International Journal of Linguistics and Computational Applications (IJLCA) ISSN 2394-6385 (Print)
Volume 4, Issue 1, January – March 2017 ISSN 2394-6393 (Online)

Implementation of Video-Object Steganography Mechanism over Robust Remote Authentication via Biometrics

Therasa M[#1], Keerthi D.M[*2], Archana A[*3], Hema S.C[*4]

[1]*Assistant Professor, Department of Computer Science and Engineering, PanimalarInstitute of Technology, ,*
[2,3,4]*Research Scholar, Department of Computer Science and Engineering, PanimalarInstitute of Technology,*

Abstract— Remote verification over remote is a tested one. Many creators proposed a considerable measure of arrangements like, the remote human confirmation plot over remote channels under misfortune tolerant transmission conventions, means to guarantee: (a) strength against translating, commotion and pressure, (b) great encryption limit, and (c) simplicity of execution. For this reason we: (an) utilize wavelet based steganography, (b) encode biometric signs to take into consideration common verification, (c) include a Disordered Pseudo-Arbitrary Piece Generator (C-PRBG) to make the keys that trigger the entire encryption to expand security, and (d) the scrambled biometric flag is covered up in a VO, which can dependably be distinguished in present day applications that include remotely coordinating. The calculations utilized as a part of the current paper was very hard to accomplish the above requirements.In proposed conspire, the strong remote verification is accomplished through three procedures like semantic segmentation, encryption and information hiding. The primary commitment of this proposed framework is, Biometrics based human verification over remote channels under blame tolerant conventions. Programmed extraction of semantically significant video objects for implanting the scrambled biometrics data. Confused figure, which works like an onetime cushion, to scramble biometrics identifiers.

Keywords— C-PRBG (Chaotic Pseudo-Random Bit Generator), Chaotic Cipher, Biometrics, Authentication

1. Introduction

Biometric verification is considered a subset of biometric confirmation [4]. The biometric technologies included depend on the courses in which people can be particularly recognized through at least one recognizing natural characteristics, for example, [11] fingerprints, hand geometry, ear cartilage geometry, retina and iris designs, voice waves, keystroke dynamics, DNA and signatures. [6][9]Biometric confirmation is the use of that evidence of way of life as a component of a procedure approving a client for access to a system. Biometric innovations are utilized to secure an extensive variety of electronic interchanges, including undertaking security, online trade and managing an account - even simply signing into a PC or advanced cell. In [1], for remote secret word confirmation conspire, it utilizes a restricted hash work. In any case, in his plan a check table ought to be kept up on the remote server and if gatecrashers break into it, they can adjust the table. In [2][8], they have been proposed the most famous of which depends on long and irregular cryptographic keys. Irregular cryptographic keys are hard to remember, in this way they are put away some place and they are discharged in view of some option validation system (e.g. password).In, a few passwords are basic and they can be effortlessly speculated or broken. Moreover, a great many people utilize a similar secret key crosswise over various applications; if a pernicious client decides a solitary watchword, they can get to numerous applications. Another fascinating and extremely encouraging class of remote client verification plans includes shrewd cards utilizing dynamic users'[9][10],identities per exchange area. These techniques meant to beat a typical disadvantage of more seasoned remote validation plans utilizing brilliant cards: client's personality was static in all the exchange sessions, which may release some data about that client and can make danger of ID-burglary amid the message transmission over an unreliable channel.[12][13] Additionally: (a) clients ought to dependably have their keen cards with them so as to do exchanges, (b) if a client loses his/her savvy card, he/she won't have the capacity to do any exchanges and ought to sit tight for the reissuing of the card (in some cases a few days), (c) shrewd cards cost cash and exertion every time they are (re)issued, (d) because of low power they can't perform extremely complex calculations, (e) as per cardwerk.com their memory ought to hold information for up to 10 years without electrical power and (f) they ought to bolster no less than 10,000 read-compose activities amid the life of the card.[3][5]Recent inquires about of picture encryption calculations have been progressively in view of tumultuous frameworks, yet the downsides of little key space and frail security in one-dimensional disorganized cryptosystems are self-evident. In this way, in our proposed framework, BLOWFISH calculation, Minimum Huge Piece calculation and HUFFMAN COMPRESSSION calculation are utilized as a part of request to guarantee the safe confirmation and to beat the accompanying issue explanations.

1.1 Problem Statement

- Authentication on remote server is difficult on existing while using human face.

- Background color matching problem also difficult in existing. Remote server will check face with background color for every time authentication.
- Authentication is 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. The Overall Architecture diagram is explained in the following phases.

