International Journal of Advanced Science and Technology
Vol. 29, No. 12s, (2020), pp. 2705-2711

A Combined View of Biometrics with Steganography in Pervasive Environment

Sonali Goyal[1], Neera Batra[2]
[1] *Computers Science & Engg. Department, MMEC, Maharishi Markandeshwar (Deemed to be University) Mullana*
[2] *Computers Science & Engg. Department, MMEC, Maharishi Markandeshwar (Deemed to be University) Mullana*

[1]*sonaliguglani21@gmail.com*, [2]*batraneera1@gmail.com*

Abstract

An evolving concept in pervasive environment is the recognition of individuals by biometric data as opposed to password-dependent authentication strategies that were traditionally used. The biometric system has gained significant interest due to the necessity for safety and security. The approaches like watermarking and steganography are being used to enhance the biometric data protection. Several biometric system attacks and security approaches to protect the biometric data have been discussed in this paper. Furthermore, the study gives an outline of the combined view of steganography approach with multimodal biometric system (Face + Voice). The findings concludes with the proposal of a new generic integrated approach for a smart and secure biometric system.

Keywords: *Pervasive computing, Biometrics, Face recognition, Voive recognition, Steganography*

1. Introduction

Weiser defines pervasive computing as a fully connected medium which is integrated with normal environment and that is not distinguishable from that [11]. Pervasive computing devices are very small devices in a range of a few millimeters to small meters and these devices are connected to each other via wired or wireless links. The aim of this computing is to make simpler life of every individual by using a number of tools so that information can be managed successfully and easily. Pervasive computing technique is beyond the concept of personal computers. It is based on the concept that from clothing to any type of devices, they are integrated with chips in a way to connect with the network of other devices. These devices are consists of a number of characteristics like: they have small, inexpensive processors with limited memory, these devices are connecting with other devices without any user interaction and they will be connected by wired or wireless links.

In Pervasive environment, Biometrics is one of the technique used for authentication purpose irrespective of login ID/ password method as well as smart card method due to its drawbacks like stolen card, password forgotten etc. Due to these problems, Biometric technique has been used. Biometric word is made up of two words: bio and metric which means measurement of life [12]. Use of Biometric technique is needed to identify the presence of valid user. From last some years, biometric technique is integrated in phones by Apple and Samsung companies for the process of phone unlocking with the entity's finger print data and face recognition. However, with the development of applications, security can't be ignored. This constitutes a big challenge as number of biometric techniques are there like fingerprint technology which is having minutia points i.e. very sensitive information for the identification of each fingerprint uniquely, face recognition which contains several landmark points for the identification of facial features, hand geometry which automatically measures the number of dimensions of the hand and fingers and

then compares those measurements to a prestored data, voice recognition which recognizes an entity on the basis of voice signals, face thermo grams are the heat patterns emitted on skin. These patterns are formed by branching of blood vessels etc. If data is stolen by any technique then that data can be used for any illegal purpose like thefts, fraud etc. Therefore, security is required in biometric authentication. From all biometric techniques, Face and Voice recognition technique is the most reliable and accurate technique used for an entity's recognition. So, a combination of face and voice recognition i.e multimodal technique, is used irrespective of using an unimodal technique. In a biometric system of authentication, sensitive data is at risk. So, the measures for security of data protection must cover all possibilities. There are three ways to be applied for security as shown in figure 1.

a.)Cryptography- It is where the digitised data is securely encrypted whereby the decryption of the contents can only be possible with the help of appropriate key available with the receipent.

b.)Watermarking- It is a visible mark for biometric image authentication.

c.)Steganography- It is a technique in which digitised biometric data is embedded into a host file in a way to obscure the real purpose of host image.

