isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 3 ,May,2016 ,ISSN_NO: 2321-3337

Robust Biometric Based Authentication Scheme Using Watermarking

T.Akshaya[1], K.Kalaiselvi[2] , Dr.G.R.Suresh[3] PG Scholar, Department of CSE,

Saveetha Engineering College,Thandalam-638112, Chennai, Tamilnadu, India.

Assistant Professor, Department of CSE, Saveetha Engineering College,

Thandalam-638112, Chennai, Tamilnadu , India.Professor, Department of ECE,

Easwari Engineering College, Bharathi Salai, Ramapuram - 600089, Chennai, Tamil Nadu, India.

[1] akshayathangavel93@gmail.com [2] mkkalai1981@gmail.com [3] sureshgr@rediffmail.com

ABSTRACT— *In wireless communications sensitive information is frequently exchanged, requiring remote authentication. Remote authentication involves the submission of encrypted information, along with visual and audio cues (facial images/videos, human voice etc.). Nevertheless, Trojan Horse and other attacks can cause serious problems, especially in cases of remote examinations (in remote studying) or interviewing (for personnel hiring). This paper proposes a robust authentication mechanism based on semantic segmentation, chaotic encryption and data hiding. Biometric verification is considered a subset of biometric authentication. The biometric technologies involved are based on the ways in which individuals can be uniquely identified through one or more distinguishing biological traits, such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, keystroke dynamics, DNA and signatures. Biometric authentication is the application of that proof of identity as part of a process validating a user for access to a system. Biometric technologies are used to secure a wide range of electronic communications, including enterprise security, online commerce and banking -- even just logging in to a computer or smart phone. The main aim of this project is to propose a authentication on Steganographic video object using biometrics in wireless networks and to perform robust authentication mechanism based on semantic segmentation, encryption and data hiding.*

Keywords— Biometrics Hiding, Steganographic System, Remote Authentication, Biometrics, Video Object.

1, INTRODUCTION

Wireless network is the transfer of information between two or more points that are not connected by an electrical conductor. The most common wireless technologies used are radio waves. Wireless communication involves the transmission of information over a distance without help of wires, cables or any other forms of electrical conductors. The transmitted distance can be anywhere between a few meters, example - a television's remote control and thousands of kilometers for example radio communication. Some of the devices used for wireless communication are cordless telephones, mobiles, GPS units, wireless computer parts, and satellite television.

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks and enterprise installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication.

Examples of wireless networks include cell phone networks, Wi-Fi local networks and terrestrial microwave networks. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools.

In wireless networks, biometrics is used for the measurement and statistical analysis of people's physical and behavioral characteristics. The technology is mainly used for identification and access control, for identifying individuals that are under surveillance. The basic premise of biometric authentication is that everyone is unique and an individual can be identified by his or her intrinsic physical or behavioral traits. The term "biometrics" is derived from the Greek words "bio" meaning life and "metric" meaning to measure.

Biometric authentication is a type of system that relies on the unique biological characteristics of individuals to verify identity for secure access to electronic systems via a wireless networks. There are two main types of biometric identifiers they are physiological characteristics and behavioral characteristics it defines the shape or composition of the body and behavior of a person. Examples of physiological characteristics used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odor. Behavioral characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice. Certain biometric identifiers, such as monitoring keystrokes or gait in real time, can be used to provide continuous authentication instead of a single one-off authentication check.

2, REQUIREMENTS

The main aim of this project is to propose an authentication on Steganographic video object using biometrics in wireless networks and to perform robust authentication mechanism based on semantic segmentation, encryption and data hiding.

- Biometrics based human authentication over wireless channels under fault tolerant protocols.
- Automatic extraction of semantically meaningful video objects for embedding the encrypted biometrics information.
- Chaotic cipher, which works like a onetime pad, to encrypt biometrics identifiers.

The objective of the system is to develop a remote human authentication scheme over wireless channels under loss tolerant transmission protocols, This system is used to ensure a robustness against deciphering, noise and compression and to develop a good encryption capacity, and ease of implementation. For this purpose this system encrypt biometric signals to allow for natural authentication and involve a Chaotic Pseudo-Random Bit Generator (C-PRBG) to create the keys that trigger the whole encryption to increase security, and the encrypted biometric signal is hidden in a VO, which can reliably be detected in modern applications that involve teleconferencing.

