Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-6, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

IWT Based Remote Authentication Via Biometrics

Mrs. Hima Jose
M. Tech in Computer Science & Engineering, Thejus Engineering College, Vellarakkad

Abstract: *In remote communications data is as often as possible exchanged, requiring remote confirmation. Remote verification includes the accommodation of encrypted data, alongside visual and sound prompts (facial pictures/recordings, human voice and so on.). Trojan Horse and different assaults can bring about genuine issues, particularly in instances of remote examinations (in remote studying) or meeting (for personal hiring). This paper proposes a powerful authentication in view of semantic division, blowfish encryption and data embedding. Accepting that client X needs to be remotely authenticated, at first X's video frame (VO) is naturally fragmented, utilizing a head and-body finder. Next, one of X's biometric signs is encrypted. Next, the encrypte signal is embedded to the most significant wavelet coefficients of the VO, utilizing its Qualified Significant Wavelet Trees (QSWTs). QSWTs give both imperceptibility what's more, critical resistance against lossy transmission and compression, conditions that are regular in remote systems. At last, the Inverse integer Wavelet Transform (IIWT) is applied to give the stego-object(SO).*

1. 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. 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 users 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. The proposed scheme is a positive authentication system and for security reasons elements from at least two, and preferably all three, of the following factors should be verified:

- 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.)

2. Literature survey

In 1981, [2] 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 [2] proposed a password-based authentication scheme using password tables to authenticate remote users over insecure network. Since then, many passwordbased 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

Liao et al. [3] 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 [10],[11]
- Most people use the same password across different applications
- If a malicious user determines a single password, they can access multiple applications.

In 2009 [4] Wang, 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: users identity was static in all the transaction sessions.

In 2000, Huang et al. [14] presented a password-based remote user authentication scheme using smart cards. However, Chien et al. [16] 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. [16] pointed out that Chien et l.s scheme is vulnerable to a reaction 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. [19] found that Ku et al.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. [13] pointed out that Yoon et als 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 [15, 18], 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

In 2014 [5] 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 [7], [8].

Disadvantage

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

In 2000 [9] 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.

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

To enhance the security of the password based user authentication schemes in smart cards, the authors have presented a new scheme which introduces a new technology “Biometrics" in the field of information security. This scheme does not require the system to store password tables and hence makes the system more secure. It is proven that this scheme can withstand the replay attacks and impersonation attacks. But the system can face impersonation attacks if one of the secret keys used in this scheme is hacked by the attackers. It can work efficiently and with an enhanced security on a remote user authentication system. The security of this approach is based on the ElGamal public key cryptosystem, with two secret keys. The biometrics used in this approach uses fingerprint verification with minutiae matching techniques.

Adavantage

- Efficient
- Enhance the security
- Withstand the replay attacks

Disdavantage

- Make mistakes with the dryness or dirty of the finger

2. Features of Novel Video Steganography

The features of NVS are given below:

- Secure

Since data are also placed in frames that are not used in the video, the attacker is left clueless to know the real secret data hidden in the video. Hence highly confidential data like military secrets and bank account details can be easily steganography in ordinary video and can be transmitted over internet even in unsecured connection.

- Capacity

Content based steganography has constrained limit and Image steganography attempted to enhance the limit where 50.

- Imperceptibility

It is less imperceptible because of quick display of the frames. It becomes harder to be detected by human perception system.

- Video error correction

Since the transmission of any data is always subject to corruption due to errors, then transmission must deal errors. This is another application for steganography rather than security purpose.

3. Proposed System

3.1 System Architecture

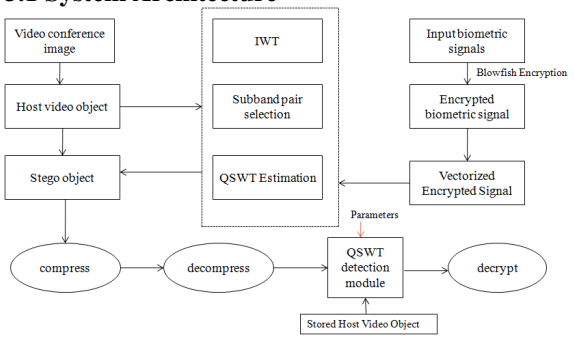

Figure 1: Data Flow of Proposed Scheme

This system proposes a robust authentication mechanism based on semantic segmentation, Blowfish encryption and data hiding. Assuming that user X wants to be remotely authenticated, initially X video object (VO) is automatically segmented, using a headand- body detector. Next, one of X biometric signals is encrypted by a blowfish encryption.

Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes). The algorithm was developed to encrypt 64-bits of plaintext into 64-bits of cipher text efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required to encrypt and decrypt data on 32-bit processors. A conscious attempt was made in designing the algorithm to keep the operations simple and easy to code while not compromising security. As with DES, Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round left 32-bits. Blowfish incorporated a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32- bits for the next round. Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation.

For decryption, the same process is applied, except that the sub-keys Pi must be supplied in reverse order. The nature of the Feistel network ensures that every half is swapped for the next round. The basic algorithm for Blowfish is illustrated as follows:

Divide X into two 32-bit halves XL and XR
For i=1 to 16:
XL = XL Pi
XR = F (XL) XR
Swap XL and XR

End for
Swap XL and XR
XR = XR P17
XL = XL P18
Recombine XL and XR
Output X (64-bit data block: cipher text)

Next a IWT-based algorithm is proposed for hiding the encrypted biometric signal to the host VO. The proposed algorithm hides the encrypted information into the largestvalue QSWTs of energy-efficient pairs of subbands. Compared to other related schemes, the incorporated approach has the following advantages:

- It is one of the most efficient algorithms of literature that facilitates robust hiding of visually recognizable patterns
- It is hierarchical and has multiresolution characteristics
- The embedded information is hard to detect by the human visual system (HVS)
- The best known techniques with survival of hidden information after image compression.

