Remote Authentication Via Biometrics Using Steganography, Visual Cryptography

S.Venkatasubramanian[1], G.Akshaya[2], C. Dhivya[3], S.Karunya Preethi[4], R.Keerthiga[5]
Department of Computer Science and Engineering
[1, 2, 3, 4, 5]Saranathan College of Engineering, Trichy-620 012, Tamil Nadu

Abstract-*In Wireless communication, 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, and so on). Nevertheless, Trojan horse and other attacks can cause serious problems, especially in the cases of remote examinations (in remote studying)or interviewing (for personnel hiring). This project work 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. 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 of wireless networks. Experimental results regarding: 1) security merits of the proposed encryption scheme; 2) robustness to steganalytic attacks, to various transmission losses and JPEG compression ratios; and 3)bandwidth efficiency 1 measures indicate the promising performance of the proposed biometrics-based authentication scheme.*

Keywords-Finger print, Encryption, Decryption, Compression, Authentication, Remote.

I. INTRODUCTION

In today's world, hackers are increasing day by day. So there is a need to provide authentication in a remote manner. 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. By applying a real-valued negative selection algorithm, a different layer is added for authentication, preventing unauthorized users from gaining network access.

1.1.PIC16F877A

PIC16F877A is the heart of this system. It consists of clock circuit and power on reset circuit. Clock circuit is built around crystal oscillator and ceramic capacitor. Purpose of crystal oscillator is to stabilize the frequency and the capacitor is to stabilize the amplitude if the clock. This circuit determines the operating speed. Here we use 4MHz crystal oscillator, so the microcontroller will work at the speed of 1uSec. Purpose of the microcontroller is to control the speed of the DC shunt motor according to the load. It uses internal ADC and complete one port for reading load and control the speed. That is it reads voltage output and produces the digital output according to this input voltage. This microcontroller will set the load limit and terminate the DC shunt motor to prevent from over load. PIC16F877A uses Analog to Digital Converter. The GO/DONE bit during a conversion will abort the current conversion.

1.2.BOARD FEATURES OF PIC16F877A

- Includes 3 Zip Sockets to Program various series of PIC.
- Microcontrollers.
- PIC16F877A Microcontroller provided along with the chip.
- A Serial Port for In-System Programming.

- A Serial Port for RS232 Communication.
- Connector provided to connect LCD.
- 4 , 7-Segment Displays with chip select facility using a Dip Switch.
- LED's Connected to all I/O's.
- Keys Connected to all I/O's.
- Pin outs for Port extension for users ease.

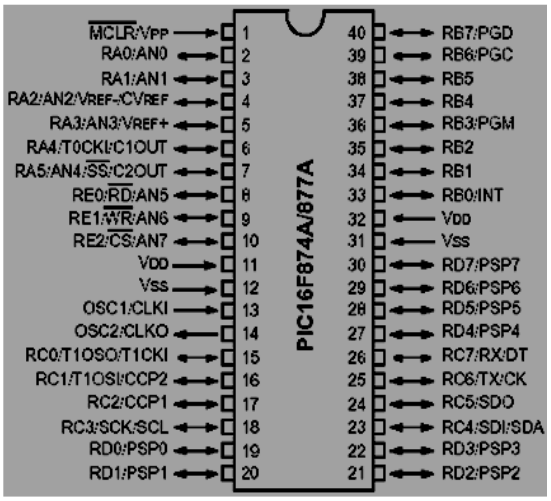
1.3. CHIP FEATURES OF PIC16F877A

- High-Performance RISC CPU
- Only 35 single-word instructions to learn
- 10-bit, up to 8-channel Analog-to-Digital Converter (A/D)
- Self-reprogrammable under software control
- Operating speed: DC – 20 MHz clock input
- Low-power consumption
- Up to 8K x 14 words of Flash Program Memory,
- Up to 368 x 8 bytes of Data Memory (RAM),
- Up to 256 x 8 bytes of EEPROM Data Memory
- 14 interrupts ,3 timers.

