INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) www.irjaet.com

ISSN (PRINT) : 2454-4744 | ISSN (ONLINE): 2454-4752

Vol. 1, Issue 4, pp.240 - 245, November, 2015

IRIS RECOGNITION ON VIDEO BASED IMAGES WITH ZOOM CONSTRAINT USING HAMMING DISTANCE OF HOUGH TRANSFORMS

N.Nigila[1] | M.Vijayasuresh[2]

PG student, Bharathidasan Engineering college, Natrampalli

Asst professor, Bharathidasan Engineering college, Natrampalli

ARTICLE INFO

Article History:

Received 21st Nov, 2015

Received in revised form 23rd Nov,2015

Accepted 25th Nov, 2015

Published online 29th Nov, 2015

Keywords:

Recognize, wavelets, deformation, iris.

ABSTRACT

Identification of a person to be himself has been a historical concern. The persons today get identified by their signatures, PIN, passwords. But with the increasing insecure environment, where a person does not know when his ID card, password or signature will be stolen, there is an increased need for providing an identification system that recognize a person based on attributes that are impossible to steal. The Iris with its unique characteristics provides the errorless way of recognizing individuals. The unique nature of the Iris guarantee that the individual is recognized to be himself. No two persons have the same Iris structure, not even the same person's two eyes have the same structure of iris. The image of iris is captured with a black and white video camera in a well-lit environment. The pattern is extracted after elastic deformations are reversed mathematically, which is possible after localizing the inner and outer boundaries of iris. After pseudo polar coordinate mapping and using a method called complex valued 2D Gabor wavelets, a bit stream, typically total 256 bytes of information, is obtained. The amount and uniqueness of extracted information make the False Accept probability lowest of all known biometrics.

1. INTRODUCTION

Reliable, automatic recognition of person has long been an attractive goal. In this discussion one of the most promising biometric technique called Iris recognition system is described. It is the most efficient of all the techniques used for biometric authentication. Iris recognition system uses the Iris of the human to

recognize him. Non-invasive, non-contact and extremely fast, high-resolution cameras are used to capture the image of the iris, translating it into an encrypted digital code, called IrisCode.

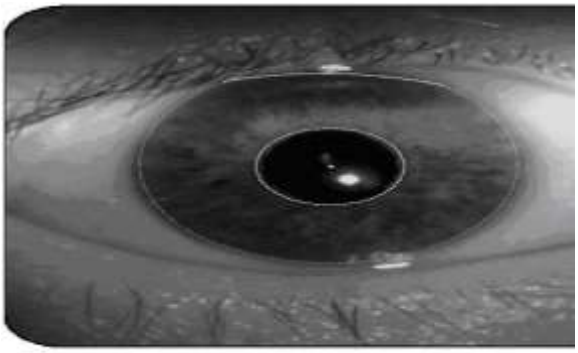

Figure 1: Iris marked in an eye

This is stored into the database for future identification of the person. When the person needs to prove his identification, the same camera and process is used to build the IrisCode. The code previously stored in the database is then used to compare with the obtained code and the result is informed. The complete process of assessment may take not more than two seconds thus avoiding the wastage of time as is done in other techniques such as Fingerprint recognition system. This technology does not use the retinal scan technology and no laser is projected in the eye as in the retinal scan.

The Iris is a protected internal organ of the eye, behind the cornea and the aqueous humor. It is the only internal organ of the human that is externally visible**.** Although small (11 mm) and sometimes problematic to image, the iris has the great mathematical advantage that its pattern variability among different persons is enormous such that no two persons have the same Iris pattern. Even the identical twins have different patterns for their irides As a planar object its image is relatively insensitive to angle of illumination, and changes in viewing angle cause only reversible affine transformations; even the non-affine pattern distortion caused by pupillary dilation is readily reversible.

2. FINDING IN IRIS AS IMAGE

To capture the rich details of iris patterns, an imaging system should resolve a minimum of 50 pixels in iris radius. In the field trials to date, a resolved iris radius of 100 to 140 pixels has been more typical. Monochrome CCD cameras (480 x 640) will be been used because NIR (near infrared) illumination in the 700nm - 900nm band was required for imaging to be invisible to humans. Some imaging platforms deployed a wide-angle camera for coarse localization of eyes in faces, to steer the optics of a narrow-angle pan/tilt camera that acquired higher resolution images of eyes.