Generally wavelet domain allows us to hide data in regions that the human visual system (HVS) is less sensitive to, such as the high resolution detail bands (HL, LH and HH), Hiding data in these regions allow us to increase the robustness while maintaining good visual quality. Integer wavelet transform maps an integer data set into another integer data set. In discrete wavelet transform, the used wavelet filters have floating point coefficients so that when we hide data in their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information which may lead to the failure of the data hiding system. To avoid problems of floating point precision of the wavelet filters when the input data is integer as in digital images, the output data will no longer be integer which does not allow perfect reconstruction of the input image and in this case there will be no loss of information through forward and inverse transform. Due to the mentioned difference between integer wavelet transform (IWT) and discrete wavelet transform (DWT) the LL sub band in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL sub band is distorted. 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 (IIWT) is applied to provide the stego-object (SO). Afterwards, a head-and-body image of the biometric signals owner is analyzed and the host VO is automatically extracted.

3.2 Advantages of Proposed System

- Robustness against deciphering, noise and compression.
- Good encryption capacity.
- Ease of implementation.
- Encrypt biometric signals to allow for natural authentication.
- Hiding Capacity of the secret data bits is high.
- It is faster and lower complexity compared to existing algorithms, making it practical and suitable for real-time.

4. Conclusion

Biometric signals enter more and more into our everyday lives, thus there is an urgent need to further develop and integrate biometric authentication techniques into practical applications. Since steganography by itself does not ensure secrecy, it was combined with a blowfish encryption system. Since steganography by itself does not ensure secrecy, it was combined with a blowfish encryption system. The proposed procedure, except of providing results that are imperceptible to the human visual system, it also outputs a stego-object that can resist different signal distortions, and steganalytic attacks. Use of IWT provide a round-off operations into a invertible encryption procedure. Experimental evaluation and detailed theoretical security analysis illustrate the performance of the proposed system in terms of security.

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).

5. References

[1] Klimis Ntalianis, Nicolas Tsapatsoulis,(2016),Remote Authentication via Biometrics: A Robust Video-object Steganographic Mechanism Over Wireless Networks, IEEE Transactions on Emerging Topics in Computing ,Volume: 4, Issue: 1,Page(s): 156 - 174.

[2] L. Lamport,(2000),Password Authentication With Insecure Communication, Communications Of The Acm, Vol. 24, No. 11, Pp. 770-772.
[3] I.-E. Liao, C.-C. Lee, And M.-S. Hwang,(2006),A Password Authentication Scheme Over Insecure Networks,Journal Of Computer And System Sciences, Vol. 72, Pp. 727-740.
[4] Y.-Y.Wang, J.-Y. Liu, F.-X. Xiao, And J. Dan,(2009), A More Efficient And Secure Dynamic Id-Based Remote User Authentication Scheme,Computer Communications, Vol. 32, No. 4, Pp. 583-585.
[5] A. K. Jain, A. Ross, And S. Prabhakar(2004),An Introduction To Biometric Recognition,Ieee Transactions On Circuits Systems For Video Technology, Vol. 14(1), Pp. 420.
[6] C.-T. Li And M.-S. Hwang,(2010),An Efficient Biometrics-Based Remote User Authentication Scheme Using Smart Cards, Journal Of Network And Computer Applications, Vol. 33, No. 1, Pp. 15.
[7] E.-J. Yoon And K.-Y. Yoo,(2013), 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.
[8] H. Kim, W. Jeon, K. Lee, Y. Lee, And D. Won,(2012),Cryptanalysis And Improvement Of A Biometrics-Based Multi-Server Authentication With KeyAgreement Scheme, In Computational Science And Its Applications, Ser. Lecture Notes In Computer Science, Vol. 7335. Spinger-Verlag, Pp. 391-406.
[9] S.Areepongsa, Y.F.Syed, N.Kaewkamnerd, And K. R. Rao,(2000),Steganography For A Low Bit-Rate Wavelet Based Image Coder, In Proceedings Of The IEEE International Conference On Image Processing Vol. 1. Ieee,, Pp. 597-600.
[10] Klimis Ntalianis, Member, Ieee, And Nicolas Tsapatsoulis, Member, Ieee(2015) Remote Authentication Via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks IEEE Transactions On Emerging Topics In Computing , Vol.2
[11] M. Jakobsson And M. Dhiman,(2013),The Benefits Of Understanding Passwords, In Mobile Authentication, Ser. Springerbriefs In Computer Science, Springer New York, Pp. 524.
[12] M. Weir, S. Aggarwal, M. Collins, And H. Stern,(2010),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,Pp. 162-175.
[13] H. C. Hsiang and W. K. Shih, (2009),Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards, Computer Communications, no. 32, pp. 649-652.
[14] M. S. Hwang and L. H. Li,(2000),A new remote user authentication scheme using smart cards,IEEE Transactions on Consumer Electronics, vol. 46, no.1, pp. 28-30.
[15] P. Kocher, J. Jae, and B. Jun,(2002),Proceedings of Advances in Cryptology, Erential power analysis, (Crypto99), pp. 388-397, Santa Barbara, USA.