ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Life- Your Heart Speaks Your Password

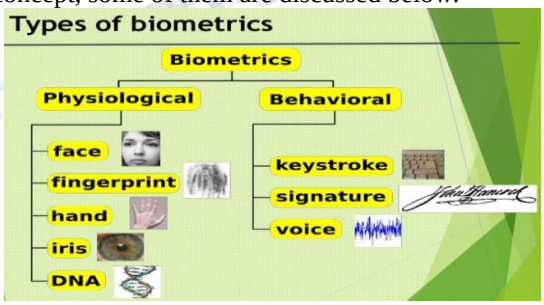
[1] Sujith nair.P, [2] Paramsivam.S, [3] Dhananjayan, [4] S.Nithin Krishna, [5] G Manjula.
[1,2,3,4] UG Scholars ,Dept. of Computer science & Engineering, SSCE, Bengaluru.
[5] Asst. Prof. ,Dept of Computer Science & Engineering , SSCE,Bengaluru

Abstract:- **The security is an important aspect of our daily life whichever the system we consider security plays a vital role. The biometric person identification technique based on the pattern of the human Iris, face, fingerprint or heartbeat is well suited to be applied to access control and provides /Strong security. In this paper, we focus on an efficient methodology of fingerprint, heartbeat, iris and face for identification and verification with total success rate. In this method, the image of the fragment taken is normalized and converted into binaries. The anatomy image and the series of operations such as segmentation, normalization, feature encoding are performed and it is converted into binaries. These bits are compressed and crossed over into a combined biometric key. This combined biometric key is used to bind each bit of the cryptographic key. This bound version of the key is used for enrolment and to release the key. Instead of storing the actual key, its hashed version is stored in order to conceal the cryptographic key to provide a secure comparison method for key verification. This bound version of the key is released only if this matches with the one identically. During enrolment, these features are used to bind a cryptographic key. The operation involved is the binary XOR. Here, the goal of the system is to reject, an unauthorized subject who does not possess the original features, for example, used during enrolment. In contrast, a genuine subject with the correct features will be accepted. By this spoofing can be avoided, since two kinds of keys are needed to encrypt the data and these keys are generated at once. This reduces the false acceptance rate and false rejection rate thereby the total success rate seems to be high since the key preserves security level to high.**

***Keywords*---** **Biometric key, Cryptographic key, Helper data, Hashed key.**

I. INTRODUCTION

The word biometric is derived from the Greek words bio and metric. Where bio means life and metric means to measure.Biometric authentication is the primary and prevalent system for security and surveillance activities in the past several years. The automation in every field of daily life has made human identification and verification is a prime issue for ensuring the security. The biometric techniques are relates to the parts of human body which are unique, cannot be stolen and is not easily transferable compared to traditional methods such as Identification badges, Personal Identification Number (PIN), password, smartcards etc., The commonly used biometric features include speech, fingerprint, and face, Iris, voice, hand geometry, retinal identification. A biometric sensor is a transducer that changes a biometric treat of a person into an electrical signal. Biometric treats mainly include biometric fingerprint reader, iris, face, voice, etc. Generally the sensor reads or measures light, temperature, speed, electrical capacity and other types of energies. Different technologies can be applied to get this conversation using sophisticated combinations, networks of sensors and digital cameras. Every biometric device requires one type of sensor. The biometrics applications mainly include: used in a high definition camera for facial recognition or in a microphone for voice capture. Some biometrics is specially designed to scan the vein patterns under your skin. Biometric sensors are an essential feature of identity technology. Biometric sensors or access control systems are classified into two types such as Physiological Biometrics and Behavioral Biometrics. The physiological biometrics mainly include face recognition, fingerprint, hand geometry, Iris recognition and DNA. Whereas behavioral biometrics include keystroke, signature and voice recognition. For better understanding of this concept, some of them are discussed below.



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

II. PROPOSED ALGORITHM

a. Biometric key generation
Step 1: Images acquisition.
Step 2: Enhancement of the images.
Step 3: Feature extraction.
Step 4: Biometric key is generated.
b. Combined key generation
c. Generation of helper data and hash key
Step 1: Performing Hashing function on the cryptographic key and Store the hashed key in the database.
Step 2: Helper data is generated as a result of binding the cryptographic key with the combined biometric key.

