A NOVEL REMOTE AUTHENTICATION VIA ENHANCED BIOMETRICS THROUGH INTERNET

T.Sathya,
PG Student,
Sasurie Academy of Engineering,
Coimbatore,India.

T.Krishnan,
Assistant Professor,
Sasurie Academy of Engineeriing,
Coimbatore,India.

T.Laksmanakumar,
Assistant Professor,
Sasurie Academy of Engineeriing,
Coimbatore,India.

Abstract: Password-based authentication schemes have been widely deployed to verify the legitimacy of remote users. Smart card-based user authentication technology has been widely deployed in various kinds of applications, such as remote host login, withdrawals from automated cash dispensers, and physical entry to restricted areas. The above mentioned scheme can create parallel session attack, masquerading attack and password guess attack. In any type of communications in order to share sensitive information between 2 or more entities remote authentication could be used. This process contains three sub functions. The first sub function is the encryption of finger print image i.e change the original image into chaotic image then converts encrypted chaotic image into set of vectorized value. The second sub function is the taking human object from the playing video or teleconferencing. Then third function is the merging those vector value into the extracted video object. Trojan horse and other those types of attacks could be mostly created in cases of remote examinations or in or in personnel hiring which may create serious pressure. This survey proposes a robust remote authentication mechanism via enhanced biometric based on semantic segmentation, chaotic encryption and data hiding and wireless transfer at the sender side. The wireless data receive; object recovery and quality enhancement and interview are the receiver side function. Remote authentication is a method to authenticate remote users over insecure communication channel.

Key Words: - Biometrics Hiding, Steganographic System, Remote Authentication, Biometrics

I. INTRODUCTION

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be. The two main directions in the authentication field are positive and negative authentication.

a) Positive Authentication: Positive authentication is well-established and it is applied by the majority of authentication systems. In positive authentication, the passwords of all users that are authorized to access a system are stored, usually in a file. Thus the passwords space includes only users passwords and it is usually limited (according to the number of users).

Disadvantage of Positive Authentication

- If crackers receive the passwords file, then their work is to recover the plaintext of a very limited number of passwords.

b) Negative Authentication

Negative authentication has been invented to reduce cyber attacks. On the contrary, in negative authentication the anti-password space is created, (theoretically) containing all strings that are not in the passwords file. If crackers receive the very large anti-password file, their work will be much harder.

Advantages of Negative Authentication

- Negative authentication can be introduced as a new layer of protection to enhance existing security measures within networks.
- This allows the current infrastructure to remain intact without accessing the stored passwords or creating additional vulnerabilities.
- By applying a real-valued negative selection algorithm, a different layer is added for authentication, preventing unauthorized users from gaining network access.

Factors of Negative Authentication

- The ownership factor: Something the user has (e.g. ID card, security token, cell phone etc.)
- The knowledge factor: Something the user knows (e.g., a password, a PIN, a pattern etc.)
- The inherence factor: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence, face, other biometric identifier etc.)

Assuming that user X is a person who needs wants to be remotely authenticated. Initially X's video object (VO) is automatically segmented, using a head and-body detector at the interview time of interviewing. Next, one of X's biometric signals is encrypted by a chaotic cipher which generate the unknown image in form of black and white signals. Then the chaotic image should be should be generated in form of vector value which contains 0's and

IJCRCST © 2016 | All Rights Reserved

1's.This vector value should be hided into the video object and then compressed. The compressed image should be send through network. At receiver side the image should be decompressed. In data extraction module the original image and biometric image should be recovered.

II. LITERATURE SURVEY

ONE WAY HASH FUNCTION

[1]In 1981, Lamport proposed a remote password authentication scheme, by employing a one-way hash function. However, in his scheme a verification table should be maintained On the remote server. Lamport [1] proposed a password-based authentication scheme using password tables to authenticate remote users over insecure network. Since then, many password- based authentication schemes were proposed to improve the security, efficiency or cost [11, 12, 13].

Disadvantage

- If intruders break into it, they can modify the table.

