ISSN 2320 - 2602

Volume 5 No.1, January 2016

International Journal of Advances in Computer Science and Technology

Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst02512016.pdf

Emerging Biometric Technology-A Review

Suman Chakraborty[1], Prof. Samir Kumar Bandyopadhyay[2]

[1] Lincoln University, Malaysia,suman75@gmail.com

[2] Lincoln University, Malaysia,skb1@vsnl.com

ABSTRACT

Biometric recognition is the task of identifying an individual on the basis of his/her physiological or behavioral traits. Over the last three decades there has been a lot of work done on development of systems based on fingerprint, face, iris, voice etc., but in the recent past some new biometric measures have emerged which have shown prospect of enhancing the performance of the traditional biometrics. In this paper a review on emerging biometric techniques is presented.

Key words : Biometrics, Identification, Verification and Modalities

1. INTRODUCTION

Today, in this current era we all have a strong digital identity so as the real one. Day by day as this digital world is expanding faster we also find us more tightening to zeros and ones. From social networking to stock marketing, from private banking to military, digitally are connected to everywhere. Every day the trillions of trillion's information are transmitting in this enormous digital network. So, naturally the obvious question comes into our mind is, how we can make us unique from each-other and how we can protect those information from unauthorized one? There comes an important aspect is maintaining our unique identity digitally and also it's required to match it with the real uniqueness because today we are dealing with the real world both digitally and manually. Secondly, we must ensure the most fundamental requirement of information exchange, security and the answer of it is Cryptography. It ensures all the fundamental requirement of information exchange.

2. HISTORY AND REVIEW

Around 2000 BC in Egypt, the biography of the deceased was engraved on the tombs to make them nobler, majestic and ceremonial using a technique of hiding the message known as hieroglyphics. During earlier times, hieroglyphics was primarily used for adornment rather than ensconcing information or messages. However, we thus find that the roots of cryptography dates back to the ancient Egyptian times. Cryptography in today's world has immense significance and our ancestors were wise enough to coin different methods of cryptography in their times.

Cryptography has a variety of forms which uses various encryption techniques on some given data. One specimen is the Hebrew cryptographic method where the alphabets were flipped in the reverse order, such as follows:-

ABCD	EFGHI	JKLMN	OPQRS	TUVWX	YZ
ZYXW	VUTSR	QPONM	LKJIH	GFEDC	BA

This method is termed as *atbash*. This is a kind of substitution cipher where an alphabet is substituted by another alphabet. This type of substitution cipher can also be called monoalphabetic substitution since it considers only one alphabet at a time. This is one of the most simplistic encryption methods and worked well in its time. With the development of society and culture, more complex cryptographic methods also came into vogue.

Around 400 B.C. the Spartans used a more strategic method of encryption. Here, a message was written on a sheet of papyrus and was wrapped around a staff of some specific shape and diameter. The one who had the exact replica of the original staff was only able to decipher the message. If someone else tried to read out the information, it would appear to be a page of randomly written alphabets. A correct staff would only allow the actual message to be read. This method is known as the scytale cipher [Figure 1]. This was mainly used by the Greek government to send important directives or messages to its soldiers. The scytale cipher was a highly advanced cryptographic scheme used in those times.

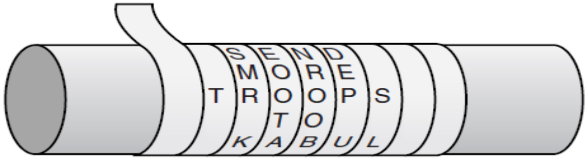


Figure 1: Scytale Cipher

Julius Caesar was one of the pioneers of his age who established a type of encryption method of shifting letters of the alphabet, similar to the atbash system that was quite popular and successful in those times.

In the Middle Ages and late 1800s, extensive research regarding various methods of cryptography was in full swing and during those times mostly military factions used this system to communicate amongst themselves. As mechanical and electromechanical technology advanced, the telegraphic and radio communication came into existence. Tactical communication, using simplistic encryption devices was practised at large during the World War II.

The rotor cipher machine that substitutes letters using different rotors present in a system proved to be a highly convoluted cryptographic method. This work paved the way for the introduction of the most highly acclaimed cipher machine till date, Germany's *Enigma*. The *Enigma* machine was composed of three rotors, a plugboard and a reflecting rotor. The Enigma had a specific and unique way for encryption. The initiator of the message had to configure the Enigma to its initial settings prior to the beginning of the encryption procedure. The user was supposed to write in the first letter of the message and the Enigma would move its rotors till a specified count and thereby replace the original word with an encrypted character presented to the user. Let us consider an example, if the character F has been encrypted as V, this V would have to be noted by the user. The rotors would again be moved to enter the next letter. Thus each time, the rotors had to be set to a new setting to enter a character and this procedure kept on going until the complete message was successfully encrypted. Next to this, the encrypted text was transmitted over the airways, most likely to a U-boat. Based on the rotor setting, the substitution letter was generated, so the crucial and secret part of this process was how the rotors were operated when encrypting and decrypting a message. To decipher the message, users at both ends were required to know the sequence of increments using which the rotors moved. The Enigma was a highly pragmatic device and it helped the Germans to communicate with ease since decoding the encryption format by Enigma was almost next to impossible. Still, a team of Polish cryptographers decoded it resulting in shortening of the World War II.

William Frederick Friedman, the *Father of Modern Cryptography*, published *The Index of Coincidence and Its Applications in Cryptography.* He, in his lifetime had broken and decoded many cipher text during World War II. Governments and military all over the world have used encryption in some way or the other to become victorious mostly because of its covert man oeuvres that required shrouded security. Cryptography was at that time indispensible for their victory. Simultaneously when the cryptographic system of some countries got decoded by their enemies, it brought great defeat to them.

With the advancement of technology, encryption methods and devices also got updated. Cryptographic designers and encryption techniques received ample opportunity for their growth. The U.S. National Security Agency (NSA) adopted and modified as per needs, the most well-known and successful project IBM’s Lucifer that used complex mathematical equations and functions, paving the way for the U.S. Data Encryption System. DES has a variety of uses. The DES, used as the principal tool for worldwide financial transactions, has also been adopted as the federal government standard, besides use in numerous other applications. For the last 20 years DES has been popularly in use worldwide.

Cryptography has also had its share of political commotion where several governments imposed trans-border restrictions and abolished the use of cryptography in several sectors by introducing export regulations. The Clipper Chip developed by the Law enforcement deciphered communication regarding suspicious illicit activities or drug peddling. However, this aspect invited lots of criticisms where public's privacy was at stake because of government's eavesdropping. Now-a-days cryptography is in use in banking transactions, e-mail to corporate extranets, and almost all events.

Nowadays, hackers are becoming smarter by the day and thus the need of increased protection has arisen. The code breakers and cryptanalysis efforts and increasing capabilities of microprocessors quickened the evolution of cryptography each year. Cryptanalysis’s a science of studying and breaking the secrecy of encryption algorithms and their necessary pieces. Different types of cryptography have been used throughout civilization, but today it is used in every part of our communication and computing world. Since secrets have always meant to be hidden, our dependency upon cryptography will also remain intact.

3. PRINCIPLE OF SECURITY

Confidentiality: Only the sender and the intended recipient(s) should be able to access the contents of a message. That is, if sender A sends the data to B, then that data sends by the A to the B can access or can understood only by either A or B. Even if someone else gets the data he/she does not able to know the meaning of that data.

Connection Confidentiality: Here we protect all user data on a connection.

Connectionless Confidentiality: Here we protect all user data in a single data block.

Selective-Field Confidentiality: Here we protect selected fields within the user data on a connection or in a single data block.

Traffic Flow Confidentiality: Here we protect all information that might be derived from observation of flow of traffic in a communication network.

Integrity: The contents of message remain unchanged after the sender sends is until it reaches the intended recipient. That is, if sender A sends the data to B, then after A sends the data, the data remains unchanged until it reaches to the receiver, i.e. B. That means no one can tamper the data.

Authentication: It helps to establish the proof of identities. That is, if X sends the data to Y, then Y must assure that the data has indeed come from X, not from someone else posing as X. E.g., Z send a data to Y posing as X, and Y found that the sender of that data is X, is going to violate the authentication principle. Peer Entity Authentication: It provides confidentiality in the identity of the connected entities used in association with a logical connection. Data Origin Authentication: It provides assurance that the sender of received data is as claimed when using connectionless transfer.

Non-repudiation: The ownership of the data sent by sender is never refused by the sender. That is, if A send a data to B, then A does not refuse the ownership of that data.

Access control: It specifies and controls who can access what. That if after A sends the data to B, access control specify that the B can view the data or might B allow to make change as well. All the accesses perform by the users are specified by this principle, i.e. access control.

Availability: It promises availability of resources to authorized parties at all times. E.g. Due to the intentional actions of another unauthorized user C, an authorized user A may not be able to communicate with server computer B. this defeat the principle of availability.

4. CATEGORIES OF SYMMETRIC AND A SYMMETRIC CRYPTOGRAPHY

Cryptosystems using symmetric cryptography, have the same key, known as the secret key, used by both parties for encryption and decryption, providing dual functionality. This type of encryption requires each user to keep the key secret and properly protected. If not, any intercepted message encrypted with this key, can be decrypted by the intruder.