III. DIFFERENT TYPES OF BIOMETRICS

a. Fingerprint scanner
A fingerprint scanner system has two basic jobs -- it needs to get an image of your finger, and it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images.
Only specific characteristics, which are unique to every fingerprint, are filtered and saved as an encrypted biometric key or mathematical representation. No image of a fingerprint is ever saved, only a series of numbers (a binary code), which is used for verification. The algorithm cannot be reconverted to an image, so no one can duplicate your fingerprints.

b. Iris scanner
First the system has to localize the inner and outer boundaries of the iris (pupil and limbs) in an image of an eye. Further subroutines detect and exclude eyelids, eyelashes, and secular reflections that often occlude parts of the iris. The set of pixels containing only the iris, normalized by a rubber sheet model to compensate for pupil dilation or constriction, is then analysed to extract a bit pattern encoding the information needed to compare two iris images .In the case of Daugman's algorithms, a Gabor Wavelength transform is used. The result is a set of complex numbers that carry local amplitude and phase information about the iris pattern. In Daugman's algorithms, most amplitude information is discarded, and the 2048 bits representing an iris pattern consist of phase information (complex sign bits of the Gabor wavelet projections). Discarding the amplitude information ensures that the template remains largely unaffected by changes in illumination or camera gain, and contributes to the long-term usability of the biometric template.
For identification (one-to-many template matching) or verification (one-to-one template matching) a template created by imaging an iris is compared to stored template(s) in a database. If the Hamming distance is below the decision threshold, a positive identification has effectively been made because of the statistical extreme improbability that two different persons could agree by chance ("collide") in so many bits, given the high entropy of iris templates.

c. Face recogniser
All of these systems take in data – often an image – from an unknown person, analyse the data in that input, and attempt to match them to existing entries in a database of known people's faces or voices. Facial recognition does this in three steps: detection, face print creation, and verification or identification. When an image is captured, computer software analyses it to identify where the faces are in, say, a crowd of people. In a mall, for example, security cameras will feed into a computer with facial recognition software to identify faces in the video feed.

d. Voice recogniser
To convert speech to on screen text or a computer command, a computer has to go through several complex steps. When you speak you create vibrations in air, the analog to digital converter (ADC) translates this analog wave into digital data that computer can understand. To do this, it samples, it digitalises, the sound wave taking the precise measurements of the wave of frequent intervals. The system filters digitalise the sound to remove unwanted noise and sometimes separate it into different bands of frequency. It normalises the sound or adjusts it to the constant volume level. It may also have to be temporarily aligned. People don't always speak at the same speed, so the sound must be adjust to match the speed of the template, sound sample already stored in the system memory.
Next the signal divided into small segments as short as a few hundredth of a second, or even a thousand in case of plosive consonant sounds. Consonant stops produced by obstructing air flow in vocal tract like 'p' or 't'. The program then matches the segments to known phonemes in the appropriate language. A phonem is a smallest element of the language a representation of the sounds we make and put together for a meaningful statements.

e. Heartbeat sensor
The heartbeat sensor is based on the principle of photo plethysmography. It measures the change in volume of blood through any organ of the body which causes a change in the light intensity through that organ (a vascular region). In case of applications where heart pulse rate is to be monitored, the timing of the pulses is more important. The

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

flow of blood volume is decided by the rate of heart pulses and since light is absorbed by blood, the signal pulses are equivalent to the heart beat pulses.

There are two types of photo plethysmography: Transmission: Light emitted from the light emitting device is transmitted through any vascular region of the body like earlobe and received by the detector. Reflection: Light emitted from the light emitting device is reflected by the regions.

IV. THE FUTURE- HEARTBEAT PASSWORD SECURITY

A device measures your heartbeat and uses it as a unique biometric to identify you. It measures your heartbeats, it confirms that you – the rightful owner are wearing it, and then it's able to communicate that identity to whatever system or service you use. So, what we're hoping is that it means the end of things like passwords and pin numbers. But it could even replace things like car keys, house keys, credit cards, and boarding passes. These are all different proxies for identity. We think that a wearable device that's paired with your biometric can be a much easier, more secure form of user identification.

