International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876, Impact Factor: RJIF 5.44
www.engineeringresearchjournal.com
Volume 2; Issue 3; May 2016; Page No. 18-20

Implementation of remote authentication using chaotic encryption over biometric sample image

[1] Manisha N Narote, [2] Korde SK

[1] PG Scholar, Computer Department, Pravara Rural Engineering College, Maharashtra, India.
[2] Asst. Professor, Computer Department, Pravara Rural Engineering College, Maharashtra, India.

Abstract
In today's world security is the very important issue while doing any transaction. As we are like to use online applications like snapdeal.com for shopping. The payment transaction should be secure so that in this system we are using biometric threats for identification that identity is unique. No one can steal that identity. When message will get transferred. When there is remote authentication so verification is most important while communication. QSWT is used for embedding and locating object into an image. In this system biometric signal is encrypted with chaotic encryption and then through video object steganographic image is hidden in a video which is captured runtime after that it will send it to server then after decryption extracted biometric sample is compared with already stored sample then identity is verified.

Keywords: Steganography, Encryption, Biometric, Password, Smart card

1. Introduction

1.1. Overview

Security is mainly important issue in today's life. Applications having security is in the form of password. But this cannot be a strong security. As mentioned in paper [2] there is details of identity fraud detection is increasing day to day.so there is need of fulfil the three main security goals:

- Confidentiality
- Integrity
- Availability

Confidentiality

Confidential means only authorized person can have access to that data. The confidentiality discusses to limiting the disclosure and access of information to the users those are authorized and avoiding those not authorized from accessing it. With this technique, a company or society is able to avoid extremely delicate and vital information from getting into the hand of the wrong people while still making it accessible to the right people.

Integrity

Data is not altered by unauthorized person. It consist set of rules which is limit for access information. e. g. access control. Integrity is another security concept that involves maintaining data in a constant, accurate and trustworthy manner over the period in which it will be existent. In this case, one has to ensure that data is not changed in the course of a certain period. In addition, the right procedures have to be taken to ensure that unauthorized people do not alter the data.

Availability

Make data available whenever user need he/she can access his/her data. The concept of availability refers to the up time maintenance of all resources and hardware. This means that all the hardware and resources one have are functional all the time. It can also involve carrying out of regular hardware repairs.

1.2 Structure of Biometric System

There are four modules in any biometric system

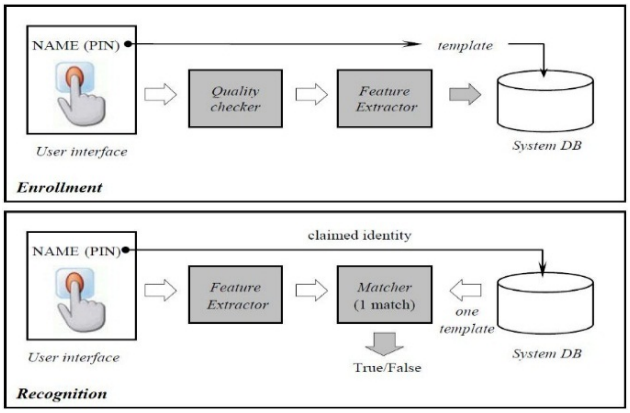

Fig 1: Working of Biometric System

1. Enrolment Unit: In this module users are get registered into this systems database. During this phase, reader of biometric will scan and capture biometric characteristic and represent it in the form of digital format.
2. Feature Extraction Unit: This element processes the input sample and it generates a compressed representation called as template. This is stored in main database.
3. Matching Unit: In this unit it will compare current input to the template. If the system performs identity verification, this compares new feature with stored template and produce match value.
4. Decision Maker: In this section works on threshold which matches the score.

2. Literature Survey

P.-Y. Chen and H.-J. Lin in 2006 paper entitled" A dwt based approach for image steganography" explains about how message is embedded in frequency domain in the form of matrix. Discrete Wavelet Transform is used for image hiding.

I.-E. Liao, C.-C. Lee, and M.-S. Hwang, in 2006 [6]. "A password authentication scheme over insecure networks", explain about people uses same password for different applications. So by guess anyone can have access to system and system may hacked.

