International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 04, April-2015

Intrinsic Biometrics

Apurva Khemani
Department of Computer Engineering
Bhagwant University
Ajmer, India

Abhishek Choudhary
Department of Computer Engineering
Bhagwant University
Ajmer, India

***Abstract*— In case of biometrics, we generally refer to security biometrics which is a set of techniques or methods used to identify an individual using his biological or behavioural features. The word biometrics can be divided into two types i.e. Security Biometrics and Medical Biometrics. When dealing with medical biometrics, we refer to some specific methods that are used to measure some parameters derived from medical data. In this paper, we aid security biometrics with medical biometrics and we try to focus on the individual identification and verification with the help of medical data such as MRI images and X-Ray images. This is why it is termed as "Intrinsic Biometrics" or "Hidden Biometrics".**

Keywords—: Biometrics, biological, security biometrics, medical biometrics, identification, verification, X- Ray images, MRI images, intrinsic biometrics, hidden biometric.

I. INTRODUCTION

Extrinsic Biometrics refers to the visible and tangible parts of the body to be used for security biometrics. These include Face Recognition biometrics security, Fingerprint Identification , Hand Geometry biometrics security, Retina Scan , Iris Scan , Signature biometrics security , Voice Analysis. These are all accessible parts of body which can be used as Security Biometrics. This way we use medical biometrics for security purposes. In case of Intrinsic Biometrics, we use the inaccessible parts of the body which are not visible directly. These features are not easily accessible and cannot be imitated at all. This type of Security biometric system is called "Hidden Biometrics" or "Intrinsic Biometrics". We can use "Brain print", "Chest print"," Bone print" etc for intrinsic biometrics. Extrinsic Biometric techniques are prone to attacks by malicious users.

1.1 MODES OF BIOMETRIC SYSTEM

In case of security biometrics there are two modes in which the entire process is divided.

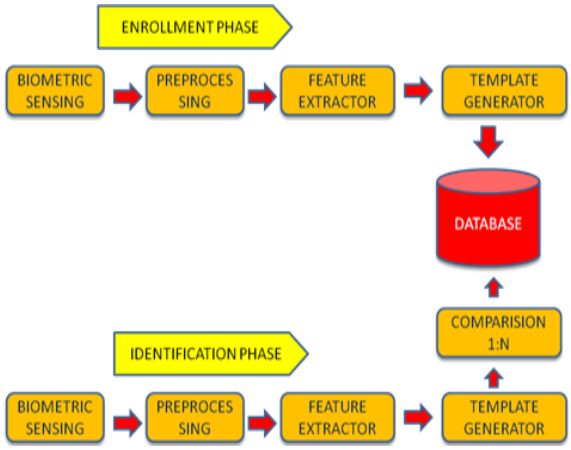
a. Verification mode

In **verification** (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify theindividual is the person they claim to be. Three steps are involved in the verification of a person.In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using same identity".

b. Identification mode

In **identification** mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, Pins or keys are ineffective.

1.*2 PROCEDURE OF SECURITY BIOMETRIC SYSTEM*



At the first stage, Sensing is done. Biometric Sensing can be of various types MRI imaging, ECG, EMG, X-Ray, etc. These methods are used to take samples of the internal structure and specific areas of the body and then those samples are thoroughly examined in the Pre-processing phase after which a particular area is selected for Feature Extraction like in case of MRI imaging of Brain a small minute part for example gyrus, cerebrum etc is selected for feature extraction. The next phase includes Template Generation which is the most important part of Security biometrics. In this phase, the chosen feature is examined and is converted into a typical CODE which is also known as Template. This is done using a particular algorithm and various mathematical equations. This template is then stored in the database so that it can be used in the identification and verification modes of security biometrics.

Next comes the Matching phase, where comparisons are done so as to prove the identity of the person and allow secure form of transactions. This is done by comparing the existing templates stored in the database with the incoming templates.