2. System architecture diagram

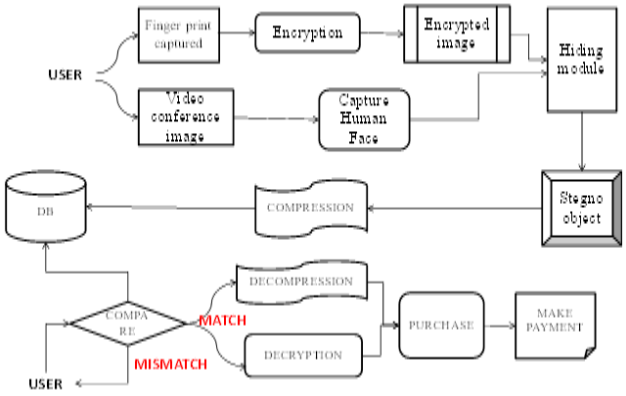

Fig.1: Overall Architecture Diagram

2.1 Registration Phase

Step 1: client will fill the fundamental individual data.
Step 2: client's face will be caught from the video conferencing.
Step 3: client confront alone get trimmed and after that put away incidentally.
Step 4: client unique mark is inquired.
Step 5: Fingerprint is then scrambled and watermarked into the edited picture of client.
Step 6: This single picture is then get put away for all time.

2.2 Login Phase

Step 1: client ought to give his face and unique mark to confirmation.
Step 2: Admin will decompress the put away picture just on the off chance that it matches with the client's face.
Step 3: once it get matches, the two separate pictures are drawn by doing reverse process.
Step 4: Then it will contrast the put away face and unique finger impression and the present one.
Step 5: If it matches, he is confirmed, else, he is an unapproved individual. In this way, he can't login to the application.

3. Methodology Used

- Capturing video object.
- Uploading biometrics and hiding into video object.
- Remote Server Authentication.
- Application Access & Bank Transaction

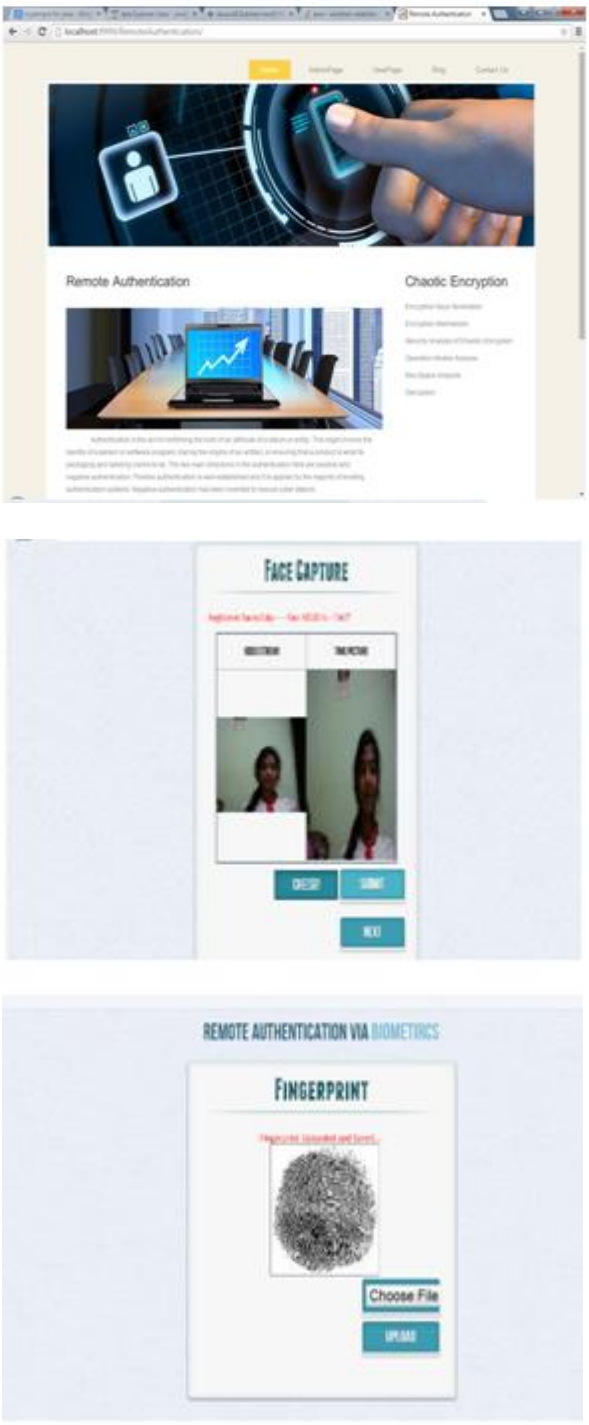

Fig.2: Screenshots of Module1

The Overall Module1 Results has been shown in the fig3.1.1, which explains how the user will enter his personal information and the way semantic segmentation is processed to capture only the user's image.