M. Weir, S. Aggarwal, M. Collins, and H. Stern, in 2010 [7]. "Testing metrics for password creation policies by attacking large sets of revealed passwords" explains about testing passwords from large data sets. In this paper there is explanation about how password is set which symbols mostly used among special symbol to set password. By comparison with data sets which are collected from different database from different sites. Drawback is it is related to text messages only and time consuming.

S. Hemalatha, U. Dinesh Acharya, A. Renuka, and P.R. Kamath in 2013 [9]. "A secure color image steganography in transform domain" explains about image and key hidden in cover image. PSNR values to hide image. In the form of matrix PNSR values are displayed.

Klimis Ntalianis, and Nicolas Tsapatsoulis, in 2015 [1] "Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism over Wireless Networks. "Explains about remote authentication implemented with biometric security. Biometric image is encrypted and this image is sent through a video by hiding it. At server side after decryption verification is done.

3. Implementation

3.1 Existing System

As explanation in fig.1client server communication using smart card. This is the multiuser environment where user i.e. client is communicating with server. Internet is the media through which client is communicating with server.

But there is disadvantage of smart card which is having some bottlenecks.

- User have to carry smart card every time
- Several days required for reissuing, if lost.
- They should support read- write actions limitations.
- Due to low power not able to perform larger computation
- Without electricity it may retain data up to 10 years.

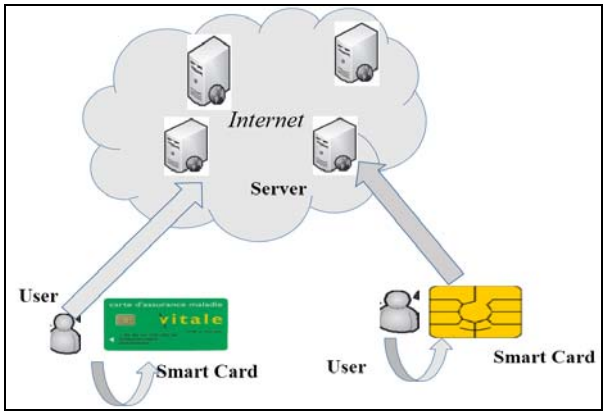

Fig 2: Remote Server-client communication with smart card

3.2 Proposed System

In this system there is restriction that each and every time user have to carry smart card always for identification purpose. If identity is verified then only user is allowed to perform transaction.so this drawback is overcome in proposed system. For identification biometric threat is considered again for verification.so this identification is so much secure than any other security measure like password. Advantage of using biometric as an identity is it requires physical presence of that particular person then and then only identity will get verified.

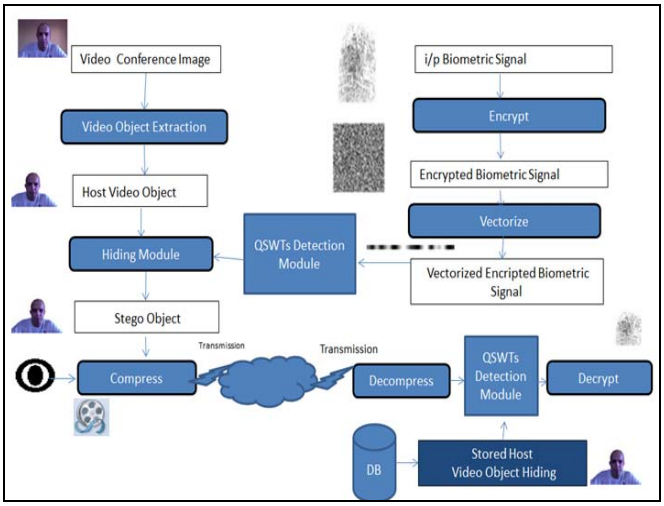

Fig 3: System Architecture

In proposed system firstly biometric signals image is encrypted in the form of steganography. Encryption is perform using chaotic encryption in which initial condition and control parameter will get combined and using C-PRBG key is generated and encryption is performed on image. Biometric signal in hidden behind any image that encrypted signal is vectorized. This image after vectorization that will pass to QSWT module. QSWT stands for Qualified Significant Wavelet Transform. Which is used to embed watermark data as well as for searching location in extraction process. An image we want to send to server is extracted and that stego object is embedded in a video which is real time captured video so that more security is provided. In Second part at server side it is already having storage of authenticated biometric samples. Which is verified after extraction of signal from video. For this extraction process also QSWT is used to

separate biometric sample and image. If match found then only allow.