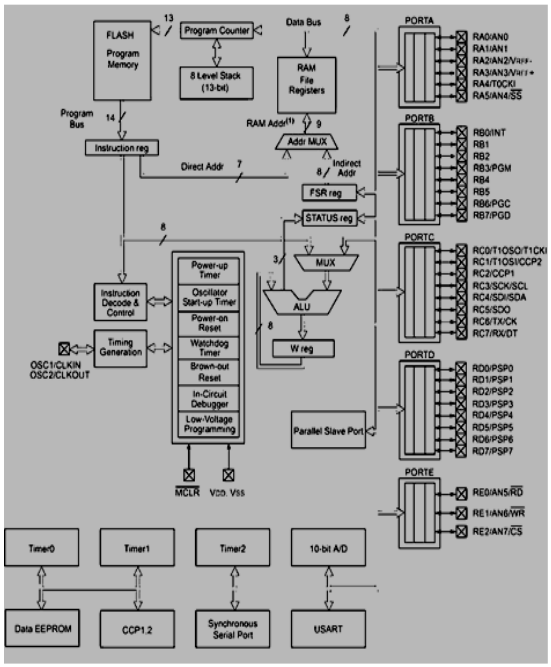
1.4. INTERRUPTS OF PIC 16F877A

The PIC16F877 A family has up to 14 sources of interrupt. The interrupt control register (INTCON) records individual interrupt requests in flag bits. It also has individual and global interrupt enable bits. A global interrupt enable bit, GIE (INTCON<7>) enables (if set) all unmasked interrupts, or disables (if cleared) all interrupts. When bit GIE is enabled, and an Interrupt's flag bit and mask bit are set, the interrupt will vector immediately. Individual interrupts can be disabled through their corresponding enable bits in various registers. Individual interrupt bits are set, regardless of the status of the GIE bit. The GIE bit is cleared on RESET. The "return from interrupt" instruction, RETFIE, exits. The interrupt routine, as well as sets the GIE bit, whichre-enables interrupts. The RB0/INT pin interrupt, the RB port change interrupt, and the TMR0 overflow interrupt flags are contained in the INTCON register.The peripheral interrupt flags are contained in the special function registers, PIR1 and PIR2. The corresponding interrupt enable bits are contained in special Function registers, PIE1 and PIE2, and the peripheral interrupt enable bit is contained in special function register INTCON. When an interrupt is responded to, the GIE bit is cleared to disable any further interrupt, the return address is pushed onto the stack and the PC is loaded with 0004h. Once in the Interrupt Service Routine, the source(s) of the interrupt can be determined by polling the interrupt flag bits. The interrupt flag bit(s) must be cleared in software before re-enabling interrupts to avoid recursive interrupts. For external interrupt events, such as the INT pin or PORTB change interrupts, the interrupt latency will be three or four instruction cycles. The exact latency depends when the interrupt event occurs. The latency is the same for one or two-cycle instructions. Individual interrupt flag bits are set, regardless of the status of their corresponding mask bit, PEIE bit, or GIE bit.

1.5. PIN DIAGRAM OFPIC16F877A



1.6. ARCHITECTURE OF PIC16F877A



II. OBJECTIVE

The overall objective of our project is to develop a secure means of communication by combining biometrics, visual cryptography and steganography in a hack proof manner. The following are some of the main objectives

1) DIGITAL IMAGE AND VIDEO COMPRESSION: The message is hidden in the sign/bit values of insignificant children of the details bands, in non-smooth regions of the image.

2) EFFICIENCY OF COMPRESSION: The message is comprised of two components: a soft-authenticator watermark for authentication and tamper assessment of the given image, and a chrominance watermark employed to improve the efficiency of compression.

3) INTEGER WAVELET TRANSFORM (IWT) : It was recently proposed, where the secret images and the key are encrypted in a cover image.

4) AUTHENTICATION: In fingerprints are hidden in the region of interest of images. Both a machine and a human remotely authenticate a person. The machine can authenticate the fingerprint. Then the message will be displayed.

III. PROPOSED SYSTEM

- In proposed system, we implement secure combined remote authentication approach with advantages of the systems retained while the flaws discussed are removed.
- First data is taken.
- Next biometrics are used to generate a key- this is secure.
- The key generated using fingerprint biometrics is used to encrypt the data
- The data thus encrypted is then covered with a visual cryptographic cover.
- The visual cryptography object is then compressed so that it occupies the least space when embedding.
- Now the compressed object is embedded into a video.
- Neither the video size nor the quality should be affected.
- This data is then transmitted to the destination or stored in the server.
- The above process is then reversed to extract the data from the video.
- To recover a password is required which is emailed –thus secure.
- Then after extraction the data should be decompressed.
- Then the visual cryptographic object should be decrypted using the biometrics.