DIFFIE-HELLMAN KEY AGREEMENT PROTOCOL

Liao et al. [2] proposed a scheme that utilizes the Diffie-Hellman key agreement protocol over insecure networks, which allows the user and the system to agree on a session key to encrypt/decrypt their communicated messages using a symmetric cryptosystem. Random cryptographic keys are difficult to memorize, thus they are stored somewhere and they are released based on some alternative authentication mechanism (e.g. password).

Advantage

- Their memory should retain data for up to 10 years without electrical power and (f) they should support at least 10,000 read-write actions during the life of the card.

Disadvantage

- However several passwords are simple and they can be easily guessed or broken [9], [10].
- Most people use the same password across different applications.
- if a malicious user determines a single password, they can access multiple applications.

SMART CARD

[3] In 2009Wang, J.-y. Liu, F.-x. Xiao, and J. Dan proposed "A more efficient and secure dynamic id-based remote user authentication scheme". In these work dynamic users identities per transaction section could be used. These methods aimed to overcome a common drawback of older remote authentication schemes using smart cards: user's identity was static in all the transaction sessions.

In 2000, Huang et al. [13] presented a password-based remote user authentication scheme using smart cards. However, Chien et al. [11] found Huang et al.'s scheme could not withstand masquerade attack and proposed an efficient password based remote user authentication scheme. In 2003, Ku et al. [15] pointed out that Chien et al.'s scheme is vulnerable to a re°ection attack, inside attack, and is not reparable. Ku et al. also proposed an improved scheme to eliminate the security vulnerability of Chien et al.'s scheme. Yoon et al. [18] found that Ku et al.'s scheme was still susceptible to parallel session attack and insecure for changing the user's password in password change phase. Yoon et al. also developed an improved scheme.

Very recently, Hsiang et al. [12] pointed out that Yoon et al's scheme is vulnerable to parallel session attack, masquerading attack and password guess attack. They proposed an improved scheme to remedy these pitfalls. They claimed their scheme can against parallel session attack, masquerading attack and password guess attack. However, we find that Hsiang et al.'s scheme is vulnerable password guess attack, masquerading user attack and masquerading server attack.

According to the researches in [14, 17], all existing smart cards are vulnerable since the secret values stored in a smart card could be extracted by monitoring its power consumption. Therefore, we further assume that the attacker *A* can steal the user's smart card and extract the values stored in the smart card. Under these two assumptions, we will examine some weaknesses of Hsiang et al.'s remote user authentication method.

Disadvantage

- It may leak some information about that user and can create risk of ID-theft during the message transmission over an insecure channel.
- Users should always have their smart cards with them in order to do transactions
- if a user loses his/her smart card, he/she will not be able to do any transactions and should wait for the reissuing of the card (sometimes several days).
- Smart cards cost money and effort each time they are (re)issued.
- due to low power they cannot perform very complex computations

BIOMETRICS

[4] In 2014 A. K. Jain, A. Ross, and S. Prabhakar, propose a "An introduction to biometric Recognition" Biometrics is inherently more reliable, since biometric traits cannot be lost or forgotten, they are more difficult to forge, copy, share, and distribute and they do not require the person being authenticated to be present at the time and point of authentication[5]. Recently, the biometrics have been extensively applied in remote authentication and several methods were reported [6], [7].

Disadvantage

- They cannot provide anonymity and three-factor security while they are vulnerable to the privileged insider and the user impersonation attacks.

STEGNOGRAPHY

[8] In 2000 S. Areepongsa, Y. F. Syed, N. Kaewkamnerd, and K. R. Rao, propose a "Steganography for a low bit-rate wavelet based image coder," .In this work the message is hidden in the sign/bit values of insignificant children of the detail sub bands, in non-smooth regions of the image. Using this technique steganographic messages can be send in lossy environments, with some robustness against detection or attack.

Disadvantage

- Low losses are considered and the problem of compression remains.
- Embedding algorithm is quite complex and sensitive to lossy transmissions.
- Nevertheless if opponents know the embedding algorithm, they can easily extract the hidden information.
- No encryption is incorporated.

