HeartID:A Modern way of Authentication

Priyanka M.Verma, Pratibha S.Bramhane, Ashwini R.Zade

Abstract—There is need to develop a powerful mechanism so Instead of using unreliable and hackable passwords, the software, called HeartID, uses a person’s heartbeat to authenticate their identity and protect access to important information. HeartID is more convenient than existing biometric identification techniques; like fingerprints, irises; a cardiac signal requires a simple touch. Cardiac signals are also highly secure and their accuracy is rated at greater than 99 %. “HeartID is currently the only commercially available biometric authentication solution that uses the cardiac signal”. An individual holds a mouse-like controller with built-in sensors, and their unique cardiac rhythm is recognized by the connected computer. Authorized users with a recognized cardiac rhythm are immediately allowed access and logged in. As a further security measure, HeartID uses continuous monitoring, immediately logging off any user without an authenticated cardiac rhythm.

Keywords— *Air pad, Authentication, Biometric, Breathing waveform, First-to-Second ratio, Heart sound waveform, Piezoelectric sensor, Segmentation, Security*.

1 INTRODUCTION

A novel personal authentication system using heart sound waveform and/or breathing waveform pattern which promptly judges personal authentication of a person to be authenticated with a very high degree of accuracy. The personal authentication system is comprised of a waveform detection means which detects a heart sound waveform pattern and a means which compares a heart sound waveform pattern detected by the waveform detection means with a previously registered heart sound waveform pattern. If the detected heart sound waveform pattern coincides with the registered heart sound waveform pattern, the system authenticates the person to be identical. In such constitution, the system can check the autonomic heart sound which cannot be controlled by a personal will based on the previously registered heart sound waveform pattern in real time, and performs personal authentication of the person to be authenticated with very high accuracy promptly.

The strength of a biometric system is determined mainly by the trait that is used to verify the identity. Plenty of biometric traits have been studied and some of them, like fingerprint, iris and face, are nowadays used in widely deploy systems.

Today, one of the most important research directions in the field of biometrics is the characterization of novel biometric traits that can be used in combination with other traits, to limit their shortcomings or to enhance their performance.

The aim of this paper is to introduce the usage of heart sounds for biometric recognition, describing the strengths and the weaknesses of this novel trait and analyzing in detail the methods developed in future and their performance.

2 BIOMETRIC

2.1 What is biometric?

The term biometrics comes from the Greek words bios, meaning life, and metrics, meaning measure. Biometrics can be defined as measurable physiological and/or behavioural characteristics that can be utilized to verify the identity of an individual, and include fingerprint verification, hand geometry, retinal scanning, iris scanning, facial recognition and signature verification [2]. Biometric authentication is considered the automatic identification, or identity verification, of an individual using either a biological feature they possess physiological characteristic like a fingerprint or something they do behaviour characteristic, like a signature [3]. In practice, the process of identification and authentication is the ability to verify and confirm an identity. It is accomplished by using any one or a combination of the following three traditional identification techniques: something you possess; something you know; or something you are [2].

Something you possess: often referred to as a token and can be produced from a multitude of different physical objects. There are two basic types of tokens in use today: manual and automated. If a token is described as manual it means that the identification process requires some form of human intervention; in other words, a person will make the final decision of whether an identity is approved or not. Good examples of manual tokens are paper ID documents and passports. Automated tokens, on the other hand, do not involve human intervention in the identification process, but rather the identity is verified by a system/computer such as magnetic-stripe cards, memory cards, or smart cards [1].

Something you know: the knowledge should not be commonly held, but secret. Examples of regularly used secrets are passwords, pass-phrases, and personal identification numbers PINs.

Something you are: recognizing an entity through what "they are" requires measuring one or more of their biological features. Biological features can be either physiological characteristics like fingerprints or behavioural traits like an individual's signature [2],[3].

