Biometric Authentication with Steganography for Wireless Networks

S.M.Chougule[1] Prof. S.R.Mahadik[2]
[1]PG student [2]Professor
[1]Department of Electronics Engineering
[2]Department of Electronics and Telecommunication Engineering
[1,2]Dr J.J.Magdum college of engineering jaysingpur, Shivaji University Kolhapur,India, Bhopal

Abstract— In wireless communications sensitive information is frequently exchanged, requiring remote authentication. Many authentication schemes using passwords and smart cards have been proposed. However, passwords might be forgotten and smart cards might be shared, lost, or stolen. This paper tries to gives an idea about the previous researches and authentication scheme using hybrid crypto-stenographic schemes. Remote authentication involves the submission of encrypted information, along with visual and audio cues (facial images/videos, human voice etc.).

Key words: remote authentication, crypto-steganography, audio cues

I. INTRODUCTION

In wireless communications sensitive information is frequently exchanged, requiring remote authentication. 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. 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 networkaccess. Interested readers can also check.

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:

1) The ownership factor: Something the user has (e.g. ID card, security token, cell phone etc.)
2) The knowledge factor: Something the user knows (e.g., a password, a PIN, a pattern etc.)
3) The inherence factor: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence, face, other biometric identifier etc.)

Person authentication is one of the most important issues in contemporary societies. It ensures that a system's resources are not obtained fraudulently by illegal users. Real-life physical transactions are generally accomplished using paper ID while electronic transactions are based on password authentication, the simplest and convenient authentication mechanism over insecure networks. In a remote password authentication scheme was proposed by employing a one-way hash function, which was later used for designing the famous S/KEY one-time password system. However, in such schemes, a verification table should be maintained on the remote server in order to validate the legitimacy of the requesting users; if intruders break into the server, they can modify the verification table. Therefore, many password authentication schemes have recognized this problem, and different solutions have been proposed to avoid verification tables.

II. BIOMETRIC RECOGNITION

A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Examples of such applications 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 and/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)

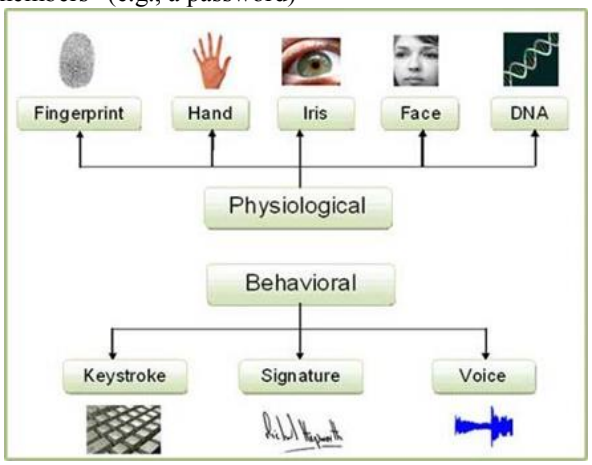

Fig. 1: Classification of Biometrics

Although biometrics emerged from its extensive use in law enforcement to identify criminals security clearance for employees for sensitive jobs, fatherhood determination, forensics, and positive identification of convicts and prisoners), it is being increasingly used today to establish person recognition in a large number of civilian applications.

Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- Universality: each person should have the characteristic.
- Distinctiveness: any two persons should be sufficiently different in terms of the characteristic.
- Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
- Collectability: the characteristic can be measured quantitatively. However, in a practical biometric system (i.e., a system that employs biometrics for personal recognition), there are a number of other issues that should be considered, including, performance, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;
- acceptability, which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;
- circumvention, which reflects how easily the system can be fooled using fraudulent methods.

A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.

A. Biometrics Authentication:

There are four factors of physical attributes that are used or can be used in user authentication:

Finger print scans- which have been in use for many years by law enforcement and other
government agencies and is regarded as a reliable, unique identifier.

Retina or iris scans- which have been used to confirm a persons identity by analyzing the arrangement of blood vessels in the retina or patterns of color in the iris

Voice recognition-which uses a voice print that analyses how a person says a particular word or sequence of words unique to that individual.

Facial recognition-which use unique facial features to identify an individual

III. CRYPTOGRAPHY

Image data are frequently shared and stored in worldwide at various end to end. Images may contain highly confidential and responsive informations. Image type of data are particularly used in the area of military wing, forensic department, intelligent agencies, medicine researches, government sectors, multimedia, film division etc. During their transmission ,the data can be accessed illegally and misuse by the hackers and unauthorized user. These troubles are usually happened in the internet communication. Hence data needs high protection on consistently. Ensure high protection of data, cryptography is the suitable technique keeps the data as safe as in transfer. Main reason behind using cryptography is authentication, secrecy, non disclaimer, consistency and honesty at any instant of data transfers. Cryptography can be describe as the skill of protection file and it makes sure that only the related people to access the content Cryptography is the intelligent art to make a data as secret. It refers sometimes study or analysis of data in secret type. Cryptography is the best tool for protected communication of image, text, video etc. Cryptography is exploiting the study of hidden information and makes information as secret. It classifies three different kinds-

1) Secret key cryptography
2) Public key cryptography
3) Hash function.

