International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 3 (March'2016)

ROBUST BIOMETRIC BASED AUTHENTICATION USING WATERMARKING

P.Revathi,
Student,
Computer Science and Engineering,
Velammal Institute of Technology,Chennai,India.

P.R.Jaya Kavitha,
Student,
Computer Science and Engineering,
Velammal Institute of Technology,Chennai,India.

R.Nithya,
Assistant professor,
Computer Science and Engineering,
Velammal Institute of Technology,Chennai,India.

Abstract: In wireless communications, significant information are getting exchanged frequently. Inorder to avoid the illegal access of that sensitive information remote authentication is being done extensively. Remote authentication involves the submission of encrypted information, along with visual and audio cues. Incase of remote examination or interviewing, Trojan Horse and other attacks can cause severe security threats to the sensitive information. Inorder to overcome these issues regarding security, we propose a robust authentication mechanism based on encryption and watermarking(data hiding). Assume that a user wants to be remotely authenticated, initially user's video object (VO) is captured by using a camera. Next, one of his/her biometric signals is encrypted by using Blow fish algorithm. Then the encrypted biometric signal and the captured human face is watermarked using LSB(Least Significant Bit) Algorithm.The LSB algorithm will read the encrypted biometric image and find the RGB value of each pixel. Then embed it into the appropriate RGB value of the captured human face**.** This enhances the security of the user information and remote authentication can be done more securely.

Keywords: Remote authentication,encryption,watermarking,Blow fish algorithm,Least Significant Bit algorithm.

I. INTRODUCTION

Authentication is a critical part of any trustworthy computing system; it ensures that only individuals with verified identities can log on the system or access system resources. In addition, authentication also serves as the first step for many other security purposes, such as key management and secure group communication. Passwords or smartcards have been the most widely used authentication methods due to easy implementation and replacement; however, memorizing a password or carrying a smartcard, or managing multiple passwords/smartcards for different systems (one for each system), is a significant overhead to users. In addition, they are artificially associated with users and cannot truly identify individuals. More seriously, they can be lost or stolen, resulting in impersonation and other security breaches. As a result, biometrics is becoming a promising authentication/identification method because it binds an individual with his identity and overcomes the main shortcomings inherent in the use of passwords and smartcards. Biometrics is a technology which uses physiological or behavioral characteristics to identify or verify a person. Typical characteristics used for authentication include fingerprint, face, and iris. A conventional biometric authentication system consists of two phases: enrollment and verification. During the enrollment phase, a biometric feature set is extracted from user's biometric data and a template is created and stored. During the verification phase, the same feature extraction algorithm is applied to query biometric data, and the resulting query feature set is used to construct a query template. The query template is matched against the stored template(s) for authentication. Compared to password/smartcard-based authentication approaches, biometrics-based solutions have many desired features such as being resistant to losses incurred by theft of passwords and smartcards, as well as user-friendliness. Biometrics bears a user's identity and it is hard to be forged. Unfortunately, biometrics brings its own complications:

• Security concern: conventional biometric authentication system record biometric templates in a Central Authentication Entity's (CA's) database. The stored templates, which correlate to users' biometric data, become potential targets to be attacked. Some literature, has identified the vulnerabilities caused by the compromise of stored templates.

• Privacy concern: Biometrics identifies individuals. To the best of our knowledge, conventional biometric authentication system is primarily built upon a fully-trusted model; that is, the central authentication entity (CA) is trusted to take full control of users' biometric information and is assumed to not misuse the information. This assumption of trustworthiness about the CA is not sufficient in the current malicious environments, since handing over one's biometric information to other parties or loss/compromise of one's biometric template will cause serious user privacy concern.

• Irreplaceability: biometric data is permanently bound to a user, and it is almost impossible to generate a new set of biometric features for a legitimate user. Thus compromised biometrics is not replaceable. Many approaches addressing the security and privacy issues of biometrics have been proposed in the literature. These approaches avoid storage of plain biometric templates by recording them in a "distorted" way. In this research we propose a privacy-preserving yet replaceable biometrics-based authentication approach.