1.3 *SENSING- BIO SIGNALS FOR INTRINSIC BIOMETRICS*

In case of Intrinsic Biometrics, we use the inaccessible parts of the body which are not visible directly. These features are not easily accessible and cannot be imitated at all. This type of Security biometric system is called "Hidden Biometrics" or "Intrinsic Biometrics". We can use "Brain print", "Chest print", "Bone print" etc, for intrinsic biometrics.

In order to visualize the shape of a brain, we need to use MRI images. Within the same context, one should use X-Ray scanners to extract and visualize body skeleton, including skull and other bones, etc. But, we can expect that, in the near future, some systems, developed initially for medical biometric applications can be used also for security biometrics to access to some protected resources .For instance, to increase the security in some airports, low radiation X-Ray machines are used to control the borders (basically to detect forbidden objects). We believe that this concept can be performed and adapted for some specific applications dedicated to biometrics by developing scanners to perform efficiently and safety, the "Hidden biometrics" applied to some specific parts of the human body.

a. Electrocardiogram

Using the ECG as a biometric signal to identify an individual is not new .The main approach requires a classical recording as it is the case in clinical applications . The only exception is that no pathological cases are considered. As shown if Figure 1.1[3], only ECG beats are analyzed. For instance, a reference ECG beat is extracted during the enrolment phase. As shown in Figure 1.2[3], this reference is modelled using a neural-network system which means that each individual signature is characterized by a set of parameters.. Certainly, this rate is not better than the performances provided by some "visible" biometric techniques, but potentially it remains interesting and promising for future investigations in this field.

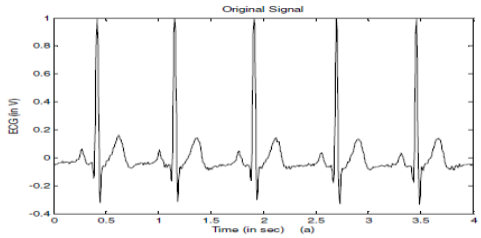


Fig 1.1

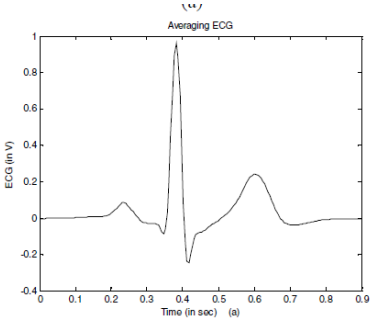


Fig 1.2

b. Electromyogram

Another biometric approach inspired from the medical field consists in using the Electromyogram (EMG) as a signature. As it is shown on Figure 1.3[6], the muscle of the forearm is exited by an impulsional electrical stimulation where the intensity belongs within the range [20-30] mA. The response is recorded using two electrodes .This technique is very efficient since the performances obtained from ten individuals vary between 93% and 100%. A simple response signal can be easily modeled using a parametrical model which means that few parameters are required to identify an individual. Another characteristic of this technique is that the signature may change over the time since human morphology is subject to slow variations. This aspect can be regarded as an advantage since this characteristic can be useful within the context of cancelable or volatile biometrics which makes it interesting when dealing with applications that require frequent update of the reference signature.

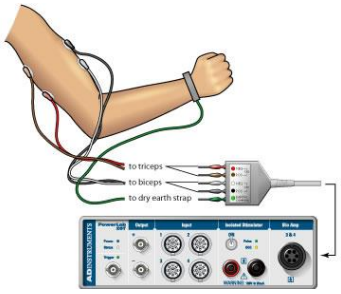


Fig 1.3

c. X-Ray

Starting from the approaches described above, the hiddenbiometrics can be generalized to the whole human body.For example,as given in Figure 1.4[6], using an X-ray scanner, one can produce a digitised image of the whole body.

Fig 1.4

Any part of the skeleton can be studied and analyzed using some automatic signal and image processing algorithms. For example, the skull, cervical vertebrae,humerus, ulna, radius can totally modeled and valuable parameters can be extracted for the purpose of hidden biometrics.