For each pair of users exchanging data using symmetric key encryption must have their own set of key, whose security lies totally on how they protect it, else all messages encrypted by the key can be decrypted by an intruder. The sharing and update of symmetric keys adds to the complication. Since both users use the same key for encryption and decryption, it can provide confidentiality but not authentication or non-repudiation.

There is no way to prove who actually sent a message if two people are using the exact same key. Compared to asymmetric systems, symmetric algorithms scream in speed. Large volumes of data can be encrypted and decrypted in a very short time compared to the use of asymmetric algorithm. Data encrypted through symmetric algorithm using a large key size, is very difficult to uncover.

Symmetric key cryptography provides a single secret key is used between a pair of users, whereas in public key systems, each user uses two different mathematically related asymmetric keys – one for encryption and the other for decryption of the message. [Figure 2].

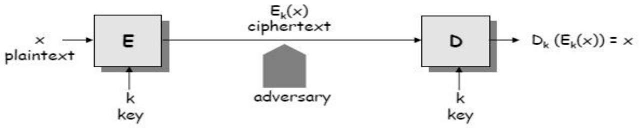


Figure 2: Symmetric key crypto system

The pair of keys, used in a public key system, is made up of one public key and one private key. Public keys can be known to all users while the owner only must know the private key. During communication of two entities, for encryption or decryption of data, public keys can be obtained from directories and databases of e-mail addresses, providing availability to everyone.

In asymmetric key encryption technology, the exact same key cannot be used for both encryption and decryption, moreover the private and public keys may be mathematically related but cannot be derived from one another. Decryption of the message by a particular public key is possible only if the corresponding private key was used for encryption, which provides authentication. The receiver can also encrypt his response with his private key instead of using Sender's public key. If confidentiality is the most important security service, the receiver's public key will be used for encryption, providing a secure message format, as decryption is possible only by the person who knows the corresponding private key. If the most important security service is considered to be authentication, then the encryption is to be done by the private key. Hereby the receiver is assured that the message has been encrypted by the person who possesses the private key. Each key type can be used to encrypt and decrypt, so do not get confused and think the public key is only for encryption and the private key is only for decryption. They both have the capability to encrypt and decrypt data. If encryption is done through private key, the decryption must be through a public key and not private key. This holds good for the converse as well. [Figure 3].

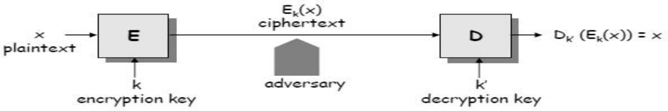


Figure 3 : Encryption and Decryption Process

Symmetric cryptosystems are faster than asymmetric cryptosystem but lacks confidentiality, authentication, and non-repudiation depending on its configuration and use. Moreover key distribution is more manageable in asymmetric systems and don't have scalability issues that are present in symmetric systems.

5. IRIS BIOMETRICS RECOGNITION

Most important aspect of security system is the authentication. Authentication defines the authorize access on information. Authorization is the most vulnerable principle of security as it prevents any unauthorized access of confidential information, i.e. apart from the intended user no one will able to access the data. Now, the important question is how we can ensure the user authorized to access the data or information? Some techniques must be there to identify the authorized user. In real, we may have such things which others don't have or we may know some information which others don't know or something we are, i.e. our unique characteristics or features. Now, these three are basically the three different levels of authentication. For example, we often have some keys or badges which authorize us over other for access on some information. This is the possession-based identification features. Again, we all go to ATM now days to withdrawal the money or many of us used to connect ourselves in the social networking platform. But what specify us as us? The answer is PIN or log in ID and password. We know such things and we uses it for authorize our self. This is knowledge-based identification features. But the main problem in "know something" or "have something" is it can be easily stolen or can be easily lost. If I forget my PIN or password or lost my keys I cannot able to define myself as an authorized person even if that true [1]. Again if someone else is able to steal my PIN or password or my keys somehow, I lose the privilege of accessing my account and therefore authorization which he acquires. So, we can see that in both the cases though it specifies the authentication but there are some loopholes and these are not so concrete. But we cannot deny who we are. It is certainly not possible for anyone to steal our characteristic from us. Also it is equally not possible to lose these features. These are our basic unique features which we have by birth and its makes us unique from each other. This is called Biometrics.

The modern trend on security system is based on biometrics-based identification system. There are few concrete reasons for that. But before explain those points let us understand what does biometrics mean? and, what makes it useful upon other two, i.e. possession-based and knowledge-based system? By definition, Biometrics is a way to verify identity through the automated use of physiological or behavioural characteristics. Here automated use means using computers or machines, rather than human beings. But why it's so useful over other two? As biometrics only deals with the individual's biological samples i.e. measuring the physical and behavioural characteristics of the individual candidate's biological information, its quit obvious that biometric traits cannot be forgotten or lost. They are very difficult to copy, share and distribute and the individual must have to present at the time of authentication [2]. These makes the biometrics-based system much more secure over other standard security systems.

5.1 Typical Biometric System

Most of the typical biometric system is based on the real-time identification process i.e. comparing the measurement of unique feature information of individual with the database which already contains several enrolled candidates. Figure 4 shows a typical biometric system.

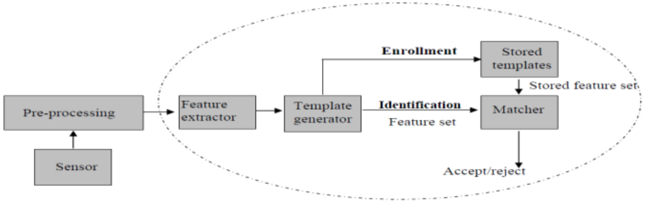


Figure 4：Evaluation Simplified block diagram representation of a biometric system

Sensor is the interface between the individual and the biometric system with collects the required data for processing. Advanced image processing techniques are used to enhance the acquire data removing noise or artefacts done in Pre-processing phase. Feature extractor generates the unique feature vectors for every individual which later is used for enrolment or matching process. Here template generator uses those feature vectors, one for enrolment by storing them in a database or comparing them with the existing data on that database by passing through a matcher. The output of the biometric system receives a decision from a similarity distance that is calculated with the aid of an algorithm that ultimately allows or restricts the individual for further operations. Based on the context and the application, a biometric system can be either i) a verification/ authentication or ii) an identification system. Verification can be termed as a process which affirms that the claimant, whose biometric information is already stored in the system, is actually the person he asserts to be. This is a 1:1 match verification process that takes in new biometric features and then collates them with the pre-existing ones in the database in order to confirm or deny a person's claimed identity. On the contrary, identification involves ensconcing a person's identity done through comparing extracted biometric information to the database.. It is a 1: N match verification operation. Since most databases tend to contain a large number of templates, it is said to be a more computationally expensive process.

5. 2 Categories of Physiological and Behavioral Trait

Categorically we can differentiate biometrics in two, i.e. physiological traits and the behavioral traits. In practice physiological characteristics of a person are relatively stable than the behavioral one. The main reason for that is the behavioral characteristic depending on some factors such as aging, injuries, or even mood. For example, the signatures of a person vary each time or the voice of the same may vary depending on the mood. Some possible behavior that can be used for biometrics are how one speaks, types on a keyboard, or walks. Generally, behavioral biometrics work best with regular use with low security. On the other hand, the physiological characteristics are the fingerprint, hand silhouette, iris pattern, blood vessel pattern of the retina, or DNA fingerprint which are essentially fixed and neither will change over the time nor it is possible to make alteration on that. That's why the intra-personal variation in physiological characteristic is much lesser than in a behavioural characteristic. Like, apart from injuries the iris pattern remains the same over time, whereas speech characteristics change and are influenced by many factors, e.g. the emotional state of the speaker. Therefore, it has been a harder job in compensating for those intra-personal variations for the behavioural based biometric system designers.

5.3 Properties of Biometrics

A Biometric system should meet certain predefined standards to achieve good performance at the authentication and matching levels. The following are the properties that are to be met:-

Invariance: The recognizable biometric characteristics should remain the same over a long period of time. It discards the requirement to update the biometric feature templates that are stored in the database. Simultaneously, it improves the recognition rate highly as a result of persistent usage and also reduces the complexity of the system. For example, a person's facial characteristics may change with age but the iris features remains constant throughout a person's lifetime.

Measurability and Timeliness: The process of extraction of biometric samples should be performed rapidly and with ease. For applications with real-time identification and authentication, the process must work fast and easily as it is one of the main requirements for continuous authentication. For example, in airports, biometric samples are taken at a distance and computation is done rapidly, that is, within the time, the subjects walk by the gate.

Singularity/Uniqueness: Identification and differentiation are the two main concepts on which biometrics work. To distinguish one person from the other, there should be enough unique properties of the biometric characteristics of each individual. One's characteristics should not match the others'. It should be distinct and unique. Singularity is a prime property of the biometric system. This implies to all biometrics barring the ones that present more unique and accurate features compared to others, i.e. iris contains more information than hand geometry.

