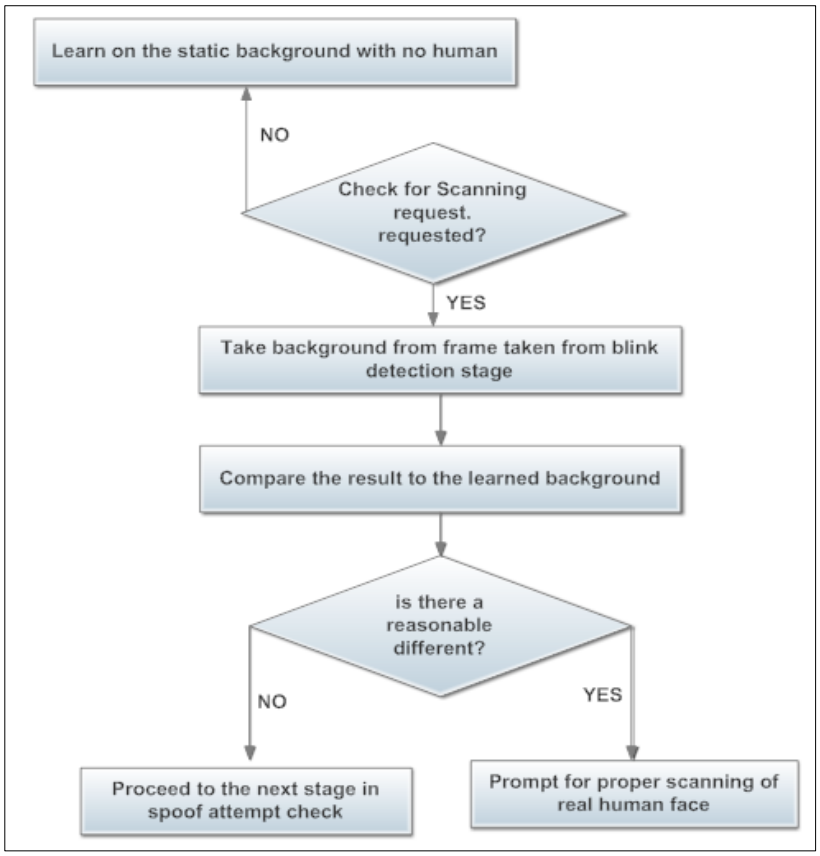

Figure 4 Background subtraction and comparison flowchart

As enlightened by [25, 26, 28], background subtraction, also known as foreground detection, is a technique in the fields of image processing and computer vision wherein an image's foreground is extracted for further processing (object recognition, etc.). Background subtraction is a widely used approach for detecting moving objects in videos from static

cameras, in this work it is used for detecting any change in the background which under no spoofing scenario, no background changes are expected. The implementation follows the flowchart in Figure 4.

In this work, a background mixture model is implemented to achieve the objective. The proposed algorithm models each pixel as a mixture of Gaussians and uses an on-line approximation to update the model. In this approach, it is assumed that every pixel's intensity value in the frame can be modeled using a Gaussian mixture model. A simple heuristic determines which intensities are most probably in the background [9, 10]. Then the pixels which do not match these are called the foreground pixels. Foreground pixels are grouped using 2D connected component analysis and are of no interest at this stage. Figure 5 shows some results obtained.

Four frames of different individuals from ZJU Eyeblink database, more than 70% of the background were masked off and served for comparison, the first background was extracted and used in comparison with other frames

Figure 5 Results of the implemented method

2.1.4. Border edge lines detection

Edge detection approach suggested by us in [11] is employed with an adaptive Gaussian filter to detect edges, see [11] for method details.

2.2. Segmentation

After spoof attempt check, the program counter is passed to the next step in recognition which is segmentation. This step is performed using a variety of boundary and region detection and active contour techniques [2]. The eyelid boundaries may be described as quadratic or cubic splines, whose parameters can be estimated by statistical model-fitting techniques. The techniques are implemented by software; here for research purposes a MATLAB algorithm has been developed for testing the g final result, Daugman inter deferential operator (Equation 6) is adopted for localization of the iris [2, 4] in this work, locating the iris is a challenge and still a research window, many approaches have been suggested like Hough Transform, Active Contour Models etc.

$$\frac{\partial}{\partial r}\{\int_0^{2\pi} I(r*\cos\theta+x_0, r*\sin\theta+y_0)\} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (6)$$

Where; (x_0, y_0) denotes the potential center of the searched circular boundary, and ***r*** is its radius.