II. CLASSIFICATION OF HIDDEN BIOMETRICS

Volatile and Non-Volatile Biometrics:

Volatile Biometrics refers to the type of security biometrics in which the biometric template chosen for "identification" and saved in the database changes over time. In such cases, we need to update our templates regularly in our database so that our stored data does not become obsolete. Also if the template has been modified with age then the Security Biometrics system will not identify the template in the "verification" mode of the security process even if the template belongs to the right person. To avoid such problems, we use Non- Volatile Biometrics, in which the template used for "identification" and saved in the database does not change at all. These templates remain the same even when the person was a child and after fifty years when he/she has grown old. Non-Volatile Biometrics include "finger print scan", "retina scan", "iris scan" etc which do not change over time.

III. TYPES OF INTRINSIC BIOMETRIC SYSTEMS

1. *Vascular Biometrics or Vein Matching*

Vein matching, also called vascular technology, is a technique of biometric identification through the analysis of the patterns of blood vessels visible from the surface of the skin. In case of Fingerprint Scanners, direct contact of the skin with the scanner is required. Also in case of skin diseases like psoriasis, accuracy of the results is affected. Vascular scanners do not require contact with the scanner, and since the information they read in on the inside of the body, skin conditions do not affect the accuracy of the reading. Vascular scanners also work with extreme speed, scanning in less than a second. As they scan, they capture the unique pattern veins take as they branch through the hand.

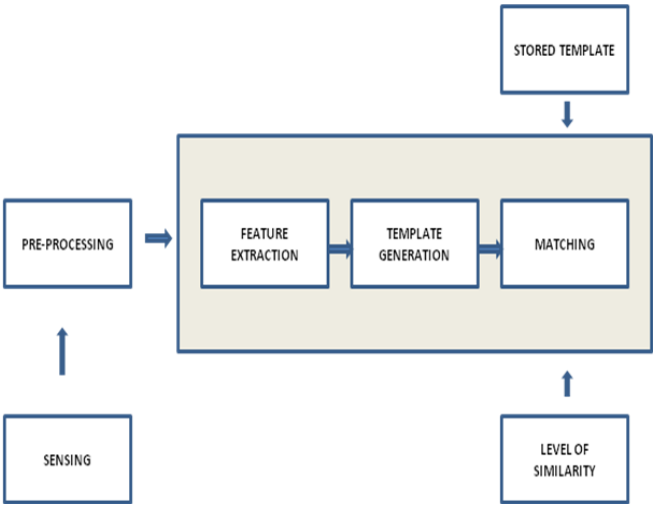
2. *Retinal Biometrics*

A retinal scan is a biometric technique or method that makes use of the unique patterns on a person's retina blood vessels. The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. As the Retina of each and every person is unique and does not change except due to some medical conditions like diabetes and glaucoma, it is considered as the most reliable biometric, after DNA.

3. Brain Biometrics

A numerous studies have shown that every individual has certain parts of the brain which are completely unique. This new proposed biometric approach is based on numerous anatomical studies that show a significant inter-individual variability of the brain shape and show that these characteristics are stable for adults.

a. *BLOCK DIAGRAM OF BRAIN BIOMETRIC SYSTEM*



At first, Sensing of the brain is done. This can be done by Magnetic resonance imaging, nuclear magnetic resonance imaging, or magnetic resonance tomography is a medical imaging technique used in radiology to investigate the anatomy and physiology of the body in both health and disease. MRI scanners use strong magnetic fields and radio waves to form images of the body. The technique is widely used in hospitals for medical diagnosis, staging of disease and for follow-up without exposure to ionizing radiation. Pre-processing deals with the procedure of selection of the part or area of brain we are going to use for SECURITY BRAIN BIOMETRICS. The basic Brain Biometrics system starts with this phase, that is, Feature Extraction. This phase basically includes the extraction or acknowledgement of the feature of the brain to be used for security purposes which was selected in the pre-processing phase. After this phase, different algorithms are implemented to find out and generate a template. These templates are stored in the database and are used for matching for Security purposes.

b. *MEDICAL IMAGING: BRAIN WAVE SIGNALS*

Medical imaging is the process of creating visual representations of the interior parts of a body for clinical analysis and medical intervention to improve a particular medical condition. Medical imaging reveals internal structures hidden by the skin and bones, also to diagnose and treat disease. Medical imaging also creates a database of normal anatomy and physiology to identify abnormalities.