Reducibility: The extracted feature templates in a biometric system should be reduced in size so that they can be easily handled and stored as long as they cannot be copied or duplicated. This is considered to be a crucial property especially when the information is transmitted over protected channels. Also when the controller of the results is located in a remote area.

Reliability: A biometric system should ensure that it is highly reliable and integrated as it becomes quite inconvenient and expensive to handle when the results declared by a biometric system is found to be inconsistent. Installation and handling of such a high end system is quite exorbitant, thus, its reliability should be checked primarily.

Privacy: The information extracted about a person should be kept confidential and is not to be leaked out under any circumstances. The privacy of an individual is of prime importance and should not be violated. If this property is not kept, people will become hesitant to use the biometric system.

Each of the above mentioned property is indispensable in a biometric system and must be ensured in order to provide accurate authenticated results.

Biometric systems can be classified according to six perspectives as follows:-

Overt / covert: Biometric system applications that are performed with the knowledge and co-operation of the user is said to be an overt application where the user is aware that his biometric data is being acquired. On the contrary, applications which are performed without the user's knowledge is termed as a covert application. People are concerned about their privacy in covert applications such as at an airport checkpoint; face images of passengers are captured and compared to a watch list without their knowledge. In overt applications, data acquisition and sample quality are of high standards since they are taken in a controlled environment, unlike in covert applications which are taken in an uncontrolled environment without the user's knowledge and as a result the quality of the captured images can be problematic.

Attended / non-attended:- When a biometric recognition process is performed, if the user is under the guidance of supervisors, then the process is said to be an attended one, while, in a non-attended process, there are no supervisors to help or attend the user and user co-operation does not exist in such processes. In attended processes, biometric samples are of better quality than the ones acquired during a non-attended process.

Standard / non-standard environment: An environment is said to be a standard one when the processes performed are controlled and recognition is done indoors within a constrained environment. On the contrary, in a non-standard environment, none of the before mentioned conditions exist. For example, customs and airport security systems are considered standard since the entire biometric recognition process is completed in a controlled environment.

Habituated / non-habituated: The recognition process of a biometric system is said to be a habituated one if the users interact with the biometric system on a daily/frequent basis. When the system's usage frequency is low, the recognition process is performed in a non-habituated mode. The degree of cooperation and training demanded from the users is a point of relevance in this matter.

Public / private: If the users of the biometric recognition system are not employees of the organization or work in the organization that uses the system, then the application is considered to be a public one. If the users are employees, then the application is said to be a private one. An example of a private application is internal bank security where employees are asked to provide their biometric features voluntarily for authentication.

Open / closed: The biometric system is said to be a closed one if completely proprietary formats are used by the system. On the other hand, when the system is allowed to share and exchange data with other systems then it is termed as open and privacy issues should be addressed properly.

The probability distribution of genuine and imposter matching score is uses for measuring performance of a biometric system. Comparing two feature sets of the same individual validate the genuine matching score, while comparing the feature sets of two different individual generate imposter matching score. It reflects that the two feature sets belong to the same individual if the matching score is higher than a certain threshold; otherwise it is assumed to come from two different individuals. Therefore two most common types of error can occurs in a biometric system are i) false rejection (type I error) and ii) false acceptance (type II error). The false rejection error will occurs if the threshold is higher than the genuine matching score which means the legitimate user is rejected. On the other hand, false acceptance error will occur if the threshold is lower than the imposter matching score indicating the illegitimate user is accepted as someone else. Now the probability of accepting the imposter one as a legitimate user is known as the false acceptance rate (FAR) while that of denying a genuine user is been called false rejection rate (FAR). (Figure 5). Now, we can show the relation between false rejection rate and false acceptance rate by plotting receiver operating characteristic curve (ROC). In that curve, false rejection represents the percentage of genuine scores not exceeding the certain threshold where false acceptance represents the imposter scores exceeding that threshold. In the plot where both false rejection rate and false acceptance rate are equal is called equal error rate (EER) (Figure 6). The EER is a parameter that gives valuable information about the quality of a biometric product or method. However, this information is generally not sufficient. A related but more specific quality measure obtains closer information by determining how fast the two error rate functions FAR and FRR increase when moving the security level away from the optimal EER point (Equation 1).

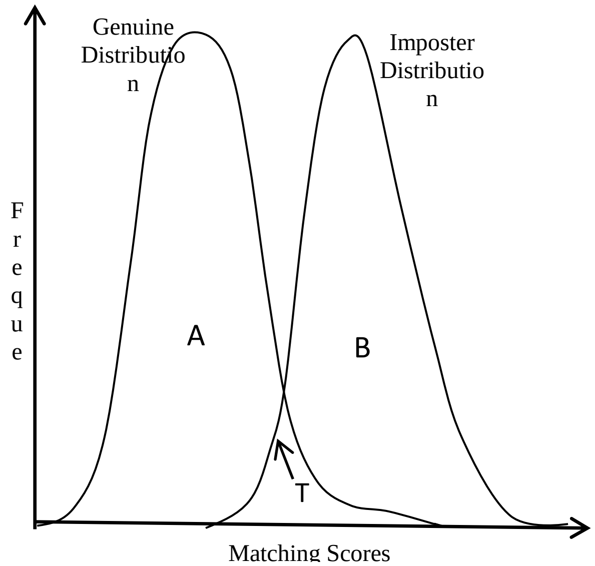


Figure 5: Evaluation of the matching accuracy of a biometric system. Histograms of the genuine and impostor matching scores are represented as well as the two types of errors that can arise in a biometric system given a matching score threshold (T). The areas A and B represent false accept rate (FAR) and false reject rate (FRR), respectively.

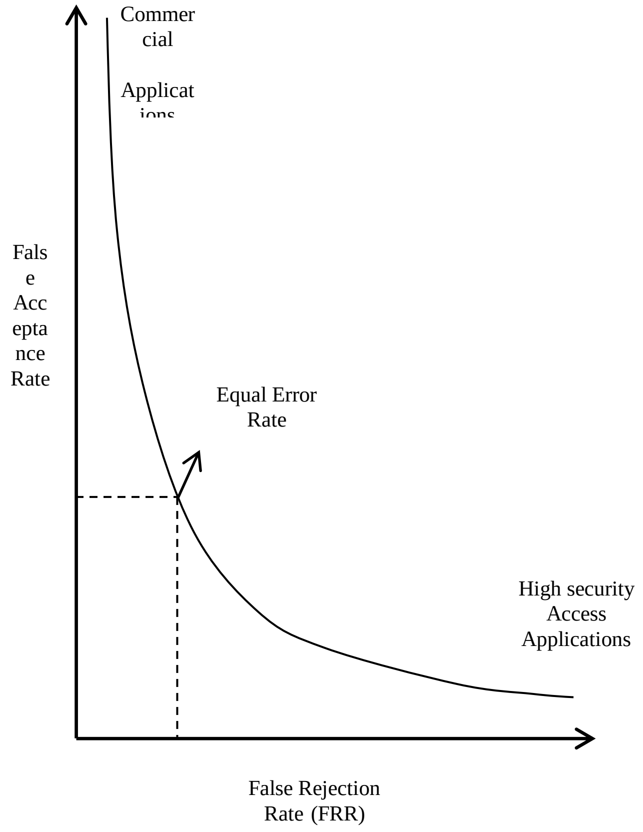


Figure 6 : Receiver operating characteristic curve (ROC) showing the relation between false acceptance and false rejection in a biometric system.

For this purpose, a fixed value Δ =5 % is considered and the size of the zone where FAR(λ) and FRR (λ) are both below EER + Δ is calculated. Figure 7 shows the two curves for FRR and FAR with the crossover point at the EER. The area A between the horizontal line for EER + Δ and the two curves represents the measurement for the discriminatory power and can be calculated with

$$A = (EER + \Delta)(\lambda_1 - \lambda_0)\int_{\lambda_0}^{\lambda_{EER}} FAR(\lambda)d\lambda - \int_{\lambda_{EER}}^{\lambda_1} FRR(\lambda)d\lambda \quad (1)$$

In practical applications it is often difficult to determine an adequate security level λ. Many biometric systems show substantial FAR and FRR deviations for only small changes from the theoretically optimal λ_{EER}. This makes it difficult to fine-tune the security level λ. However, methods with a large A are less prone to minute changes in λ and are thus more robust and have a larger discriminatory power.