The remapping of the iris image $I(x, y)$ from raw Cartesian coordinates (x, y) to the dimensionless non-concentric coordinate system (r, θ) can be represented as

$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta)$$

Where; $x(r,\theta)$ and $y(r,\theta)$ are defined as linear combinations of both the set of pupillary boundary points $(x_p(\theta), y_p(\theta))$ and the set of limbus boundary points along the outer perimeter of the iris $(x_s(\theta), y_s(\theta))$ bordering the sclera[4]. The coordinates become.

$$x(r,\theta) = (1-r)x_p(\theta) + rx_s(\theta)$$

$$y(r,\theta) = (1-r)y_p(\theta) + ry_s(\theta)$$

Both of these are detected by finding the maximum of the operator (Equation 7) [4]. i.e. Figure 6 illustrate the normalization process.

$$\max(r, x_0, y_0) = \frac{\partial}{\partial r}\{\int_0^{2\pi} I(r*\cos\theta + x_0, r*\sin\theta + y_0)\} \quad \text{..... (7)}$$

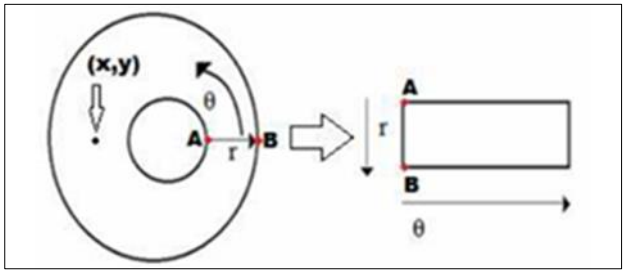

Figure 6 Polar to Cartesian coordinates normalization

2.3. Normalization

After segmentation we need to prepare a segmented iris image for the feature extraction process, this process is called normalization [11]. In Cartesian coordinates, iris images are highly affected by their distance and angular position with respect to the iris scanner. Moreover, illumination has a direct impact on pupil size and causes non-linear variations of the iris patterns. A proper normalization technique is expected to transform the iris image to compensate these variations. A Daugman's normalization method transforms a localized iris texture from Cartesian to polar coordinates [2-4]. The proposed method is capable of compensating the unwanted variations due to the distantcet of eye from camera (scale) and its position with respect to the iris scanner [1, 2]. Figure 7 shows the iris and the normalized version of it.

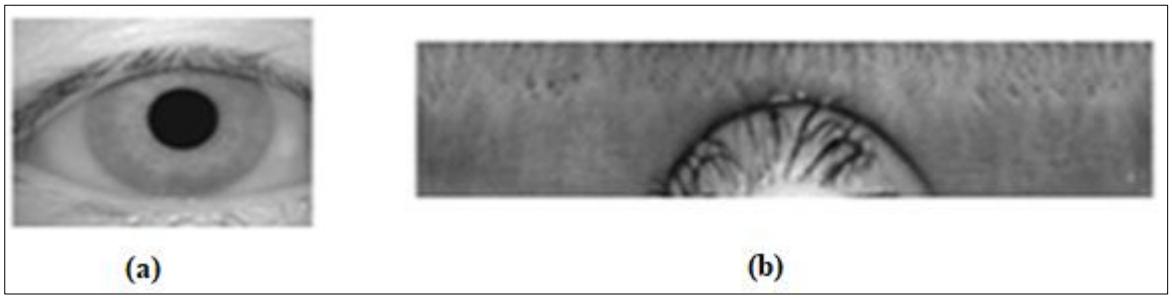

Figure 7 (a) Iris image and its (b) Normalized version

2.4. Enhancement

Image enhancement is a technique of predicting some of the missing details in an image such as a blurred image, to produce output(s) that is suitable for a particular application or a next stage in a given application [11]. In the field of iris recognition, many approaches for image enhancement have been suggested, see [4] for details. Generally, they are of two groups, spatial domain enhancement techniques and frequency domain enhancement techniques, this work employs a spatial domain approach called adaptive histogram equalization where by the contrast of a pixel is enhanced by equalizing the histogram of the small neighboring area, the details of this method can be read in [3, 4].