Medical imaging can be done by various processes like magnetic resonance imaging, nuclear magnetic resonance imaging, or magnetic resonance tomography, CT scan, X-ray, endoscopy, medical photography, medical ultrasonography, thermography and many other medical processes.

i. CT SCAN

Computed tomography, sometimes called "computerized tomography" or "computed axial tomography", is a noninvasive medical examination or method that uses specialized X-ray equipment to create cross-sectional images of the body. Each cross-sectional image represents a "slice" of the person being imaged, like the slices in a loaf of bread. These cross-sectional images are used for a variety

of diagnostic and therapeutic purposes. CT images of internal organs, bones, soft tissue, and blood vessels provide greater clarity and more details than conventional X-ray images, such as a chest X-Ray. As shown in Figure 1.5[6], it is done using a CT Scan suite. The CT image of the male skull is shown in the Figure 1.6[6].

Fig 1.5

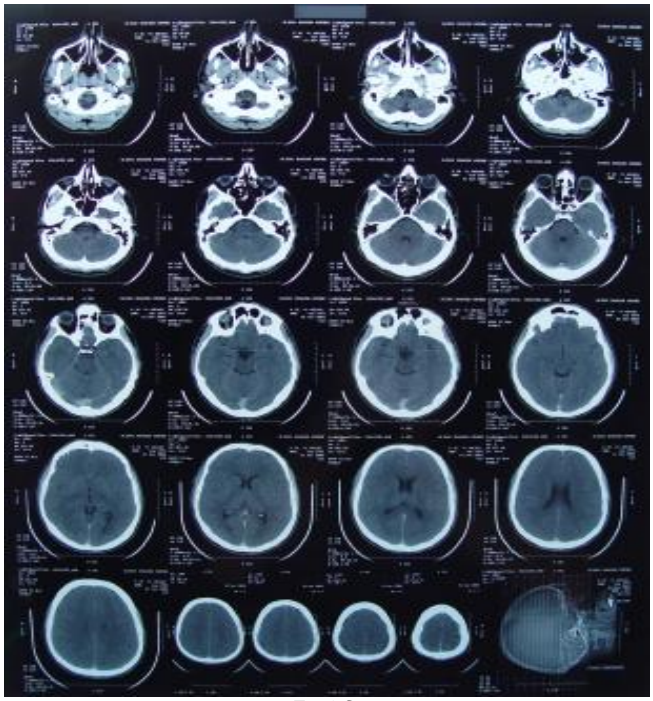


Fig 1.6

CT scans are performed to help the doctor to study various parts of the body and identify and monitor medical problems. The major areas of the body which are monitored using the CT Scan are head, neck, spine, chest, pelvis and abdomen.

ii. MEDICAL RESONANCE IMAGING

Magnetic resonance imaging (MRI) is a non-invasive medical test that helps physicians diagnose and treat medical conditions.MRI uses a powerful magnetic field, radio frequency pulses and a computer to produce detailed pictures of organs, soft tissues, bone and virtually all other internal body structures. Detailed MR images allow physicians to examine various parts of the body and determine the presence of certain diseases. As shown in Figure 1.7[6], the images can then be examined on a computer monitor, transmitted electronically or even printed.