II. LITERATURE SURVEY

1. Wavelet-based Robust Digital Watermarking Scheme for Fingerprint Authentication.Authors: Rajlaxmi Chouhan, Agya Mishra and Pritee Khanna,2010 .

Fingerprints are unique biometrics mainly used for the establishment of instant personal identity but they susceptible to accidental/intentional attacks. In this paper, 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 itself. Embedding watermarks in the detail regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality. It has been experimentally shown that when a binary watermark is embedded into detail coefficients of an indexed fingerprint image using spread spectrum PN sequence, the perceptual invisibility and robustness have anticlinal response to change in amplification factor "K" and smaller watermarks have better transparency than the larger ones. The DWT-based technique has been found to be very robust against noises, geometrical distortion and JPEG compression attack.

2.A robust remote user authentication scheme using smart cards,Authors:Chun-Ta Li, Cheng-Chi Lee,2011.

Remote user authentication is important to identify whether communicating parties are genuine and trustworthy using the password and the smart card between a login user and a remote server. A number of password-based authentication schemes using smart cards have been proposed in recent years. We find that two most recent password-based authentication schemes (Hsiang and Shih 2009, Chen and Huang 2010) assume that the attacker cannot extract the secret information of the smart card. However, in reality, the authors in (Kocher et al. 1999 and Messerges et al. 2002) show that the secrets stored in the card can be extracted by monitoring its power consumption. Therefore, these schemes fail to resist smart card security breach. As the main contribution of this paper, a robust remote user authentication scheme against smart card security breach is presented, while keeping the merits of the well-known smart card based authentication schemes.

3.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.

Conventional single-server authentication schemes suffer a significant shortcoming. If a remote user wishes to use numerous network services, he/she must register his/her identity and password at these servers. It is extremely tedious for users to register numerous servers. In order to resolve this problem, various multi-server authentication schemes recently have been proposed. However, these schemes are insecure against some cryptographic attacks or inefficiently designed because of high computation costs. Moreover, these schemes do not provide strong key agreement function which can provide perfect forward secrecy. Based on these motivations, this paper proposes a new efficient and secure biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem (ECC) without verification table to minimize the complexity of hash operation among all users and fit multi-server communication environments. By adopting the biometrics technique, the proposed scheme can provide more strong user authentication function.

4.Robust Biometrics-based Key Agreement Scheme with Smart Cards towards a New Architecture.Authors: Hongfeng Zhu , Man Jiang , Xin Hao and Yan Zhang, 2015.

In a traditional single server authentication scheme, if a user wishes to access network services from different servers, the user has to register with these servers separately. To handle this issue, multi-server authentication scheme has been proposed.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. In other words, users do not need to register at numerous servers repeatedly. However, MSAKA schemes are created with defects about the centralized registration center architecture. This architecture will make the centralized registration center become unsafe and have to deal with many registered and authenticated tasks.

III. EXISTING SYSTEM:

In existing system, QSWT(Qualified Significant Wavelet Trees) and IDWT(Inverse Discrete Wavelet Transform) are the two algorithms that were used to perform remote authentication using biometrics. The stego object here is formed by using those two algorithms. IDWT algorithm is actually used for converting the obtained biometric into encrypted signal. It performs encryption by forming a tree structure of the image's pixel value.On the other hand,QSWT algorithm performs watermarking. At first, it segregates the captured human face into four bands(LL,LH,HL,HH).Then it appends each part of the human face with the biometric.

DISADVANTAGES:

1. It is a time consuming process.
2. Lots of computations are needed to form a stego object.
3. Inaccuracy of results at times.

IV. PROPOSED SYSTEM:

In the proposed system,we are using the Least Significant Bit (LSB) algorithm for watermarking(i.e. hiding biometric into the face). This algorithm will read the encrypted biometric image and find the RGB value of each pixel.Then embed it into the appropriate RGB value of the captured human face**.**This enhances the security of the user information.We are going to apply the same concept in ration shop.Nowadays,in ration shops the officials are not checking whether the appropriate card holders are buying their own products.So for validating in ration shops, we are going to apply this authentication. If the user wants to purchase the product in the

ration shop,the following steps has to be done. At first,his face has to be captured by the camera and then his biometric(finger print) has to be given as input to the system in ration shop.Then the server validates whether the obtained details matches the existing one.Once the user details gets validated(remote authentication) he can buy the ration product after paying the amount via bank transaction.