2.5. Features Extraction using Gabor Filters

2D Gabor filter are applied to extract the iris features. A number of banks of Gabor filters are applied on images including 8 orientations

$$\theta \in \left\{0^0, 22.5^0, 45^0, 67.5^0, 90^0, 112.5^0, 135^0, 157.5^0\right\}$$

Filters, by varying the wavelengths and orientations angles of the filters [21], the result for each bank is evaluated and compared.

2.5.1. Steps in features extraction

- Locating the region of interest around the pupil, which has been done in session 2.2 and 2.3.
- Filtering this region in a total of eight different directions using a bank of Gabor filters (eight directions are required to completely capture the local ridge characteristics in an Iris while only four directions are required to capture the global configuration) pin pointed in [11].
- Computing the Average Absolute Deviation from the mean (AAD) of gray values in individual sectors in filtered images to define the feature vector which is the IrisCode.

Locating region of interest

Consider the gray scale image below in figure 12(a) above, Let P(x, y) denote the gray level at pixel (x, y) in an M × N Iris image and let P(Xo,Yo) denote a point in pupil. The region of interest is defined as the collection of all the sectors Si, where the ith sector Si is computed in terms of parameters (r, θ) as follows [19]

$$S_i = \{(x,y) \mid b(T_{i+1}) \le r < b(T_{i+2}), \theta_i \le \theta < \theta_{i+1}, 1 \le x \le N, 1 \le y \le M\}$$

$$T_i = \text{int}(i/k)$$

$$\theta_i = (i \bmod k) x (2\pi / k)$$

$$r = \sqrt{(x-x_0)^2 + (y-y_0)^2}$$

$$\theta = \tan^{-1}((y-y_0)/(x-x_0))$$

Where by b represents width of each band, k is the number of sectors considered in each band, and i = 0, (B × k- 1), where B is the number of concentric bands considered around the reference point for feature extraction [3, 4]. For testing, CASIA images are used (image size = 256 × 256 pixels, scanned at 600 dpi), we considered five concentric bands (B = 7) for feature extraction and segmented into sixteen sectors (k = 20), we have a total of 20 × 7 = 140 sectors figure 7(b) (S0 through S139) and the region of interest is a circle of radius 60 pixels, centered at the reference point. 140 features for each of the eight filtered images provide a total of 140 × 8 =1120 features per Iris image.

Filtering

A 2D Gabor filter in spatial domain is defined by Equation 8

$$G(x, y : \theta, f) = \exp\left\{-\frac{1}{2}\left[\frac{x'^2}{\delta x^2} + \frac{y'^2}{\delta y^2}\right]\right\}\cos(2\pi f x') \quad \text{..... (8)}$$

Where by

$$x' = x\cos\theta + y\sin\theta$$

$$y' = y\cos\theta - x\sin\theta$$

In equation 19 above, f is the frequency of the sinusoidal plane wave along the direction θ from x-axis, δ y' and δ x' are the space constants of the Gaussian envelope along x' and y' axes respectively. Further details of Gabor filters may be found in [3. 4] also enlightened in [19].

Features vector is obtained by convolution between Gabor filter banks (8 filters one for each orientation in this case) and setting the filter frequency to the average ridge frequency (1/k), where k is the average inter-ridge distance. The average inter-ridge distance is approximately 6 pixels in a 600 dpi (CASIA iris database) Iris image

$$\theta \in \left\{0^0, 22.5^0, 45^0, 67.5^0, 90^0, 112.5^0, 135^0, 157.5^0\right\}$$

Each sub image is respectively filtered by these Gabor filters. This leads to a total of 1120 (8 for each sub image) output-image ROM from which the iris features are extracted.

Computing AAD

This is an average of the absolute deviations from a central point. It is a summary statistic of statistical dispersion

Let $F_{i\theta}(x, y)$ be the filtered image for sector Si in θ orientation and then the features value $V_{i\theta}$ is the Average absolute deviation from mean which is given by

$$V_{i\theta} = \frac{1}{n_i}\left(\sum | F_{i\theta}(x, y) - P_{i\theta} |\right)$$

For all i_s $\forall i \in 0....139$

Where is the number of pixels in Si and is the mean of pixel values of $F_{i\theta}(x, y)$ in sector Si.