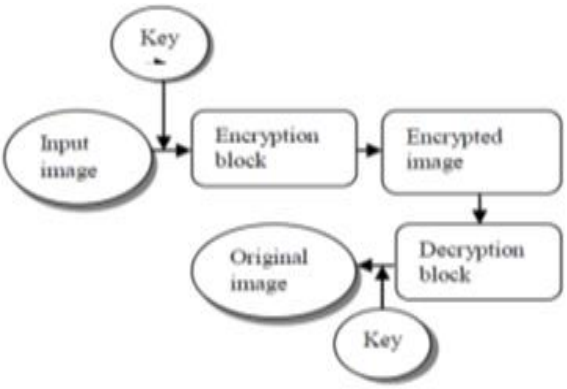

Fig. 2: Block Diagram of Encryption and Decryption

IV. STEGANOGRAPHY

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden exclusively in images.

Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

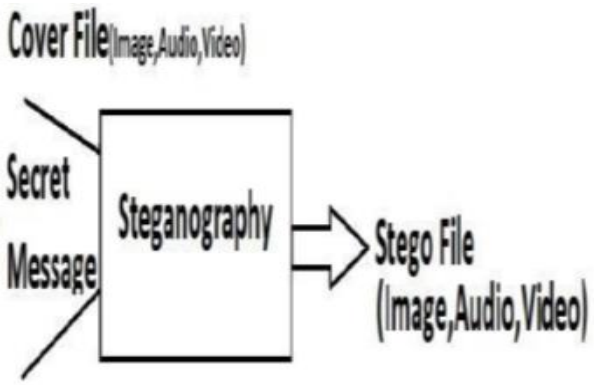

Fig. 3:

Steganography is a method of hiding secret information using cover images. The various steganography techniques are:

1) Substitution technique: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even simple attacks such as compression, transforms, etc.
2) (ii)Transform domain technique: The various transform domains techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) are used to hide information in transform coefficients of the cover images that makes much more robust to attacks such as compression, filtering, etc.
3) Spread spectrum technique: The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information. The SNR in every frequency band is small. Hence without destroying the cover image it is very difficult to remove message completely.
4) Statistical technique: The cover is divided into blocks and the message bits are hidden in each block. The information is encoded by changing various numerical properties of cover image. The cover blocks remain unchanged if message block is zero.
5) Distortion technique: Information is stored by signal distortion. The encoder adds sequence of changes to the cover and the decoder checks for the various differences between the original cover and the distorted cover to recover the secret message.

The main aspect of steganography is to achieve high capacity, security and robustness.

Cover Image: It is defined as the original image into which the required secret message is embedded. It is also termed as innocent image or host image. The secret message should be embedded in such a manner that there are no significant changes in the statistical properties of the cover image. Good cover images range from gray scale image to colored image in uncompressed format.

Stego image: It is the final image obtained after embedded the payload into a given cover image. It should have similar statistical properties to that of the cover image.

Hiding Capacity: The size of information that can be hidden relative to the size of the cover without deteriorating the quality of the cover image.

Robustness: The ability of the embedded data to remain intact if the stego image undergoes transformation due to intelligent stego attacks.

Security: This refers to eavesdropper's inability to detect the hidden information.

Mean Square Error (MSE): It is the measure used to quantify the difference between the initial and the distorted or noisy image.

Image Steganography has many applications, especially in today's modern, high-tech world. Privacy and anonymity is a concern for most people on the internet Image Steganography allows for two parties to communicate secretly and covertly. It allows for some morally-conscious people to safely whistle blow on internal actions; it allows for copyright protection on digital files using the message as a digital watermark. One of the other main uses for Image Steganography is for the transportation of high-level or top-secret documents between international governments. While Image Steganography has many legitimate uses, it can also be quite nefarious. It can be used by hackers to send viruses and trojans to compromise machines, and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely2.

V. METHODOLOGY

A. Module Names:

1) Extraction of the host video object from a videoconference frame ..
2) Encryption of the fingerprint.
3) Detection of the QSWTs to hide the encrypted signal.
4) Hiding of the encrypted signal to the host video object
5) Transmission of the stego object.
6) Extraction of the encrypted signal and Decryption

B. Video Object Extraction:

A video object extraction system for real-time applications requires the following criteria.-

1) Segmented object should conform to human perception i.e., semantically meaningful objects should be segmented.
2) Segmentation algorithm should be efficient and achieve fast speed.
3) Initialization should be simple and easy for users to operate.