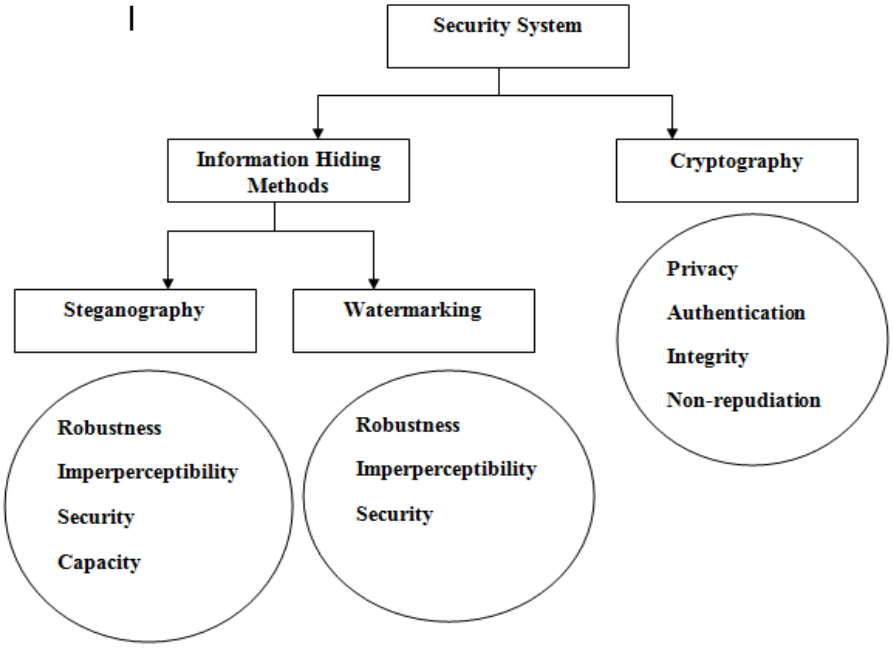

Figure. 1. Ways of Security

From these number of ways for security optimization with biometric data i.e. information hiding, steganography can be used in this paper instead of cryptography and watermarking technique due to its imperperceptibility feature with its invisibility attribute in which the secret data in not visible, it stays out of the idea and less attacks are attracted [2]. Fig. 2 shows different attacks that may possible on biometric security systems.