PROCESS:

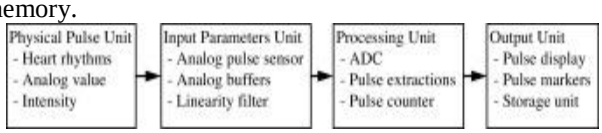
1. Physical pulse
2. Input parameters
3. Central processing units
4. Output parameters
5. Storage units

First step: Physical pulse is defined pulse that represents the heartbeat rhythm is defined as the number of beats per minute.

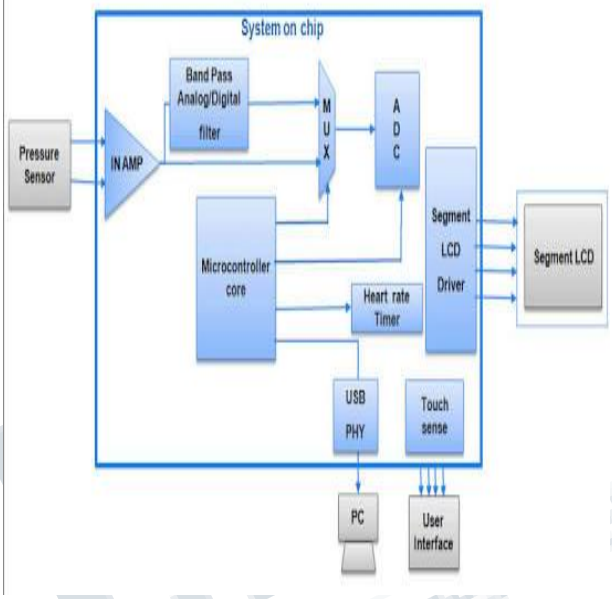
Second step; Input derived parameters are parameters which are then used to make physical linearity filter by buffer circuit to forward it to the central processing unit.

Third step; Central processing unit serves as calculation algorithm to analyze the results transmitted to the output.

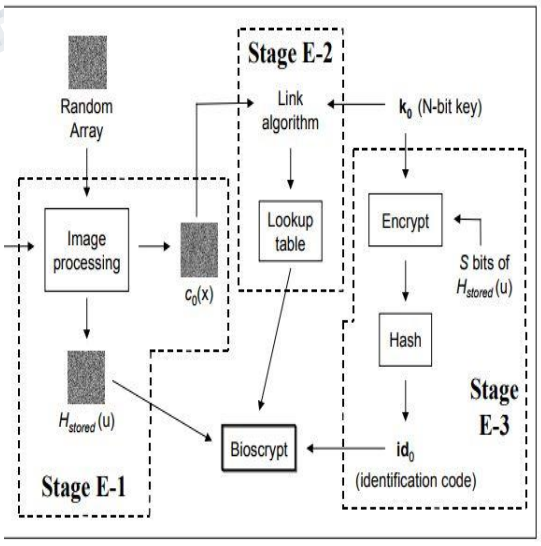
Fourth step; Output parameters such as the amount of pulse rate, dynamic number of pulse signal, and stored into memory.



The first unit, input sensor value is the pulse rate by detecting the intensity of the light and into the calculation and processing. The second unit calculation and processing serve as a hub to receive and send information, including the calculation of the software. The third unit, display unit is used to represent data obtained from measurement through LCD display. The fourth unit, analysis is analyzing or classification of information to group the symptoms of subjects. The fifth unit, storage unit stores the information into the SD card to store data records of subjects



Algorithm implementation: the system implementation in term of software control consists of functions such as pin Mode, LCD begin, analog Value, and interrupt Setup, etc. This preliminary study composes optical sensor input and then process unit for calculation and monitor to display unit. The algorithm shown in below:



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

```
# Algorithm design and implementation
//Include preprocessor
//Variables of Pulse sensor
//The interrupt service routine
    data type ;          //initialization the variable
// Programming procedure
void setup() {

  File dataFile = SD.open("neramitr.csv", FILE_WRITE);
                              //  open head file of SD card
  {
   pinMode(data_type, INPUT);     //define PIN status
   pinMode(data_type, OUTPUT);    //define PIN status
   Serial.begin(bit rate);          //define data bit rate
   lcd.begin(x,y);                  //define display unit
                             //Subject_ID, SEX, AGE calibration
       analogValue = analogRead(data type);
   clear();                                  // clear temporary
   interruptSetup();                 // sets up to read Pulse Sensor
   }
   dataFile.close();                 // close file of SD card
}

void loop() {
  analogValue = analogRead(data type);
                                    //ID,SEX,AGE set calibration
  reading=digitalRead(IN_PIN);          //read from Digital PIN
  sendDataToProcessing('S', Signal);
                           //send Processing the raw Pulse Sensor data
  }
```

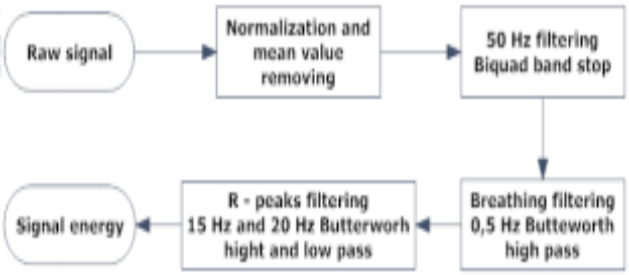
DETAILED CONVERSION OF HEARTBEAT SIGNALS INTO DIGITAL SIGNALS

A transducer comprising a pair of flexible walls, one of which senses mechanical pulsations and transfers the pulsations to a volume of gas, and the other of which receives the pulsations from the gas and produces an electrical signal there from. The invention provides a sensitive device that produces an electrical signal in response to heartbeat pulsations. In one embodiment, the invention employs a wrist- mounted case or housing in which slightly pressurized gas, preferably air, is confined in a chamber between a pair of flexible walls, one of which is a high compliance follower membrane that senses the heartbeat pulse signature and the other of which is a piezoelectric membrane. Heartbeat pulsations applied to the follower membrane are transferred to the piezoelectric membrane through pressure oscillations in the air, serving as a coupling medium. In another embodiment, two chambers containing gas, preferably air, are wrist-mounted at separate locations. A first chamber has a wall constituted by a piezoelectric membrane and is contained in a case positioned on a wrist, like a watch. A second chamber has a wall constituted by a compliant follower membrane exposed to heartbeat pulsations, and is mounted on a band attached to the case, like a watch band. The two chambers are connected by tubing that transfers heartbeat pulsations from the second chamber to the first chamber via air in the tubing, serving as a coupling medium. Both embodiments preferably employ electronics including, for example, an amplifier with a high input impedance stage to convert the current output of the piezoelectric membrane to a voltage, and a voltage amplifier stage to produce an output signal that can be displayed locally or at a distance. This digital signal taken is recorded using a storage device as an image using an encryption code. This encryption code is referred using a similar cipher code that creates image for each signature entry found and compares with the previously stored image in the database.

Signal acquisition

ECG signal for digital signal processing and heart rate calculation was acquired by measurement card with sampling frequency fs = 500 Hz. The first ECG lead was measured. Analogue signal pre-processing was done on simple amplifier circuit designated for ECG signal measurement. The circuit with ECG amplifier is fully described in raw ECG signal sampled by measuring card. This signal was used as input signal for the digital filters and the heart rate detection algorithms designing and testing.

Digital signal processing with digital filters in this part there is described noise elements filtering and baseline wander elimination with digital filters. The main noise elements are power supply network 50 Hz frequency and breathing muscle movements. These artifacts have to be removed before the signal is used for next data processing like heart rate frequency determination. The block schema of digital signal processing with digital filters:



At the beginning, the mean value is removed from signal. Then signal is normalized for unit maximum amplitude. Network interference at 50 Hz frequency is removed by first filter. This filter type is bi-quad band stop. Advantage of this filter is very narrow band stop which is created by poles and zeros location. Baseline wander was provided by means of the next filter. This filter is second order Butterworth filter set to frequency of 0.5 Hz. This filter is usually used in professional ECG filtering applications .The signal filtered by these filters.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