2.6. Classification and Decision

Hamming distance (HD) is calculated and used in classifying, if X and Y represent two binary patterns from iris image being verified and one in the database, HD is calculated by taking XOR of the two [3]. HD is the decision making parameter that was suggested by Dr. JG Daugman [4], mathematically, hamming distance (H.D) is computed by the following equation.

$$HD = \frac{No\_of\_different\_bits}{Total\_No\_of\_bits}$$

Matching algorithm

1. HD_array= {size (database)}
2. For j=1 to size (database) do
3. For i = 1 to 1120 do // for all 1120 bits in this work case
4. XOR bit-by-bit code Xi with the code Y(j)*i* in the database
5. If the result of the XOR is (1), this mean the 2 bits are different, so count the number of ones
6. Else don't count it and continue to the next bit
7. Next *i* until reaching the final bit in IrisCode of position j.
8. Compute HD for j IrisCode

$$HD_j = \frac{total\_ones}{1120}$$

9. j=size (database)?
10. If yes end
11. If No j=j+1

2.6.1. Decision

The smallest HD is selected from the array above then if is equal or less that the acceptable value, the corresponding individual is granted access, otherwise if HD is too large

2.7. Open system development

The details on coding can be requested through my email, this section shows the results and brief of the designed system, Figure 8 shows the main menu of the system designed.

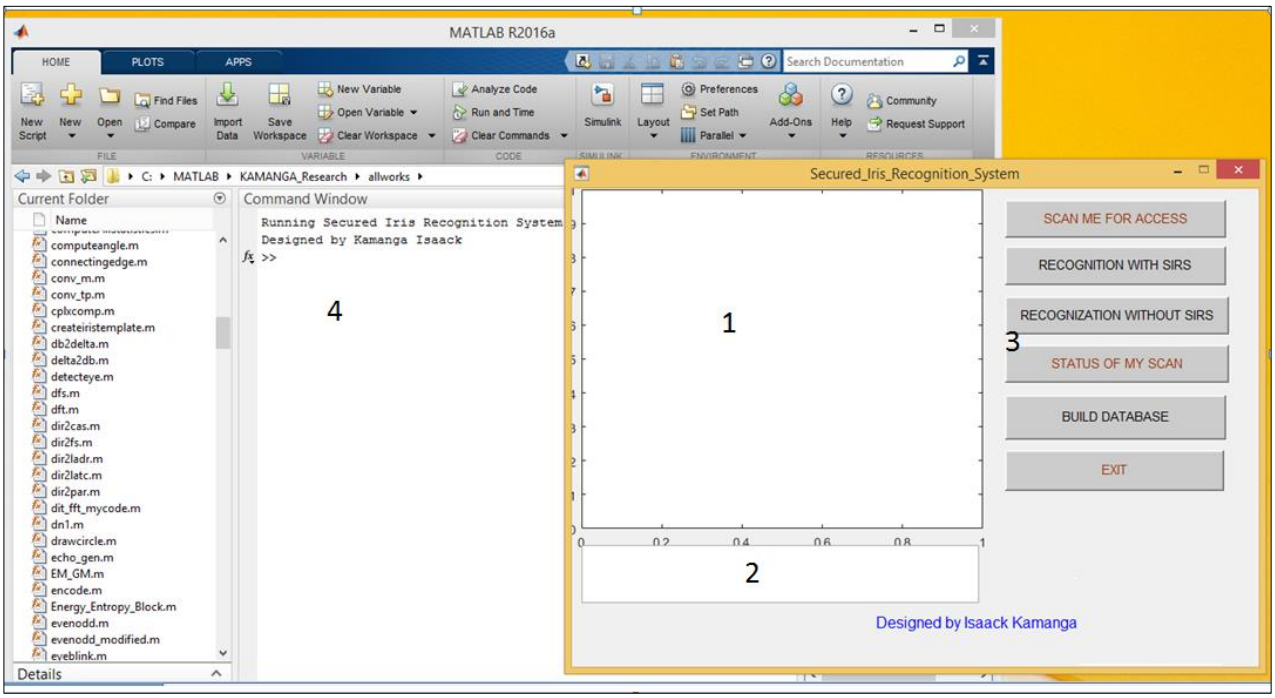

Figure 8 Designed system's main menu

Where by

- Face preview area, the design is such that the algorithm zooms the detected individual face and then crop one eye for recognition, figure 3.16 shows the face preview of individual requesting scan to be granted an access.
- Display 2 is used as an optional for viewing scanning status.
- Control buttons, here all buttons are shown as it is for complete testing of the design but in real application, the individual shall be presented with only "scan me" control and shall be authenticated accordingly, display 2 is used as an optional for viewing scanning status. On the other hand, administrator shall be presented with "Build Database" control, to assist learning process of recognized personnel.
- Main command window, this shows the current task being executed e.g. features extraction of scanned eye, result of recognition process etc. (Figure 9).