Finally the data is shown.

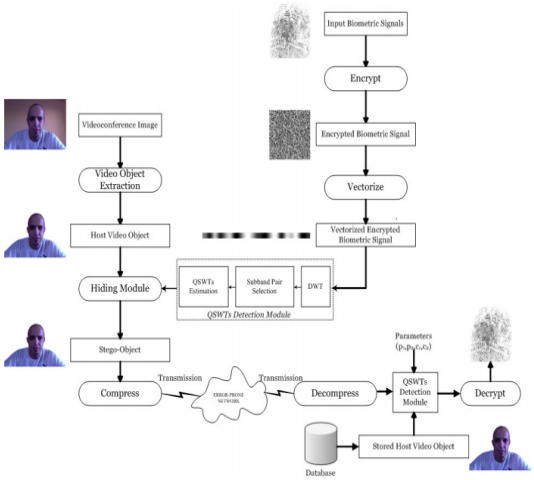


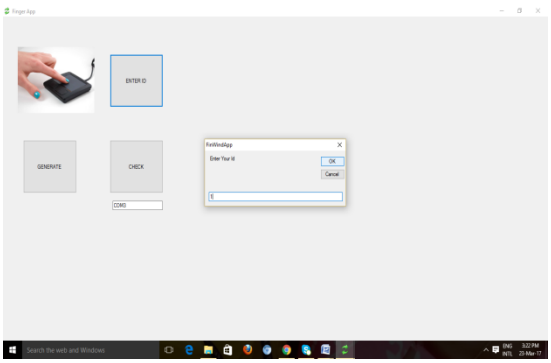
Fig 3.1 System Architecture

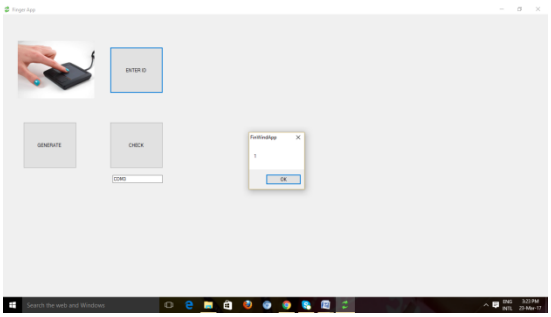
The following are five major modules in this proposed system

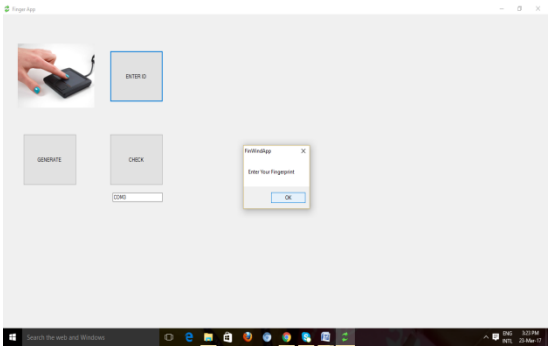
- Bio-metric encryption.
- Visual cryptography.
- Data compression.
- Transmission.
- Pin generation.

1) BIO-METRIC ENCRYPTION

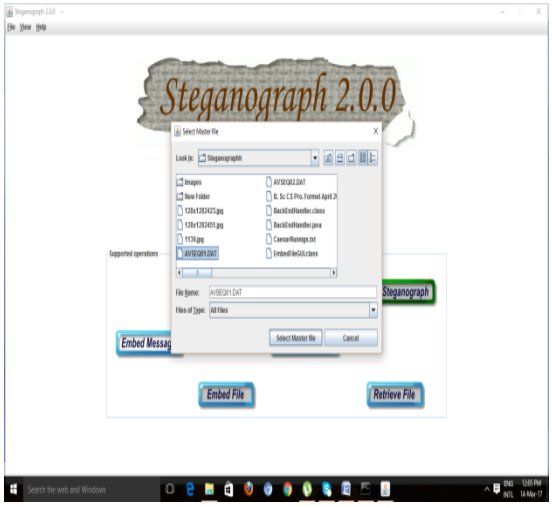
We are using fingerprint for authenticate. embedding algorithm is quite complex and sensitive to lossy transmissions. There are also some schemes focusing on steganography of biometric signals. In an amplitude modulation based proposed, which however is not tested under compression or lossy transmission. In a wavelet-based steganographic method for minutiae embedding is proposed. Nevertheless if opponents know steganographic scheme is the embedding algorithm, they can easily extract the hidden information. In fingerprints are hidden in the region of interest of images. Both DFT and DWT domains are examined. However, again, no encryption is incorporated. Another interesting, but not resistant to compression, method is proposed in where a remote multimodal biometrics authentication framework that works on the basis of fragile watermarking is designed. Finally in a DCT-SVD based watermarking scheme is proposed for ownership protection using biometrics. The scheme is not tested under compression lossy transmission. A last category of approaches involves data hiding within image or video objects of the cover image. Object-oriented data hiding is more secure and robust against deciphering attacks but it usually creates visually sensitive artifacts, thus, lowering the capacity of encryption.