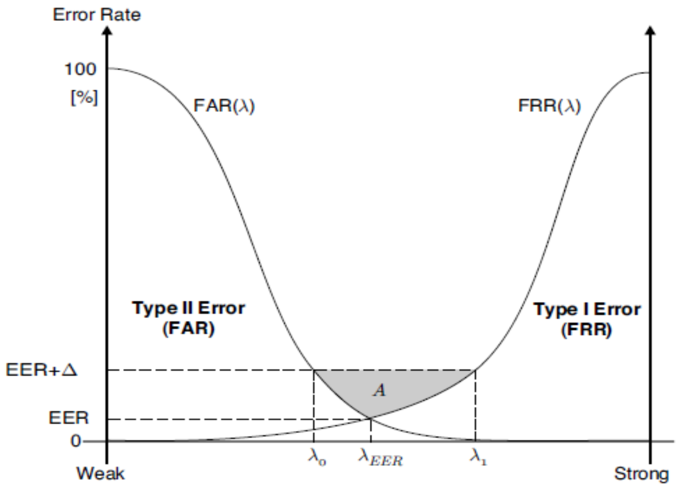


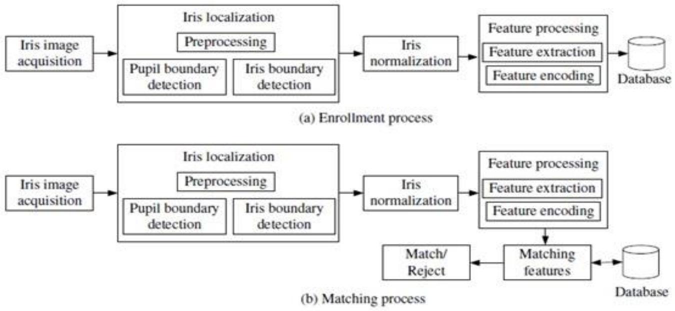
Figure 7: Plot of the dependencies of FAR, FRR from the security level.

The performance measure independent of threshold of a system can be calculated through EER, whose lower value indicates better system performance. The total error rate which is calculated as the sum of the False Accept Rate (FAR) and the False Reject Rate (FRR) at the point of the EER decreases. It is also important to mention that generally, in watch list applications, it is preferable that the biometric system produce a low FRR while in a high security context, the objective is to obtain a low FAR. Besides these types of errors, in some cases, some individuals cannot provide good biometric data (i.e. poor quality fingerprint ridges) since they do not have the biometric feature from which there can be produced repeatable templates. The expected proportion of the population for whom the biometric system is unable to obtain good templates is called the failure to enrol rate (FTE). Similarly, a system may also be unable to capture or locate an image of sufficient quality (Mansfield et al. (2002)). For example, this could be because of worn, cut or unrecognizable prints as well as the quality of the captured image is inadequate. In this case, the expected proportion of cases that failed to provide good features is called the failure to acquire rate (FTAR).

5.4 Iris Recognition

The structure of iris is has multiple layers. The posterior layer is composed of epithelial cells having iris pigments whereas the anterior layer has two sets of muscles, one is the sphincter muscle and the other is the dilator muscle. The contraction and release of the pupil of our eye is dependent on the sphincter and the dilator muscle respectively. The stromal layer that is composed of collagenous tissues is found in the anterior side. The major portion of an iris image is generated with the help of this muscle.

Iris recognition is one of the highly evolved technologies in biometrics. The basic characteristic of iris makes it an obvious choice for modern biometric system and researches. Human iris contains rich amount of unique texture not only for two different subjects, even we also have two distinct patterns in our two different eyes. This makes iris features extremely accurate for user identification. Yet, there are still some issues which restricts iris recognition to a limitation for practical use. The main reason is the structure of an iris. The small diameter of the iris makes it very difficult to be imaged at high resolution without sophisticated camera systems. Any conventional system needs the user cooperation for image capturing as user must adjust the position of his eyes with the position of the camera for accurate feature extraction process while being captured. Any distortion or movement can restrict the capturing from successful imagining. This step is crucial in iris recognition as for using iris features, proper segmentation and localization of the iris region is required. Many iris localization techniques exist and have been developed. Figure 8 illustrates the major stages of a typical iris recognition system. The initial stage is image acquisition process involved in imaging techniques to get the iris texture images.



(a) Enrollment process

(b) Matching process

Figure 8 : Stages for typical iris recognition system for both enrolment and matching process

5.5 Imaging System

Lighting source implementation is the main point of difference between this two imaging system. The daugman system implementation comprises lateral light sources whereas the wilds system applies the diffuser to illuminate the entire eye region [3]. The Daugman system is shown in Figure 9 which demonstrates the position of the light source to the side of the eye. The camera captures the reflected light after passing through a beam splitter. The resulting iris image has a diameter ranging from to pixels, which gives enough information for iris recognition. On the other hand, the Wildes imaging system applies a series of light sources, illuminating the iris region through a diffuser and a circular polarizer (Figure 10). Using this system, the captured iris image has a diameter of around pixels. The Wildes system generates iris images with reduced specular reflections compared to a single light source system since it uses an evenly distributed light illumination system.

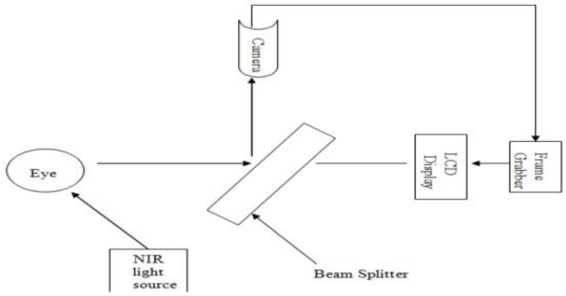


Figure 9 : Daugeman imaging system

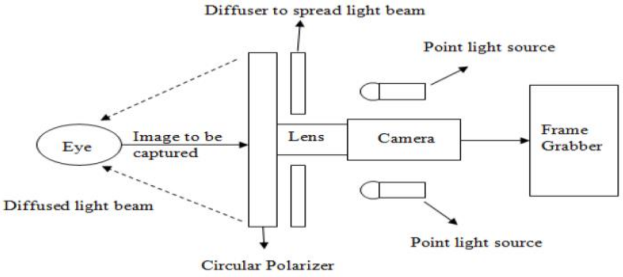


Figure 10 : Wildes Imaging System.

5.6 Iris Pattern Texture and Colours

Various components compose the iris texture features within the iris. They are crypts, furrows, arching, collarets and rings of various shapes (Figure 11). Different colour pigments are also associated with the iris pattern such as red, green, and blue. The melanin pigments combine in a certain arrangement and generate the natural iris colours, mostly in the anterior and stromal layers. Visible light passes through the iris and the absorption and reflection of light depends on the wavelength of the light. The variation in the pigment density and the amount of reflected light is accountable for the determination of iris colour.

In iris recognition, near infrared (NIR) cameras are more preferable than visible light which accentuates the iris texture pattern, particularly for darker regions. The wavelength spectrum of the NIR camera ranges from 700nm to 900nm . NIR imaging is widely used all over the globe in the field of iris recognition because of the fact that NIR illumination is a more comfortable imaging modality for subjects in comparison to regular light source.

A unique and rich texture of the iris can be used in high security applications. The exclusive and varied texture patterns in the iris images are "determined epigenetically by random events in the morphogenesis process" . Genetically identical images from the left and right eye of the same individual were taken put under scrutiny. After cross-comparisons, it was shown that that the statistical distributions were the same for iris images coming from genetically related and genetically unrelated subjects. In order for any upcoming biometric technology to be accepted by the community, an independent party is required to perform certain functions:-

- performing evaluations
- designing the protocols
- collecting the data sets
- supervising the tests and
- analyzing the results (Philips et.(2000))

The iris recognition systems use certain standards and frameworks that indicate the level of accuracy of a typical iris recognition system. The FNMR, FMR and the detection error rate curve are used for this purpose. The International Biometric Group (IBG), the Authenti-Corp and the National Institute of Standards and Technology (NIST) performed various evaluations using different iris recognition systems to test and analyze its accuracy and performance levels.

The accuracy of the Daugman algorithm was further testified by a project conducted by the University of Cambridge and United Arab Emirates interior ministry which stated that for 632500 iris images acquired in the Middle East and over 200 billion cross-comparisons generated between different eyes that a false match rate (FMR) of less than 1 in 200 billion was achieved. The US Department of Homeland Security funded an experiment named ITIRT for border control and security access consulting. The experiment was performed in July 2004 on several state-of-the-art iris recognition systems such as: “Iridian Kno Who OEM SDK”, “LG Iris Access 3000”, “Oki IRISPASS-WG” and “Panasonic BM-ET300”. In this experiment, more than 100,000 iris images were acquired using different devices at different times. These images were taken from people belonging to different ethnic cultures as well as different age groups. In order to get the false accept rate, the false reject rate, the failure to enrol and the failure to acquire rates, the image templates were compared. The generic version of the Daugman algorithm was implemented for feature extraction and matching algorithms. To indicate the error rates, the FNMR at FMR of 0.001 was used. The Panasonic BM-ET300 module achieved a FNMR of around 0.014. The Oki system achieved a FNMR of around 0.03 at an FMR of 0.001. The LG unit achieved a FNMR of around 0.038 . This ensures that very high identification rates, a strong inter-operability and repeatability are achieved through all the tested iris recognition systems.

