International Innovative Research Journal of Engineering and Technology
Melange Publications ISSN NO:2456-1983

Stegnographic Mechanism Using Biometrics

Mrs.G.Kalaiarasi(PhD)[1], R.Gayathri[2], R.S.Banupriya[3]
Dhanalakshmi Srinivasan College of Engineering and Technology, Chennai,India

Abstract :
Remote authentication involve the submission of encrypted information, all along with image and auditory cue (facial images/videos). Our paper proposes a robust authentication mechanism based on the concept of chaotic encryption, semantic segmentation and data hiding. Finally, the Inverse Discrete Wavelet Transform (IDWT) has applied to provide the stego-video object. In Our technology, we applied biological traits, such as fingerprints, hand geometric, ear lobe geometric, retinal and iris pattern, DNA and signatures. Biometric authentication is the application to validate user for accessing a system. These are used to secure a wide range of electronic communications includes online commerce and banking.

Key words-DataHiding,Steganographic Mechanism, Remote Authentication, Biometrics, IDWT, VideoObject.

I.Introduction

Authentication is an act of confirming the truth of a datum or entity. This might involve confirming the identity of a person or program and tracing the artifact. The two main directions in authentication fields are positive authentication and negative authentication. The Positive authentications are well-established and applied by majority of sting systems. Negative authentication was invented to reduce cyber attacks. The differences between these two are explained for this example: Assume that password-based authentication. In this case positive authentication, passwords of all users are authorized to accessing a system, usually the passwords space includes only users passwords and limited (according to number of users). If crackers receives the passwords files, then their work is to Klimis Ntalianis is in Department of Marketing, Educational Institute of Athens. GREECE, Tsapatsoulis is on the Department of Communication and Internet and Cyprus University of Technology. Recovering the plaintext of limited numbers of passwords .In negative authentication, anti-password space was created, theoretically containing all strings that not in password files. If crackers receives very large anti- password file, their works are much harder. In this negative are flunced in an new layer of protecting to enhance the existing security measures in networks. These allow the present infrastructure to remain without access the passwords and creates the additional vulnerability .By applying the real-value negative algorithm, different layer is added to authentication prevents unauthorized user from gaining the networking access. Interested readers can also check. Proposed scheme is positive authentication system and for the security purpose elements .All three of the factors have to be verified: Ownership factor: the user has ID card and security token. Knowledge factor: the user knows password and pin. Inherence factor: the user does fingerprint, and DNA sequence.In order to investigate the full potential, biometrics can incorporate on hybrid cryptosteganographic mechanism. Cryptographic algorithm can scramble the biometric signals so that they cannot be understood, while steganographic methods to hide encrypted biometric signal, that they not seen. In our paper, build further principle to confirm the problem of remote authentication over the wireless channels and under loss tolerant protocol. An effective wavelet-based steganographic attacks for proposed system to hide encrypted biometric signal into semantic segmentation. They cannot provide anonymity an also three-factor security. They are vulnerable to privilege insider and user attacks.

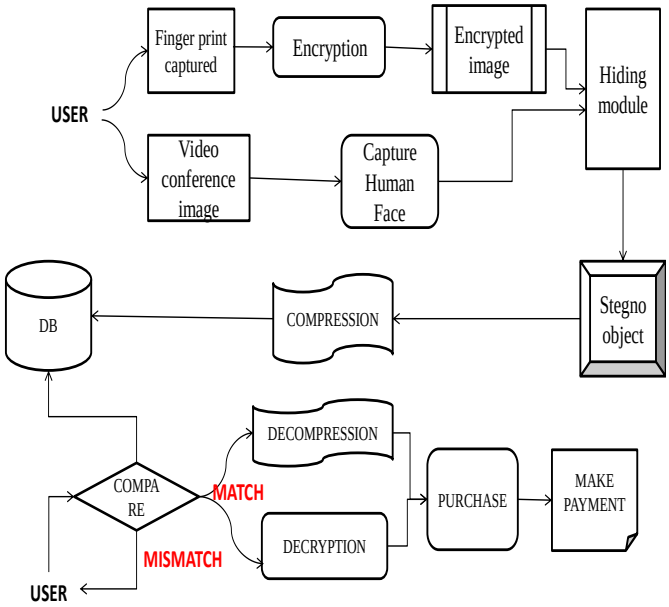
II.Related Works

Remote user authentication is significant to identify that communicating the parties are genuine and trustworthy by using the passwords and smart cards between login user and also the remote server .Number of password-based authentication mechanism using smart cards have proposed in recent years. So find that most two recent password-based authentication systems .The main contribution of our paper, robust remote user authentication mechanism against smart card security breach was presented, while they are keeping the merits of well-known smart cards based authentication systems. An Improved Biometric-based Multi-server Authentication Scheme to for protecting the resources from the unauthorized users and remote user authentication scheme forms an essential part in communication networks. Currently, the smart card-based remote user authentication for multi-server environment is widely used and also researched method. In our paper, shown that our scheme is not secure as they have claimed and they can suffer from impersonation attacks and stolen smart card attack. Later in the paper, they not only overcomes the mentioned weaknesses and also can provide more functionality features. Wavelet based Robust digital watermarking for Fingerprint authentication are used

