A ROBUST METHOD TO OVERCOME COMPRESSION LOSS IN VIDEO OBJECT STEGNOGRAPHY

C.Deepthi Nivetha, E.P.Prakash, G.Poorni

[1]*PG Student, SNS College Of Engineering, Coimbatore*
[2]*Assistant Professor, SNS College Of Engineering, Coimbatore*
[3]*PG Student, SNS College Of Engineering, Coimbatore*

ABSTRACT

In wireless communications secret information is frequently transmitted between 2 or multiple users which requiring remote authentication. Remote authentication works based on the three methods they are encryption of biometric signal, hiding of encrypted along with visual and audio cues (facial images/videos, human voice etc.).Otherwise, In cases of remote examinations, Trojan horse and other attacks could occur which may cause serious problems. This type of attack could occur especially in cases of remote examinations or interviewing (for personnel hiring). This paper proposes a robust remote authentication mechanism based on semantic segmentation, chaotic encryption and data hiding. 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 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.

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

INTRODUCTION

Authentication is the process of providing assurance about the truth of a characteristic or entity. Now a day the identity of a person should be confirmed by the software program which traces the origins of an object. Authentication mechanism makes sure that a product contain information as its packaging time also make sure that a person provide a identity information as original information stored into the database. If the assurance is correct then only the access a system are stored usually in a file format along with identity information. The passwords space in the file includes only user's passwords. This space should be vary according to the number of users and it is usually limited. The advantages of positive authentication is if the attackers receive or hack the passwords file means they can easily recover the plaintext of each password from password fil and Password file should store only very limited number of passwords.

person login otherwise the person cannot login. There are two main types authentication field are positive and negative authentication. Majority of the authentication system follows the Positive authentication and it should be a well-established structure. In positive authentication system the passwords or secret information's of all persons i.e. passwords which need to be authorized to

The second type called negative authentication is directly opposite to the positive authentication. Negative authentication used to reduce cyber attacks. The negative authentication also use the space like positive authentication but that space is named as anti password space. The anti password space contain the strings or characters which is not in the passwords file. Even though the attacker receive the very big anti-secret file, their work will be much harder.

ISSN: 2278 – 1323

The advantages of Negative Authentication are new layer of protection scheme is introduced by the negative authentication scheme in order to enhance the security. If the attacker cannot access the stored passwords means the current negative infrastructure should remain unbroken and creating additional security. Applying this negative selection algorithm prevents unauthorized users from gaining network or information access.

The Factors of Negative Authentication is varying in three types. They are ownership factor, knowledge factor and Inherence factor. The ownership factors are something the user has as its own information e.g. ID card, security token, cell phone etc. The knowledge factors are something the user knows e.g., a password for Gmail access or desktop access, PIN Number for an ATM access, a pattern for mobile access etc. The inherence factor are something the has in its body e.g., fingerprint, retinal pattern, DNA sequence, face, other biometric identifier etc.

EXISTING SYSTEM

DIFFIE-HELLMAN KEY AGREEMENT PROTOCOL [2]

Liao et al proposed a scheme that utilizes the Diffie-Hellman key agreement protocol over insecure networks. In this scheme the user and the system to agree with a session key. By using this session key the symmetric crypto system encrypts and decrypts the communicated messages.
The session key is a random cryptographic key. This key was difficult to memorize because they are random in nature. They are stored at some location and they are released based on some alternative authentication mechanism.

The major advantage of this scheme is they retain memory and data within memory up to 10 years without electrical power. They should support at least 10,000 read-write actions during the life of the card. The major disadvantage of this scheme is several passwords are simple and they can be easily guessed or broken by the attacker as referred in [9], [10]Most people use the same password across different applications so if a malicious user or attacker determines a single password, they can access multiple applications.

- **ONE WAY HASH FUNCTION**
- **DIFFIE-HELLMAN KEY AGREEMENT PROTOCOL**
- **SMART CARD**
- **BIOMETRICS**
- **STEGNOGRAPHY**

ONE WAY HASH FUNCTION [1]
In 1981, Lamport proposed a remote password authentication scheme. This type of authentication scheme follows a one-way hash function. In this scheme the users password and identity information should stored at verification table should be maintained at the remote server at different location. When the user login into the system by providing username and password the given password should be compared with the password at the remote server. If the password matches the user can login otherwise user cannot login. The major drawback of this one way hash function is if intruders break into it, they can modify the table.

SMART CARD[3]

In 2009 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. This method could be discovered in order to overcome a common drawback of older remote authentication schemes. By using smart cards user's identity was static in all the transaction sessions. The smart card is a printed circuit board it contains the users authentication information. This printed information could be invisible to a person. While showing this smart card to the authentication system the information could be read and verified by the sensor in the authentication system.

Disadvantage

- It may leak some information about that user and
- Create risk of ID-theft during the message transmission over an insecure channel.

ISSN: 2278 – 1323

- User need to 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.

This Scheme is essentially more reliable, since biometric characters cannot be lost or forgotten, they are more difficult to forge, copy, share, and distribute. They require the person being authenticated to be present at the time and point of authentication [5]. Recently, the biometrics has been broadly applied in remote authentication [6], [7].

Disadvantage

- They cannot provide three-factor security.
- They are vulnerable the user impersonation attacks.

