International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Heart Beat Based Security System Using Sampling Technique

G.Venkatesh[1], M.Sugumar[2], S.Pradeep[3] ,R.N.Vasantharaj[4]

[1]G.Venkatesh M.E, Asst Professor ,Panimalar Engineering College ,Chennai.
[2]M.Sugumar, Panimalar Engineering College ,Chennai
[3]S.Pradeep Panimalar Engineering College ,Chennai
[4]R.N.Vasantharaj, Panimalar Engineering College ,Chennai

Abstract - *To provide a security system using the pulse interval of heart beat of a person which is unique for each individual which can provide high security and also establish an interface between the security system the individual for real time access.*

Key Words: Security System , Heart Beat , Biometric Authentication, Sampling Technique , Heart Beat Security ,etc (Minimum 5 to 8 key words)…

1.INTRODUCTION

THIS heart-beat-based security is mainly used for improving our security encryption. In this System, a security key is derived from the time difference between consecutive heart beats (the inter-pulse interval, IPI).In heart-beat-based security (HBBS), each sensor measures a heart-related biosignal, for example, cardiac activity or blood flow, and forms a biometric security key based on the time interval between consecutive heart beats.The time interval between consecutive heartbeats (interpulse interval, IPI) has previously been suggested for securing mobile-health solutions. This time interval is known to contain a degree of randomness, permitting the generation of a time- and person-specific identifier. It is commonly assumed that only devices trusted by a person can make physical contact with him/her, and that this physical contact allows each device to generate a similar identifier based on its own cardiac recordings. Under these conditions, the identifiers generated by different trusted devices can facilitate secure authentication. Recently, a wide range of techniques have been proposed for measuring heartbeats remotely, a prominent example of which is remote photoplethysmography (rPPG).

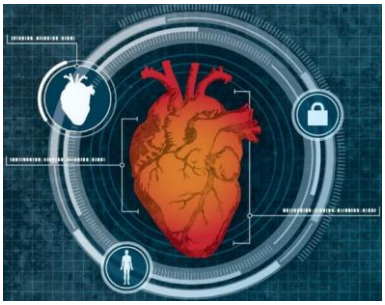


Fig 1.1 Heat Beat Security

Automated security is one of the major concerns in modern time where secure and reliable authentication is in great demand. However, traditional authentication methods such as password and smart card are now outdated because they can be lost, stolen and shared. In this project, biometric system based on heartbeat signals which is also known as Electrocardiographic (ECG) signals is proposed. Heartbeat is chosen as modality due to an individual's ECG signals cannot be faked. Compared to fingerprint it can be fooled with fake fingers, face can be extracted using user's photo and voice can be imitated conveniently. As ECG signals are reflection of the mechanical movement of the heart, these features contain unique physiological information which make them a promising authentication technology.

A Report From Binghamton University Had Proved it.Scientists from the Binghamton University in New York have explored with using a person's heartbeat as a password for encrypting and then decrypting personal data. Researchers say that each person possesses a unique electrocardiograph (ECG), which just like fingerprints and iris, can be used for authentication.

Fig 1.2 Heart Beat Replace Passwords

1.1 Introduction to Heart Beat

Heart Beat Rate , also known as pulse, is the number of times a person's heart beats per minute.The heart rate can vary according to the body's physical needs, including the need to absorb oxygen and excrete carbon dioxide. It is usually equal or close to the pulse measured at any peripheral point. Activities that can provoke change include physical exercise, sleep, anxiety, stress, illness, and ingestion of drugs.