Biometrics can be divided into following categorization:

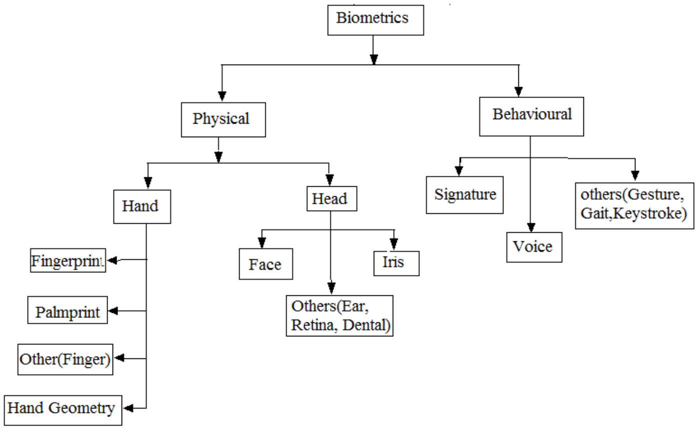

Fig 1: physical and behavioural characteristics used by biometrics

Today there are several biometric characteristics that are in use in various applications. Each biometric has its own strengths and weaknesses, and suitable applications for each biometric methodology. There are no particular biometrics which may successfully meet the requirements of all applications. Depending on the application's usage and the biometric characteristic's features we are able to suitably match a particular biometric to an application. Explain that the fingerprint- and iris-based techniques are more accurate than the voice-based technique. Nevertheless, in a phone banking application, the voice-based technique might be preferable as the bank could integrate it seamlessly into the existing telephone system.

3 DESCRIPTION

A primary object of this paper is to provide a personal authentication system which has not been researched before and enables to promptly verify personal authentication with a high degree of accuracy. The system comprises: detecting a heart sound waveform pattern and/or a breathing waveform pattern which is autonomic rhythm that cannot be controlled by personal will in real time based on the heart sound and/or breathing of a user; and verifying the detected with the previously registered heart sound waveform and/or breathing waveform pattern of the user. If the user does not keep touching a personal authentication device using heart sound waveform and/or breathing waveform pattern, the apparatus cannot be used. If anyone else touches the apparatus (when the apparatus recognizes a different heart sound and/or breathing from the registered heart sound waveform and/or breathing waveform pattern), the system can take measures such as an apparatus action stop by regarding the access as an unauthorized use. The object is to provide a breakthrough personal authentication system using heart sound waveform and/or breathing waveform pattern which surely prevents an unauthorized use of apparatus.

The present invention has been accomplished under these circumstances. A primary object of this paper is to provide a personal authentication system which has not been researched before and enables to promptly verify personal authentication with a high degree of accuracy.

A personal authentication system comprises: a waveform detection, which detects a heart sound waveform and/or breathing waveform pattern; and a means comparing the heart sound waveform and/or breathing waveform pattern detected by the waveform detection means with the previously registered heart sound waveform and/or breathing waveform pattern to judge, wherein, if the detected heart sound waveform and/or breathing waveform pattern coincides with the registered heart sound waveform and/or the registered breathing waveform pattern, the user is identified.

The waveform detection contain an air pad being filled inside with a foamed resin and the air and a piezoelectric sensor detecting a change in air pressure in the air pad, in which the air pressure of the air pad side of the piezoelectric sensor is held and other side is open up to the air so as to form a difference in pressure between the air-filled chamber and the open-up-to-the-air side. Other side of the body contacting surface of the air pad is characterizing by that a plate material is installed.

The plate material is characterized by being formed in a wedge shape where a thickness decreases in one direction.

The personal authentication system using heart sound waveform and/or breathing waveform pattern according to any one of the first to fourth, the waveform detection means is characterized by being installed in parallel.

Detection of heart sound waveform and/or breathing waveform with the waveform detection means is characterized by being carried out continuously or more than once.

The personal authentication device is characterized by being installed in a computer mouse or other input devices.

The personal authentication device is installed in a body contacting region of a mobile telephone, a portable terminal, a copy machine, a fax machine, a printer, a lighting fixture, a doorknob for building, an electric train, an automobile car, a large size construction machine, a cultivator, an aircraft, a ship and vessel, a bicycle, a two-wheeled motor vehicle, a wireless remote control and an electric appliance.

Tension or degree of excitement of a user is characterized by being measured by the heart sound waveform and/or breathing waveform pattern pitch of the user measured by the personal authentication device.

The personal authentication device registers a heart sound waveform and/or breathing waveform pattern of a user detected by a waveform detector as data, and is equipped with a learning function means for analyzing the recorded data to improve the authentication accuracy and the speed.