ADVANTAGES:

- Using LSB for watermarking,is more efficient than other techniques.
- The number of computations that is being done while watermarking is quite lesser when compared to other techniques.
- The system complexity is less.
- Accurate results are obtained.

V. ARCHITECTURE DIAGRAM:

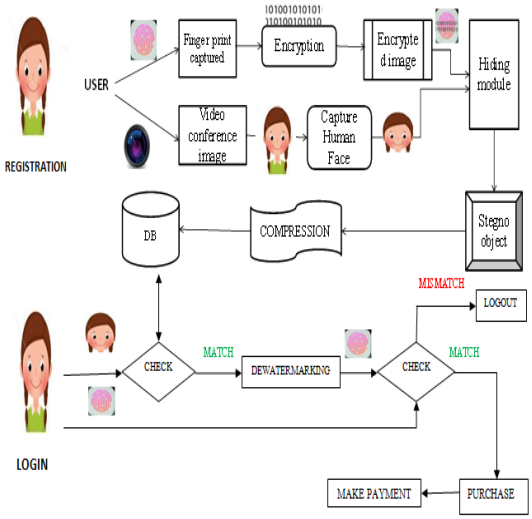

Figure 1:Architecture diagram

VI. MODULES DESCRIPTION:

The purpose of this paper could be achieved in the following four modules

- Capturing video object
- Uploading biometric and hiding into video object.
- Remote Server Authentication.
- Application Access.

CAPTURING VIDEO OBJECT:

This is the first module wherein we have to get the profile information of each user and perform registration. Also capturing of user's face by using camera is done. The captured image will then be stored in the server.

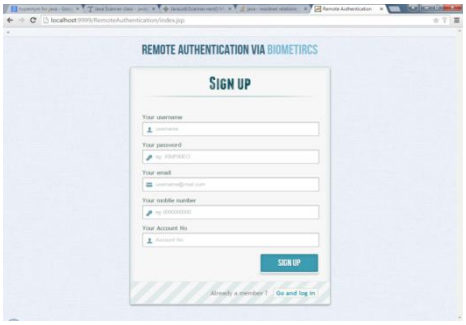

Figure 2: User registration

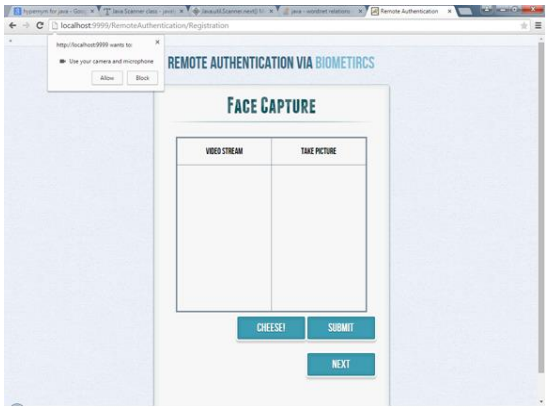

Figure3. Capturing human face

UPLOADING BIOMETRIC AND HIDING INTO VIDEO OBJECT:

In this module,the user's biometric(here,fingerprint) is obtained.The obtained biometric will be encrypted using blow-fish algorithm.This algorithm reads each pixel value of the biometric and then it generates random key values for it..After encryption,the server will embed the encrypted biometric into the human face.For embedding(watermarking),we apply Least Significant Bit (LSB) algorithm. This algorithm will read the encrypted biometric image and find the RGB value of each pixel.Then embed it into the appropriate RGB value of the captured human face**.**This enhances the security of the user information.Now the watermarked image will be compressed(using Huffman compression)and then be stored in the database.