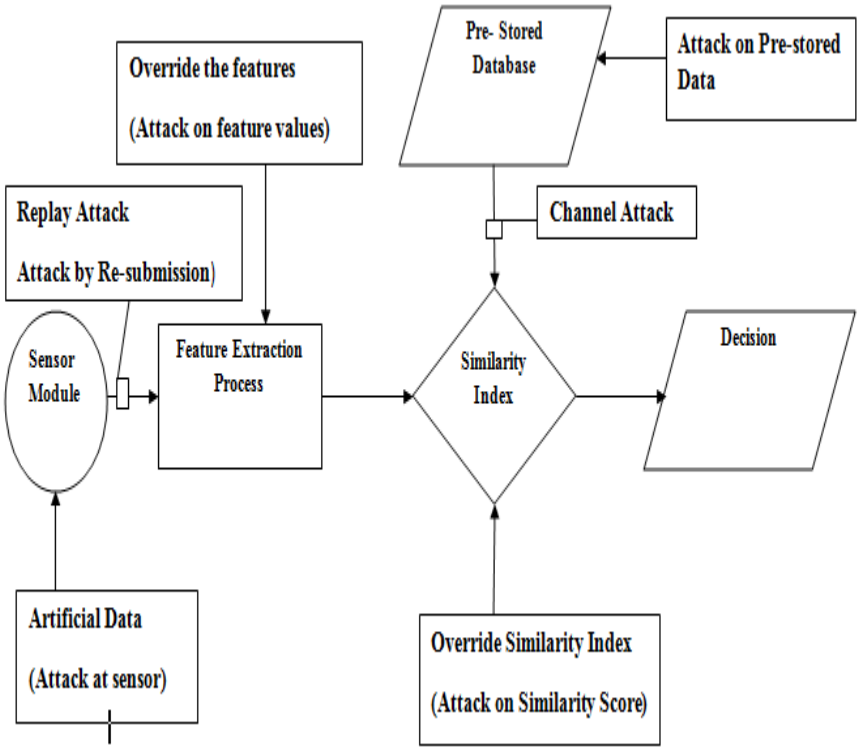

Figure 2. Biometric Security System Attacks

Steganography is a way by which critical data is hidden in a trustworthy medium without third person's awareness that some data exists [3]. This technique can be used by two ways: reversible technique that helps in full recovery of actual file after hidden data is extracted and irreversible technique in which recovery of actual file is distorted after extraction of hidden data.
The remainder of this paper is summarized in such a way: Section 2 describes the previous work, Section 3 gives an overview of biometric security system, Section 4 gives an overview of steganography, section 5 describes a real life application for this technique and in section 6, conclusion and future work suggestions are listed.

2. Literature Review

In the past few years, different researchers have given their ideas with their experience for the security of biometric technique with steganography. So, this section summarizes the evaluatation of the performance of different techniques used for the security of biometric data.

One of the first work of this category was proposed by Mandy Douglas [3]. The authors main focus is on fingerprint biometric technique. Various strengths and weaknesses are defined for different two steganalysis strategies (targeted and blind) for breaking number of techniques of steganography.

In the next paper, Maytham Mohammed has defined that how to integrate biometric technique with cryptography in order to encrypt the extracted data of anatomical features. In this, main focus is on identification of acceptance level of steganography embedding into the applications of biometric technique[4]. It also defines how to exchange steganography keys securely, to identify and provide address for legal implications and to develop standards for industry. Fingerprint authentication is used by author by taking three levels of biometric security.

Another method used for authentication for network security is the use of biometrics with steganography which is three factor approach and the factors includes smartcard, IP, fingerprint biometric with steganography. This three factor authentication technique is upgraded by the given scheme of biometric with steagnography in which IP is replaced by password and it provides strong protection against the attacks at a very reasonable price defined by P. Dhivya [7].

This paper has been given by Priya Yankanchi to define a new framework that how to secure data hiding by integrating biometric approach with steganography technique. Image steganography[8] is used irrespective of other methods as they are easily vulnerable to attacks. So, proposed framework uses steganography with hand geometry biometric technique by extracting hand image features of individuals and this provides double layer data security.

3. Biometric System with Security

Biometric systems are one of the recognition system for a particular pattern which verifies a human being by using his/her unique characterstics i.e first is physical and other one is personal. An example of the physical qualities used for biometric system are: face recognition, iris recognition, hand geometry etc. and some personal qualities used for biometric system are: voice recognition, handwriting pattern etc. In this system, there is no need to remember password, pin etc. This biometric system is also helpful in finding unauthorized entity which can gain access for computers, workplaces, mobile devices, banks etc. Biometric systems are automated systems to identify an entity by physiological or behavioural characterstics. Physical characterstics are if an entity is identified by the shape of the body e.g. fingerprint patterns, face recognition, ear recognition etc. and behavioural characterstics are if an entity is identified by its behavior e.g. signature, voice etc. There is a need of regular verification in behavioural characterstics as they can be changed during their lifetime. The biometric system can be used in two ways: identification and verification mode. Identification mode tries to identify a person by comparing an entity's input with all prestored templates saved on the system. The template which is most similar to an entity's input will be declared as an output. Verification mode determines the person by using the phrase "Is this person who they say they are". Verification mode works as an one-to-one matching system[2]. Every biometric technique consists of four parts: Acquisition of data in which data is collected of an entity from a number of sources, Feature Extraction in which collected information is processed in order to extract the features, Matching which compares the extracted features with prestored features in the database and Decision Control system in which decision is taken in order to accept or reject the identity of an entity. The face is one of the most promising techniques of biometric technology and it is the most common method of recognition. A problem with other biometric techniques based on fingerprint, iris, signature recognition etc. is for collection of data e.g. in case of fingerprint recognition [1], the user has to put finger in proper manner and direction. But in face recognition, collection of face images is not difficult and thus it can be used as a biometric technique. Each face has special features that defines a particular entity. Emotions can also be recognized by using pixel intensity which corresponds features used for detection of emotions [5]. Face recognition is a biometric technique which is most frequently used in a number of applications like banking, security information, virtual reality etc.