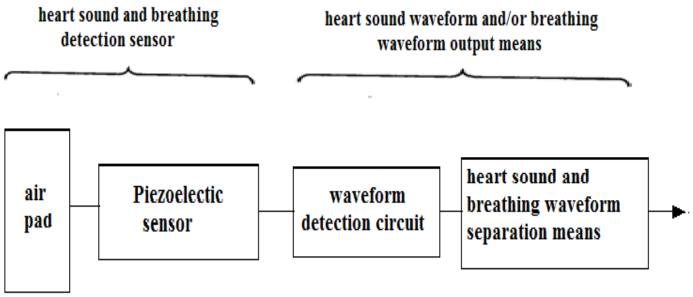
heart sound and breathing detection sensor
heart sound waveform and/or breathing waveform output means
air pad
Piezoelectic sensor
waveform detection circuit
heart sound and breathing waveform separation means

Fig 2: A block diagram showing an example of the waveform detector.

The air pad is attached to the body side, a change in the air pressure inside the air pad accompanied by a change in microseism and by breathing can be surely picked up, the sensitivity of the waveform detector can be kept well. So an air pad part of piezoelectric sensor is kept airtight and other part is constituted so as to open up to the air, the system is constituted so as to produce a difference in pressure between the air-filled space side and the air side

A known piezoelectric pressure sensor may be used for detecting a change in the air pressure inside the air pad and since the system can transmit a produced difference in pressure between the air-filled space side and the air side. The piezoelectric sensor detects slight change in pressure by the heart sound vibration or the breathing vibration which are applied to the air pad, a heart sound waveform and/or breathing waveform data can be extracted with a high degree of accuracy.

Fig 2: shows the output is representing of a waveform detection circuit and a heart sound and breathing waveform separation. The waveform detection circuit detects a heart sound and breathing waveform detected by the heart sound and breathing detection sensor which include the air pad and the piezoelectric sensor. In the heart sound and breathing waveform separation, a heart sound waveform and a breathing waveform is separated.

The heart sound and breathing waveform separation circuit is connected to a comparison circuit which is described later, and is represent so as to prevent a malfunction and a wrong judgment.

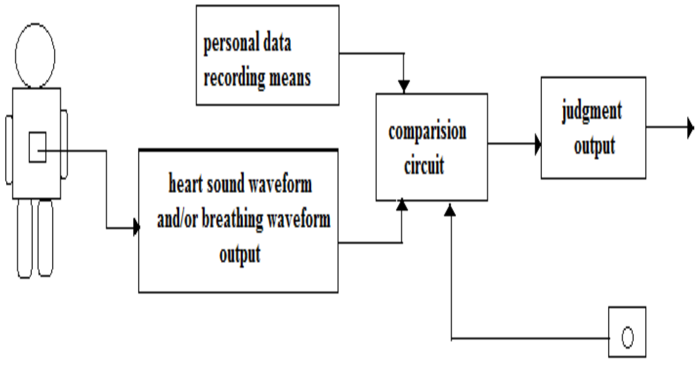
personal data recording means
heart sound waveform and/or breathing waveform output
comparision circuit
judgment output

Fig 3: is a basic block diagram of the proposed biometric system.

The heart sound waveform signal and the breathing waveform signal obtained in such a way is transmitted to the comparison circuit shown in Fig. 3 and then transmitted further to a judgment output means. The small circle inside a rectangle in Fig. 3 shows an information storage means.

The comparison circuit compares a heart sound and/or breathing waveform detected from the output with a heart sound and/or breathing waveform pattern of the user which is previously registered in the information storage means. The judged results are transmitted to the judgment output means. The judgment output means transmits to a device requiring the personal information the information where a heart sound and/or breathing waveform detected from the output means coincides or does not coincide with the heart sound and/or breathing waveform pattern of the user which is previously registered in the information storage means.

Thus, this method enables to judge personal authentication with a very degree of accuracy even in a simple system and then to take necessary action.

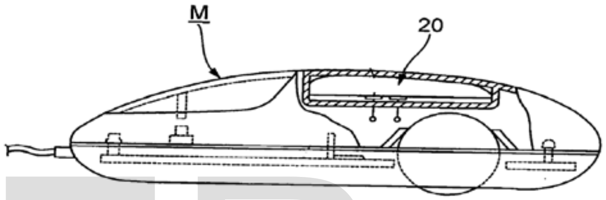

Fig 4: is the waveform detector is installed in a computer mouse.

As shown Fig 4, for example, the waveform detector equipped with detection sensor, is mounted in a mouse M which is connected to a computer body (not shown). When a heart sound and/or breathing waveform detected by the sensor is compared with the heart sound and/or breathing waveform pattern of the user which is registered in the computer body, the computer can be constitute in the following way: if these coincide with each other, the computer may be used; if these do not coincide with each other, the computer is automatically shut down. Further, if the computer is rebooted in a specific manner, the computer can be constituted so as not to be available.