3.1 Uploading Biometrics and Hiding into Video Object

When human face catching procedure is finished, server will catch the client suitable biometrics. Here biometrics are not specifically putting away into the server. Each biometrics must be scrambled and watermarked into the client confront. For encryption here we will apply blowfish calculation. This calculation read each pixels estimations of the biometrics and change the pixel estimations of it. After encryption handle, server will implant encoded biometrics into the human face. For implanting (watermarking) we will apply Least Significant Bit (LSB) methods. These methods will read each lines and segments of the biometrics and implanting into the fitting lines and sections of the human face. So every watermarked picture is kept up in the server. The process is shown in the fig.1

Fig.3: Screenshots of Module2

The Overall Module2 Results has been shown in the fig.3, which explains how the Admin process the user's image and his biometrics by doing data hiding, encryption and compression. Then the stegno video object get stored in the directory permanently. As we applied this mechanism in the ration shop application, the admin side will verify the stock details for each month.

3.2 Remote Sever Authentication

In the module, remote server validation will be performed. In the event that client needs to get to the application implies he/she needs to give his face and biometrics to the server. Server will coordinate face with each face on the database. On the off chance that server recognized the coordinated face implies, server will remove the unique finger impression from that picture. Subsequent to separating, server checks the face and biometrics into the coordinated face and biometrics. In the event that both are matches just server will vyalidate the client. This has been appeared in the fig2.1.

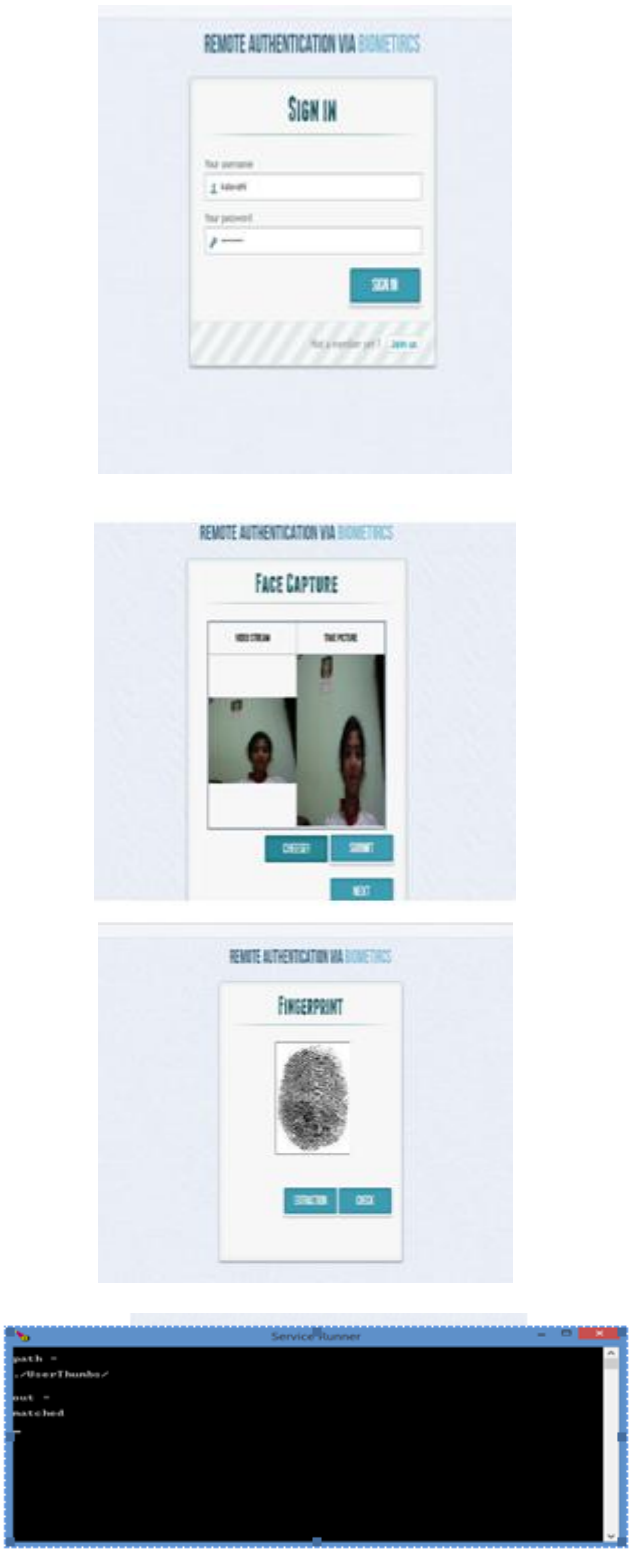

Fig.4: Screenshots of Module3

The Overall Module3 Results has been shown in the fig3.1.3, which explains how the user get secure authentication to enter into an application. Firstly, the user should give his face. Then by using Face match application, it will extract the user image from the database, also extract the fingerprint image which is hided into the user face and then ask for the fingerprint of the user. After the user enter his fingerprint, it will check for the fingerprint match. If it matches, user can buy his products or else he will return back to the home page.