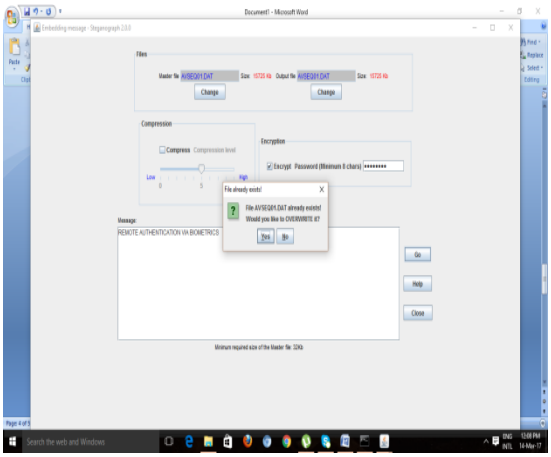


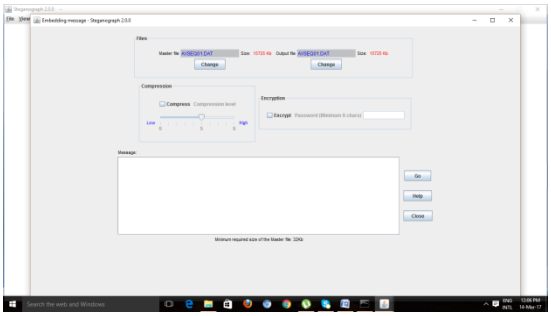


2) VISUAL CRYPTOGRAPHY Detection of semantic objects in both images and videos is by no-means trivial. As a result the majority of methods in this category hide data either in the skin (or skin like) areas of the cover images or in areas implicitly defined through the extraction of specific descriptors.

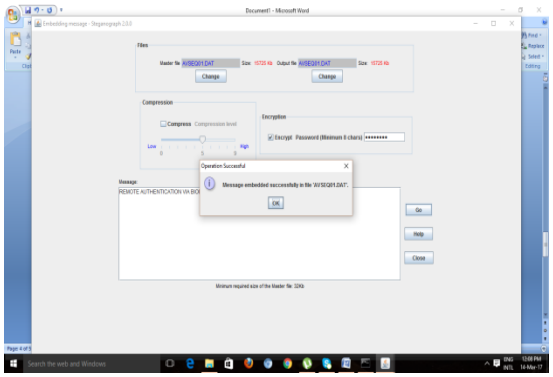


3) DATA COMPRESSION Steganographic algorithms can be roughly divided into those performed in the spatial domain and those applied in atransform domain. Given that the latter are more robust against low-pass filtering and compression attacks , they became the preferred approach. Among transform-based datahiding approaches, DCT and DWT methods are by far, the most popular since they are related with popular digital image and video compression schemes (i.e., JPEG,MPEG, JPEG-2000, H264, etc). In the message is hidden in the sign/bit values of insignificant children of the details bands, in non-smooth regions of the image. Using this technique steganographic messages can be send in lossy environments, with some robustness against detection or attack. However, low losses are considered and the problem of compression remains. In , the message is comprised of two components: a soft-authenticator watermark for authentication and tamper assessment of the given image, and a chrominance watermark employed to improve the efficiency of compression.

