Secure Remote Authentication using Biometric Data

Prof. Dr.D.B.Kadam[1] Asmita Vilasrao Patil[2] Akshata Ajit Patil[3] Neha Avinash Sutar[4]
[1]Assistant Professor [2,3,4]UG Student
[1,2,3,4]Department of Electronics & Telecommunication Engineering
[1,2,3,4]P.V.P. Institute Technology Budhgaon, India

Abstract— In wireless communications sensitive information is frequently exchanged, requiring remote authentication. Remote authentication involves the submission of encrypted information along with visual and audio cues (facial image/ videos, human voice etc.). Many authentication schemes using password and smart cards have been proposed however, password might be forgotten and smart card might br shared, lost or stolen. This paper gives an idea about the previous researches and authentication scheme using hybrid crypto-stenographic schemes.

Key words: MATLAB Software, Biometric, Data Hiding, Face, Fingerprints, Steganography

I. INTRODUCTION

Authentication is act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identy of a person or software programme. The two main directions in the authentication field are positive and negative authentication. Positive authentication is well established and it is applied by the majority of existing authentication system. Negative authentication has been invented to reduce cyberattacks.

The difference between the two is explained by the following example: Let us assume password based authentication. In positive authentication, the password of all users that are authorized to access a system are stored, usually in a life. Thus the passwords space includes only user's passwords and it is usually limited (according to the number of users). If crackers receive the password file, then their work is to recover the plaintext of a very limited number of passwords. A remote authentication mechanism based on segmentation, encryption and data hiding. Assuming that user X wants to be remotely authenticated, initially X's video object (vo) is automatically segmented using head and body detector. Next, one of X's biometric signal is encrypted by a chaotic cipher. Afterwards the encrypted signal is inserted to the most significant wavelet coefficients of the video object, using its Qualified Significant Wavelet Trees (QSWT). QSWTs provide both invisibility and significant resistance against lossy transmission and compression, conditions that are typical in wireless networks. Finally, the Inverse Discrete Wavelet Transform (IDWT) is applied to provide the stego-object (so).

II. EXISTING SYSTEM

Year	Concept
1981	One Way Hash Function
2000	Diffie-Hellman Ket Agreement Protocol
2006	Smart Card
2009	Bio Metrics
2014	Stegenography

Table 1: Existing System

III. PROPOSED WORK

Fig. 1: Proposed Work

IV. METHODOLOGY

- Input: The input is biometric signal such as Fingerprint, Iris, DNA we use fingerprint for remote authentication, acquire biometric data from an individual or data available on internet.
- Encryption: In this proposed approach, input processing involves Encryption of biometric signal. Encryption can scramble biometric signal so that cannot be understood.
- Video Conference Image: A video conference of the biometric signal's owner is analysed.
- Host Video Object: Host video object is extraction of video conference frame and video object automatically segmented, using a head and body detector.
- QSWTs Detection Module: In the proposed video object stenographic scheme, coefficients with local information in the sub bands are chosen target coefficients for casting the encrypted biometric signal. Coefficients selection is based on Qualified Significant Wavelet Trees (QSWT).
- DWT- DWT: Based algorithm is proposed for hiding the encrypted biometric signal to the host video object. Initially the extracted host object is decomposed into two levels by the separable 2-D wave late transform, providing three pair of sub bands (HL2, HL1), (LH2,LH1) and (HH2,HH1).
- Sub band Pair Selection: Select the pair of sub band that contains the highest energy contain among the three pairs.
- QSWTs Estimation: QSWTs approach is incorporated in order to select the coefficients where the encrypted

biometric signal should be casted. Finally, the signal is redundantly embedded to both subbands of the selected pair, using a non-linear energy adaptable insertion procedure.