Further in this, the system is constituted so that the personal authentication process is performed more than once during a period when the body of the user is contacting to the heart sound and breathing detection sensor ; and if a heart sound waveform and/or breathing waveform pattern is not continuously detected and personal authentication is not continuously repeated more than once, the user is not authenticated as the same user. Personal authentication by the system may be constituted in a manner so that the heart sound and breathing detection sensor continuously detects the heart sound waveform and/or breathing waveform more than once and the detected heart sound waveform and/or breathing waveform pattern is compared with the registered heart sound waveform and/or breathing waveform pattern more than once at optional timing. In this case, since the timing of personal authentication is optional and cannot be forecasted, the abuse can be more accurately prevented. As used herein, the term 'optional' means all timings except for 'at regular time intervals', and include a continuation of personal authentication at irregular timing and a continuation of personal authentication at random timing.

In this, the authentication work may be constituted so that a heart sound waveform and/or breathing waveform that the heart sound and/or breathing detection sensor continuously detects is compared with the registered heart sound waveform and/or breathing waveform pattern at regular time intervals (for example, per pulse interval) more than once for leading a judgment.

As explained above, the personal authentication system using heart sound waveform and/or breathing waveform pattern of this is constituted so that a user is authenticated to be identical when a heart sound waveform and/or breathing waveform detected by the heart sound and/or breathing detection sensor coincides with the registered heart sound waveform and/or breathing waveform pattern. Further, a heart sound produced by the heart pulse which is autonomic that cannot be controlled by will and a breathing which is not completely autonomic are used.

Further, in this, every heart sound waveform and/or breathing waveform of the user detected by the heart sound and/or breathing detection sensor is recorded and stored as data. With applying a learning function means which analyzes the recorded data, even if the heart sound waveform and/or breathing waveform pattern changes according to the change of health condition and physical condition of the user, this pattern is automatically updated. Even if the heart sound waveform and/or breathing waveform gradually changes according to the aging, the system can accurately judge the user without modifying the authentication system. Besides, the authentication speed can be improved. With using the system, a health of employee and the family can be controlled without being known to the person.

When the user is so nervous or excited that the heart sound waveform and/or breathing waveform pattern pitch of the user which is detected by the waveform detector is different from the registered heart sound waveform and/or breathing waveform pattern pitch.

4 PROCESSING HEART SOUND

4.1 Segmentation

In this, a variation that was employed in to separate the S1 and S2 tones from the rest of the heart sound signal, improved to deal with long heart sounds. Such a separation is done because we believe that the S1 and S2 tones are as important to heart sounds as the vowels are to the voice signal. They are stationary in the short term and they convey significant biometric information that is then processed by feature extraction algorithms [1].

A simple energy-based approach cannot be used because the signal can contain impulsive noise that could be mistaken for a significant sound. The first step of the algorithm is searching the frame with the highest energy that is called SX1. At this stage, we do not know if we found an S1 or an S2 sound. Then, in order to estimate the frequency of the heart beat, and therefore the period P of the signal, the maximum value of the autocorrelation function is computed. Low-frequency components are ignored by searching only over the portion of autocorrelation after the first minimum.

The algorithm then searches other maxima to the left and to the right of SX1, moving by a number P of frames in each direction and searching for local maxima in a window of the energy signal in order to take into account small fluctuations of the heart rate. After each maximum is selected, a constant-width window is applied to select a portion of the signal.

After having completed the search that starts from SX1, all the corresponding frames in the original signal are zeroed out, and the procedure is repeated to find a new maximum-energy frame, called SX2, and the other peaks are found in the same way.

Finally, the positions of SX1 and SX2 are compared, and the algorithm then decides if SX1, and all the frames found starting from it, must be classified as S1 or S2; the remaining identified frames are classified accordingly.

The nature of this algorithm requires that it work on short sequences, 4 to 6 seconds long, because as the sequence gets longer the periodicity of the sequence fades away due to noise and variations of the heart rate.

To overcome this problem, the signal is split into 4-seconds wide windows and the algorithm is applied to each window. The resulting sets of heart sounds endpoint are then joined into a single set.

