IMPLEMENTATION OF HAMMING-CUT-MATCHING ALGORITHM IN IRIS RECOGNITION

[1]K. R Ingole, [2]Sanskruti Malani , [3]Anuja Gosavi
Professor, Department of Computer Science & Engineering, Sipna COET, Maharashtra, India[1], Student, Department of Computer Science & Engineering, Sipna COET, Maharashtra, India[2], Student, Department of Computer Science & Engineering, Sipna COET, Maharashtra, India[3]

ABSTRACT

This paper deals with the basics of iris, its properties and how it adds some advantageous features to recognize the correct person. In this paper we discuss the details regarding the information about how the iris is located, to distinguish it from other parts of the eye, how the scanner scans the whole pattern of the iris while enrolling and matching and how the scanned patterns are converted into 256 bytes of data so that it can be stored in the database. We compare the iris codes of the current person who wants to access the database and gives the matched results to the user accordingly. This paper includes the implementation of HAMMINGCUT-MATCHING algorithm which reduces the comparison time for matching the iris code with database so that we can use iris recognition.

1. INTRODUCTION

The determination, measuring, and codification of the unique characteristic traits that each of us is born with is known as the science of biometrics. Various forms of computer-based biometrics for personal authentication have been around for the past twenty years, but not until recently have some reached maturity and a quality/reliability that has enabled their widespread application. In the past, *hand geometry*enjoyed the advantage of very small templates (codes containing the biometric data), but with modern computers this is no longer the main issue and iris based solutions are steadily gaining ground.

Retinal, iris, and ***fingerprint***recognition are mature technologies with the most reliable performance. Of the three methods,

iris recognition is the least intrusive (*unwanted involvement*) with greater accuracy.

In addition to reliable performance some of the other advantages of using biometrics are:

- **High security:** It is based on physical characteristics, which cannot be lost or stolen.
- **Certainty/accountability:** A specific person, not just a holder of a token or somebody who knows a PIN/password, has been authenticated. Users need not worry about someone using their token or PIN code without their knowledge.
- **Ease of administration:** The problems of handling forgotten PINs/passwords and lost/stolen keys or access cards are eliminated, the benefit is a lot of time and resources saved.

Iris recognition is one of the biometric systems which utilize ***iris patterns*** as a method of gathering unique information about an individual. It is considered to be one of the most reliable biometrics with some of the lowest ***false rejection*** and ***false acceptance*** rates and so it is less intrusive.

IRIS:

The iris, the colored portion of the eye, is approximately 11mm (.433 inches) in diameter and consists of several layers and distinct features such as furrows, ridges, coronas, crypts, rings which controls the amount of light that enters into the eye. Varying in shades of brown, blue and green, ***no two irises are alike***, not even within the same individual or identical.

2. PROPERTIES

Glasses and contact lenses, even colored ones, do not interfere with the process. In addition, recent medical advances such as refractive surgery; cataract surgery and cornea transplants do not change the iris' characteristics. In fact, it is impossible to modify the iris without risking blindness. And even a blind person can participate. As long as a sightless eye has an iris, that eye can be identified by iris recognition

Glasses and contact lenses, even colored ones, do not interfere with the process. In addition, recent medical advances such as refractive surgery; cataract surgery and cornea transplants do not change the iris' characteristics. In fact, it is impossible to modify the iris without risking blindness. And even a blind person can participate. As long as a sightless eye has an iris, that eye can be identified by iris recognition.

3. PROPOSED WORK

An iris has a mesh-like texture to it, with numerous overlays and patterns that can measured by the computer. The camera such as CCD having a high resolution can be set at a distance of four inches (10 centimeters) to 40 inches (one meter), depending on the scanning environment. When iris recognition is used for logging on to a personal computer or checking in at an airport, people need to be somewhat closer to the camera. An automatic cash machine, on the other hand, does not require such nearness.

The iris-recognition software uses about 256 ***"degrees of freedom"*** or ***"points of reference"*** to search the data for a match. The iris is found by using an integrodifferential operator (1), which determines the inner and outer boundaries of the iris's colored pigmentation. Not all of the iris is used: a portion of the top, as well as 45˚ of the bottom, are unused using the Each isolated iris pattern is then demodulated to extract its phase information using quadrature 2D Gabor wavelets. It amounts to a patch-wise phase quantization of the iris pattern, by identifying in which quadrant of the complex plane each resultant phasor lies when a given area of the iris is projected onto complex-valued 2D Gabor wavelets. Such a phase quadrant coding sequences. A desirable feature of the phase code is that it is a cyclic, or grey code: in rotating between any adjacent phase quadrants, only a single bit changes, unlike a binary code in which two bits may change, making some errors arbitrarily more costly than others. Altogether 2,048 such phase bits (256 bytes) are computed for each iris.