III.EXISTING SYSTEM

This paper proposes a robust authentication mechanism based on semantic segmentation, chaotic encryption data hiding, compression, Decompression and Data Extraction. In our case, biometric identifiers are encrypted by a chaotic cipher, which works like a one-time pad in terms of key-size, since the generated key has size equal to the size of the data to be encrypted as shown on figure 1. Chaotic systems are good for such kinds of tasks, since they present an infinite number of unstable orbits, thus an infinite number of different values. Firstly, the scheme provides a secondary complementary authentication mechanism in case when the person under authentication is also captured by the camera. Thus her face and body is transmitted together with another biometric feature for possible double authentication. Secondly, in every recent transaction, the overall architecture can store the latest sample pictures of one's face and body. This could help in cases of hybrid remote authentication, when both a machine and a human remotely authenticate a person. The machine can authenticate the fingerprint and the human can authenticate the face (like the teller does in a bank). Another advantage has to do with more efficient bandwidth usage, especially in the aforementioned case of hybrid remote authentication. An image usually does not only contain semantically meaningful information but also background blocks.

Advantages of Existing System

- Robustness against deciphering, noise and compression.
- Good encryption capacity.
- Ease of implementation.
- Encrypt biometric signals to allow for natural authentication
- Chaotic Pseudo-Random Bit Generator (C-PRBG) to create the keys that trigger the whole encryption to increase security
- The encrypted biometric signal is hidden in a VO, which can reliably be detected in modern applications that involve teleconferencing.

Disadvantages of Existing System

- In wireless communications sensitive information is frequently exchanged, requiring remote authentication.
- Remote authentication:-The submission of encrypted information, along with visual and audio cues (facial images/videos, human voice etc.).
- Trojan horse and other attacks can cause serious problems, especially in cases of remote examinations (in remote studying) or interviewing (for personnel hiring).

IV.PROPOSED SYSTEM

In Proposed system firstly video conferencing the object is extracted with the host object then it is going through the hiding module this consist of QSWT I. e. Qualified Significant Wavelet Tree this is beneficial where lossy transmission and compression in wireless network. In this module the input signal is also encrypted with biometric samples so individuals identity is encrypted then vectorise this biometric signal [4]. Then stego object which is compressed is transmitted to decompress through QSWT's module and decrypted. Database of stored host object which is hidden is also maintained.

Fingerprint verification system manufactured by Digital Person, Inc., is used for computer and network login. Fingerprint-based point of sale (POS) terminal manufactured by Indivos, Inc., that verifies the customers before charging their credit cards and speeds up payment in retail shops, restaurants and cafeterias. Fingerprint-based door lock manufactured by BioThentica Corporation used to restrict access to premises is shown.

Advantages of Proposed System

- Non intrusive.
- Cheap technology also available
- Very high accuracy.
- High Accuracy

V.RESULTS AND DISCUSSION

Video Object Encryption

The general methodology included: (a) extraction of the host video object from a videoconference frame. The encrypted biometric signal is robustly hidden in the host video object. Towards this direction we aim at producing a stego-video object that could protect its hidden message even in cases of compression or lossy transmission.

Fingerprint Encryption

Before hiding, each biometric signal is initially encrypted. Encryption is performed by the proposed chaotic cryptographic module. The module includes a Chaotic Pseudo-Random Bit Generator (C-PRBG) and a chaos-based cipher mechanism. In most contemporary schemes security of the encrypted content mainly depends on the size of the key. In this paper, the generated key has size equal to the size of each biometric signal.

Wireless Band Selection for Data Hiding

The proposed video objects oriented biometric signals hiding scheme is examined in terms of security, effectiveness, robustness and bandwidth usage efficiency. it is one of the most efficient algorithms of literature that facilitates robust hiding of visually recognizable patterns,_ it is hierarchical and has multi resolution characteristics, the embedded information is hard to detect by the human visual system (HVS), and it is among the best known techniques with regards to survival of hidden information after image compression

Decryption

The decryption module receives at its input a vector of encrypted samples, the initial control parameters and initial conditions for the triplet of chaotic maps (C-PRBG module) and the initial cipher value C0 (used at the first feedback). Afterwards the digital chaotic systems produce the same onetime pad used during encryption, but now for decryption purposes. The procedure is terminated after the final sample is decrypted and a ll decrypted samples are reordered (in case of 2-D signals), to provide the initial biometrics signal.