Other used technique for this paper is Voice recognition in which the total data amount which is generated during the voice production is very large and not all of them contain useful information. So, fewer data is required to represent characteristics of voice and the person who has spoken it. Voice recognition is a method used to recognize a word automatically which is spoken by any speaker. The concept of voice recognition was originated by the way human communicate to each other. No two individuals have similar voice. Voice recognition technique is selected on the basis of a criterion: accessibility, distinctiveness, robustness etc. Distinctiveness is used to measure the differences in the patterns among the individuals, robustness is no repeatable pattern and cannot be subjected to large changes and accessibility defines the easiness for presentation of data to sensor device [6]. Recognition through a voice is very economical as the equipments for collecting speech samples are cheaply and easily available.

If work is done on single authentication technique, it is called as a unimodal technique of biometric but it does not fulfill the requirements regarding performance, noise etc. So to overcome these issues, multimodal technique of biometric system has been taken into consideration in the proposed modal. A combination of two authentication techniques has been used: face recognition at first and then, voice recognition in a single system. The main aim to combine these systems is to increase the performance and accuracy of the modal.

4. Overview of Steganography

Steganography word is derived from the Greek words- stegos means "cover" and grafia means "writing"[10]. Its use is to hide the messages into some other type of information as videos, audio or images and these types are known as mediums. One of the benefit of using steganography is humans can't notice minor changes of the medium. Some important terms used for steganography are: Secret data (It is the data which requires covered form to send from one area to another), Cover Medium (It describes the medium used for secret data covering), Stego Object which provides the cover medium as early as the secret is successfully embedded, Stego Key gives us the key of procedure that how the data is embedded into the cover medium. This key is used at both the sides: embedding and retrieving side, Imperceptibility is used to define stego object's quality and Capacity defines how much data is embedded into the cover. There are two algorithms used for a stegnographic system: for hiding and for retrieving. In first algorithm, data is embedded with the cover medium for hiding process and this complete process must be undetectable by making the stego object as similar as the cover medium. To increase the security of the hidden data, secret key is used in such a way that without knowing the secret key, the data will not be retrieved even though the hiding algorithm is known[9]. It provides more security as very less chances are there for an unintended entity to discover that a message is sent. In cryptography, an entity knows that something has been encrypted but in steganography, no entity is aware of hidden message's existence. Anoother technique used for authentication purpose and protection of copyrights is watermarking technique. It is mainly used for the prevention of illegal copying of digital media ownership.

5. Real Life Application

One of the most promosing application based on this integrated approach is Smart Home Security System. In a way to make home network more intelligent, smart devices are used with high processing and networking abilities. Networking ability means collection of sensors which can gather data and transmit that sensed data like temperature, humidity, light etc. Secure door entry is the must component of overall home security strategy and for this component, face and voice recognition technique has been used which can stay connected to smart home security system with mobile phones. In today's world, phones and gadgets can unlock with voice, a finger scan or a face-scan. Biometrics have been used for high security facilities and businesses for security purpose instead of traditional methods like locks for door entry at homes. In smart home security systems, PINs or fobs are used for unlocking doors. How good would it be if door lock is able to recognize you and unlock the door without the need of a PIN or key? Home security systems with biometrically secured door entry (e.g. face and voice recognition) can help to achieve it.

Individual care is other important factor to provide security and safety to an individual who is residing alone at home. So, to obtain this objective, recognition of a person who is at door is done by using two modules: Face Recognition and Voice Recognition. Initially, when a person knocks at the door, face of that person is recognized. If recognised, for double layer security, next module i.e. Voice Recognition system becomes active. If voice is also recognized, then, access to home is provided to that person by an individual who is living alone at home.