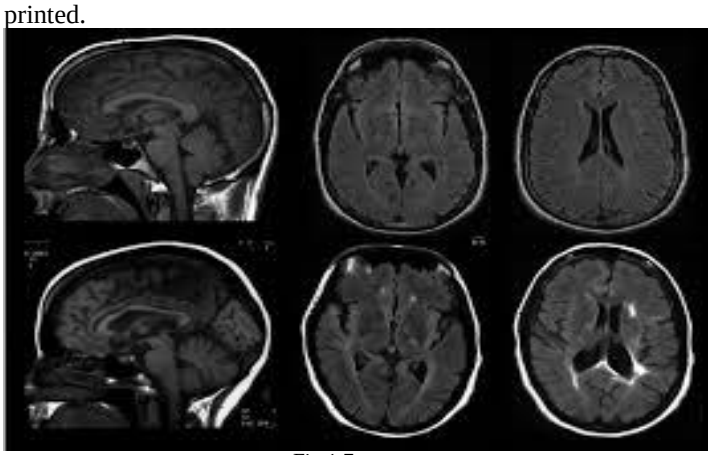


Fig 1.7

MRI can be done on various parts of the body such as organs of the chest and abdomen including the heart, liver, biliary tract, kidneys, spleen, bowel, pancreas, and adrenal glands, pelvic organs including the bladder and the reproductive organs such as the uterus and ovaries in females and the prostate gland in males, blood vessels (including MR Angiography) and lymph nodes. As shown in Figure 1.8[6], the magnetic resonance imaging is done using the MRI machine.

Fig 1.8

iii. USE OF MEDICAL IMAGING FOR BIOMETRICS

As we have seen earlier, the procedure or method of Biometric System starts with biometric sensing. Sensing is the process of taking samples of the internal structure and specific areas of the body. Sensing can be done by various methods such as magnetic resonance imaging, CT scan, nuclear magnetic resonance imaging or magnetic resonance tomography. These sampled images are then examined thoroughly in the pre-processing phase after which a particular area is selected for feature extraction like in case of MRI imaging of Brain a small minute part for example gyrus, cerebrum, etc is selected for feature extraction. Next comes the template generation, which is the most important part of Security biometrics. In this phase, the chosen feature is examined and is converted into a

typical code which is also known as template. This is done using a particular algorithm and various mathematical equations. This template is then stored in the database so that it can be used in the identification and verification modes of security biometrics. There are various geometrical methods used for template generation. These methods extract the required feature or conversion into the desired template. In this paper, we will discuss two geometrical methods.

IV. GEOMETRICAL METHODS OF TEMPLATE GENERATION

a. *SLICE SELECTION*

It is a step wise procedure which starts with the MRI of the entire brain. This MRI is the first step of Brain Biometric system also known as biometric sensing. The next step involves the 3D segmentation of the MRI images. Then these segmented images are examined thoroughly to generate Region of interest. The region of interest is the part of the brain which we select for feature extraction. This means a particular section of the brain which is unique for every individual and does not change with age or time. There are various minute parts of the brain which can be selected and used for further evaluation. But the most important thing is that it should be non-volatile i.e. it should remain the same for the entire life time of the individual. For example, in Figure 1.9[3] a particular region is extracted and chosen for template generation. Figure 1.10[3] shows the complete brain.