Data Loss Detection and Recovery

Considering that the stego-object (or a distorted version of it) has reached its destination, the encrypted biometric signal is initially extracted by following a reverse (to the embedding method) process. Towards this direction let us assume that the recipient of the stego-object has also received the size of the encrypted 2-D biometric signal (axb), the scaling constants (c1, c2) and possesses the original host video object (or he/she has the algorithm to segment it from the initial head- and body image). The original biometric signal is recovered by decrypting the enciphered signal (see subsection IV-F). Here it should be mentioned that if the same video object X is used for every authentication attempt, the scheme may become vulnerable to attacks. In order to confront this problem the sender and receiver may share multiple video objects (poses) for each user. In each authentication session, the sender may select one pose and inform the receiver of the selected pose's ID. This is a more resistant to attacks methodology, which can become even more efficient if new poses of the users are periodically collected.

VI.CONCLUSION

Using biometric signals we can encrypt information with biometric sample and transmission is done through video or any other media. This information is hidden in the form of steganography image. 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 applications. can be used for this purpose. For instance, the lost biometric data can be concealed from the authentication module, so that it attempts to perform authentication even though parts are missing (parts that do not contain any crucial information, e.g. terminations/bifurcations in case of fingerprints).

VII.REFERENCES

[1] L. Lamport, "Password Authentication With Insecure Communication," Communications Of The Acm, Vol. 24, No. 11, Pp. 770–772, 1981.

[2] 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.

[3] Y.-Y. Wang, J.-Y. Liu, F.-X. Xiao, And J. Dan, "A More Efficient And Secure Dynamic Id-Based Remote User Authentication Scheme," Computer Communications, Vol. 32, No. 4, Pp. 583–585, Mar. 2009.

[4] A. K. Jain, A. Ross, And S. Prabhakar, "An Introduction To Biometric Recognition," Ieee Transactions On Circuits Systems For Video Technology, Vol. 14(1), Pp. 4–20, 2004.

[5] C.-T. Li And M.-S. Hwang, "An Efficient Biometrics-Based Remote User Authentication Scheme Using Smart Cards," Journal Of Network And Computer Applications, Vol. 33, No. 1, Pp. 1–5, Jan. 2010.

[6] 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.

[7] 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.

[8] S. Areepongsa, Y. F. Syed, N. Kaewkamnerd, And K. R. Rao, "Steganography For A Low Bit-Rate Wavelet Based Image Coder," In Proceedings Of The IEEE International Conference On Image Processing, Vol. 1. Ieee, 2000, Pp. 597–600.

[9]Klimis Ntalianis, Member, Ieee, And Nicolas Tsapatsoulis, Member, Ieee" Remote Authentication Via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks" IEEE Transactions On Emerging Topics In Computing , Vol. ..., No. .., January 2015.

[10] 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.

[11] H. Y. Chien, J. K. Jan, and Y. M. Tseng, \An efficient and practical solution to remote authentication smart card," Computers & Security, vol. 21, no. 4,pp. 372-375, 2002.

[12] H. C. Hsiang and W. K. Shih, \Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," Computer Communications, no. 32, pp. 649-652, 2009.

[13] M. S. Hwang and L. H. Li, \A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no.1, pp. 28-30, 2000.
[14] P. Kocher, J. Ja®e, and B. Jun, \Di®erential power analysis," Proceedings of Advances in Cryptology (Crypto'99), pp. 388-397, Santa Barbara, USA, 1999.

[15] W. C. Ku and S.M. Chen, \Weaknesses and improvements of an e±cient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no.1, pp. 204-207, 2004.

[16] L. Lamport, \Password authentication with insecure communication," Communications of ACM, no. 24, pp. 770-772, 1981.

[17] T. S. Messerges, E. A. Dabbish, and R. H. Sloan,\Examining smart card security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541-552, 2002.

[18] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, \Further improvement of an e±cient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no.2, pp. 612-614, 2004

.