In Video Object (VO) segmentation methods, which are using mathematical morphology and perspective motion model, objects of interest should be initially outlined by human observer. From the manually specified object boundary, the correct object boundary is calculated using a morphological segmentation tool. The obtained VOP is then automatically tracked and updated in successive frames.

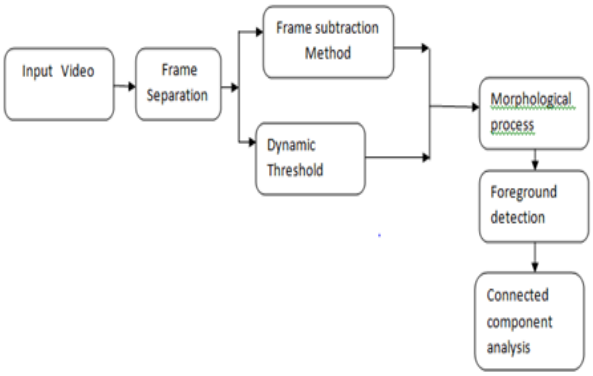

Fig. 4:

C. Encryption of Fingerprint:

Image encryption is necessary for future multimedia Internet applications. Password codes to Identify individual users will likely be replaced are biometric images of fingerprints and retinal scans in the future. However, such information will likely be sent over a network. When such images are sent over a network, an eavesdropper might duplicate or reroute the information. By encrypting these images, a degree of security can be achieved.

Encryption procedure

1) Input the image
2) Assign a valid key
3) Read the volume of image as matrix
4) Generate matrix of arbitrary numbers
5) Round the random values
6) Apply XOR operation of rounded values
7) Shows encrypted image effect

For Example: Below we have the image message "Rose image" embedded in a 128 by128-bit image. For a key, we have collected a 128 by 128 matrix of random bits. We will combine the two matrices using XOR

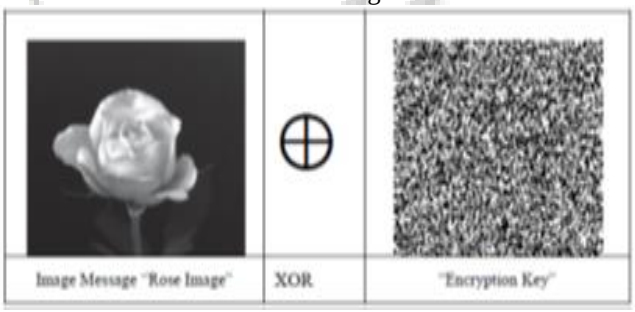

Fig. 5:

When we apply XOR bit-by-bit to the two matrices, we get the following 128 by 128 matrix of encrypted bits.To decrypt the message, we simply take the encrypted message and compute XOR with the encryption key, bit-by-bit. This yields the original image "Rose image" message

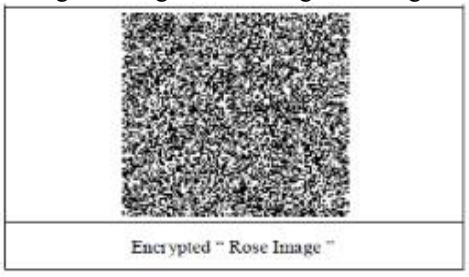

Fig. 6:

Sometimes an image may contain text embedded on to it. Detecting and recognizing these characters can be very important, and removing these is important in the context of removing indirect advertisements, and for aesthetic reasons. Our system aims at the automatic detection of text. This is done by the algorithm. Fig. 1 shows the flow diagram of text detection algorithm.

D. Haar-Dwt:

The frequency domain transform we applied in this research is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:

Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 2. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

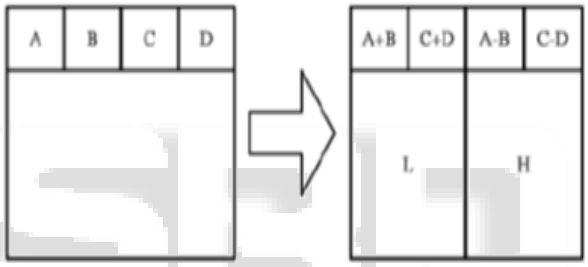

Fig. 7:

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustratedin Figure 3. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image.