6. Proposed Solution

A new integrated approach has been proposed in this paper, which combines the steganograpgy technique with existing multimodal smart home security system (face+voice). In this integrated approach, if steganogarphy technique is integrated in a way to hide the personal details of an entity who is coming at the door, then, there will be no awareness by third person about the data existence and very less chances of misusing the data will be there. Figure 3 depicts the working flow diagram of the proposed integrated approach to protect the original user data by using the concept of steganography. The proposed system may include different phases: pre-processing, feature extraction, template, stego data creation, extraction of stego data and then recognition. In the first module, the sensor captures the biometric data from the entity and then that data is converted into feature set. In the second module, stego data is created by using cover image for

encryption method and then in the third module, the stego data is extracted by decryption method in order to recognize the entity. Finally, the proposed system may match the template with pre stored data and check the similarity to find whether that entity is authorized or not.

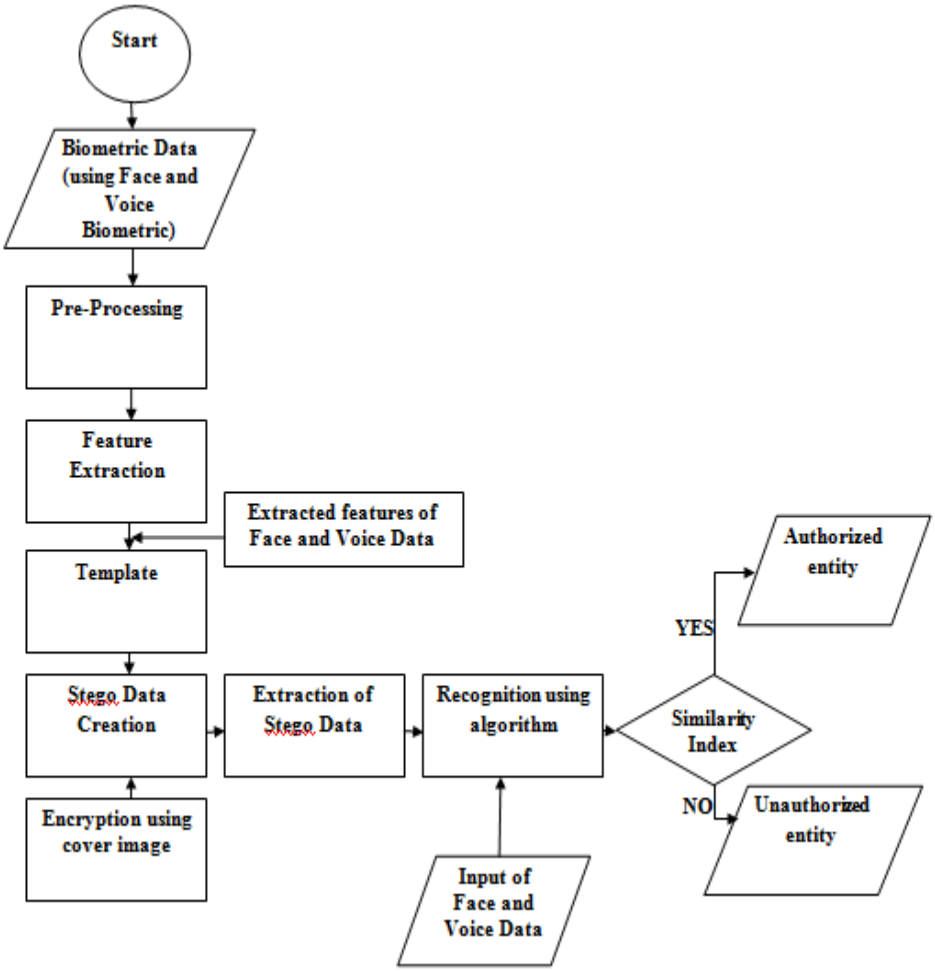

Figure 3. Flow diagram of Proposed Modal

7. Conclusion and Future Work

In this paper, number of biometric security system attacks have been studied and represented diagrammatically and different security techniques have been studied and analysed to secure biometric data. In today's era, the home automation paradigm in the pervasive environment is growing and diverging. However, security is an important key concern in a smart home system. Hence, there is a need of such integrated approach which should be implemented aligned with proposed solution.