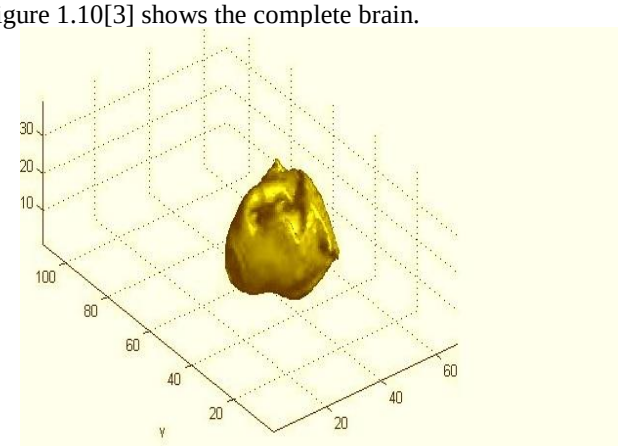


Fig 1.9

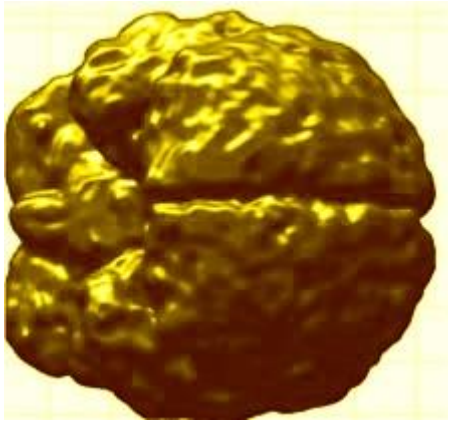


Fig 1.10

This region of interest is studied deeply and a particular feature is extracted which is chosen for template generation. Template generation involves the conversion of that feature into BRAIN CODE. This is done by applying various methods one of which is Slicing. As shown in figure 1.11[3] and 1.12[3], this process starts with slice selection which involves choosing a particular slice and taking the MR image of that slice. This MRI is then studied and evaluated thoroughly to produce the desired template. There are various algorithms which have been implemented till to complete this process of feature extraction. This paper aims at reviewing the overall procedure of brain biometric system.

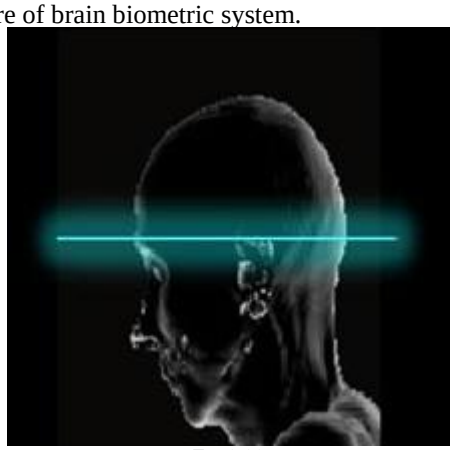


Fig 1.11

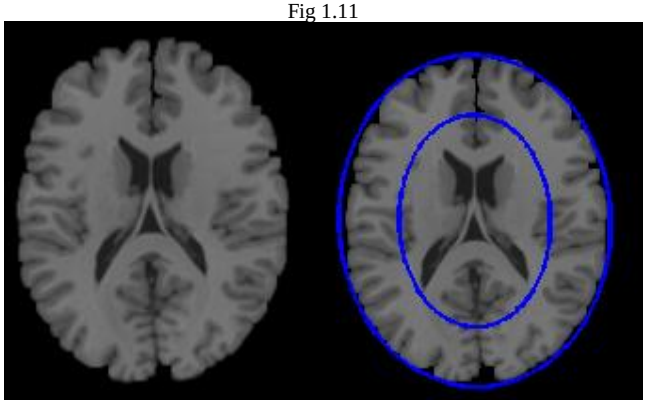


Fig 1.12

As shown in Figure 1.13, this slice can further be expanded and then by mathematical implementations can be converted to desired Template or Brain Code.

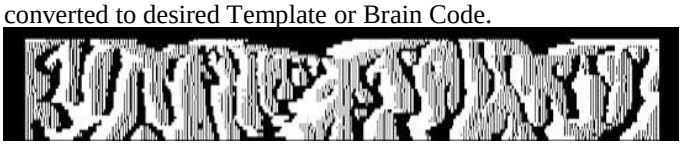


Fig 1.13

b. *ELLIPTICAL EVALUATION*

In this method, the steps of biometric system are the same as those in the slice selection process. The only difference occurs when it comes to the Template Generation phase. In this phase, as we have seen in slice selection a particular slice of the brain is selected and then the MRI of that slice is then implemented to produce the brain code. But in Elliptical Evaluation, as shown in figure 1.14[5], the region of interest is extracted and evaluated as an ellipse. The ellipse is then substituted into equations. Figure 1.15[2] shows the geometrical way of depicting an ellipse. First,

we find out the semi-major axis, semi-minor axis and eccentricity of the obtained ellipse.