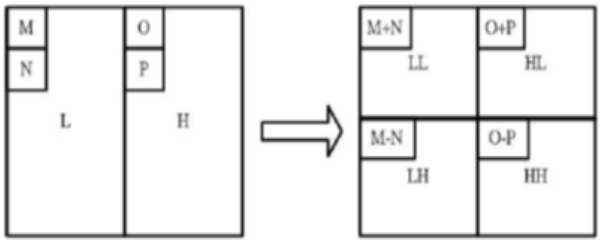

Fig. 8:

E. Formation of Stego Image:

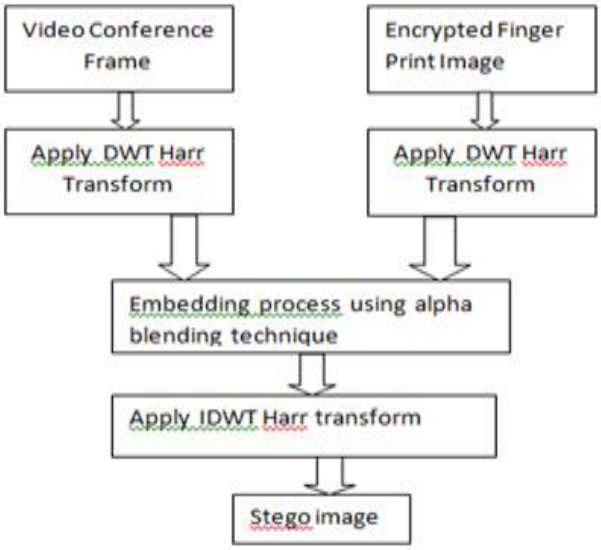

Fig. 9:

Fingerprint Embedding Process consist of decomposing Original image into 1-level sub bands using DWT which generate Four sub-bands (LL, LH, HL, HH) out of which LL (Lowest Level) has selected for Fingerprint embedding as it contains maximum energy. The Fingerprint of 128×128 is embedded into LL, obtained image is called stego Image,

F. Extraction of Stego Image:

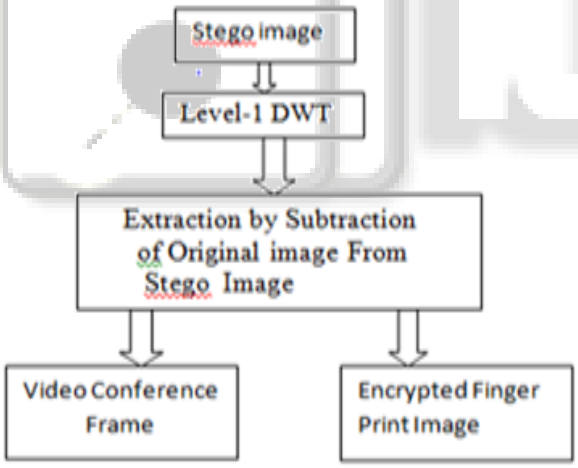

Fig. 10:

Fingerprint extraction is a process of removing fingerprint from stego image, Inverse Discrete Wavelet Transform is used for Extraction of Watermark with Daubechies (db1)filter as shown in Figure (1).The Watermarked image is again decomposed using level 1 IDWT then DWT of image is obtained, DWT image is compared with Original image and fingerprint is extracted from stego image.

VI. Conclusion

We have implemented cryptography and stegnography with biometric authentication for wireless network. The strength of steganography amplified by combining it with cryptography. Image Steganography allowed for two parties to communicate secretly. Preposed method provides hybrid remote authentication, when both a machine and a human remotely authenticate a person

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometricrecognition," IEEE Transactions on Circuits Systems for Video Technology,vol. 14(1), pp. 4–20, 2004.
[2] D. He and D. Wang, "Robust biometrics-based authentication schemefor multi-server environment," IEEE Systems Journal, pp. 1–8, 2014
[3] M. Ramkumar and A. N. Akansu, "Capacity estimates for data hidingin compressed images," IEEE Transactions on Image Processing, vol.10(8), pp. 1252–1263, 2001.
[4] S. Li and W. Li, "Shape-adaptive discrete wavelet transforms forarbitrarily shaped visual object coding," IEEE Transactions on Circuitsand Systems for Video Technology, vol. 10(5), pp. 725–743, Aug. 2000.
[5] N. D. Doulamis, A. D. Doulamis, K. S. Ntalianis, and S. D. Kollias, "Anefficient fully-unsupervised video object segmentation scheme using anadaptive neural network classifier architecture," IEEE Transactions onNeural Networks, vol. 14(3), pp. 616–630, 2003.
[6] A. M. Fard, M. R. Akbarzadeh-T, and F. Varasteh-A, "A new geneticalgorithm approach for secure jpeg steganography," in Proc. of IEEEInt'l Conference on Engineering of Intelligent Systems. IEEE, 2006.