Types of Heart Beat

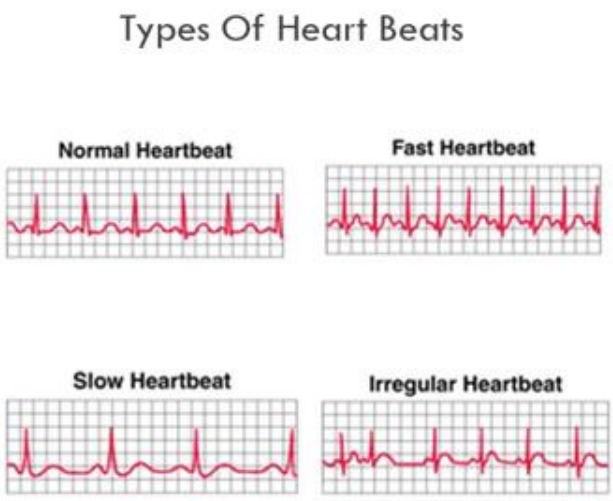


Fig 1.3 Types of Heartbeat

Tachycardia is a fast heart rate, defined as above 100 bpm at rest.

Bradycardia is a slow heart rate, defined as below 60 bpm at rest.

When the heart is not beating in a regular pattern, this is referred to as an **arrhythmia**.

1.2 Heart Beat Pattern

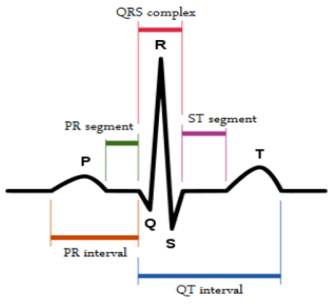
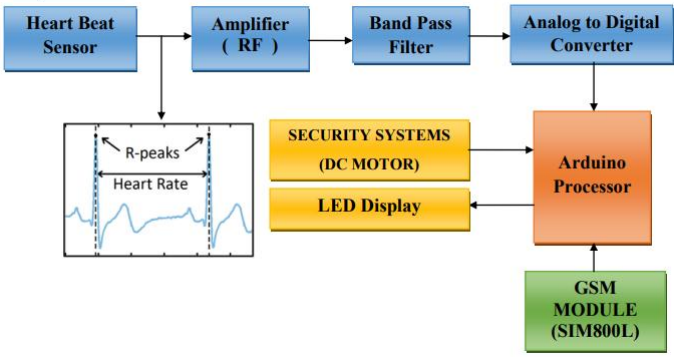


Fig 1.4 Heart Beat Pattern

One pulse(Beat) pattern = P-Q-R-S-T

2. WORKING METHADOLOGY



2.1 Block Diagram

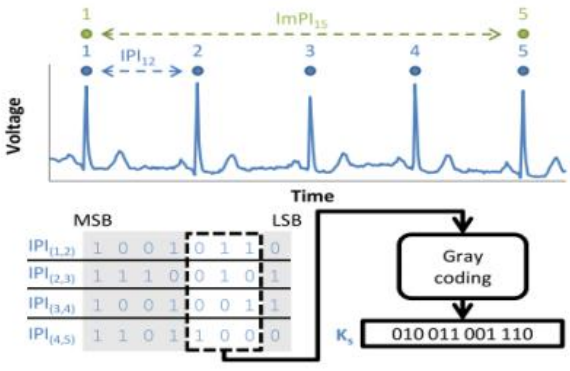
2.1 WORKING:

The method used here is photoplethysmography. This sensor is used to measure heartbeat, that is it senses the rate of flow of blood through arteries and provides the electrical signals of the sensed heart rate. Hence beat rate depends on the rate of flow of blood through the arteries. Hence, it uses the bodily structure to measure the heart rate. At this time some of the light gets dispersed due to the beat rate and corresponding signal is obtained as electrical signal. The signal obtained from the photoplethysmography has small amplitude very small and so an amplifier is used to convert it to a suitable signal form for further processing.Usually a bandpass filter has two cutoff frequency between which it passes the signal without any unwanted noises. Here we take frequency at P as lower cutoff frequency and T as higher cutoff frequency. The bandpass filter sends only the cardiac cycle from PQRST to the ADC converter.Now an input of required amplification and required band is given to the A to D converter.The amplified analog signal is given as input to the ADC. The main function of this unit is to convert the analog signal to the digital signal using suitable sampling technique. Here we use ideal sampling technique to get the corresponding digital signal.Thus, this signal is given to the processor. The processor has a set of instructions to convert the corresponding digital signal (Binary code) to Grey code format.