3, PROPOSED METHOD

The proposed remote human authentication scheme over wireless channels under loss tolerant transmission protocols, aims to ensure robustness against deciphering, noise and compression, good encryption capacity, and ease of implementation. The main features of the proposed systems are as follows

- Employ wavelet based steganography,
- Encrypt biometric signals to allow for natural authentication,
- Involve a chaotic pseudo-random bit generator (C-PRBG) to create the keys that trigger the whole encryption to increase security, and
- The encrypted biometric signal is hidden in a VO, which can reliably be detected in modern applications that involve teleconferencing.

3.1 Advantages of Proposed System

- Biometrics based human authentication over wireless channels under fault tolerant protocols.

- Automatic extraction of semantically meaningful video objects for embedding the encrypted biometrics information.
- Chaotic cipher, which works like a onetime pad, to encrypt biometrics identifiers.

4, ARCHITECTURE

4.1 Introduction

System architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. The system comprised the components, the externally visible properties of those components, the relationships (e.g. the behavior) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADLs).

4.2 Design Structure

Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition and retina.

4.2.1 Capturing Video Object

In this phase user profile and face can be captured by Remote server. Before capturing human face, every user has to register their profile information into the server. Once the registration process is completed, server capturing the face. On capturing, video mode automatically capture image object from that video. The user face is captured automatically storing into the server.

4.2.2 Uploading Biometrics And Hiding Into Video Object

Once human face capturing process is completed, server will capture the user appropriate biometrics. Here biometrics are not directly storing into the server. Every biometrics has to be encrypted and watermarked into the user face. For encryption here we are going to apply blowfish algorithm. This algorithm read every pixel values of the biometrics and changes the pixel values of it. After encryption process, server will embed encrypted biometrics into the human face. For embedding (watermarking) we are going to apply Least Significant Bit (LSB) techniques. These techniques will read every rows and columns of the biometrics and embedding into the appropriate rows and columns of the human face. So every watermarked image is maintained in the server.

4.2.3 Remote Server Authentication

In the module, remote server authentication is going to be performed. If user wants to access the application means he/she has to give his face and biometrics to the server. Server will match face with every face on the database. If server identified the matched face means, server will extract the fingerprint from that image. After extracting, server checks the face and biometrics into the matched face and biometrics. If both are matches only server will authenticate the user.

4.2.4 Application Access & Bank Transaction

Once all authentication process was completed, user can access the application. Here we are going to develop ration shop application. Now a day's person want to buy ration products means they will use ration card and buy the product. In ration shop they are not validating that appropriate ration card holder only buy their own product. So for validating on ration shop, we are going to apply this authentication. For every time user has to purchase product means, he/she has to give his own face and biometrics into the server. Once validating only user can buy ration product. After purchasing the product user can pay amount through bank transaction.

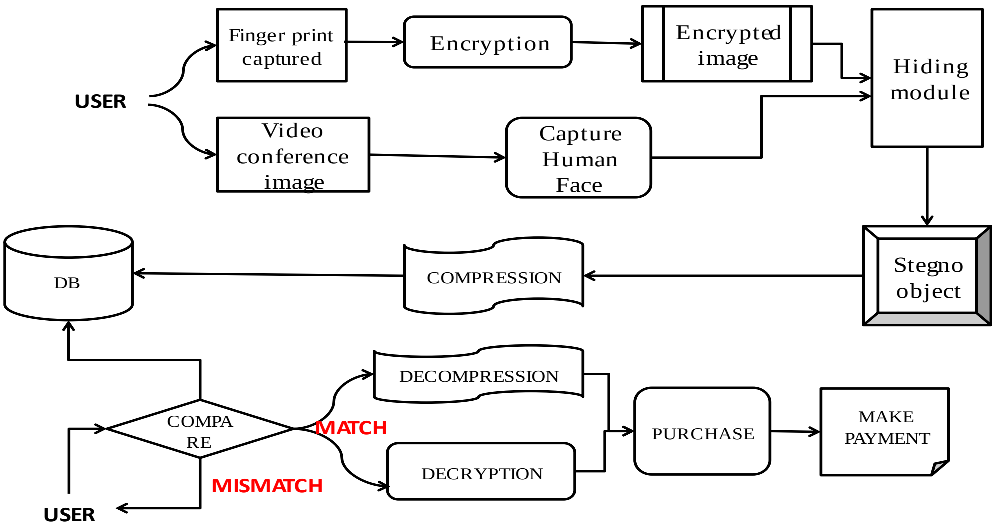

Figure 4.1 System Architecture

5, CONCLUSION.