5 THE FIRST-TO-SECOND RATIO (FSR)

In addition to standard feature extraction techniques, it would be desirable to develop ad-hoc features for the heart sound, as it is not a simple audio sequence but has specific properties that could be exploited to develop features with additional discriminative power.

This is why a time-domain feature called First-to-Second Ratio (FSR) is used. Intuitively, the FSR represents the power ratio of the first heart sound (S1) to the second heart sound (S2).

Some people tend to have an S1 sound that is louder than S2, while in others this balance is inverted. So it must to try to represent this diversity using the new feature.

6. FEATURE EXTRACTION

All segmented heartbeat waveforms are aligned by their R-peak, and clipped taking into account the typical physiological latencies between the P-R and RT complexes, which are approximately 200 and 400 milliseconds respectively. In this paper, the feature vector for each heartbeat waveform i, consists of a vector xi with the waveform amplitude values, which corresponds to 600ms of collected signal. During the enrollment stage, the patterns xi are stored in the database of known users, whereas in the recognition stage, it is the pattern which will be checked against the database. Depending on the latency requirements of the application, we can also use an average of m feature vectors, which is prone to further improve the recognition rates.

CONCLUSION

Biometric authentication is one of the most exciting technical improvements of recent history and looks set to change the way in which the majority of individuals live.

The discussion above shows that biometric authentication is an interesting topic that a lot of research is going on in this area and that it can be used for secure systems despite all disadvantages. At the moment it is recommended to combine biometric authentication with any other authentication technology.

Biometric authentication is one of the most exciting technical improvements of recent history and looks set to change the way in which the majority of individuals live.

A novel biometric identification technique is more advantageous and secure over the previously design biometric techniques. Such multi-factor authentication systems are always more secure and it is also common practice to use combinations of different authentication methods.

REFERENCES

[1] Beritelli, F. & Spadaccini, A. (2010a). An improved biometric identification system based on heart sounds and gaussian mixture models, Proceedings of the 2010 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, IEEE, pp. 31–35.

[2] Ashbourn, J., Biometrics: Advanced Identity Verification: The Complete Guide. Springer-Verlag, London, . . 2000: Springer. 201.

[3] Wayman, J.L. and L. Alyea, Picking the Best Biometric for Your Applications, in National Biometric Test Center Collected Works. 2000, National Biometric Test Center: San Jose. p. 269-275.

[4] Beritelli, F. & Spadaccini, A. (10). A statistical approach to biometric identity verification based on heart sounds, Proceedings of the Fourth International Conference on Emerging Security Information, Systems and Technologies (secureware10), IEEE, pp. 93–96. URL: http://dx.medra.org/10.1109/SECURWARE.10.23

[5] El-Bendary, N., Al-Qaheri, H., Zawbaa, H. M., Hamed, M., Hassanien, A. E., Zhao, Q. & Abraham, A. (10). Hsas: Heart sound authentication system, Nature and Biologically Inspired Computing (NaBIC), 10 Second World Congress on, pp. 351 –356.

[6] Fatemian, S., Agrafioti, F. & Hatzinakos, D. (10). Heartid: Cardiac biometric recognition Biometrics: Theory Applications and Systems (BTAS), 10 Fourth IEEE International Conference on, pp. 1 –5.

[7] Fatemian, S., Agrafioti, F. & Hatzinakos, D. (10). Heartid: Cardiac biometric recognition Biometrics: Theory Applications and Systems (BTAS), 10 Fourth IEEE International Conference on, pp. 1 –5.

[8] Jasper, J. & Othman, K. (10). Feature extraction for human identification based on envelogram signal analysis of cardiac sounds in time-frequency domain Electronics and Information Engineering (ICEIE), 10 International Conference On, Vol. 2,pp. V2–228 –V2–23.

[9] Phua, K., Chen, J., Dat, T. H. & Shue, L. (08). Heart sound as a biometric, Pattern

[10] Recognition 41(3): 906–919Jain, A. K., Ross, A. A. & Pankanti, S. (06). Biometrics: A tool for information security, IEEE Transactions on Information Forensics and Security 1(2): 125–143.

[11] Prabhakar, S., S. Pankanti, and A.K. Jain, Biometrics Recognition: Security and Privacy Concerns. IEEE Security & Privacy, 03. 1(2): p. 33-42.

[12] Biel, L. & Pettersson, O. & Philipson, L. & Wide, P. (01). ECG Analysis: A New Approach in Human Identification, IEEE Transactions on Instrumentation and Measurement 50(3): 808–812.