STEGNOGRAPHY

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

Disadvantage

- Low losses are considered and the compression problem creates the data loss.
- Embedding algorithm is quite complex and sensitive to lossy transmissions.

The machine can be used to authenticate the fingerprint or bio metric information and the human can authenticate the face (like the teller does in a bank). Another advantage is efficient bandwidth usage. Especially it applies the hybrid remote

- Due to low power they cannot perform very complex computations.

BIOMETRICS [4]

In 2004 A. K. Jain, A. Ross, and S. Prabhakar, propose a "An introduction to biometric Recognition". In Biometrics authentication scheme face, thumb and eyes could be used.

- If opponents know the embedding algorithm, they can easily extract the hidden information.
- No encryption is incorporated.

PROPOSED SYSTEM

This paper proposes a robust remote authentication mechanism based on five factors . At sender side three factors could be used they are semantic segmentation, chaotic encryption data hiding, compression. At receiver side two factors are used they are decompression and Data Extraction. In this case, biometric entities are encrypted by a chaotic cipher scheme generate the binary image it contains only a black and white pixels. 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 encryption tasks, because they present an infinite number of unstable bits in form of black and white pixel for an finite number of stable values.

After completing this chaotic scheme the remote authentication provides a secondary complementary authentication mechanism in this the person under authentication is also captured by the camera. Thus his/her face and body is hided into the chaotic image for which provide a double authentication. Secondly, in every recent transaction, the overall architecture can store the latest sample pictures of one's face and body as shown in figure1. This could help in cases of hybrid remote authentication. In this scheme both a machine and a human remotely authenticate a person.

authentication because it applies both human and machine authentication.

ISSN: 2278 – 1323

ADVANTAGES OF PROPOSED 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.

ARCHITECTURE DEIGN

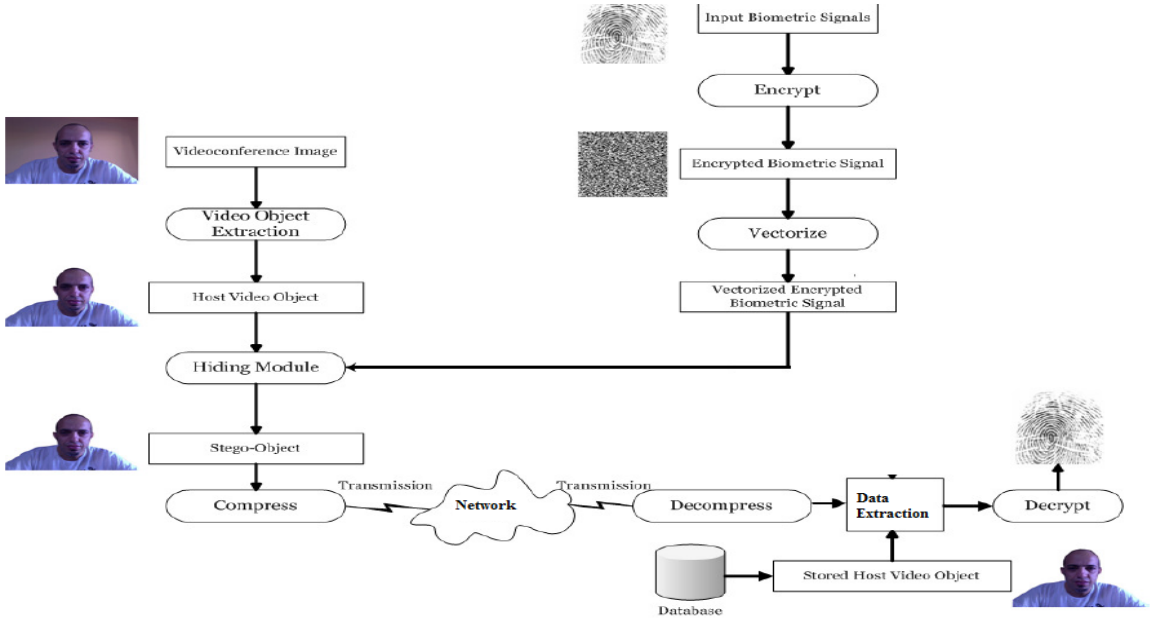

Figure 1:-Remote Authentication Scheme

The architecture diagram of remote authentication describes when the user gives the input biometric signal it should be encrypted by the chaotic encryption scheme and binarized image could be generated. Then the vector values of binarized image could be created and it should be stored into the buffer. From the video signal by using the video stored face image and biometric information should be discovered. Finally the extracted object should be compared with the image stored into the database.

CONCLUSION

In our daily lives Biometric signals enter more and more into our daily lives. Since governments, as well as other private organizations, resort use this type of biometric authentication and it is also called as citizen authentication. Thus the development and integration of biometric authentication techniques into practical applications is increases nowadays. If the steganography scheme alone applied means it does not ensure secrecy when it was combined with a chaotic encryption system it provides additional security. In the proposed procedure when the images send through networks that are imperceptible to the human visual system, it also outputs a stego-object that can resist different signal distortions, and steganalytic attacks.

object extraction scheme the head of the user should be discovered. The face image should be hidden by the vector value and it should be send through the network. Before sending this image it should be compressed. At receiver side first the image should be decompressed and by using the data extraction scheme the

ISSN: 2278 – 1323

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.
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.

[11] 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.

[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

ISSN: 2278 – 1323