A ROBUST VIDEO-OBJECT STEGANOGRAPHIC MECHANISM

S.Rathika[1], Dr. R.Gayathri2

[1]Research Scholar, [2]Asst.Professor
Department of Electronics and Communication Engg, Annamalai University, Chidambaram

ABSTRACT

This project proposes a robust authentication mechanism based on secure force encryption and data hiding. 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. QSWT provide both invisibility and significant resistance against Lossy transmission and compression, conditions that are typical in wireless networks. 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. However, these authentication schemes are designed for a single server environment and result in users needing to register many times when they want to access different application servers. To solve this problem, the project proposes an anonymous multi-server authenticating key agreement scheme based on trust computing using smart cards, password, and biometrics.

Keywords: *QSWT, Lossy transmission and compression, Authentication*

INTRODUCTION

The proposed scheme not only supports multi-server environments but also achieves many security requirements. In addition, the scheme is a lightweight authentication scheme which only uses the nonce and a hash function. From the subsequent analysis, the proposed scheme can be seen to resist several kinds of attacks, and to have more security properties than other comparable schemes. Biometrics has already incorporated in remote authentication but only as password substitution in smart cards. Most people use the same password across different applications; if a malicious user determines a single password, they can access multiple applications.

II. LITERATURE SURVEY

"An Introduction to Biometric Recognition", Anil K. Jain, Arun Ross and Salil Prabhakar,2004, A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of these schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. Examples include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition, or simply biometrics, refers to the automatic recognition of individuals based on their physiological or behavioral characteristics. 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). The author give a brief overview of the field of biometrics and summarize some of its advantages, disadvantages, strengths, limitations, and related privacy concerns.

"Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme", Hakhyun Kim, Woongryul Jeon, Yunho Lee and Dongho Won, 2012, A robust biometrics based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. The author, however, show that Yoon et al.'s scheme is vulnerable to off-line password guessing attack and propose an improved scheme to prevent the attack.

"Dynamic ID-based remote user password authentication schemes using smart cards", RK Madhusudhan, 2012, Remote user authentication is a mechanism, in which the remote server verifies the legitimacy of a user over

an insecure communication channel. Until now, there have been ample of remote user authentication schemes published in the literature and each published scheme has its own merits and demerits. A common feature among most of the published schemes is that the user's identity (ID) is static in all the transaction sessions, which may leak some information about that user and can create risk of identity theft during the message transmission.

"Password secured systems and negative authentication", A. Madero, 2013, Today's industry, government, and critical infrastructure and independent on software systems. In their absence, our modern world would come to a stop. Given the dependence, the mounting cyber threat is of critical concern. In the majority of the systems, passwords are the keys to the system. Unfortunately, there has been little innovation and vulnerabilities keep mounting. Even with established and well known defenses, no authority has emerged to establish policies or laws that guarantee their implementation. The response has been more complex passwords. This is not working. This scheme presents the state of the practice in password systems and introduces work in negative authentication and implementations.

"Robust authentication based multi-server key agreement scheme for smart cards on elliptic curve cryptosystem", E.J. Yoon and K.Y. Yoo, 2013, Conventional single-server authentication schemes suffer a significant shortcoming. If a remote user wishes to use numerous network services, he/she must register his/her identity at these servers. It is extremely tedious for users to register numerous servers. In order to resolve this problem, various multi-server authentication schemes recently have been proposed. However, these schemes are insecure against some cryptographic attacks or inefficiently designed because of high computation costs. Moreover, these schemes do not provide strong key agreement function which can provide perfect forward secrecy.

"An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics", Ming-Chin Chuang, 2014, 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. However, these authentication schemes are designed for a single server environment and result in users needing to register many times when they want to access different application servers. To solve this problem, the author propose an anonymous multi-server authenticating key agreement scheme based on trust computing using smart cards, password, and biometrics. The proposed scheme not only supports multi-server environments but also achieves many security requirements. In addition, it is a lightweight authentication scheme which only uses the nonce and a hash function.

III. BLOCK DIAGRAM

The schematic procedure involved in the proposed system is shown in the figure 3.1 as follows.

