IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 06-08
www.iosrjournals.org

Remote Authentication Via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks

R.Ramani[1,] V.Sowmiya[2,] T.Shabana[3,]K.Babu[3] Dr. C. Kumar[4]
[1,2,3] Final year CSE students S.K.P Engineering College, Tiruvannamalai
[4] Assistant Professor, CSE S.K.P Engineering College, Tiruvannamalai
[5] Director Academic, Sri Rangapoopathy College of Engineering, Alampoondi

Abstract: *Inwireless communications sensitive information is frequently exchanged, requiring remote authentication. Remote authentication involves the submission of encrypted information, along with visual and audio cues (facial images/videos, human voice etc.). Nevertheless, Trojan Horse and other attacks can cause serious problems, especially in cases of remote examinations (in remote studying) or interviewing (for personnel hiring). This paper proposes a robust authentication mechanism based on semantic segmentation, chaotic encryption and data hiding. Assuming that user X wants to be remotely authenticated, initially X's video object (VO) is automatically segmented, using a head and- body detector. Next, one of X's biometric signals is encrypted by a chaotic cipher. Afterwards the encrypted signal is inserted to the most significant wavelet coefficients of the VO, using its Qualified Significant Wavelet Trees (QSWTs). 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). Experimental results, regarding: (a) security merits of the proposed encryption scheme, (b) robustness to steganalytic attacks, to various transmission losses and JPEG compression ratios and (c) bandwidth efficiency measures, indicate the promising performance of the proposed biometrics-based authentication scheme.*

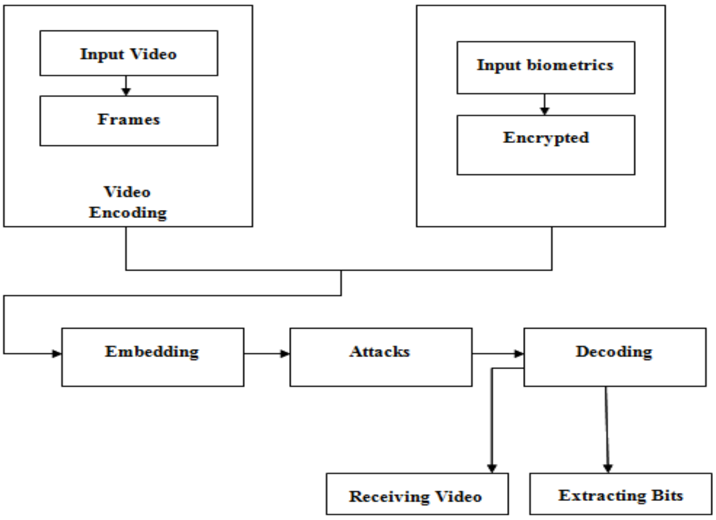
IndexTerms: *Wireless communication, Authentication, Data hiding, Encrypted information, Choatic encryption, Sematic segmentation*

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 it's packaging and labeling claims to be. 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 systems. Negative authentication has been invented to reduce cyber-attacks. The difference between the two is explained by the following example: Let us assume password-based authentication. 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 user's passwords and it is usually limited (according to the number of users). If crackers receive the passwords file, then their work is to recover the plaintext of a very limited number of passwords. 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. This way, 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. According to, in 2012 identity fraud in US affected 12.6 million consumers, and resulted in a loss of $4.6 billion ($365/consumer). Furthermore, the probability of becoming an identity fraud victim is approximately 5.3%. As a result, robust remote human authentication becomes one of the most important issues of contemporary societies and several works have been proposed in the literature to effectively tackle it. The majority is based on passwords or smart cards.

Biometrics has already been incorporated in remote authentication (but only as password substitution in smart cards. In order to investigate their full potentiality, biometrics can be incorporated in hybrid crypto-Steganographic schemes. In particular, cryptographic algorithms can scramble biometric signals so that they cannot be understood, while Steganographic methods can hide the encrypted biometric signals so that they cannot be seen. In this paper we build further on this principle to confront the problem of remote human authentication over wireless channels, under loss tolerant protocols.