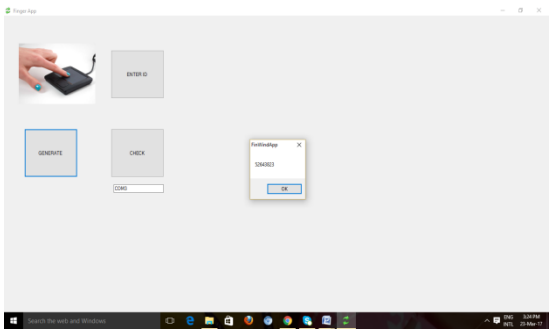


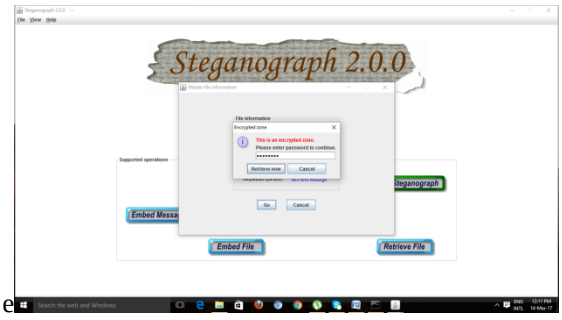


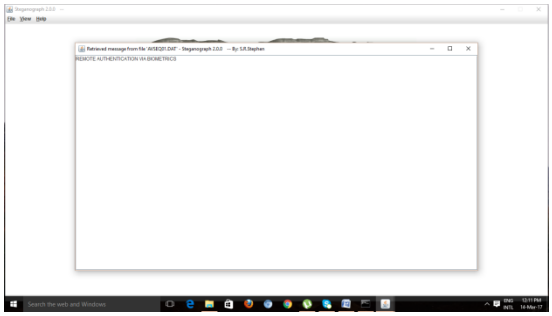
4) TRANSMISSION Most of the existing schemes do not consider semantically meaningful VOs as hosts, but a whole image. The proposed scheme offers some possible advantages. Firstly, the scheme provides a secondary complementary authentication mechanism in case when the person under authentication is also captured by the camera. Thus her face and bodyis 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 one's face and body. This could help in cases of hybrid remote authentication, when both a machine and a human remotely authenticate a person. The machine can authenticate the fingerprint and the human can authenticate the face (like the teller does in a bank). Another advantage has to do with more efficient bandwidth usage, especially in the forementioned case of hybrid remote authentication.An image usually does not only contain semantically meaningful information but also background locks. On the other hand, in order to hide a specific amount of information,a host with proper capacity should be selected. If the host is an image, then irrelevant blocks will also be transmitted, occupying valuable bandwidth. On the contrary, when the host is a semantic VO, all transmitted information is relevant to the authentication task. Last but not least, the proposed scheme allows for more efficient rate control and can better confront traffic congestions. For example, in a typical steganographic algorithm which uses images, if traffic congestion occurs, all image blocks (except those that contain hidden information) would be probably considered of equal importance. On the other hand, the proposed scheme is content-aware.



5) PIN GENERATION Pin can be generated randomly for sender. when the host is a semantic VO, all transmitted information is relevant to the authentication task. Last but not least, the proposed scheme allows for more efficient rate control and can better confront traffic congestions.







IV. 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 are 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 ofthe proposed system in terms of security. The well-known NIST tests were applied to the encrypted biometric signals(fingerprints in our case) to verify the robustness of the proposed chaotic encryption scheme. A series of steganalytic attacks were also applied, using state-of-art steganalysis tools. Results indicate that the use of QSWTs provides high levels of robustness, keeping at the same time the ease of implementation and the compatibility to well-known and widely used image and video compression standards such as JPEG-2000 and H.264. Last but not least, the system is able to recover the hidden encrypted biometric signal under different losses. Even though simulated, losses fluctuated in the typical ranges, encountered in real communication channels. Finally it should be mentioned that all these merits are accompanied by efficient bandwidth usage, since the rate control mechanism is provided with the content-awareness feature.

REFERENCES

[1] A. Madero, ‘‘Password secured systems and negative authentication,’’ Ph.D. dissertation, Dept. Eng. Manage., Massachusetts Inst. Technol., Cambridge, MA, USA, 2013. [Online]. Available: http://hdl.handle. net/1721.1/90691

[2] A. Pascual and S. Miller, ‘‘Identity fraud report: Data breaches becoming a treasure trove for fraudsters,’’ Javelin Strategy Res., Pleasanton, CA, USA, Tech. Rep. 1/2013, 2013.

[3] E.-J. Yoon and K.-Y.Yoo, ‘‘Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem,’’ J. Supercomput., vol. 63, no. 1, pp. 235–255, Jan. 2013.