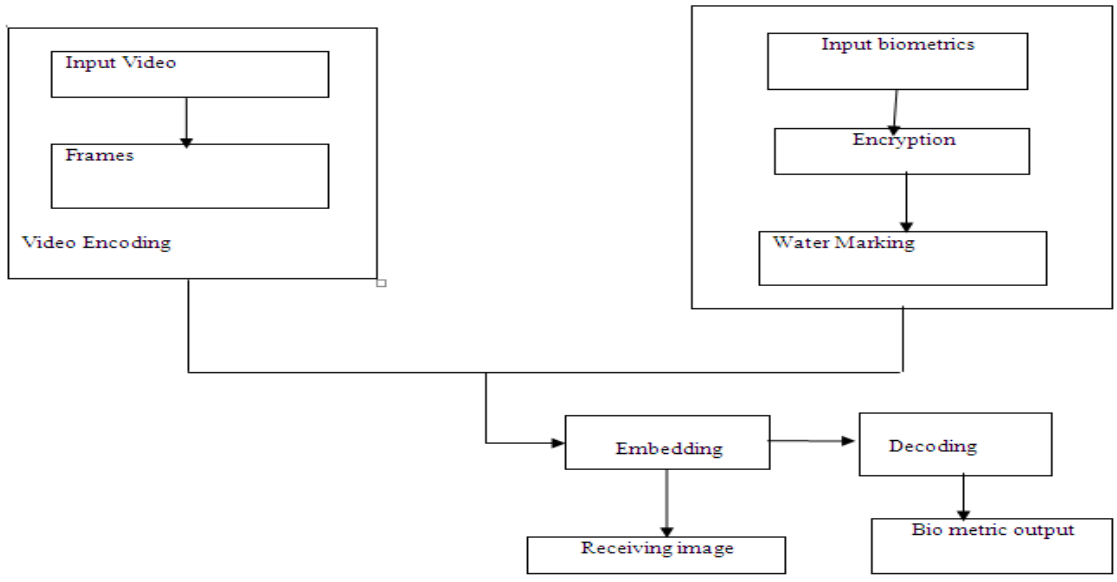

Figure 3.1 Proposed System

3.2 PROJECT DESCRIPTION

3.2.1 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 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 proposed remote human authentication scheme over wireless channels under loss tolerant transaction protocols, aims to ensure: (a) robustness against deciphering, noise and compression, (b) good encryption capacity, and (c) ease of implementation. For this purpose we: (a) employ wavelet-based steganography, (b) encrypt biometric signals to allow for natural authentication, (c) involve a secure force algorithm to create the keys that trigger the whole encryption to increase security, and (d) the encrypted biometric signal is hidden in a VO, which can reliably be detected in modern applications that involve teleconferencing.

The incorporated approach has the following advantages:

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

3.3.2 Video to frame

The extraction of valid information from the video is do in order to process video data efficiently and reduces the transfer stress of network, hence more and more attention being paid to the video processing technology, the segmentation is one of the most popular in the reduction of data which is carried by the video signal along with the key frame extraction so the present researchers are ore concentrating on the above two techniques here we are using the background information and histogram as a key parameter for the frame conversion techniques. The frames segmented from the input video clip are shown in figure 3.2 below.

Figure 3.2 Video to Frame

The frame can be defined as a rigid structure that surrounds something such as picture, door or window pane. An image is a representation of the external form of a person or thing; it is a visual representation of something.

3.3.3 Grayscale

In photography and computing, a grayscale or grayscale digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest. Grayscale images are distinct from one-bit bi-tonal black-and-white images, which in the context of computer imaging are images with only the two colors, black, and white. Grayscale images are also called monochromatic, denoting the presence of only one (mono) color (chrome). Grayscale images are often the result of measuring the intensity of light at each pixel in a single band of the electromagnetic spectrum and in such cases they are monochromatic proper when only a given frequency is captured. But also they can be synthesized from a full color image; see the section about converting to grayscale as shown in figure 3.3.

Figure 3.3 Grayscale input

3.3.4 Encryption

The Secure Force algorithm is based on a Fiestel architecture where the process of encryption and decryption are nearly the same, which minimizes the code size to a great extent. Fiestel architecture is a symmetrical structure used in the construction of block ciphers; has the advantage that encryption and decryption operations are very similar. The design of SF algorithm provides low-complexity architecture for implementation in WSN. To improve the energy efficiency, the encryption process consists of only five encryption rounds. It has been suggested in that a lower number of encryption rounds will result in less power consumption. In order to improve the security, each encryption round encompasses six simple mathematical operations operating on only 4 bit data.