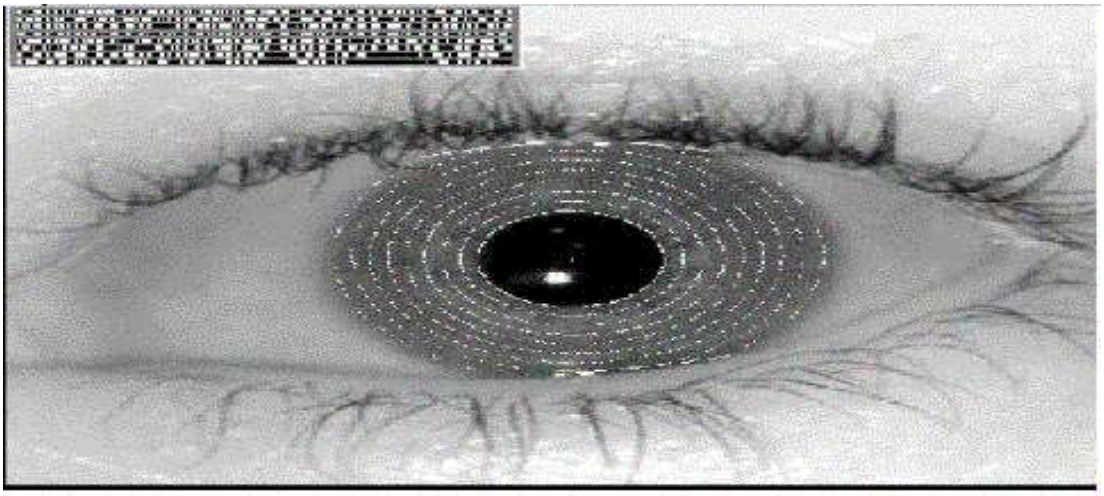

Fig.2. Iris Feature Encoding With Hough Transform

The Hough transform is a feature extraction technique used in image analysis, computer vision, and digital image processing. The purpose of the technique is to find imperfect instances of objects within a certain class of shapes by a voting procedure. The final result of the linear Hough transform is a two-dimensional array (matrix) similar to the accumulator—one dimension of this matrix is the quantized angle θ and the other dimension is the quantized distance r. Each element of the matrix has a value equal to the number of points or pixels that are positioned on the line represented by quantized parameters (r, θ). So the element with the highest value indicates the straight line that is most represented in the input image.

The feature extracted from the iris is stored into a database for the future use when the person is produced for the identification. The database generally is the central database as the Iris recognition system works for identification (one to many). The data stored is 2048 bits (512 bytes) consisting of 256 bytes of the iris pattern and 256 byte of masking pattern. The iris recognition system works even for large size database of around 1 million iris pattern stored into the database. The key to iris recognition is the failure of a test of statistical independence, which involves so many degrees-of-freedom that this test is virtually guaranteed to be passed whenever the phase codes for two different eyes are compared, but to be uniquely failed when any eye's phase code is compared with another version of itself. The test of statistical independence is implemented by the simple Boolean Exclusive-OR operator (XOR) applied to the 2,048 bit phase vectors that encode any two iris patterns, masked (AND'ed) by both of their corresponding mask bit vectors to prevent non-iris artifacts from influencing iris comparisons.

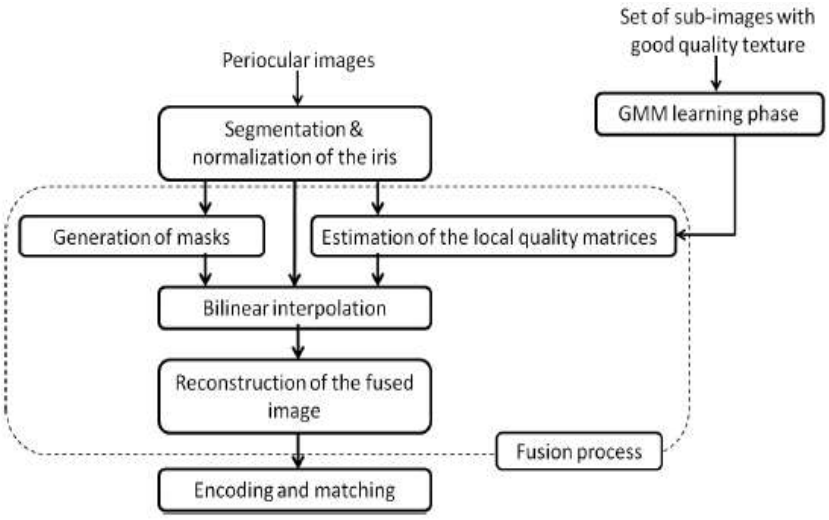

Fig.3. Storing into database

Here we don't need to consider the camera differences. Because here we consider the block difference from image to image. Hence any difference in acquisition process will be automatically considered in this process.

- So enormous amount of time is saved in this method with good accuracy.
- The Input image is first denoised using a median filter.
- The denoised image is histogram equalized for normalizing the intensity levels.
- Segmentation based on thresholding is applied on to the normalized image.
- Block variations are observed and averaged for same iris images and stored as feature vectors.