Biometric signals enter more and more into our everyday lives, since governments, as well as other organizations, resort to their use in accomplishing crucial procedures (e.g. citizen authentication). Thus there is an urgent need to further develop and integrate biometric authentication techniques into practical applications Towards this direction in this paper the domain of biometrics authentication over error-prone networks has been examined. Since steganography by itself does not ensure secrecy, it was combined with a chaotic encryption system. The proposed procedure, except of providing results that is imperceptible to the human visual system, it also outputs a stego-object that can resist different signal distortions, and steganalytic attacks.

Experimental evaluation and detailed theoretical security analysis illustrate the performance of the proposed system in terms of security. The well-known NIST tests were applied to the encrypted biometric signals (fingerprints in our case) to verify the robustness of the proposed chaotic encryption scheme. A series of steganalytic attacks were also applied, using state-of-art steganalysis tools. Results indicate that the use of QSWTs provides high levels of robustness, keeping at the same time the ease of implementation and the compatibility to well-known and widely used image and video compression standards. The system is able to recover the hidden encrypted biometric signal under different losses. Even though simulated, losses fluctuated in the typical ranges, encountered in real communication channels. Finally it should be mentioned that all these merits are accompanied by efficient bandwidth usage, since the rate control mechanism is provided with the content awareness feature.

6. Future Enhancement.

In future research, the effects of compression and mobile transmission of other hidden biometric signals (e.g. voice or iris) should also be examined. The problem of lost biometric data is also of high interest. Techniques from the areas of image error concealment, region restoration or region matching can be used for this purpose. For instance, the lost biometric data can be concealed from the authentication module, so that it attempts to perform authentication even though parts are missing (parts that do not contain any crucial information, e.g. terminations/bifurcations in case of fingerprints). Finally, the hash value of a biometric identifier could be utilized (which could save us from seeking large video objects or lead to much more robustness to losses), so that there is a centralized authentication service (trusted third party) and the biometric identifier could not be retrieved by other legal entities.

REFERENCES

#1. A. Madero, Password secured systems and negative authentication. Thesis: S.M. in Engineering and Management, Massachusetts Institute of Technology, Engineering Systems Division, 2013. [Online]. Available: http://hdl.handle.net/1721.1/90691

#2. 2013, "Identity fraud report: Data breaches becoming a treasure trove for fraudsters," Javelin Strategy and Research, Tech. Rep., 2013.

#3. E.-J. Yoon and K.-Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," The Journal of Supercomputing, vol. 63, no. 1, pp. 235–255, Jan. 2013.

#4. H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, "Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme," in Computational Science and Its Applications, ser.Lecture Notes in Computer Science, vol. 7335. Spinger-Verlag, 2012,pp. 391–406.

#5. M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," Expert Systems with Applications, vol. 41, no. 4, pp.1411–1418, Mar. 2014.

#6. L. Lamport, "Password authentication Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981. [7] W. Stallings, Cryptography and Network Security: Principles and Practices. Prentice-Hall, 5th edition, Upper Saddle River, NJ, USA, 2010.

#8. I.-E. Liao, C.-C. Lee, and M.-S. Hwang, "A password authentication scheme over insecure networks," Journal of Computer and System Sciences, vol. 72, pp. 727–740, 2006.

#9. M. Jakobsson and M. Dhiman, "The benefits of understanding pass- words," in Mobile Authentication, ser. SpringerBriefs in Computer Science. Springer New York, 2013, pp. 5–24

#10. M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in Proceedings of the 17th ACM Conference on Computer and Communications Security. ACM, 2010, pp. 162–175.