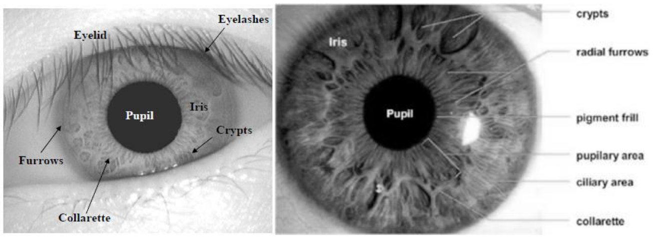


Figure 11: Example of an Iris Image

5.7 Iris Localization and Segmentation

Iris localization and segmentation has proved to be a critical step in the process of iris recognition since it has a severe impact on the system's performance. This particular portion of the algorithm segments the specific iris region from an eye image by locating certain features like the exact iris boundary, the pupil region, and the upper and lower eyelids. Eyelash occlusion, eyelid occlusion and/or noise can combine to create artefacts in the resulting iris image. In order to remove these artefacts successfully, advanced algorithms are required to generate a clean iris region for further recognition. To identify and eliminate different artefacts in iris images various methods have been proposed. Some of them are detection and removal of eyelash occlusion and elimination of specular reflection. In general, most algorithms perform reasonably well except that they tend to overestimate eyelash occlusion.

5.8 Pupil and Iris Localization

Daugman proposed the integro-differential operator that locates the pupil, the iris inner and outer boundaries as well as the upper and lower eyelid boundaries.

$$max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right| \quad (2)$$

$$G_\sigma = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{(r-r_0)^2}{2\sigma^2}} \quad (3)$$

In the above mathematical expression, *I(x,y)* represents the eye image, *r* is a parameter that corresponds to a circle of diameter *r* and (x_0, y_0) are parameters that subsequently correspond to center coordinates (x_0,y_0) respectively. $G_\sigma(r)$ is a radial smoothing

Gaussian function with center r and standard deviation σ. This function searches the entire eye image for integrations along various circular outlines with (x_0,y_0) as its center coordinates and an increasing radius *r*. The maximum contour integral derivative is achieved and then classified as the most acceptable circle tracing the iris. Similarly, for localization of the circular boundaries for the pupil and iris regions, the entire iris image is searched for the maximum integration along various circular contours.The upper and lower eyelids are approximated with two open curves that are part of two different circles. In the iris recognition process, further feature extraction can be accomplished by considering the iris region surrounded by the upper and lower eyelids as well as the extracted circular pupil and iris boundaries (Figure 12).

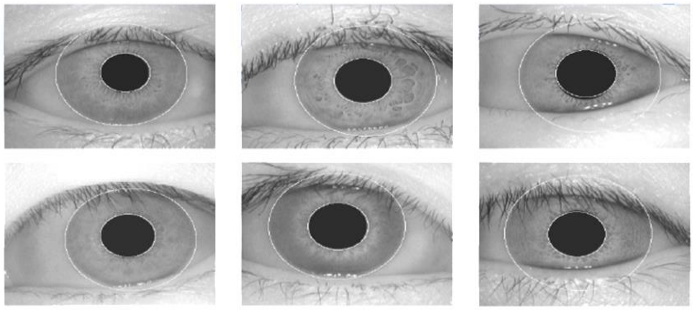


Figure 12: Detected Curvilinear Boundaries

The integro-differential uses the first derivatives of the image and search for geometric parameters, so considered as a variation of the Hough transform. Unlike Hough transform, it does not suffer from threshold problems, since it works with raw derivative information. However, the algorithm works on a local scale and can fail where there is noise in the eye image, such as from reflections.

6. HOUGH TRANSFORM

The Hough transform is a standard algorithm representing computer vision used to determine the parameters of simple geometric objects, present in an image, mostly containing lines and circles. Its circular form can be employed to deduce the centre coordinates and length of radius of the pupil and iris regions. An automatic segmentation algorithm based on the circular Hough transform is employed [8-11]. The circular Hough transform is used to locate circular contours in images. This transform is implemented directly on an intensity gradient edge map usually obtained through a gradient-based edge detector. First, the entire iris image *I(x,y)*is smoothed with a Gaussian filter *G(x,y)* with centers (x_0,y_0) and a standard deviationσ *of 3/4* (equation 3 and equation 4). Then, the intensity gradient image map *M(x,y)* is generated from the smoothed image *F(x,y)*, as shown in equation (5) using the gradient operation defined in (6). Subsequently, the binary edge map is generated by setting a threshold on the intensity gradient image *M(x,y).* The threshold is usually determined based on experimental data and depending on the application. Finally, using the binary image map, the Hough transform is performed to locate a circle with the largest number of edge points and with circular parameters(x_0,y_0,r) calculated as shown in equation (7). (x_0,y_0,r) represents a circle to be located within the iris image such that the circle is characterized by a radius *r*and center coordinates $(x_0,y_0)$with possible edge point (x_i,y_i).

$$F(x,y) = G(x,y) * I(x,y) \qquad (3)$$

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{-\frac{(x-x_0)^2+(y-y_0)^2}{2\sigma^2}} \qquad (4)$$

$$M(x,y) = |\nabla F(x,y)| \qquad (5)$$

$$\nabla \equiv \left(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}\right) \qquad (6)$$

$$(x-x_0)^2 + (y-y_0)^2 = r^2 \qquad (7)$$

From here, the entire collection of edge points is implemented with the Hough transform. Whenever equation (7) is satisfied, it means that the circular contour goes through (x_0,y_0),and one extra vote is added to the histogram count for possible circular contours. After scanning of the entire image all possible contours, the contour that obtained the highest amount of votes represents the most likely circle in the edge map.

7. ACTIVE CONTOUR MODEL

The Discrete Circular Active Contour (DCAC) model can also be used to locate the pupil and iris boundaries in an iris image. The variance image is computed from the original iris image to localize the pupil region. An active contour model is formed by the so-called "internal and external" forces with a starting point in the center of the pupil is initiated and moved within the iris image. Along the active contour, the vertex *v* moves from time *t* to time *t+1* according to the following equation:-

$$v_i(t+1) = v_i(t) + F_i(t) + G_i(t)$$

Where v_i represents the position of the vertex at a specific time *t*, F_i, G_i represent the internal and external forces, respectively.

The continuity and other prior knowledge about the iris are the characteristics of the internal force. The external force is directly related to the gray-scale intensity values within and outside the vertex, which also includes the iris region. After an extensive iterative contour searching operation which ends when equilibrium with minimum energy or minimum mean variance of the annulus is attained, the iris is segmented. In spite of showing good results, DCAC suffer from few limitations such that the performance of this method greatly depends on the iris image quality. For instance, if the image contains severe noise, specular reflections or distortions, the method will fail in locating the proper boundaries [12].

8. ROCHE AND AVILLA'S METHOD

This method is template-based and similar to Daugman's method [13]. It applies the histogram stretch to maximize the average intensity difference on the grayscale input image. The intensity differences of five circumferences with consecutive radius values:

$$D = \sum_j \left(\sum_{k=1}^{5} \left(I_{i,j} - I_{i-k,j}\right)\right)$$

Where

$$I_{i,j} = I(x_0 + i\Delta_r \cos(j\Delta_\theta), y_0 + i\Delta_r \sin(j\Delta_\theta))$$

and Δ_r andΔ_θ are the increments of radius and angle and $I(x,y)$is the image intensity. It searches in the $\mathbb{N}^3$ space for three circumference parameters (center (x, y) and radius r) where the difference between the average intensity of five successive circumferences is maximal.

9. NOISE AND ARTIFACTS

Noise & artifacts in iris images have proved to be quite detrimental. Thus, to achieve higher system performance and better accuracy in the image processing steps within an iris recognition system, noise and artifacts should be reduced or eliminated, if possible. The eyelash occlusion, the eyelid occlusion and specular reflections comprise of these artifacts. As seen in Figure 12, the iris image includes severe eyelash and eyelid occlusion. Hence, the top eyelid covers a part of the iris and some eyelashes are spread across the iris area which will affect the system's performance. During the iris image acquisition procedure, specular reflections occur. During this process, the light source gets reflected and imaged by the camera. Figure 13 shows one example of specular reflection seen on the iris region as a "white spot" due to deviation from original iris patterns resulting from high pixel values. It constitutes a major source of distortion.

Eyelashes are of two types: separable (isolated in the image), and multiple (bunched together and overlap in the eye image). The convolution of a Gaussian smoothing function with a separable eyelash results in a low output value, helping them to be detected using 1D Gabor filters. Thus, it can be concluded that a point belongs to an eyelash if a resultant point is smaller than a threshold. In the issue of detecting multiple eyelashes, if the variance of intensity values in a small window is lower than a threshold, the centre of the window is considered as a point in an eyelash. There must be connectivity between each point in an eyelash to another point in an eyelash or to an eyelid, termed as the connective criterion. Specular reflections along the eye image always have higher intensity values than any other region, hence detected using thresholding[3-7].