Generate a template code along with a mask code using hough transform Compare 2 iris templates using Hamming distances.

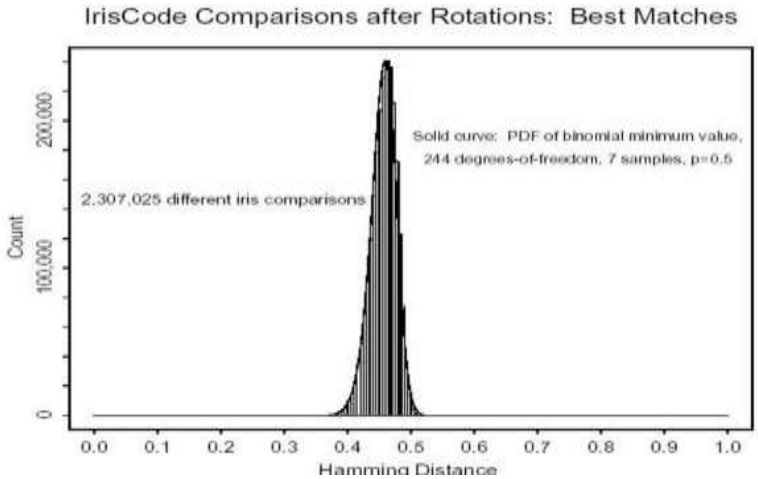

Fig.4. Iris code comarison

The XOR operator detects disagreement between any corresponding pair of bits, while the AND operator ensures that the compared bits are both deemed to have been uncorrupted by eyelashes, eyelids, specular reflections, or other noise. The norms of the resultant bit vector and of the AND'ed mask vectors are then measured in order to compute a fractional Hamming Distance (HD) as the measure of the dissimilarity between any two irides.

3. IDENTIFICATION VS VERIFICATION

Iris recognition identifies people rather than verifying their identity.

Verification asks; is this person who they say they are? This is one-to-one matching which means a person must first suggest their identity through a password, card or name and the system then seeks to determine whether or not there is a match between the suggested and true identities.

Identification asks; who is this person? This is one-to-many matching meaning that the person is not required to carry anything or volunteer any information. The system simply captures the iris image, searches the entire database and either finds their identity or reports that they are unknown. This is obviously a much more powerful form of authentication as no information is required from the user.

Stability asks the iris image remains stable from the age of about 10 months up until death. This means that an iris image need only be captured once and does not need to be updated. Other biometric measures change over time. Hands and fingers grow, our voices change, our skin degrades and other biometric measures are subject to labor, health, genetics, climate and age.

What this means is that the performance of such systems is unreliable and frequent re-enrolments are required to accommodate these changes.

user can stand as far as 10" away from the unit, and even wear glasses or contact lenses without compromising system accuracy. Unlike some other popular biometrics, iris authentication involves no physical contact.

It is also important to note that iris recognition is a completely separate technology to retinal scanning. No bright lights or lasers are beamed into the eye, only a digital photography is taken. This means that not only is iris recognition the most accurate biometric technology, it is also the safest. The birth rate of identical twins is 1 in 121 births or 0.82%. As identical twins share the same DNA, the false acceptance rate for any DNA based system must be at least 0.82% due to the birth rate alone. DNA testing is an invasive technology with a cotton swab inserted into the mouth the most common method of obtaining a sample. This makes iris recognition the most preferred of all authentication system.

4. APPLICATIONS

The Iris recognition system covers a wide range of application in authenticating persons It can be deployed in:

- Border control system
- Airports
- Biometric passports
- Banking systems, ATM's
- Authorized access to healthcare records, intellectual property, etc
- Identification of criminals
- In Govt. organization where restricted access exists
- Productivity enhancing applications like time and attendance.

CONCLUSION

Iris provides the highly accurate and positive personal recognition technique for authentication. This unique and complex organ, which has more dimensions (measures) of variation than any other biometric feature currently in use, remains stable throughout a lifetime and is readily available for sampling in non-intrusive way.

REFERENCES

1. John Daugman PhD, OBE High confidence Recognition of Persons by their Iris patterns University of Cambridge, The Computer Laboratory, Cambridge CB2 3QG, U.K.
2. Ga'el Hacihez, Francois Koeune, Jean-Jacques Quisquater: Biometrics, Access Control, Smart Cards: A Not So Simple Combination. UCL Crypto Group, University catholique de Louvain, Belgium.
3. http://www.iridian.org/IrisCode
4. http://www.lgIris.com/iris/
5. http://www.biometricwatch.com
6. http://biometric.cse.msu.edu