II. Proposed System Block Diagram



III. Existing Concept

- Password-based remote user authentication schemes are widely investigated, with recent research increasingly combining a user’s biometrics with a password to design a remote user authentication scheme that enhances the level of the security.
- This paper we propose want to access different application servers. To solve an anonymous multi-server authenticating key agreement scheme based on trust computing using smart cards, password, and biometrics.

IV. Existing Technique: Single Registration And Anonymity

4.1 Technique Definition:

The user only needs to register with the registration center once and then can access different application servers. The privacy of the user has attracted increasing attention from both industry and academia. Therefore, anonymous authentication involves verifying that a user does not use the real identity to execute the authentication procedure.

V. Proposed Concept

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 images/videos, human voice etc.). Nevertheless, Trojan Horse and other attacks can cause serious problems, especially in cases of remote examinations (in remote studying) or interviewing (for personnel hiring).

VI. Proposed Algorithm: Qualified Significant Wavelet Trees (Qswts):

6.1 Algorithm Definition:

The approach is implemented as a DCT-DWT dual domain, but the authenticator watermark is not encrypted. A similar approach combining DWT and Integer Wavelet Transform (IWT) QSWTs approach is incorporated in order to select the coefficients where the encrypted biometric signal should be casted.

VII. Rawbacks

- Traceable problem: In cryptography, the user’s privacy includes anonymity and untraceability, where anonymity means that an adversary cannot obtain the user’s real identity, and untraceability means that an adversary cannot acquire the user’s behavior trajectory.
- The distribution of PSK: The distribution of the PSK is a trade-off issue. If the PSK is only kept in the RC, the server’s compromise problem will not happen.

VIII. Advantages

- It addresses both spatial and temporal domains, which leads to detecting various malicious changes in spatial and time domains.
- It is faster and lower complexity compared to existing algorithms, making it practical and suitable for real-time applications
- Hiding Capacity of the secret data bits is high.
- Hiding capacity was based on the pixel number corresponding to the two highest peaks of the image histogram

IX. Applications

- This technique reportedly has been used to detect the source of illegally copied movies.
- Content identification and management
- Content protection for audio and video content
- Forensics and piracy deterrence
- Content filtering (includes blocking and triggering of actions)
- Communication of ownership and copyrights.

X. Hardware requirements:

Processor	:	Pentium Dual Core 2.00GHZ
Hard Disk	:	40 GB
RAM	:	2GB (minimum)
Keyboard	:	110 keys enhanced

XI. Software requirements

- MATLAB 7.14 Version R2012a

XII. Future Enhancement

In future research, the effects of compression and mobile transmission of other hidden biometric signals (e.g. voice or iris) should also be examined. The problem of lost biometric data is also of high interest. Techniques from the areas of image error concealment, region restoration or region matching 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).

XIII. 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 applications. Towards this direction in this paper the domain of biometrics authentication over error-prone networks has been examined. Since steganography by itself does not ensure secrecy, it was combined with a chaotic encryption system. The proposed procedure, except of providing results that is imperceptible to the human visual system, it also outputs a stego-object that can resist different signal distortions, and steganalytic attacks. Experimental evaluation and detailed theoretical security analysis illustrate the performance of the proposed system in terms of security.

Reference

[1]. **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.

[2]. **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.

[3]. **E.-J. Yoon, S.-H. Kim**, and **K.-Y. Yoo**, “Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic id-based remote user authentication scheme’,”International Journal of Innovative Computing, Information and Control, vol. 8, no. 5(B), pp. 3661–3675, May 2012.

[4]. **R. Madhusudhan** and **R. C. Mittal**, “Dynamic id-based remote user password authentication schemes using smart cards: A review,” Intelligent Algorithms for Data-Centric Sensor Networks, vol. 35, no. 4, pp. 1235– 1248, Jul. 2012.