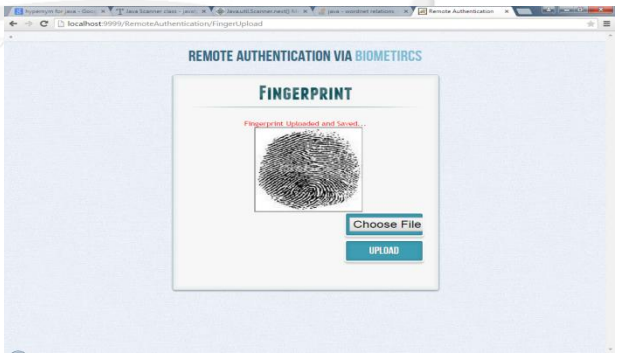

Figure 4:Uploading fingerprint.

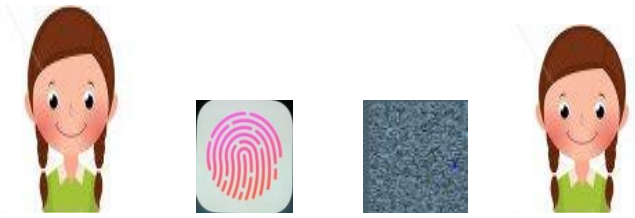

Figure5.Performing watermarking. **(a)**Video conference image.(b) Fingerprint.(c) Encrypted biometric.(d) Watermarked image (invisible watermarking).

REMOTE SERVER AUTHENTICATION:

In this module, remote server authentication is going to be performed. If the user wants to access the ration shop application,the following steps has to be followed.The user has to login into the application.The user's face has to be captured and his/her fingerprint has to be given as input.Once the inputs(captured face and fingerprint)are given,remote server authentication begins.The remote server which contains the user's info already,performs authentication by comparing the obtained input with the existing one.If the server finds a matching face,it will extract the fingerprint(dewatermarking) from it.Now the fingerprint validation takes place.Only if both the face and biometric gets validated successfully,the server authenticates the user and allows further processing.

APPLICATION ACCESS

This final module allows the user to access the ration shop application only if he/she gets validated successfully. The user can purchase the ration products as needed.And then he can pay the amount via bank transaction.

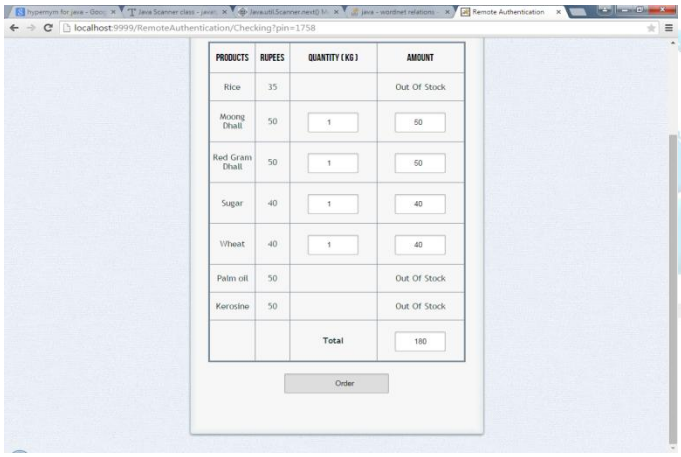

Figure 6: Purchasing product

VII. 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.We have proposed an efficient biometric based authentication using watermarking for validating in ration shops.If this is implemented in real time,it would be beneficial for the government officials to check whether or not appropriate card holders are buying their own products.

VIII. REFERENCES

[1] Wavelet-based Robust Digital Watermarking Scheme for Fingerprint Authentication.byRajlaxmi Chouhan, Agya Mishra and Pritee Khanna,2010

[2] A robust remote user authentication scheme using smart cards,by Chun-Ta Li, Cheng-Chi Lee.2011.

[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] Robust Biometrics-based Key Agreement Scheme with Smart Cards towards a New Architecture by Hongfeng Zhu, Man Jiang, Xin Hao and Yan Zhang,2015.

[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,"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 passwords,"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.