- Hiding Module: As effective wavelate-based stegnography method is proposed for hiding encrypted biometric signals into video objects such as the head-and-shoulders video object, which is common is several teleconferencing applications.
- Stego Object: The Inverse Discrete Wavelate Transform (IDWT) is applied to the modified and unchanged subbands to from the final stego object. Difference between the original and the stego object are imperceptible to the human visual system.
- Wireless Network: Stego object is wirelessly transmitted which is achieved by using suitable medium.
- QSWTs Detection: The stego object has reached its destination, the encrypted biometric signal is initially extracted by following a reverse process. The resulting hidden message coefficients are averaged and rearranged the provide the encrypted biometric signal and host video object.
- Database 1: In the database 1 host video objects are stored, The system extract a host video object and compares it with that scored in the database.
- Decryption: If two feature sets are matching, the system could recognize the individual and the original biometric signal is recovered by decrypting the enciphered signal, otherwise, the system will reject the individual.
- Database 2: In the database 2 host biometric signals are stored, the system computers decrypted signals with biometric signals stored in the database 2. If the two features sets are matching, the system could recognize the individual and authentication is performed.

V. IMPLEMENTATION ALGORITHM

Two processing are

- Encryption algorithm,
- Decryption algorithm

A. Encryption Procedure

1) Input the image
2) Assign a valid key of 256
3) Read the volume of image as matrix
4) Generate matrix of arbitrary numbers
5) Round the random values
6) Apply XOR operation of rounded values
7) Shows encrypted image effect

B. Decryption Procedure

1) Input encrypted image
2) Allot the same key of 256 mixtures
3) Read the size of encrypted image
4) Produce random number
5) Encircling the random values
6) Apply Exclusive-OR action of encircle values
7) Show original image

VI. RESULT

Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. The strength of steganography can thus be amplified by combining it with cryptography.

During their transmission, the data can be accessed illegally and misuse by the hackers and unauthorized user. These troubles are usually happened in the internet communication. Hence data needs high protection on consistently. Ensure high legitimate user and no one else. . By using biometrics, it is possible to confirm or establish an individual's identity based on "who she is," rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password). .

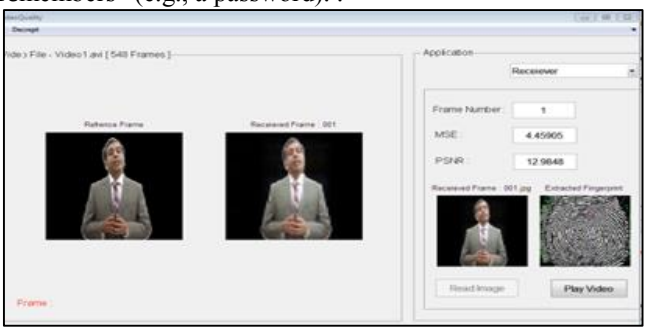

Fig. 2: Result

VII. CONCLUSION

In this paper we presented secure remote authentication using biometric data with stegnography for wireless network. Biometric signals enter more and more into our everyday lives, since governments 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.

We concluded that biometrics technology is more efficient way of authentication than the more common use of pass words, smart cards, or a combination. The purpose of such schemes is to ensure that the rendered.

REFERENCES

[1] A.K.Jain, A.Ross, and S.Prabhakar,"An introduction to biometric recognition". IEEE Transaction on Circuits System for Video Technology, vol. 14(1),pp.4-20.2004.
[2] D.He and D. Wang, "Robust biometrics-based authentication scheme for multi-server environment", IEEE System Journal,pp. 1-8, 2014.
[3] M.Ramkumar and A. N. Akansu, capacity Estimates for data hiding in compressed images", IEEE Transactions on Image Processing, vol.10(8), pp. 1252-1263,2001.
[4] N. D. Doulamis, A. D. Kollias, "An efficient fully-unsupervised video object segmentation scheme using an adaptive neural network classifier architecture", IEEE Transaction on Neural Networks, vol. 14(3), pp. 616-630, 2003.
[5] A. M. Fard, M. R. Akbarzadeh-t, and F. Varasteh-A, "A new geneticalgorithm approach for secure jpeg steganography", in Proc. Of IEEE Int'1 Conference on Engineering of Intelligent Systems. IEEE, 2006
[6] D. Kundur, Y. Zhao, and P. Campisi, "A Steganographic Framework for Dual Authentication and Compression of High Resolution Imagery", in Proceedings of the IEEE International Symposium on Circuits and System, Vol. 2. IEEE, 2004, pp. 1-4.