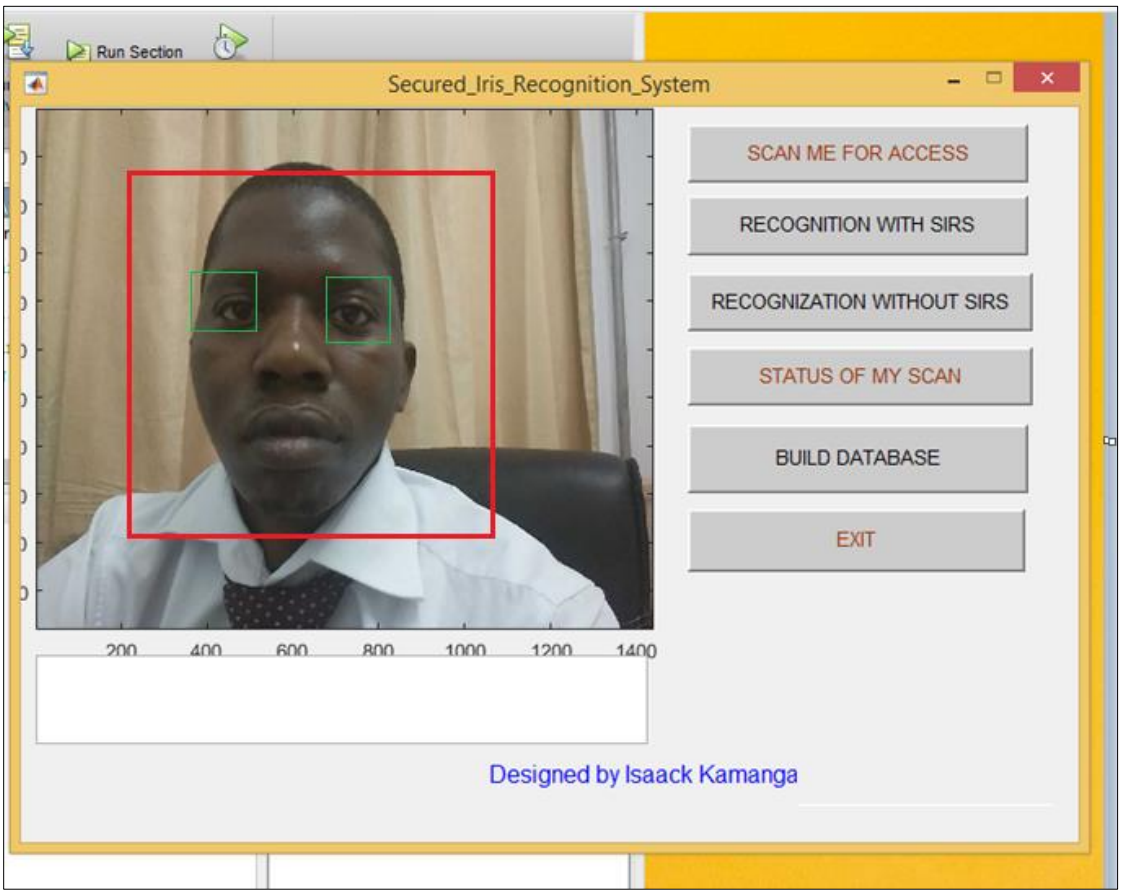

Figure 9 Designed system face preview and detected regions of interest

The system does what expected of not allowing further recognition stages from segmentation after the spoof attempt is detected, Figure 10 show the result,