The output from A\D converter is given to the Aurdino board which has been already fed with the suitable program for grey code conversion. Thus the output is fed to the Aurdino board (processor).The output from the Aurdino board has been displayed in the 16*2 LCD display.The pulse rate is displayed in the LCD display. If the sampled value matches with the pulse rate value, the security key unlocks, Here we have used a DC motor for an output unit.And if the Sampled value does not match with the pulse rate value, it sends a OTP to the registered number within 15 seconds.Here the OTP has been generated using a GSM module which has been fed with a suitable GSM coding.Thus the security system is even protected in a more secure manner using the OTP method.

2.2 BACKGROUND AND RELATED WORK

In this Section, we first compare HBBS to other biometrics qualitatively, after which we discuss works related to its security performance. HBBS is a form of cardiovascular biometrics, which use the characteristics of a person‟s cardiac cycle for entity authentication. Cardiovascular biometrics are typically based on an electrocardiogram (ECG), using either a combination of various fiducial features (e.g., “ST-slope”or “ST-interval”) or non-fiducial feature.This makes it a suitable candidate for many Health applications as.Heart beats are measurable throughout the body using many types of cardiovascular recordings, including ECG, blood pressure (BP) and Photoplethysmography (PPG).As such, it may be measured through a wide spectrum of sensors and locations (more universally than othercardiovascular biometrics.



The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits (MSBs) stay unchanged (000 to 000). In this Section we describe the most commonly used method for facilitating entity authentication in HBBS based on the IPI, after which we present our improved method using the ImPI. Entity authentication in HBBS comprises two steps: Security-key generation by two entities and entityauthentication, if these keys are similar enough.

3.HARDWARE COMPONENTS

3.1 Heart Beat Sensor

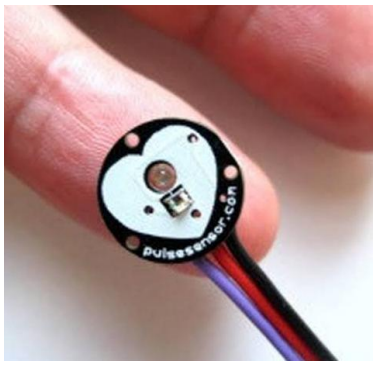
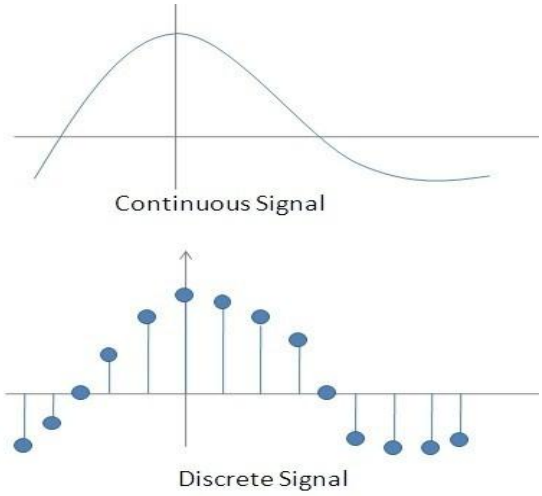


Fig 3.1 Heart Beat Sensor

Heart beat sensor is used to measure the pulse rate of heart in digital output.LED is used to detect the heart rate. The normal heart beat range is 78 bpm. This provides a direct output digital signal.

3.2 Amplifiers

An amplifier, electronic amplifier or (informally) amp is an electronic device that can increase the power of a signal (a time-varying voltage or current). It is a two-port electronic circuit that uses electric power from a power supply to increase the amplitude of a signal applied to its input terminals, producing a proportionally greater amplitude signal at its output.



3.3 Band Pass Filter

A band-pass filter, also bandpass filter or BPF, is a device that passes frequencies within a certain range and rejects (attenuates) frequencies outside that range.

3.4 Analog To Digital Converter

In electronics, an analog-to-digital converter (ADC, A/D, or A-to-D) is a system that converts an analog signal, such as a sound picked up by a microphone or light entering a digital camera, into a digital signal. An ADC may also provide an isolated measurement such as an electronic device that converts an input analog voltage or current to a digital number representing the magnitude of the voltage or current.