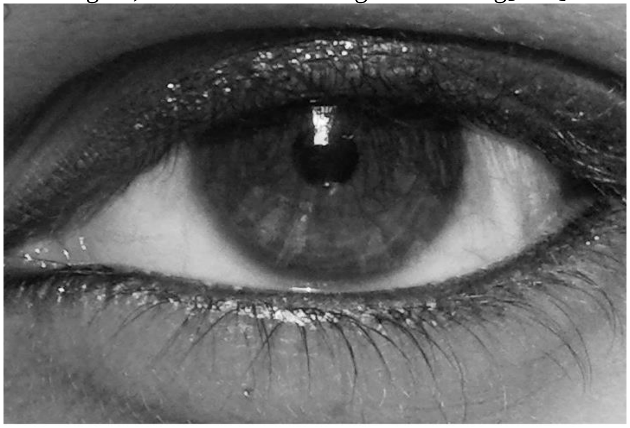
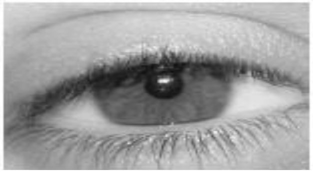
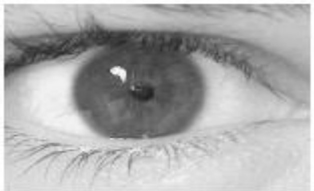
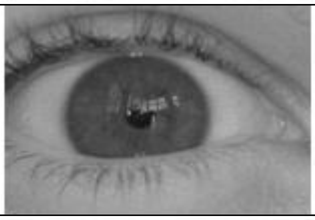
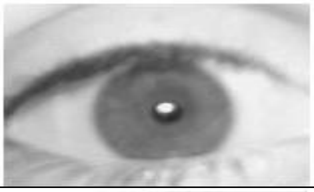
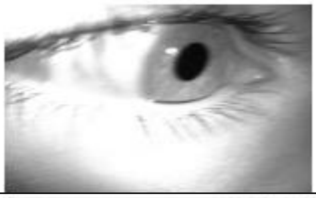
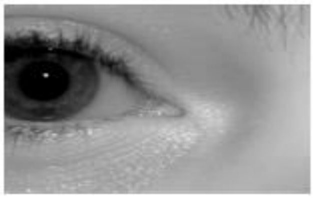
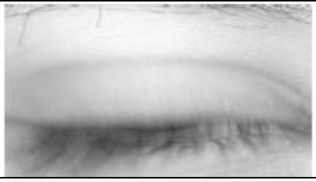
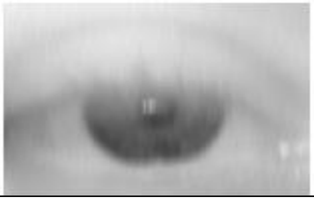


Figure 13: Iris image showing severe specular reflection

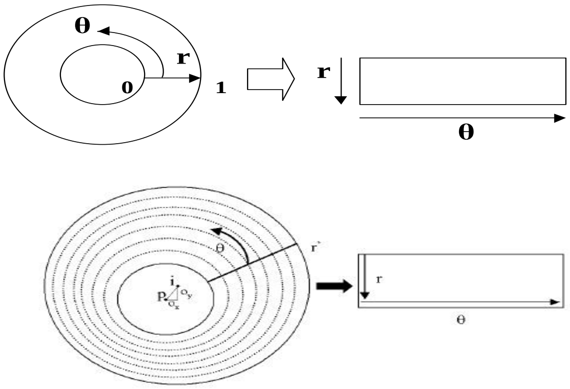
The following table 1 shows few examples of iris noise images:

Table 1 : Few examples of iris noise and artifacts images

Different iris noises	Image examples
Eyelid and eyelash occlusions	
Lighting reflections	
Specular reflections	
Out-of-focus	
Off-angle iris	
Partial captured iris	
Out-of iris images	
Motion blurred irises	

10. SIZE-INVARIANT UNWRAPPING AND REPRESENTATION

In this section, a technique to normalize the iris region after proper segmentation in order to obtain a size-invariant rectangular representation of the original iris pixels is described. This technique, known as the “Daugman’s Rubber Sheet Model”, maps the sampled iris pixels from the Cartesian coordinates to the normalized polar coordinates in order to accomplish a size-invariant sampling of the original iris points. He presented a framework that examined more disciplined methods for detecting and modelling the iris inner and outer boundaries with active contours for more flexible embedded coordinate systems. Active contours enhance iris segmentation, allowing noncircular boundaries and enable flexible coordinate systems. In his paper, off-axis gaze can be handled, through Fourier-based approached for iris projective geometry, by detecting it and “rotating” the eye into orthographic perspective. The Fourier-based trigonometry arises from the observation that Fourier series expansions of the coordinates of the detected pupil boundary contain information on shape distortion related to deviated gaze, within the relationships among the real and imaginary coefficients of the lowest frequency term when expanding each of those series. Finally the statistical inference of eyelashes and their exclusion can be handled by statistical estimation methods that essentially depend on the fact whether the distribution of iris pixels is multimodal, that needs to be determined [3]. Figure 14 illustrates the results.



Centers of iris and pupil coincide   Centers of iris and pupil do not coincide

Figure 14: Normalization of iris image through the Daugman's Rubber Sheet Model

For every pixel in the iris, Daugman’s rubber sheet model, finds an equivalent position on the polar axes(r,θ), where r is the radial distance and theta is the rotated angle at the corresponding radius. The number of data points in the radial direction refers to the radial resolution while the number of radial lines generated around the iris region refers to the angular resolution. Using equation the iris region is transformed to a 2D array with horizontal dimensions corresponding to the angular resolution and the vertical dimension to radial resolution (Figure 14).

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

where $I(x,y)$ corresponds to the iris region, (x,y) and $(r,\theta)$are the Cartesian and normalized polar coordinates, respectively. θranges from 0 to 2π and r from 0 to 1 . $x(r,\theta)$and$y(r,\theta)$ are defined as linear combinations of pupil boundary points. The following equations perform the transformation:-

$$x(r,\theta) = (1-r)x_p(\theta) + x_i(\theta)$$
$$y(r,\theta) = (1-r)y_p(\theta) + y_i(\theta)$$
$$x_p(\theta) = x_{p0}(\theta) + r_p\cos(\theta)$$
$$y_p(\theta) = y_{po}(\theta) + r_p\sin(\theta)$$
$$x_i(\theta) = x_{i0}(\theta) + r_i\cos(\theta)$$
$$y_i(\theta) = y_{i0}(\theta) + r_i\sin(\theta)$$

where (x_p, y_p) and (x_i, y_i) represent the pupil and iris coordinates along the theta direction, respectively. $(x_{p0,}y_{p0})$ and $(x_{i0,}y_{i0})$ correspond to the pupil and iris centre coordinates. After mapping the iris region from the circular Cartesian scale to the rectangular polar scale, two different instances can occur with the rubber sheet model. If the pupil and iris boundary centres are located at the same pixel point, the sampled points are uniformly distributed across the iris region, as shown in Figure 15 On the other hand, if the centre of the iris circular boundary and the centre of the pupil circular boundary are different, the feature points are then sampled non-uniformly within the iris region. In order to deal with this situation, a series of sampling lines are emitted from the centre of the pupil circle, and rotated along the circumferential direction for 360 degree. Afterwards, a fixed number of sampled points are taken inside the iris region along each sampling line, as shown in Figure 16.

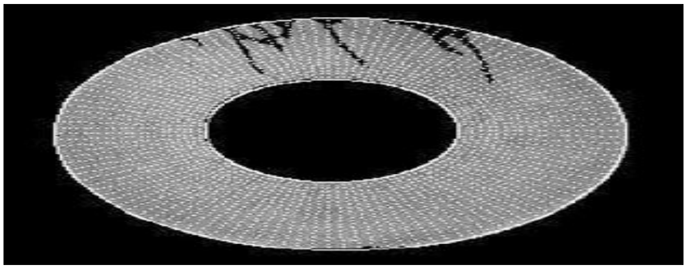


Figure 15: Uniform feature points sampling

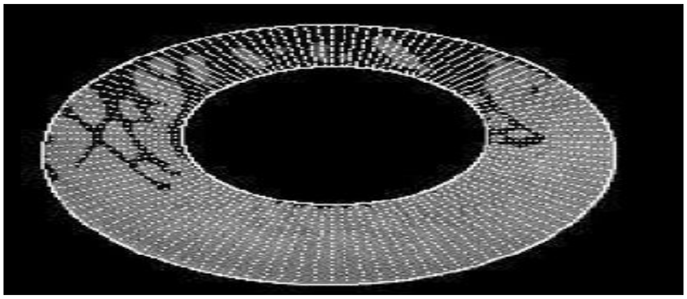


Figure 16: Feature points sampling with displaced pupil and iris centers.

The model produces a size-and-translation-invariant representation in the polar coordinate system to compensate pupil dilation and size inconsistencies. However rotational inconsistencies are not compensated here which needs to be computed during matching that requires shifting the iris templates in the θ direction until two iris templates are aligned.

11. WILDS MODEL

The Wildes et al. proposed a technique for image registration which geometrically warps a newly acquired image alignment with a selected database image [12]. In this system the intensity of new image for each coordinate values are made to be close with the corresponding points of the reference image for choosing a mapping function to transform the original coordinates. The mapping function must be chosen so as to minimise

$$\int_x \int_y \left(I_d(x,y) - I_a(x-u, y-v)\right)^2 dxdy$$

while being constrained to capture a similarity transformation of image coordinates to (x, y) to (x', y'), that is

$$\binom{x'}{y'} = \binom{x}{y} - sR(\varphi)\binom{x}{y}$$

with*s* a scaling factor and R(φ)a matrix representing rotation by φ. In implementation, given a pair of iris images I_a and I_d, the warping parameters s and φ are recovered via an iterative minimisation procedure.