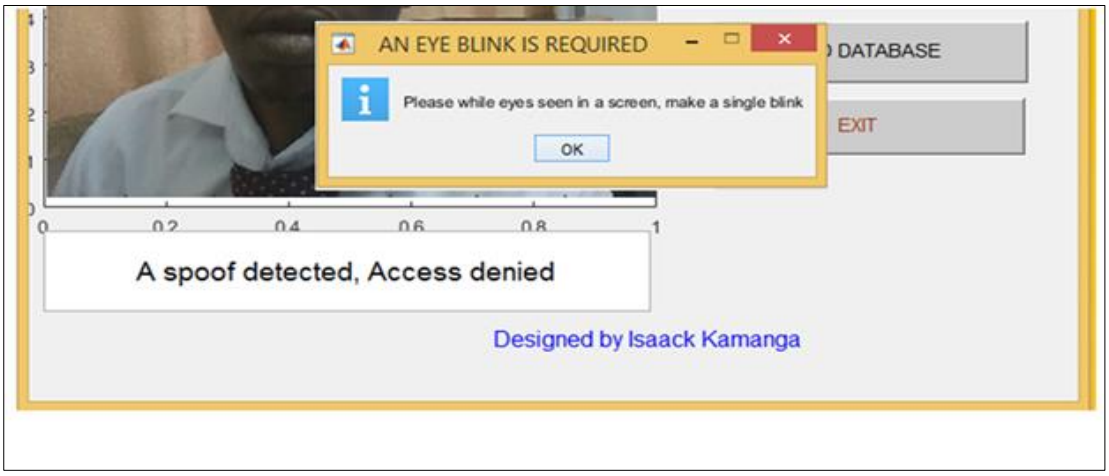

Figure 10 System reaction to spoof attempt

3. Experiment and results discussion

The performance of the anti-spoofing was examined. Tests were carried out to find the best separation, so that the false match and false accept rate is minimized, in the event of spoof attempt and no spoof attempt scenario and to confirm that iris recognition can perform accurately as a biometric for recognition of individuals. As well as confirming that the system provides accurate recognition, experiments were also conducted in order to confirm the uniqueness of human iris patterns by reducing the number of degrees of freedom present in the iris template representation.

3.1. Data set

When benchmarking an algorithm, it is recommendable to use a standard test data set for researchers to be able to directly compare the results. While there are many databases in use currently, the choice of an appropriate database to be used should be made based on the task [22]. In this work first testing was made on the capability of the developed algorithm to detect eyeblink, a suitable publicly available database from Zhejiang University, ZJU Eyeblink database and another publicly available database, the TalkingFace were used. Second testing was made on the capability of the system to detect any background variation on different picture frames, the ZJU Eyeblink database was used and finally, the testing on the accuracy of individual recognition was done using the ACASIA v3 database which is also publicly available. Figure 11 shows these results.

Figure 11 Samples from ZJU blinking database (the last line showing the upward orientation)

Table 1 Demography of blinking database

S/N	No. of Individuals	No. of Video clip	Face appearance	Total No. of blinks (TB)	Blinks detected (DB)	Blinks detected as no blink (MB)
1	20	1	Frontal	255	248	7
2	20	1	Frontal	255	248	7
3	20	1	Upward	255	215	40
4	20	1	Frontal	255	246	9

Accuracy of detection and error in detection are computed by equations (9) and (10) respectively.

$$Accuracy = \frac{DB}{TB} x100\% \quad \text{..... (9)}$$

$$Error = \frac{MB}{TB} x100\% \quad \text{..... (10)}$$

$$Acurracy = \frac{246}{255} x100\%$$

$$Acuracy = 96.47\%$$

$$Error = \frac{9}{255} x100\%$$

$$Error = 3.53\%$$

There are a number of parameters in the iris based access control, and optimum values for these parameters were required in order to provide the best recognition rate [5]. These parameters include; the radial and angular resolution, r and θ respectively, which give the number of data points for encoding each template.

4. Conclusion

Both industry and academia are focusing their efforts to make biometric devices more robust but every countermeasure can eventually be by-passed. Therefore, continual research and development activities are required. In order to counter photo spoofing, this paper investigates the use of eyeblinks as aliveness indicators in face recognition and recommends the use of background comparison and subtraction, as well as the detection of straight border edge lines, as a technique for video and 3D model spoofing attempt detection. The advantage of using eyeblink-based method is a non-intrusion, no extra hardware requirement, and prominence of activity. To recognize the eyeblink behavior, we do not need such a powerful camera, a camera as powerful as a webcam can accomplish the task. The testing found the algorithm developed to respond by 96.47% on the ZJU Eyeblink database.