3.3 Chaotic Encryption

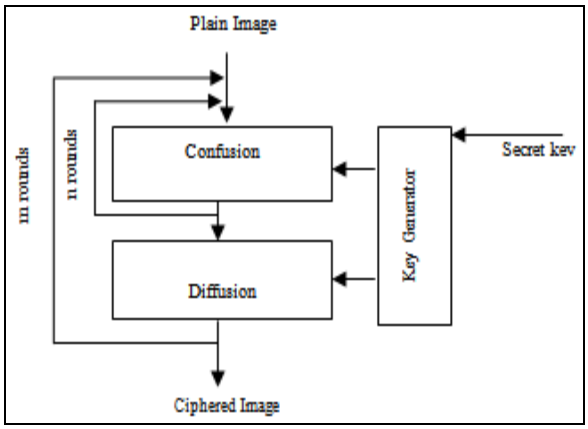

Fig 4: Chaotic Encryption

In this encryption method there are two main parts confusion and diffusion. First input image as a plain text is given. In first part confusion there is pixel permutation in this the pixels position is twisted over entire image and they do not disturb other pixel values so the image is distorted. As shown in fig 4.chaotic encryption there in initial condition and control parameter both are considered to generate secrete key. But this can be broken so to provide again security Second part is there that is diffusion in this part pixel values are changed sequentially. This confusion and diffusion rounds are repeated till suitable security level is reached.

4. Algorithm

1. Procedure QSWTEST(I,S,L)
2. Define input frame I = input frame
3. Selection of subband S = subband selection (e.g. LH)
4. Selection of level of subband L = subband level (e.g. 3)
5. Define threshold values T1 & T2
6. According to level apply DWT and point out particular location in image
7. Check subband is in node and greater than T1.
8. Perform steps till T2

5. Conclusion

Biometric is mainly important in all type of applications in day todays life that we all using. Biometric signals enter more and more into our everyday. Firstly passwords are used mostly for security in applications. With the help of password anyone who know password can have access to that application. But whenever biometric is used with password then more security is provided. Important is that person's physical characteristic is required so that no one can replace. This identity cannot be theft. In this system biometric signal is encrypted so security is provided twice. Again this is hidden in video which is captured by runtime so it seems no fake information's will get passed. With the help of QSWT this image is hidden in video as well as extracted the location of that video. Finally at server side already authenticated biometric is stored. After matching is performed and result is returned whether person is authorized or not.

6. References

1. Klimis Ntalianis, Member IEEE, Nicolas Tsapatsoulis, Member. IEEE Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks in, Ieee Transactions On Emerging Topics In Computing, 2015.
2. Identity fraud report: Data breaches becoming a treasure trove for fraudsters, Javelin Strategy and Research, Tech. Rep., 2013
3. Chuang MC, Chen MC. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart card sand biometrics, Expert Systems with Applications, 2014; 41(4):1411-1418.
4. Lamport L. Password authentication with insecure communication, Communications of the ACM, 1981; 24(11):770-772.
5. Kundur D, Zhao Y, Campisi P. A steganographic framework for dual authentication and compression of high resolution imagery, in Proceedings of the IEEE International Symposium on Circuits and Systems, 2004; 2(IEEE):14.
6. Liao IE, Lee CC, Hwang MS. A password authentication scheme over insecure networks, Journal of Computer and System Sciences, 2006; 72:727-740,
7. Weir M, Aggarwal S, Collins M, Stern H. 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, 162-175.
8. Wang Yy, Liu Jy, Xiao Fx, Dan J. A more efficient and secure dynamic id-based remote user authentication scheme in Computer Communications, 2009; 32(4):583-585.
9. Hemalatha S, Dinesh Acharya U, Renuka A, Kamath P R. A securecolor image steganography "in transform domain International Journalon Cryptography and Information Security, 2013; 3(1).
10. Rao NN, Thrimurthy P, Babu BR, A novel scheme for digital rights management of images using biometrics in International Journal of Computer Science and Network Security. 2009; 9(3):157-167,
11. Das AK. Analysis and improvement on an efficient biometric based remote user authentication scheme using smart cards in IET Information Security, 2011; 5(3):145-151.
12. Chen PY, Lin HJ. A dwt based approach for image steganography in International Journal of Applied Science and Engineering, 2006; 4(3):275-290, 127-144.