12. BOLES MODEL

W. W. Boles *et al* presented a new approach for biometric identification technique based on iris recognition using wavelet transform. They have introduced a new technique in their paper to represent the features of the iris, based on the WT zero-crossing representation, by fine-to-coarse approximations at different resolution levels. As the essential requirement for the accurate extraction of iris features for successful processing needs to ensure the reparative image capturing to produced irises in the same location within the image, had the same resolution, and were glare free under fixed illumination in many cases, they have offer such freedom in image capture because it is translation and size invariant, also tolerant to illumination variations and insensitive to any glare resulting from the reflection of the light source on the iris surface using wavelet transform, that helps in pattern matching under local distortions [4].

13. FEATURE EXTRACTION

13.1 2D Gabor Filter

A Gabor filter is constructed by the modulation of a sine/cosine wave with a Gaussian. In this, the sine wave is localised only to the frequency and so it provides the optimum conjoint representation of a signal as it is localised to both frequency and space. The modulation of the sine with a Gaussian provides localisation in space with the cost of the loss of localisation in frequency. A quadrature pair of Gabor filters are used for decomposing a signal, with a real part specified by a cosine while the imaginary part specified by a sine, both modulated by a Gaussian. The real filter forms the even symmetric component while the imaginary one forms the odd symmetric one. The width of the Gaussian specifies the bandwidth of the filter and the centre frequency of the filter is specified by the frequency of the sine/cosine wave.

A 2D Gabor filter over the an image domain (x,y) can be represented as-

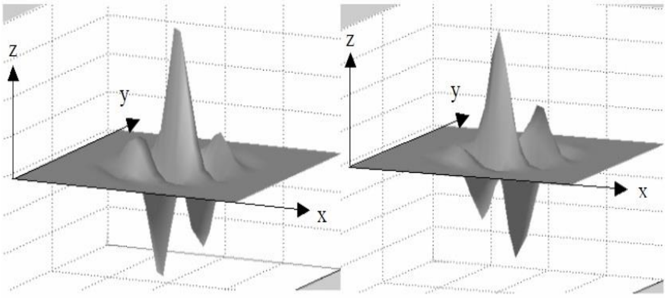


Figure 17 :A quadrature pair of 2D Gabor filters: (left) real component or even symmetric filter characterized by a cosine modulated by a Gaussian; (right) imaginary component or odd symmetric filter characterized by a sine modulated by a Gaussian.

Daugman's uses 2D versions of Gabor filters in order to encode the iris pattern data in the normalized polar coordinates in his iris recognition system. The filter wavelet function can be described as follows:

$$H(r,\theta) = e^{-i\omega(\theta-\theta_0)} e^{-\frac{(r-r_0)^2}{\alpha^2}} e^{-\frac{i(\theta-\theta_0)^2}{\beta^2}}$$

where$(\alpha, \beta)(\alpha, \beta)$specify the effective width and length, (r_0, θ_0) specify the centre frequency of the filter andωrepresents the wavelet angular frequency.

The feature encoding process begins by sampling a collection of feature points from the original iris image into the Cartesian coordinates. Afterwards, these feature points are unwrapped into a matrix representation in the normalized polar coordinates using the Daugman's rubber sheet model.

A Gabor filter bank is applied to the matrix which is then decomposed into a set of complex coefficients h at (r_0, θ_0) location as follows:

$$h_{\{Re,Im\}} = sgn_{\{Re,Im\}} \int_r \int_\theta I(r,\theta) e^{-i\omega(\theta-\theta_0)} e^{-\frac{(r-r_0)^2}{\alpha^2}} e^{-\frac{(\theta-\theta_0)^2}{\beta^2}} rdrd\theta$$

where $h_{\{Re,Im\}}$ can be regarded as a complex valued bit whose real and imaginary components are dependent on the sign of the 2D integral and$I(r,\theta)$ is the raw iris image where r and θ represent the dimensions along the radial and circumferential directions in the normalized polar coordinates, respectively. Once the complex coefficients are calculated, the complex domain is divided into four phases or quadrants, and each phase is represented by two binary bits (Figure 18).

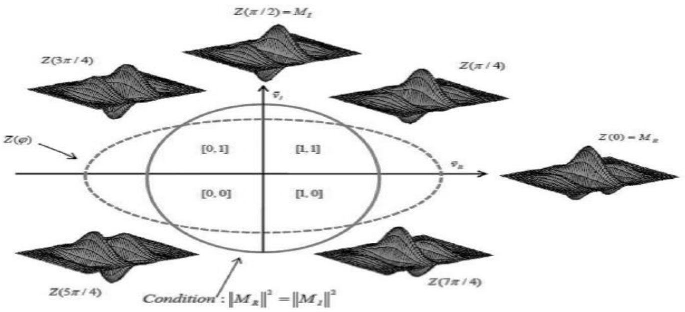


Figure 18 : Demodulation and Phase quantization.

Data compression has been achieved here by Daugman by demodulation of the output of the Gabor filters, done by quantisation of the phase information into four levels, for each possible quadrant in the complex plane. It has been shown by Oppenheim and Lim [14] that phase information, rather than amplitude information provides the most significant information within an image. In this process, discriminating information on the iris can be encoded with the phase component, but it discards redundant information such as illumination that requires the amplitude component. So each pixel in the normalised iris pattern is represented by two bits of data in the iris template to represent four levels. A total of 2048 bits are calculated for the template, while the corrupted regions within the iris are masked out using equal number of masking bits. Thus an efficient storage and irises comparison is obtained through a compact 256-byte template.

This process which includes Gabor feature extraction and phase encoding is repeated on the entire iris image. One set of Gabor filter banks will extract one pair of complex phases for each feature point. For example, by applying *k* sets of Gabor filter banks on an unwrapped image template of size $M \times N$, a phase matrix of binary bits will be created with size $2kM \times 2kN$. This will be the binary iris template that is used for the Hamming distance calculation[13-15].

13.2 Log-Gabor Filter

In the Gabor filter whenever the bandwidth in larger than one octave the even symmetric filter produce a DC component [15]. Brady et al. [16] proposed a model which uses Gabor filter that is Gaussian on a logarithmic scale, that eventually eliminate its DC component. This is known as the Log-Gabor filter. The frequency response of a Log-Gabor filter is given by

$$G(f) = exp\left(\frac{-(log(f/f_0)^2)}{2(log(\sigma/f_0)^2)}\right)$$

where f_0 and σ represent the centre frequency and the filter bandwidth, respectively.

For unwrapped iris matrix features encoding the intensities of each row corresponds to a ring of pixels centred at pupil centre. For extracting phase feature templates the Log-Gabor filter is applied to the 1D image vectors. Using normalization process involves the iris region is unwrapped from the circular shape represented through Cartesian coordinates to a rectangular matrix represented through normalized polar coordinates, the spatial relationship along the concentric sampling rings and the radius become independent. When 2D Gabor filter multiplexes over the normalized polar scale, the feature extraction mechanism will basically mix the relative spatial. Therefore, it applies a symmetric Gaussian envelope to the normalized polar image representation that is not supposed to be treated evenly between radial and circumferential directions. On the other hand, the 1D Log-Gabor filter avoids mixing the relative position information between the radial and the circumferential directions as it extracts the feature vector from each row of the normalized matrix representation.

13.3 2D Hilbert Transform

To extract the features from a normalized rectangular iris image from the daugman's rubber sheet model 2D Hibert transform can be used [10]. Here, the analytical signal $z_x(t)$ becomes:

$$z_x(t) = x(t) + jHx(t)$$

where $z_x(t)$ represents the 1-D complex feature vector generated from original signal $x(t)$, and H stands for the Hilbert transform. As it calculates the instantaneous phase and frequency in the same way as the Gabor transformed phase template in the Daugman's system, only the complex phase information is considered to compute as the iris feature template.

13.4 Zero-Crossing Of 1D Wavelet

Boles and Boashash [4] uses 1D-wavelets for encoding iris pattern data which defined as the second derivative of a smoothing function *θ(x).*

$$\Psi(x) = \frac{d^2\theta(x)}{dx^2}$$

The zero crossings of dyadic scales of these filters are then used to encode features. The wavelet transform of a signal *f(x)* at scale s and position *x* is given by

$$W_s f(x) = f * \left(s^2\frac{d^2\theta(x)}{dx^2}\right)(x) = s^2\frac{d^2}{dx^2}(f * \theta_s)(x)$$

Where $\theta_s = ({}^1/_s)\theta({}^x/_s)$

$W_s f(x)$ is proportional to the second derivative of *f(x)* smoothed by $\theta_s(x)$, and the zero crossings of the transform correspond to points of inflection in $f * \theta_s(x)$. Significant features with the iris region are represented through zero-crossings.