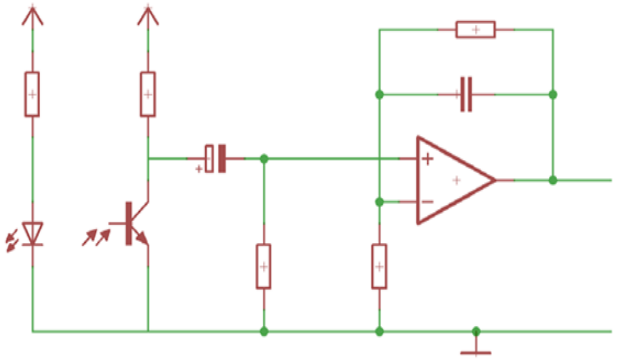
After the basic filtering, the R-peaks are detected from ECG signal. R-peaks filtering are necessary for next heart rate detection. The signal is filtered by high pass and low pass Butterworth filters with cut-off frequencies 15 Hz and 20 Hz. Both filters are fourth order because of computing difficulty in next implementation in a microprocessor. Using of these two filters has better results than one band pass filters. The signal energy of samples from voltage amplitude is calculated then by

$$E(t) = u(t)^2$$

Matching algorithms are used to compare previously stored templates of fingerprints against candidate fingerprints for authentication purposes. In order to do this either the original image must be directly compared with the candidate image or certain features must be compared.
The stored digital form of the heart beat signature is encrypted using a cipher code and stored in encrypted form.

COMPARISION OF HEARTBEAT SIGNATURES

Minutiae image is divided into segments, each segment is corresponding minutiae's group is described by parameters (x, y, nom), where x and y are the coordinates, and nom determines the number of minutiae in the group. Additionally, one implementation uses an additional parameter specifying the probabilities of damage in a given segment, which is estimated by a neural network, based on the distribution of areas rejected by the mask described by the formula. Current algorithm implementation searches small groups of minutiae that that contain up to 5 minutiae. Then, based on the neighboring groups (max 4) creates a new large group. For each, the orientation parameters and the number of characteristic points are recalculated. The last step is to create a matrix of Euclidean distances between the largest groups. When comparing the use of two parameters: dx - the distance defining the difference between groups in the pattern and tested heartbeat signature, px - the threshold of damage occurrence probability (determined by whether the group is under consideration in the analysis), we decide which groups should be compared and we set the priority for them. After that we do the comparison of the groups, which are divided according to the priority, that is defined by the number of minutiae in the group and selective attention (SA) algorithms, which are based on probabilities of damage. Heart beat signature divided into segments. The identical match between both the signatures fetches out the signal that indicates that input signature is authorized.



ADVANTAGES

- Cannot be forgotten or lost
- Reduced operational cost
- Improved security and customer experience
- User friendly
- Nearly impossible to forge
- Offers mobility
- Ensures the highest accuracy
- Biometric credentials are always with you
- Several applications can be enhanced like pc unlocking, smart appliance access, smart car access, authorising almost anything which requires an authorisation etc.
- Health issues can be lively monitored.

DISADVANTAGES

- Additionally requires a hardware to configure
- Once compromised cannot be reset
- Comparatively high cost
- An clone of the signature can be easily replicated
- The database has to be explicitly secured

V. CONCLUSION AND FORESEEK

This research is to construct the heartbeat signal measurement security, which used embedded system and pulse sensor techniques as shown in system architecture. This preliminary study will be composed the system design, analysis, testing, implementation, and performance evaluation. The research illustrates the efficiency, accuracy, quantity of subjects, and good results. This may even become practical facilitating biometric authentication, and it will be the most secure than any other biometric security made till today.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

REFERENCES

1. Anil Kumar Jain, Arun A. Ross, and Karthik Nandakumar ,"Introduction to Biometrics",
2. Book: Analog -to-Digital Conversion
3. Book by Marcel J.M. Pelgrom
4. Book by Song Y. Yan, Number theory of everything
5. The CC-BY book Openstax college, anatomy and physiology