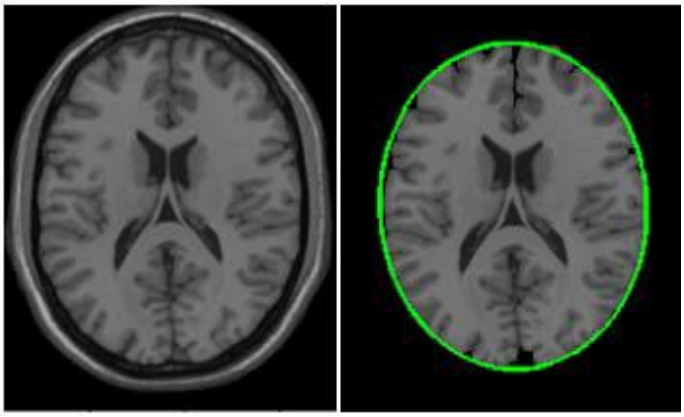


Fig 1.14

Here, a= semi major axis

b=semi minor axis

(X_c, Y_c)= centre of the ellipse

Now we can apply different equations and algorithms to generate the required template or brain code. Hence, we can see that there are various methods for template generation and we have reviewed two of them here.

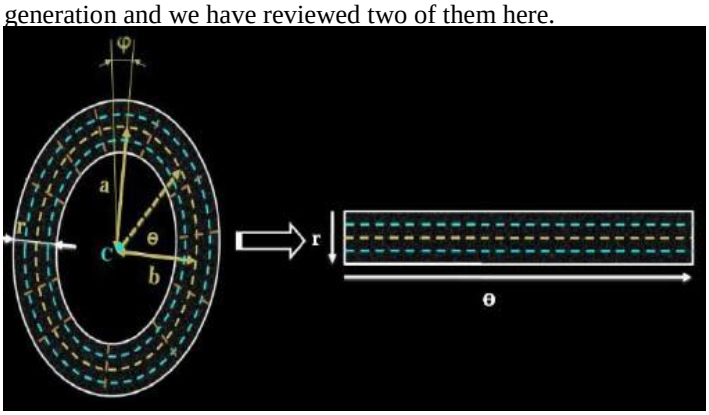


Fig 1.15

V. CONCLUSION

Our aim in this paper is to bridge the gap between security and medical biometrics, which is called "Intrinsic Biometrics" or "Hidden Biometrics". Intrinsic Biometrics deals with the study of the non-tangible parts of the body. Those parts of the body which are tangible such as figure prints or iris scan are prone to forgery. We have also included different methods of biometric sensing such as MRI, CT scan, ECG, EMG and X-Ray. At last we have reviewed some of the geometric methods which can be implemented in the brain biometrics template generation phase. This way we can see that we can use medical imaging produced by biometric sensing methods for security objectives.

VI. REFERENCES

(1) D. Maltoni, D. Maio, A. K. Jain, S. Prabahakar. "Handbook of Fingerprint Recognition", Springer – Second Edition– 2003.

(2) K. Aloui,A. Naït-Ali,M. Saber Naceur-"A Novel Approach Based Brain Biometrics: Some Preliminary Results for Individual Identification", ," IEEE Workshop on Computational Intelligence in Biometrics and Identity Management, Paris,France, April. 2011.

(3) Amine NAIT-ALI-"Hidden biometrics: towards using biosignals and biomedical images for security applications", 7th international Workshop on Systems, Signal Processing and their Applications, May, 2011.

(4) Amine NAIT-ALI-"Beyond classical biometrics: when using hidden biometrics to identify individuals"

(5) K. Aloui, A. Naït-ali, M.S. Naceur-" New biometric approach based on geometrical human brain patterns recognition: some preliminary results"

(6) Image reference, Electromyography from Empire Medical Associates website, X- Ray from sickkids- PEM curriculum, CT scan from insight clinical imaging website and two views of CT scans, MRI from Rudyard healthy-brain-MRI and flanderstoday website.