Robust Biometrics Based Authentication Scheme Using Watermarking

P.Krithika[1], S.Kavya gayathri[2], B.Jaya shree[3]

[1] *Student, Department of Computer science, Panimalar Engineering College, Tamil Nadu, India*

[2] *Student, Department of Computer science, Panimalar Engineering College, Tamil Nadu, India*

[3] *Student, Department of Computer science, Panimalar Engineering College, Tamil Nadu, India*

Abstract

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.

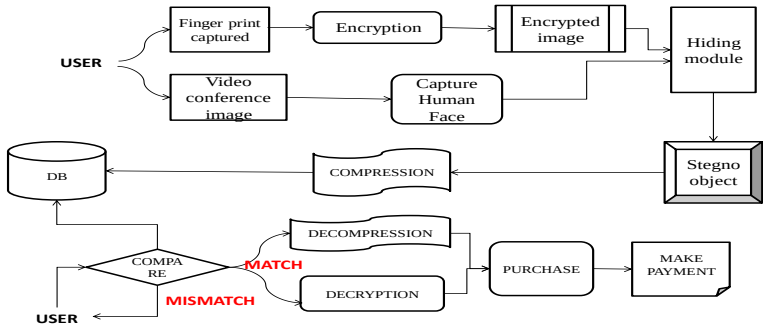
Keywords: Biometricshiding, StegnographicSystems ,remote authentication, video objects, Biometrics

1.INTRODUCTION

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. Authentication is done by using BIOMETRICS.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,irispatterns,etc.

In this project we use both fingerprints and face patterns .

Fingerprints are encrypted using blow fish algorithm and face patterns are watermarked using steganography.



2.Related work

Remote user authentication for multi-server environment has resolved theproblem of users to manage the different identities and passwords[1] .A wavelet-based blind watermarking scheme has been proposed as a means to provide protection against false matching of a possibly tampered fingerprint by embedding a binary name label of the fingerprint owner in the fingerprint [3]. The authentication scheme prevents the scenario of many logged in users with the same login identity,and does not require password/verifier table to validate the users' login request[2]. Due to the Internet's openness and lack of security concern, the user authentication scheme is one of the most important security primitives in the Internet activities[5]. Multi-server authenticated key agreement (MSAKA) protocols allow the user to register at the registration center (RC) once and can access all the permitted services provided by the eligible servers[4].

3.Proposed System

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

3.1 Capturing video Object:

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

3.2 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 pixels values of the biometrics and change 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.

3.3 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.

3.4 Application Access And 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.

4.Conclusion

Biometric signals enter more and more into our every-day 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.

5.Experimental Results

Fig 5.1:homepage

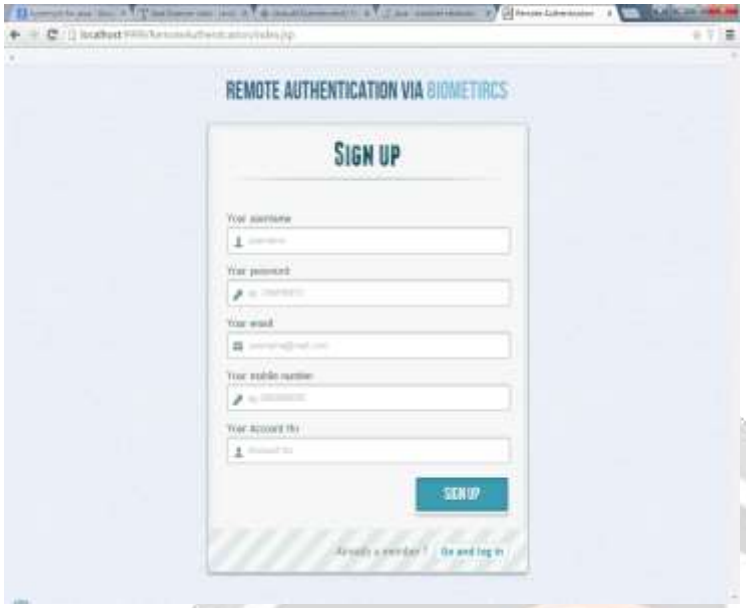


Fig 5.2:User details

Fig 5.3:video streaming

Fig 5.4:User Authentication

6.REFERENCES

[1] A. Madero, ‘‘Password secured systems and negative authentication,’’ Ph.D. dissertation, Dept. Eng. Manage., Massachusetts Inst. Technol.,Cambridge, MA, USA, 2013. [Online]. Available: http://hdl.handle.net/1721.1/90691

[2] A. Pascual and S. Miller, ‘‘Identity fraud report: Data breaches becoming a treasure trove for fraudsters,’’ Javelin Strategy Res., Pleasanton, CA, USA,Tech. Rep. 1/2013, 2013.

[3] E.-J. Yoon and K.-Y. Yoo, ‘‘Robust biometrics-based multi-server authen-tication with key agreement scheme for smart cards on elliptic curve cryptosystem,’’ J. Supercomput., vol. 63, no. 1, pp. 235–255, Jan. 2013.

[4] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, ‘‘Cryptanalysis and improve-ment of a biometrics-based multi-server authentication with key agreement scheme,’’ in Computational Science and Its Applications (Lecture Notes in Computer Science), vol. 7335. Berlin, Germany: Springer-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 Syst. Appl., vol. 41, no. 4, pp. 1411–1418, Mar. 2014.

[6] L. Lamport, ‘‘Password authentication with insecure communication,’’Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.

[7] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2010.

[8] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, ‘‘A password authentication scheme over insecure networks,’’ J. Comput. Syst. Sci., vol. 72, no. 4, pp. 727–740, Jun. 2006.

[9] M. Jakobsson and M. Dhiman, ‘‘The benefits of understanding pass- words,’’ in Mobile Authentication (SpringerBriefs in Computer Science). New York, NY, USA: Springer-Verlag, 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 Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 162–175.

[11] Y.-Y. Wang, J.-Y. Liu, F.-X. Xiao, and J. Dan, ‘‘A more efficient and secure dynamic ID-based remote user authentication scheme,’’ Comput. Commun., vol. 32, no. 4, pp. 583–585, Mar. 2009.

[12] M. K. Khan, S.-K. Kim, and K. Alghathbar, ‘‘Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic ID-based remote user authentication scheme,’’’ Comput. Commun., vol. 34, no. 3, pp. 305–309, Mar. 2011.

[13] E.-J. Yoon, S.-H. Kim, and K.-Y. Yoo, ‘‘A security enhanced remote user authentication scheme using smart cards,’’ Int. J. Innovative Comput., Inf. Control, vol. 8, no. 5(B), pp. 3661–3675, May 2012.

[14] R. Madhusudhan and R. C. Mittal, ‘‘Dynamic ID-based remote user password authentication schemes using smart cards: A review,’’ Intell.

Algorithms Data-Centric Sensor Netw., vol. 35, no. 4, pp. 1235–1248,

Jul. 2012.

[15] T.-Y. Chen, C.-H. Ling, and M.-S. Hwang, ‘‘Weaknesses of the

Yoon-Kim-Yoo remote user authentication scheme using smart cards,’’ in

Proc. IEEE Workshop Electron., Comput. Appl., May 2014, pp. 771–774.