D. M. Monro*et al* sincerely investigated potentially reliable iris matching as a means of feature extraction for later classification using zero crossings of a one dimensional Discrete Cosine Transform (DCT) and find some critical problems still persist such as system robustness, consistent performance under variability, speed of enrolment and recognition, and no cooperative identification. Subsequently they have proposed a novel iris coding method based on differences of discrete cosine transform (DCT) coefficients of overlapped angular patches from normalized iris images and a small subset of coefficients which used to form sub feature vectors. The feature extraction capabilities of the DCT are optimized on two data sets that provide perfect Receiver-Operating Characteristic (ROC) Curves with no registered false accepts or rejects delivering 100 per cent Correct Recognition Rate (CRR). A new worst-case metric for predicting practical system performance in the absence of matching failures also stated in their research [6].

13.5 Haar Wavelet

Lim et al. [17] also use the wavelet transform (Gabor transform and Haar Wavelet as mother wavelet) to extract features from the iris region. From multi-dimensionally filtering, an 87-dimension feature vector is computed whose real value ranges from -1.0 to +1.0. The feature vector is sign quantised to represent any positive and negative value by 1 and 0 respectively, resulting in a compact biometric template consisting of only 87 bits.

The recognition rate of Haar wavelet transform is 0.9% better than Gabor transform by comparison of Lim et al.

13.6 Laplacian Of Gaussian Filters

Wildes et al. system encodes the feature by decomposes the iris region with use of Laplacian of Gaussian filters, are given as

$$\nabla G = -\frac{1}{\pi\sigma^4}\left(1 - \frac{\rho^2}{2\sigma^2}\right)e^{-\rho^2/2\sigma^2}$$

where σ is the standard deviation of the Gaussian and ρ is the radial distance of a point from the centre of the filter.

This filter compressed the data a certain significant level. The filter image is represented as a Laplacian pyramid which is presented by Burt and Adelson in their paper [18]. To generate a compact iris template, four different resolution levels have been used and a Laplacian pyramid is constructed.

14. MATCHING & DISTANCE MEASURE

Using one of the previously described feature extraction schemes, an iris image is processed and transformed into a unique representation within the feature space. In order to see if two iris templates match (i.e. extracted from the same eye) which involves making an accept/reject decision, a distance measure is indeed necessary to measure the closeness of a match. For example, some widely used methods in the iris recognition field are the Hamming distance (HD), the normalized correlation (NC) and the weighted Euclidean distance (WED). Other distance measures have also recently been proposed, which aren't used in this thesis.

15. HAMMING DISTANCE

The difference between iris codes is measured by the Hamming Distance (HD), which is the number of disagreeing bits between two iris-codes. Using logical XOR operator detects disagreement between any corresponding pair of bits Hamming Distance. Comparison of Iris code records, which is a measure of variation between the Iris code record from the presented iris and each Iriscode record in the database. There have been identified about 250 degrees of freedom in the iris.

$$HD = \frac{1}{N}\sum_{j=1}^{N} X_j (XOR) Y_j$$

where N is the total number of bits in two iris codes i.e. X and Y. Here, the hamming distance between the two bit patterns *(X, Y)* is the sum of disagreeing bits (sum of the exclusive-OR between X and Y) over N.

The statistical independence and the hamming distance are tending to zero for the iris templates of same eyes. But, the hamming distance is close to 0.5 for two independent iris templates generated from two different eyes. That means, it is important to set a proper threshold when computing the Hamming distance between two iris templates in order to decide if both templates come from the same eye, thus achieving accurate feature identification.

16. NORMALIZED CORRELATION

Wildes system applied the normalized correlation to get the better match between two encoded image, i.e. the acquired image and the template image. It is defined as

$$NC = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(p_1[i,j]-u_1)(p_2[i,j]-u_2)}{nm\sigma_1\sigma_2}$$

where p_1 and p_2 represent the two encoded iris templates of size $n \times m$, u_1 and u_2 correspond to the mean and σ_1 and σ_2 are the standard deviations of p_1 and p_2, respectively.

17. WEIGHTED EUCLIDEAN DISTANCE

The closeness of match between two iris feature templates is measured by a distance metric known as the weighted Euclidean distance (WED). The norm between two iris feature vectors is measured in weighted Euclidean distance[19], as follows

$$WED = \sum_{i-1}^{N}\frac{(f_i - g_i)^2}{\delta_i^2}$$

where f_i and g_i represent the unknown and known (i.e. in database) iris templates, respectively. i denotes the index of the features in the templates, and δ_i is the standard deviation of the i^{th} feature calculated from template g .

18. PHASE-BASED MATCHING

A new is designed for iris recognition based on hierarchical phased-based matching. They eliminate steps such as normalization and eyelid masking and also enhance the speed of matching by hierarchical based matching method. It achieved highly robust iris recognition in a unified fashion using phase components in two-dimensional Discrete Fourier Transformation. Hierarchical phased matching consists pre-processing and the matching stages. The pre-processing is involved in iris localization by computing inner and outer boundary of iris image. The matching stage consists - (i) effective region extraction followed by (ii) matching score calculation. They have achieved minimum genuine matching score 0.122 and the maximum impostor matching score is 0.128. Two classes can be distinguished by choosing any value between them that act as the threshold. Thus for this experiment, they claimed that their proposed approach can give a highly accurate recognition as it achieved EER=0%, where the EER (Equal Error Rate) is the error rate where the FNMR (False Non-Match Rate) and the FMR (False Match Rate) are equal [5].

19. CONCLUSIONS

Biometrics is the science and technology of measuring and analyzing biological data of human body for increasing systems security by providing accurate and reliable patterns and algorithms for person verification and identification and its solutions are widely used in governments, military and industries.

REFERENCES

1. Kuo, C., Romanosky, S., and Cranor, L. F., ”Human selection of mnemonic phrase-based passwords”. In Proceedings of the Second Symposium on Usable Privacy and Security (Pittsburgh, Pennsylvania, July 12 - 14, 2006). SOUPS '06, vol. 149. ACM, New York, NY, 67-78.
2. Teoh, A.B.J., D.C.L. Ngo, and A. Goh, Personalised cryptographic key generation based on FaceHashing. Computers & Security, 2004. 23(7): p. 606-614.
3. J. Daugman, "New Methods in Iris Recognition," IEEE Trans. on Systems, MAN, and Cybernetics—Part B: Cybernetics, Vol. 37, No. 5, Oct.2007.
4. W. W. Boles and B. Boashash, "A Human Identification Technique Using Images of the Iris and Wavelet Transform," IEEE Trans. on Signal Processing, Vol. 46, No. 4, Apr.1998
5. C.Anand Deva Durai and M.Karnan, "Iris Recognition Using Modified Hierarchical Phase-Based Matching (HPM) Technique", International Journal of Computer Science Issues, Vol. 7, Issue 3, No 8, May 2010
6. D. M. Monro, S. Rakshit and D. Zhang, "DCT-Based Iris Recognition," IEEE Trans. on Pattern Analysis & Machine Intelligence, Vol. 29, No. 4, Apr.2007
7. S. P. Narote, A. S. Narote and L. M. Waghmare, "Iris Based Recognition System Using Wavelet Transform," International Journal of Computer Science and Network Security, Vol.9 No.11, Nov. 2009
8. R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey, S. McBride. A system for automated iris recognition. Proceedings IEEE Workshop on Applications of Computer Vision, Sarasota, FL, pp. 121-128, 1994.
9. W. Kong, D. Zhang. Accurate iris segmentation based on novel reflection and eyelash detection model. Proceedings of 2001 International Symposium on Intelligent Multimedia, Video and Speech Processing, Hong Kong, 2001.
10. C. Tisse, L. Martin, L. Torres, M. Robert. Person identification technique using human iris recognition. International Conference on Vision Interface, Canada, 2002.
11. L. Ma, Y. Wang, T. Tan. Iris recognition using circular symmetric filters. National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, 2002.
12. R. Wildes. Iris recognition: an emerging biometric technology. Proceedings of the IEEE, Vol. 85, No. 9, 1997.
13. D. Martin-Roche, C. Sanchez-Avila, and R.Sanchez-Reillo. Iris recognition for biometric identification using dyadic wavelet transform zero-crossing. IEEE Aerospace and Electronic Systems Magazine, Mag. 17, no. 10, pages 3–6, 2002
14. A. Oppenheim, J. Lim. The importance of phase in signals. Proceedings of the IEEE 69, 529-541, 1981.
15. D. Field. Relations between the statistics of natural images and the response properties of cortical cells. Journal of the Optical Society of America, 1987.
16. Brady, N., Field, D. (2000). Local contrast in natural images: normalization and coding efficiency. Perception, 29 (9): 1041-1055.
17. S. Lim, K. Lee, O. Byeon, T. Kim. Efficient iris recognition through improvement of feature vector and classifier. ETRI Journal, Vol. 23, No. 2, Korea, 2001.
18. P. Burt, E. Adelson. The laplacian pyramid as a compact image code. IEE Transactions on Communications, Vol. COM-31, No. 4, 1983.
19. Zhu, Y., Tan, T., Wang, Y.W. (2000). Biometric Personal Identification based on Iris Patterns. 15th International Conference on Pattern Recognition, 2: 801-804