In previous research works they proposed a low-complexity symmetric key algorithm for WSN, denoted as Secure Force (SF) and compare it with several existing symmetric key algorithms based on architecture, flexibility, and security level. This scheme shows the effect of increasing the key size of SF on security and computational complexity; we also performed test for key sensitivity and image encryption.

3.3.5 DWT and QSWT operations

The encrypted biometric signal is robustly hidden in the host video object. Towards this direction the scheme aims at producing a stego-video object that could protect its hidden message even in cases of compression or lossy transmission. QSWTs can play such a role, since they provide one of the most robust solutions to data recovery, after several signal processing manipulations. In particular the host video object has been extracted from the given video input. Next the host video object is decomposed into two levels using the shape-adaptive discrete wavelet transform (SA-DWT). In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. The key advantage it has over Fourier transform is temporal resolution: it captures both frequency and location information. SA-DWT is needed for efficiently coding arbitrarily shaped visual objects, which is essential for object-oriented multimedia applications. The challenge is to achieve high coding efficiency while satisfying the functionality of representing arbitrarily shaped visual texture. One of the features of the SA-DWT is identical to the number of pixels in the original arbitrarily shaped visual object. Another feature of the SA-DWT is that the spatial correlation, locality properties of wavelet transform and self-similarity across sub bands are well preserved in the SA-DWT. Also, for a rectangular region, the SA-DWT becomes identical to the conventional wavelet transforms.

3.3.6 Wavelet transform

Wavelets are wave-like oscillation with amplitude that begins at zero, increases and then decreases back to zero. Wavelets can be combined, using a “reverse, shift, multiply, and integrate” technique called convolution, with portions of a known signal to extract information from the unknown signal. Wavelets have some properties that make them useful for signal processing. Wavelet compression technique gives better performance compared to other traditional techniques. Wavelets are signals which are local in time and scale and generally have an irregular shape. A wavelet is a waveform of effectively limited duration that has an average value of zero.

3.3.7 DWT compression

Image compression is important for many applications that involve huge data storage, transmission and retrieval such as for multimedia, documents, videoconferencing, and medical imaging. Uncompressed images require considerable storage capacity and transmission bandwidth. The objective of image compression technique is to reduce redundancy of the image data in order to be able to store or transmit data in an efficient form. This results in the reduction of file size and allows more images to be stored in a given amount of disk or memory space. Image compression can be lossy or lossless. DWT is used for compression application. Wavelet transform divides the information of an image into approximation and details sub signals. The approximation sub signals shows the general trend of pixel values and other three detail sub signals show the vertical, horizontal and diagonal details or changes in the images. Lossless image compression is particularly useful in image archiving as in the storage of

legal or medical records. Methods for lossless image compression includes: Entropy coding, Huffman coding, Bit-plane coding, Run-length coding and LZW (Lempel Ziv Welch) coding.

3.3.8 Decryption

The decryption module receives at its input a vector of encrypted samples, the initial control parameters and initial conditions for the secure force algorithm which produce the same onetime pad used during encryption, but now for decryption purposes. The procedure is terminated after the final sample is decrypted and all decrypted samples are reordered (in case of 2-D signals), to provide the initial biometrics signal.

3.4 METHODOLOGIES

3.4.1 Modules

The following are the modules present in the proposed scheme,

1. Video to frames conversion
2. The encryption mechanism
3. Hiding the encrypted biometric signal
4. Message recovery

3.4.2 Module description

Video to frames conversion

The video means multiple frames. The captured video is converted into frames using MATLAB codes as it act as a video to frame converter.

The encryption mechanism

The Secure Force algorithm is based on a Fiestel architecture where the process of encryption and decryption are nearly the same, which minimizes the code size to a great extent. Fiestel architecture is a symmetrical structure, used in the construction of block ciphers; it has the advantage that encryption and decryption operations are very similar. The design of SF algorithm provides low-complexity architecture for implementation in WSN. To improve the energy efficiency, the encryption process consists of only five encryption rounds. It has been suggested in that a lower number of encryption rounds will result in less power consumption. **Hiding the encrypted biometric signal**

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. QSWTs can play such a role, since they provide one of the most robust solutions to data recovery, after several signal processing manipulations. In particular let us assume that the host video object has been extracted using the method.