Compliance with ethical standards

Acknowledgments

The authors are grateful to Prof. Dening Jiang of TUTE for his guidance in accomplishing this work. The authors also thank Dr Mbazigwa Mkiramweni of DIT for his encouragement toward research and publication.

Disclosure of conflict of interest

The authors declare that no conflict of interest exists.

Statement of informed consent

Author declare that the study did not involve any information from other individuals.

References

[1] Daugman J.D. The importance of being random: Statistical principles of iris recognition. Pattern Recognition. 2003 vol. 36, pp. 279–291,

[2] Daugman J.G. High confidence Visual recognition of persons by a test of statistical independence. IEEE Transaction on pattern analysis and machine Intelligence. 1993 vol.5 no 11, pp.1148-1161.

[3] Daugman, J.G. Probing the Uniqueness and Randomness of IrisCodes: Results from 200 Billion Iris Pair Comparisons. IEEE. 2006 Vol. 94, No. 11.

[4] Daugman, J.G. How iris recognition works. IEEE Trans Circuits System and Video Technology. 2003 vol. 14, pp. 1–17, 2003.

[5] Kong W, Zhang D. Accurate iris segmentation based on novel reflection and eyelash detection model. Proceedings of 2001 International Symposium on Intelligent Multi-media, Video and Speech Processing, Hong Kong. 2001.

[6] Wojcikiewicz W. Hough Transform, Line Detection in Robot Soccer. Coursework for Image Processing. 2008 14th March.

[7] Borovi_J. Circle Detection Using Hough Transforms Documentation. COMS30121 - Image Processing and Computer Vision. 2003.

[8] Moriyama T, Kanade T, Cohn J.F, Xiao J, Ambadar Z, Gao I, Imamura, H. Automatic Recognition of Eyeblinking in Spontaneously Occurring Behavior. ICPR'02 2002.

[9] Gang Pan, Lin Sun, Zhaohui Wu, Shihong Lao. Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Web camera. IEEE. 2007 978-1-4244-1631-8/07.

[10] Rhody H, Chester F. Hough Circle Transform. Carlson Center for Imaging Science Rochester Institute of Technology. 2005.

[11] Kamanga A.I. An Adaptive Approach to Improve Canny Method for Edge Detection. International Journal of Science and Research (IJSR).2017 Volume 6 Issue 6, June 2017, pp. 164-168

[12] Kristin A. N, Valerio A, Robert K., Rowe. Spoof detection schemes. Handbook of Biometrics, Springer. 2007

[13] Stephanie A. C., Schuckers. Spoofing and Anti-spoofing measures. Information Security Technical Report.2002 Vol 7, No. 4 ppg 56-62

[14] GUTCHESS D., COHEN-SOLAL M, T, LYONS E, JAIN A. K. A background model initialization algorithm for video surveillance. In Eighth International Conference on Computer Vision. 2001.

[15] STAUFFER C, GRIMSON, W. Adaptive background mixture models for real time tracking. In Computer Vision and Pattern Recognition. 1999.

[16] Divjak, M., Bischof, H. Real-time video-based eyeblink analysis for detection of low blink-rate during computer use. In: First International Workshop on Tracking Humans for the Evaluation of their Motion in Image Sequences 2008. pp. 99{107 (2008).

[17] Abdolhossein F, Abdali-Mohammadi F. Camera-based eyeblinks pattern detection for intelligent mouse. Signal, Image and Video Processing 9.8 (2015): 1907-1916.

[18] M C IVOR A. Background subtraction techniques. In Proceedings of Image & Vision Computing New Zealand. 2000 IVCNZ'00, Reveal Limited, Auckland, New Zealand.

[19] Kamanga A.I, Dening J. Securing Iris Recognition System for Access Control Based on Image Processing", International Journal of Science and Research (IJSR). 2017 Volume 6 Issue 10, October pp. 1131-1140.

[20] Sanpachai H, Settapong, M. A study of Image Enhancement for Iris Recognition. Journal of Industrial and Intelligent Information. 2015 Vol. 3, No. 1.

[21] Ibrahim A.A. iris recognition using Gabor filters. 2008 Al – Taqani , Vol.21, No. ١ , 2008

[22] Garg R, Mitta B, Garg S. Histogram equalization techniques for image enhancement. International Journal of Electronics & Communication Technology. 2011 vol. 2, no. 1, pp. 107- 111.