3.5 Gsm Module For OTP Generation

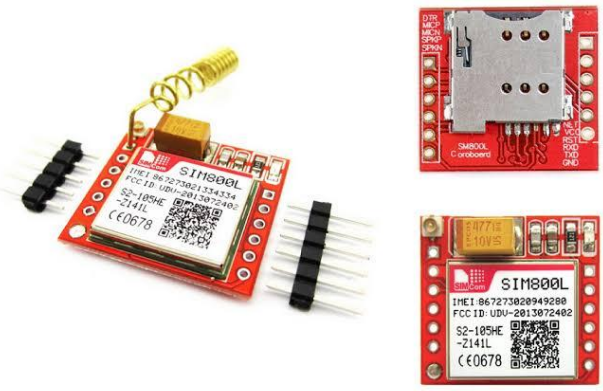


Fig 3.2 Gsm Module

SIM800L is a miniature cellular module which allows for GPRS transmission, sending and receiving SMS and making and receiving voice calls. Low cost and small footprint and quad band frequency support make this module perfect solution for any project that require long range connectivity. After connecting power module boots up, searches for cellular network and login automatically. On board LED displays connection state (no network coverage - fast blinking, logged in - slow blinking).

4. SAMPLING TECHNIQUE

A **sample** is a value or set of values at a point in time and/or space.

A **sampler** is a subsystem or operation that extracts samples from a continuous signal.

Sampling is the reduction of a continuous-time signal to a discrete-time signal. A common example is the conversion of a sound wave (a continuous signal) to a sequence of samples (a discrete-time signal).Like This we use our continuous heart beat " PQRST " wave into a sequence of samples (Discrete Time Signal)

Fig 4.1 WaveForm of Signals

There are different types of sampling techniques
1. Natural sampling
2. Flat top sampling
3. Ideal sampling

1.Natural sampling is a practical method of sampling in which pulse have finite width with time(t) carrier wave.

2. Flat top sampling same as natural but tops of carrier signal remains same with as sampled signal.

3.Ideal sampling has discrete amplitudes with carrier wave .

There two different types of sampling
1.Upsampling
2.Down sampling

Upsampling is also known as interpolation which increases the resolution of signal or image ,improves anti aliasing filter performance and reduces noise.

ex:Picture zoom -in uses interpolation

Down sampling is also known as decimation which reduces data size and image reduction

ex: Extraction of thumbnails from an image

The Output is not in continuous

➔ It is discrete by nature

➔ Using discrete signal code can be generated.

Applications

➔ Audio Sampling
➔ Speech Sampling
➔ Video Sampling
➔ 3d Sampling

5. ADVANTAGES

- Portable system
- Save risk of Havking Your Password as you can Only Access it
- Affordable system
- Improved Total 360 Security System
- Quick Access Featured Enabled
    - This system can be used in many places like banks,doors,lockers, security room and more and more it will be used in high secured places like armed forces for weapons prevention and also used as security key generating tool.

Dataset	Subjects	IPIs Avg	heart Sensor	freq.
Regular	11	21696	69.3	360
Stress	12	16008	81.7	360
Hockey	20	38424	86.4	360
Rest	58	10668	75.8	200
Exercise	53	11864	101.4	200

TABLE 1.1 : Dataset specifications

6. CONCLUSIONS

Heart Beat Security System is a new security system which should provide more secure authentication to all.When compared to other security systems , this system is more affordable and a unique security like our fingerprints and eyes.In Our Existing System,

- **Finger Print Scanner** – Hacked by Using Silica gel
- **Iris Scanner** – Fails in Some Cases like Retinal Damages
- **Pass Code** – Cracker By Hackers
- **Voice Unlock** – Throat Problems
- **Facial Recognition** – Fails in Some Situations Like Facial Surgery

Hence we Conclude that our project will be a motivational one to all.Because , this project can't work 100%.It mays have some Bugs in it .But we are almostly done and corrected most of the issues that appears.