Message recovery

The main focus of this scheme is very challenging: to investigate the possibility of remote authentication over wireless channels under lossy protocols. As a result, our interest during steganography is much more on robustness to manipulations (compression, losses during transmission etc) and less on robustness to steganalysis. In cryptography, the system is broken when an attacker can read the secret message (it does not matter how he does this). On the other hand, breaking a steganographic system has three stages: the attacker can detect that steganography has been used, the attacker extracts the embedded message from the host and the attacker is able to read the embedded message.

3.4.3 Technique

Steganography is the practice of concealing messages or information within other non-secret text or data. The word steganography combines the Greek words steganos meaning “covered, concealed, or protected”, and graphein meaning “writing”. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. The Cryptography is the study of hiding information and it is used when communicating over a un trusted medium such as internet, where information needs to be protected from other third parties. The Cryptography has a major problems that it encrypts the message, but do not hide the message. This can be overcome by Steganography. Image Stegano-graphy in which images are composed of dots called pixels. The pixel is the smallest addressable element of an image. There are 8-bit and 24-bit

per pixel image files. Each pixel gets it own color by combining percentages of red, green and blue. For 8 bit, each of these colors has values from 0-255. Video Stegano-graphy is a technique to hide any kind of files in any extension into carrying video file.

The applications of Stegano- graphy include,

1. Confidential communication and secret data storing.
2. Protection of data alteration

The MATLAB software is used to create a stego-object. The MATLAB is a multi paradigm numerical computing environment and fourth generation programming language. It allows matrix multiplications, plotting of functions and data, implementation of algorithm, creation of user interfaces and interfacing with program in other language including C, C++, Java, FORTRAN and Python.

The advantages of MATLAB includes,

1. It is an interpreted language for numerical computations.
2. It allows one to perform numerical calculations and visualize the results without the need for complicated and time consuming programming.
3. This software allows user to accurately solve problems, produce graphics easily and produce code efficiently.

RESULTS AND DISCUSSION

4.1 GENERAL

MAT LAB (Matrix Laboratory) is a numerical computing environment and fourth-generation programming language. Developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C,C++, Java and Fortran. However this handout focuses on the basic portion of MATLAB.

4.2 INDICATIVE RESULTS

The general methodology included: (a) extraction of the host video object from a videoconference frame and detection of QSWTs to embed the encrypted signal, (b) encryption of the fingerprint, (c) embedding of the encrypted signal to the host video object, (d) compression of the final content and simulated noisy transmission, (e) decompression and extraction of the encrypted signal, (f) decryption and (g) authentication.

Figure 4.1 Input video frame

The videoconference frame is extracted from the input video clip. The input video is a 10 seconds video. The start time is given 0 sec and the end time is 10 seconds. The time lap between the frames is given 2 seconds. As a result, the frames are generated from the input video clip. An example for the frame chosen from the input video clipping is shown in the figure 4.1. The biometric image is taken as another input. The biometric image is to be hidden behind the frame selected from the input video clipping. Before casting the biometric signal behind the frame selected, the biometric image is to be encrypted. The biometric is encrypted using Secure Force Algorithm. The biometric image and the encrypted form of it are shown in the figure 4.2 and figure 4.3 respectively.

Figure 4.2 Original Biometric Image

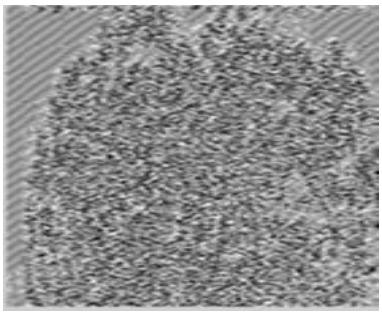

Figure 4.3 Encrypted biometric image

The secure force algorithm is adopted because of its less complexity in symmetric cryptography. It is developed based on Feistel architecture. In secure force algorithm the process of encryption and decryption are nearly the same which minimizes the code size to a great extent.

Figure 4.4 Stego-Objects

The biometric hiding method has been extensively evaluated under various simulation tests using MATLAB. In particular during experimentation the host video object of figure 4.1 was used in which the encrypted biometric signal of figure 4.3 was hidden. Then according to the size of the encrypted biometric signal QSWT was selected for the host video object to embed the signal and it can be observed that the embedded encrypted biometric signal has caused imperceptible change in the host video-object. The overriding majority of the current work does not consider fault-tolerant protocols during transmission of stego-objects. With the proposed approach several mobile applications could benefit. For example, in an emerging scenario, assume the imagine that a user would like to be authenticated via cell phone, tablet etc. The mobile device has a camera, while its touch-screen collaborates with a fingerprints capturing application. In case the signal strength is low, erroneous packets may arrive at the receiver.