for establishing the instant personal identity but they are susceptible to accidental/intentional attacks. This paper, a wavelet-based blind watermarking scheme was proposed to provide protection against false matching of a possibly tampered fingerprint by embedding a binary name label of fingerprint owner in the fingerprint itself. Embedding watermarks in the detail regions allow us to increase the robustness of our watermark, at no additional impact on image quality. It was experimentally shown that the binary watermark is embedded into detail coefficients of an indexed fingerprint image using spread spectrum PN sequence, the perceptual invisibility and robustness has anticlinal response to change in amplification factor "K" and smaller watermarks has better transparency than the larger ones. The DWT-based technique was found to the robust against noise, geometrical distortion and JPEG compression attack. A flexible and secure remote system authentication scheme using smart cards prevents the situation of a lot of logge in user with the similar logins self does not requires passwords/verifier table to authorize the users login demand. The schemes provide an available password change options, and withstand the replays, impression, stolen-verified, guess, and DOS attacks. Robust Biometrics-based Key Agreement Scheme using Smart Cards provides multi-server authentication scheme.This scheme proposes Multi-server authenticated key agreement (MSAKA) protocols allow the user to register at the registration center (RC) and access all the permitted services provided by the eligible servers. In other words, users cannot need to register at the numerous servers repeatedly. However, MSAKA schemes are created with defects about the centralized registration in center architecture. This architecture will make the centralized registration center become unsafe and has to deal with many registered and authenticated tasks. So this paper spares to eliminate three problems: single-point of security, efficiency and failure. Based on these motivations, it was proposed a new multiple servers to server architecture (MSTSA) to solved the problems caused by the centralized registration center. Then this scheme provably secure and robust biometrics-based Multiple Servers to the Server authentication with key agreement scheme was presented using chaotic maps with smart cards. Security of the protocol was based on the computational infeasibility of preventing the Chaotic Maps-Based Discrete Logarithm problem (CMBDLP) and Chaotic Maps-Based Dillie-Hellman problem (CMBDHP) and a secure symmetric encryption. At this time the proposed scheme do not only refrain from consuming modular exponential computing and scalar multiplication on elliptic curve, but was also robust to various attacks and achieves perfect forward secrecy with adjusting server as a registration center for adapting to users interests.This remote password authentication scheme, by employing a one-way hash function verification should be maintained on the remote server and intruders can break and modify the table. Therefore, many different solutions has been proposed, the random cryptographic keys. These keys are difficult to memorize based on authentication mechanism (e.g. password). Several passwords are simple and they can easily guessed or broken. These methods aimed to overcome the drawback of older remote authentication schemes using smart cards of ID-theft during the message transmission over an insecure channel. Additionally: (a) users should always has smart cards with them in order to do transactions, (b) if a user loses his/her smart card, he/she does not be able to do any transactions and should wait for the reissuing of the card (c) smart cards cost money and effort each time they are (re)issued.

III.Problem Definition: Authentication on remote server was difficult on the existing while using human face. Background color matching problem also difficult in this existing. Authentication was not properly validating on skin tone matching. If unauthorized user skin tone color matches with authorized user face means server will authenticate the user and enter into the application. So chance of entering unauthorized user into the application.

IV.Proposed System: The proposed remote human authentication scheme over wireless channels under loss tolerant transmission protocols that aims to ensure: (a) robustness against deciphering, noise and compression, (b) good encryption capacity, and (c) ease of implementation. In this purpose we: (a) employ wavelet based steganography, (b) encrypt biometric signals to allow for natural authentication, (c) involves a Chaotic Pseudo-Random Bit Generator (C-PRBG) to create the keys that triggers the whole encryption to increase security, and (d) the encrypted biometric signal is hidden in a VO, which can reliably to 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 the semantically meaningful video objects for embedding the encrypted biometrics information. Chaotic cipher, which works like a onetime pad will encrypt biometrics identifiers. Afterwards ,ahead-and body image of the Biometric signal's owner is analyzed and the host VO is automatically extracted



This proposed system, the user has to register their fingerprint and video conference image to remote server. The fingerprint captured by the user has to encrypting and stored in an encrypt image. Then the video conference image will captured the human face recognition. Finally the encrypt image and the captured human face will hiding into an modules. Then the hiding module will be stored in an stegno object and this object will be captured and stored into an database server.If the user wants to buy a product then the database server will compressed the stegno object and the object will be compared by the stegno object image. If the image will match then the user will buy the product and make payment for it. If suppose the compared user image will dismatched then the server will not allow the user to buy the product.

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.

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.

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.

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.

Conclusion

Thus we designed and developed to perform robust authentication mechanism based on semantic segmentation, encryption and data hiding using biometrics.

REFERENCES

[1]. Y.-y. Wang, J.-y. Liu, F.-x. Xiao, and J. Dan, "A more efficient and secure dynamic id-based remote user authentication scheme," Mar. 2009.

[2]. A. K. Das, "A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications," May 2013.

[3]. Te-Yu-Chen, Chung-Huei Ling , Weaknesses of the Yoon-Kim-Yoo Remote User Authentication Scheme Using Smart Cards",Jan 2014

.[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 with insecure communication.

[7] E.-J. Yoon, S.-H. Kim, and K.-Y. Yoo, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic id-based remote user authentication scheme'," International Journal of Innovative Computing, Information and Control, vol. 8, no. 5(B), pp. 3661–3675, May 2012.

[8] R. Madhusudhan and R. C. Mittal, "Dynamic id-based remote user password authentication schemes using smart cards: A review," Intelligent Algorithms for Data-Centric Sensor Networks, vol. 35, no. 4, pp. 1235–1248, Jul. 2012.

[9] T.-Y. Chen, C.-H. Ling, and M.-S. Hwang, "Weaknesses of the yoonkim- yoo remote user authentication scheme using smart cards," in Proceedings of the 2014 IEEE Workshop on Electronics, Computer and Applications. IEEE, 2014, pp. 771–774.

[10] A. K. Das, "A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications," Networking Science, vol. 2, no. 1-2, pp. 12–27, May 2013.

[11]. Klimis Ntalianis, and Nicolas Tsapatsoulis," Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks" ,in Jan 2015