The Multimodal biometric security system with Steganography is used for recognition and authentication purpose using face and voice biometric technique in pervasive environment, this system provides better data protection. This proposed system seems more secure as compared to unimodal biometric system due to integrated biometric features.

In addition, steganography technique enhances more security. So, it can be used effectively and efficiently in smart home security systems. Hacking means unauthorized access to data collected at the transmission time. With effect to steganography, this hacking problem is known as Steganalysis which is a way by which a steganalyzer cracks the cover image to get the hidden data. So, in future, use of Steganography with Cryptography could be the future work for any application.

References

1. S. Pramothini, Y.V.V.S. Sai Pavan, N. Harini. Securing Images with Fingerprint Data using Steganography and Blockchain. Int. Journal of Recent Technology and Engineering. Dec 2018;7(4S2):82-86.
2. Sukhdev Singh, Chander Kant. A Novel Approach to secure Biometric Template with Steganography. International Journal of Advanced Research in Computer Science. June 2017;8(5):1101-1105.
3. Mandy Douglas, Karen Bailey, Mark Leeney, Kevin Curran. An Overview of Steganography Techniques applied to the protection of Biometric Data. Multimed Tools Appl. 2018;77:17333-17335.
4. Maytham Mohammed, Mohammed Mahdi Hashim, Mustafa Sabah Taha. Review Paper on Biometric Data Protection Using Steganographic Techniques. Journal of Advanced Research in Dynamic and Control Systems. Oct 2018;3(4).
5. Veda D, Bhargavi V, Harshitha S, Navyashree S. A Literature Survey on Biometric Steganography using Visual Object for Remote Aunthentication. International Journal of Advanced Research in Computer Engineering and Technology. May 2017;6(5):730-736.
6. Hetal R. Patel, Khushboo Sawant, Krishnakant Kishore. Fingerprint based Image Steganography in Transform Domain. International Journal of Engineering Sciences and Research Technology. Jan 2015;4(1):189-194.
7. P. Dhivya, S. Mohanagowri, Dr. N. Saravanaselvam. An Improved Authentication Framework using Steganography along with Biometrics for Network Security. International Journal of Computer Computer Science and Mobile Computing. Oct. 2013;2(10):30-35.
8. Priya Yankanchi, Shanmukhappa A. Angadi. Biometric Steganography: A New Approach using Hand Geometry. International Journal of Recent Trends in Engineering and Research. Sep 2016;2(9): 96-104.
9. Nishant Kaushik, Parveen Sultana H, Senthil Jayavel. Remote Aunthentical using Face Recognition with Steganography. International Journal of Recent Technology and Engineering. Nov 2018;7(4S):351-354.
10. Prerana Kamble, Sangita Nikumbh. Security System in ATM using Multimodal Biometric System and Steganographic Technique. International Journal of Innovative Research in Science, Engineering and Technology. April 2015;4(4):2161-2168.
11. Shanthini, B. and S. Swamynathan. Multimodal Biometric Based Secured Authentication System using Steganography. Journal of Computer Science. 2012;8(7):1012-1021.
12. Stan Kurkovsky. Pervasive Computing: Past, Present and Future. International Conference on Information and Communication Technology. Jan 2008; 1-7.
13. Dheerender P, Ankita Chaturvedi, Sourav Mukhopadhyay. An Improved Biometric Based Remote User Authentication System for Connected Healthcare. Int. J. Adhoc and Ubiquitous Computing. 2015;18(½):75-84.
14. Sonali Goyal, Neera Batra. Towards Pervasive Computing in Individual Care: A Literature Review. International Journal of Engineering Science and Technology. Nov 2015; 7(11): 382-392.
15. Sonali Goyal, Neera Batra. A Review on Face Recognition Algorithms. International Journal of Advanced and Innovative Research. 2015; 4(12): 150-153.