This record is then stored in a database for future comparison. When a comparison is required the same process is followed but instead of storing the record it is compared to all the Iris Code records stored in the database. The comparison also doesn't actually compare the image of the iris but rather compares the hexadecimal value produced after the algorithms have been applied.

4. HAMMING DISTANCE

In order to compare the stored Iris Code record with an image just scanned, a calculation of the Hamming Distance is required. The Hamming Distance is a measure of the variation between the Iris Code record for the current iris and the Iris Code records stored in the database. Each of the 2048 bits is compared against each other, i.e. bit 1 from the current Iris Code and bit 1 from the stored Iris Code record are compared, then bit 2 and so on.

Any bits that don't match are assigned a value of one and bits that do match a value of zero. Once all the bits have been compared, the number of non-matching bits is divided by the total number of bits to produce a two-digit figure of how the two Iris Code records differ. For example a Hamming Distance of 0.20 means that the two Iris Code differ by 20%.

$$\text{Hamming Distance} = \frac{\text{Number of non-matching}}{\text{Total number of bits}}$$

The comparison of a live subject Iris Code record with all the Iris Code records in the database may seem like a large amount of data to process, in reality it normally only takes a few seconds. This comparison speed is obviously affected by the speed of the system processor the database is running on and the size of the database itself.

The proximity a user needs to be to the scanning system is usually dependant on the lens in use and the illumination. For example, systems scanning at the desktop PC level can operate with the subject seventeen to nineteen inches from the unit.

IRIS SCANNER:

Figure.4 Showing the iris scanner

5. OUR IMPLEMENTATION TO REDUCE THE COMPARISON TIME

The comparison speed of a person's iris code with iris database is obviously affected by the speed of the system processor and the size of the database itself. If the iris recognition technology is used in large database system like identifying the citizenship of a person, then the time taken for comparing his iris code with the database will be very high. So we have implemented hamming-cut-matching algorithm to reduce the comparison time.

In normal process the iris code is compared with iris code in the database and the hamming distance is calculated by comparing the whole 2048 bits. If the hamming distance is within some specified limit the person is given permission for access otherwise it rejects the person's identity. So, most of the time is spent for comparing the records in the database itself.

But we are comparing the iris codes bit by bit and simultaneously checking whether the hamming distance exceeds the given limit or not. If it exceeds the limit, then comparison with the particular record is stopped and next record is taken for comparison and so on. If both the iris code is going to be similar then it will proceed with same record by comparing the next bits. This reduces the comparison time because we are not comparing all the bits present in database. The hamming-cut-matchingalgorithm is as follows.

HAMMING-CUT-MATCHINGALGORITHM

```
START THE PROCESS
WHILE(FOR ALL RECORDS IN  DATA
BASE)
      HAM=0, I=0, K=0
WHILE ( I<2047) READ A[I] ,D[K]  /* A is the current iris code bit ,D is the
Database iris code bit */
IF ( A[I] <>  D[K])
  THEN
     HAM->HAM+1
IF( HAM = MAX )
/* HAM is the hamming match MAX is the maximum limit for hamming Distance */
```

THEN GOTO X;

ELSE I->I+1, K->K+1

ENDIF

ENDIF

END WHILE

PRINT ("YOR ARE THE CORRECT PERSON");

EXIT PROGRAM

X: TRANSFER THE CONTROL TO THE NEXT DATABASE RECORD

END WHILE

PRINT ("YOU ARE NOT OUR AUTHORISED PERSON");

STOP THE PROCESS

6. CONCLUSION

Passwords, token cards and PINs are all risks to the security of an organization due to human nature. Our inability to remember complex passwords and tendency to write these down along with losing token cards or forgbreakdown in security for an organizatioetting PINs all contribute to the possible n.

- Passwords, token cards and PINs are all risks to the security of an organization due to human nature. Our inability to remember complex passwords and tendency to write these down along with losing token cards or forgetting PINs all contribute to the possible breakdown in security for an organization. The uniqueness of the iris and low probability of a false acceptance or false rejection all contribute to the benefits of using iris recognition technology.

➢ It provides an accurate and secure method of authenticating users onto company systems, is a nonintrusive method and has the speed required to minimize user frustration when accessing company systems.

➢ Users no longer have to worry about remembering passwords and system administrators no longer need to worry about the never-ending problem of users disclosing passwords or having weak passwords that are easily cracked.

➢ As according to our implementation the comparison time of the iris code with the iris database is very much less from the current system.

➢ If a two-factor authentication system is implemented, iris recognition with a hand scanner for the verification, then the strength of authentication increases and provides another part to defense in depth for the airport.