3.3 Enhancement

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.

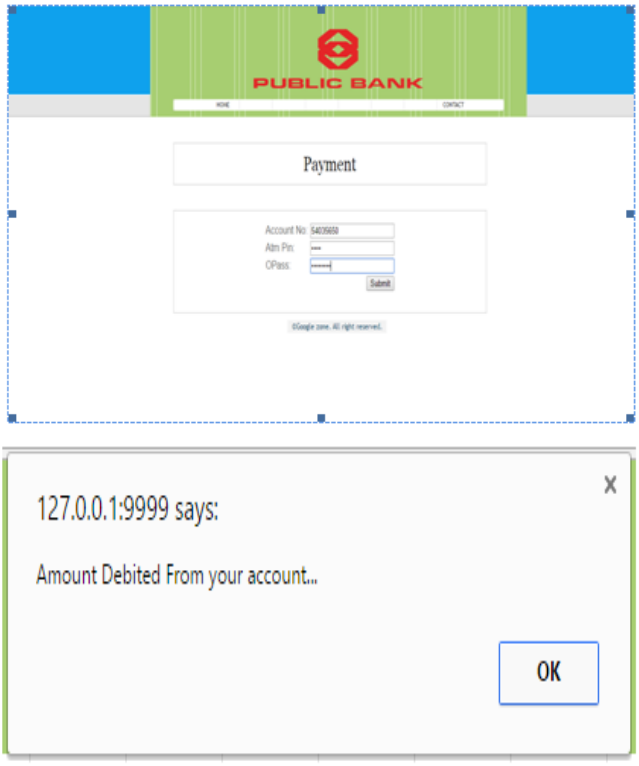

Fig.5: Screenshots of Module4

The Overall Module4 Results has been shown in the fig.5, which explains how the user buy products and do payment process. Firstly, he should create a new account in a bank and deposit some amount, he can also add amount whenever he need. Admin side will maintain the users

account. For doing payment, user should enter his password and debit an amount for the products which he bought.

4. Future enhancement

Here, Finger Prints are used to watermark into the user's face. Instead of using Finger Prints, other biometrics can also be used like earlobe geometry, retina, iris etc.., for authentication. This mechanism can also be applied in any of the online applications to carry out the secure authentication. It overcomes the background matching problem, same skin tone problem, remote authentication. Since data hiding is used, no one can able to see the fingerprints of an user which is embed in to the users face. Though if they extract, they can't able to see the fingerprint since it is encrypted. In order to make a Standard format, compression is used to store a high quality image and low quality image into a standard format. Overall implementation provides a robust remote authentication to validate an authorized and unauthorized user.

5. Conclusion

In this way the plan and development to perform powerful remote confirmation component in view of semantic division, encryption and information concealing utilizing biometrics has been actualizing to improve the security level. We can utilize this strategy in any of the web applications adequately. These techniques stay away from the general issues of the current one. Our Success to this proposition is, by utilizing the productive calculations to accomplish high security justifies and overcomes the drawbacks of a current framework.

References

[1] L. Lamport,``Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770_772, Nov. 1981.

[2] 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

[3] A new chaotic algorithm for image encryption by Haojiang Gao *, Yisheng Zhang, Shuyun Liang, Dequn Li

[4] A Novel Scheme for Digital Rights Management of Images Using Biometrics by N.Nagamalleswara Rao, Prof. P. Thrimurthy

[5] H. S. Kwok and W. K. S. Tang, ``A fast image encryption system based on chaotic maps with _nite precision representation," Chaos, Solitons Fractals, vol. 32, no. 4, pp. 1518_1529, May 2007

[6] 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.

[7] A Secure Skin Tone based Steganography Using Wavelet Transform by Anjali A. Shejul, Umesh L. Kulkarni

[8] 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 (Lecture Notes in Computer Science), vol. 7335. Berlin, Germany: Springer-Verlag, 2012, pp. 391_406.

[9] A Robust Remote User Authentication Scheme Using Smart Card by Chun-Ta Li,Cheng-Chi Lee

[10] An Improved Biometric-based Multi-server Authentication Scheme Using Smart Card Khanjan Ch. Baruah, Subhasish Banerjee

[11] Wavelet-based Robust Digital Watermarking Scheme for Fingerprint Authentication by Rajlaxmi Chouhan, Agya Mishra Pritee Khanna

[12] A Flexible and Secure Remote Systems Authentication Scheme Using Smart Cards by Manik Lal Das

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