This scheme offers some possible advantages. Firstly, the scheme provides a secondary complementary authentication mechanism I case when the person under authentication is also captured by the camera. Thus the 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 ones face and body. This could help in cases of hybrid remote authentication, when both a machine and a human remotely authenticate a person. This project is designed for user under wireless transmission. The case of mobile networks is further studied as a example and the systems resistance is investigated under different JPEG compression ratios and various Bit Error Rate. More particularly the compression ratios between 0.6 and 3.3 were used. Bit Error Rate took values between $3 * 10^{-3}$ and $3 * 10^{-4}$. The good thing about using biometrics for identification is that modern systems are built and designed to be easy and safe to use. Biometric technology gives us accurate results with minimal invasiveness as a simple scan or a photograph is usually all that's required. Moreover, it is extremely quick. Biometric signals are user friendly and that if we use high quality systems, it will also mean maintenance costs.

Biometrics are 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. Considering the typical average bit error rate for cellular mobile radio channels that are in the interval 10^{-4} and10^{-3}. In the simulation of this process we assume unreliable connection less mobile transmission protocol, where errors occur only in the data field of each packet. The results are provided in the table as follows.

Figure 4.5 Initial Fingerprint

Table 4.1 Biometric signal retrieval results for the stego-object

JPEG Compression Ratio=0.6		
BER1	BER2	BER3
R	R	R
JPEG Compression Ratio=3.3		
BER1	BER2	BER3
R	R	R
JPEG Compression Ratio=10.7		
BER1	BER2	BER3
NR	NR	NR

The use of a specific statistical steganalysis method may not be reasonable instead a universal statistical steganalysis technique may work, provided it successfully determines the steganographic algorithm. Regarding more specific security issues of the proposed steganographic scheme, there are some notes that should be observed by a steganographer:

1. Embedding into images available on the Internet is not advisable as a steganalysis devotee might notice and opportunistically utilize them to decode the stego-image. In this scheme, images are created by the user under authentication and destroyed immediately after use.

2. In order to avoid any Human Visual Perceptual attack, the generated stego-image must not have visual artifacts. The proposed scheme adapts the message energy to the energy of each wavelet coefficient, thus visual artifacts are avoided.

3. Smooth homogenous areas must be avoided. This scheme avoids smooth homogenous areas since it is based on QSWT.

4. The secret data must be a composite of a balanced bit values, since in general, the expected probabilities of bit 0 and bit1 for a typical cover image are the same. In this scheme, the data to be hidden are previously encrypted. The encryption provides balance between 0 and 1, since the encrypted file is pseudo-random.

Hence the stego-object created resists all types of transmission and compression losses when they are transmitted. The differences are imperceptible to the human visual system.

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. Towards this direction in this paper the domain of biometrics authentication over error-prone networks has been examined. The scheme offers possible advantages that are it provides a secondary complementary authentication mechanism in case when the person under authentication is also captured by the camera and in every recent transaction the overall architecture can store the latest sample pictures of one face and body that could help in cases of hybrid remote authentication. Since steganography by itself does not ensure secrecy, it was combined with a secure force algorithm 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

7. REFERENCES

1.Arun Ross and Salil Prabhakar(2004), 'An Introduction to Biometric Recognition,' IEEE Transactions on Circuits Systems for Video Technology, vol.14(1), pp. 4-20.

2. Chen. T.-Y, Ling.C.-H, and Hwamg.M.-S.,(2014) 'Weakness of the yoon-kim-yoo remote user authentication scheme using smart cards,' in Proceedings of the 2014 IEEE Workshop on Electronics, Computer and Applications, pp. 771-774.

3.Chuang.M.C and Chen.M.C,(2014) 'An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics,' Expert Systems with Applications, vol.41, no. 4, pp. 1411-1418.

4.Kim.H, Jeon.W, Lee.K, Lee.Y, and Won.D,(2012) '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, pp. 391-406.

5. Madero.A,(2013) ' Password secured systems and negative authentication.' Thesis: S.M. in Engineering and Management, Massachusetts Institute of Technology, Engineering Systems Division.

6. Madhusudhan.R and Mittal.R.C, (2012), '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.