BEST KEY STRENGTH

Dataset	Interval bits(j)	Bits Selected	Best KSeff(bit)	Single key gen time (s)
Regular	6	2-7	30.2 (+33%)	24.9 (+3.4x)
Stress	6	2-7	26.6 (+39%)	52.9 (3.6x)
Hockey	4	3-6	29.8 (+2%)	55.5 (6.7x)
Rest	5	2-6	31.3 (+92%)	47.5 (4.0x)
Exercise	8	2-6	24.9 (+3.4x)	56.8 (4.8x)

TABLE 1.2 : Best key strength per dataset using the IPI.

FUTURE SCOPE

This Heart Based Security system has a huge scope in future generations because there are more number of flaws,bugs available in existing system such as fingerprint recognition, voice unlock,facial recognition , password encryption,IRIS recognition.These systems becomes weak and the security system goes down day by day.In Future , a high security is needed to overcome the Situations.So, Heart beat is very helpful in that because heart beat is a unique like fingerprints and iris . And It can used as altenative to all other security systems

7. WAY TO OVERCOME ISSUES

1.LIMIT LOGIN ATTEMPTS

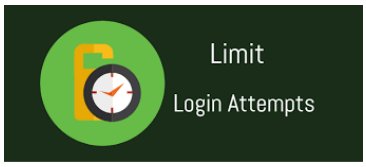


FIG 7.1 LIMIT LOGIN ATTEMPTS

LIMIT THE NUMBER OF FAILED **LOGIN ATTEMPTS** PER USER. FOR EXAMPLE, YOU CAN SAY AFTER 5 FAILED **ATTEMPTS**, LOCK THE USER OUT TEMPORARILY.

2.ADDING SECONDARY SECURITY

Fig 7.2 Secondary Security

Every System fails in some situations in order to overcome that failure issues we have to install another secondary security systems.We can either use “IRIS SCANNER” OR “OTP GENERATION”

3.PROVIDE MULTIPLE USER ACCESS

Fig 7.3 Multiple User Access

If the user is unluckily meet with any accidents or any other health problems,heartbeat may vary.or Even The user may dies in some situations so in that the security becomes permanently locked.so to overcome that this feature must be added.

4.GET NOTIFIED EVERY SECOND

Fig 7.4 Notification

You Will Get Notifications During Every Access of this system . It will show up the limits you tried and limits remaining.

REFERENCES

[1] [4] X. D. Yang,Q. H. Abbasi, A. Alomainy and Y. Hao, "*Spatial Correlation Analysis of On-Body Radio Channels Considering Statistical Significance* ", IEEE Antenna and Wireless Propagation letter, Volume 10, pp. 780-783, August 2011.

[2] H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.

[3] R. Di Bari, Q. H. Abbasi, A. Alomainy and Y. Hao, "An Advanced Ultra Wideband Channel Model for Body-Centric Wireless Networks", Progress In Electromagnetics Research (PIER), Vol. 136, pp. 79-99, 2013..

[4] O. Aziz, B. Lo, R. King, A. Darzi, and Y. Guang-Zhong, "Pervasive body sensor network: an approach to monitoring the post-operative surgical patient," in International Workshop on Wearable and Implantable Body Sensor Networks, BSN 2006., 2006, pp. 4 pp.-1C.

[5] J.K.Sowbagya, *“An approach to principles of Sampling techniques”,* Assist.Professor , Surya College Of Engineering , Villupuram.

[6] [5] S.-D. Bao et al. Using the timing information of heartbeats as an entity identifier to secure body sensor network. In T-ITB, pp. 772-779, volume 12. IEEE, 2008.

[7] M. P. Tulppo, T. Makikallio, T. Takala, T. Seppanen, and H. V. Huikuri. Quantitative beat-to-beat analysis of heart rate dynamics during exercise. American Journal of Physiology-Heart and Circulatory Physiology, 271(1):H244–H252, 1996.
K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta. Pska: usable and secure key agreement scheme for body area networks. ITB, IEEE Trans. on, 14(1):60–68, 2010.