Secure Remote Authentication Over Wireless Network Using Biometrics and Pattern Recognition Techniques

Manjusha Patil, Poonam Parate, Pruthviraj Chavan, Siddhi Velani

Department of Information Technology

RMD Sinhgad School of Engineering, Warje, Pune-411058

---***---

Abstract - *In any communication system that involves transfer of data over wireless network, there is a need of authenticating the communicating parties remotely. Using only IDs and passwords for authentication is not sufficient as it can be easily obtained by hackers. To make the authentication strong and powerful, use of biometrics becomes necessary. Remote Authentication over wireless networks using biometric data involves the use of two rapidly growing technologies namely biometric systems for authentication and wireless systems for mobility. This system proposes a secure and robust authentication based mechanism based on steganography and Pattern matching. Assuming that user X wants to be authenticated, initially a biometric signal of X will be captured and an image of the user X is clicked which is to be used as cover image for steganography. Steganography is performed and the stego object is sent to the receiver. Reverse steganography is performed on the receiver side and the two images are separated. Pattern Matching is performed on both the images to prove the identity of the user. Applications of this system include remote studying, personnel hiring, remote Examination, Health care, etc.*

***Key Words*: Remote authentication, Biometrics, LSB Steganography, CBIR, Histogram, Euclidean Distance.**

1. INTRODUCTION

Authentication is the process of verification of the true identity of a user who wishes to access a system. The two main ways of authentication are positive and negative authentication. The Positive authentication is popularly used in many of the existing authentication systems. Negative authentication is invented to reduce cyber attacks. The proposed system is a positive authentication system and for the system to be secure, elements from two and preferably all three, of the factors given below should be verified:

- The ownership factor: This ownership factor can by verified by something the user has like a ID card, security token etc.
- The knowledge factor: This factor can be verified by something the user knows like a password, PIN etc.
- The inherence factor: This factor can be verified by something the user inherits like a finger-print, face pattern etc[1].

Remote authentication is a form of authentication in which a user's credentials are submitted over a network as proof of his/her identity. Robust remote human authentication becomes one of the important issues of contemporary societies and several methods are proposed to tackle these methods effectively. Three methods were proposed for remote authentication: - password authentication, use of smart cards and Biometric authentication. In order to investigate the full potentiality of a remote authentication system, biometrics can be integrated in hybrid crypto-steganographic schemes. Cryptographic algorithms can scramble biometric signals so that they cannot be interpreted, while steganographic algorithms can hide the encrypted biometric signals so that they cannot be seen[1].

The third factor for authorization that is given above is the factor that deals with biometric. Biometric authentication is a process of verifying a user's claimed identity by comparing a biometric value with a stored value of the user's biometric characteristic. Common types of biometrics are: Fingerprint / palm-print, hand geometry, iris scan, signature dynamics, retina scan, facial scan, voice recognition, etc[2]. Biometric signals enter more and more into our daily life, since governments and other organizations utilize it in accomplishing pivotal procedures. Thus there is a need to develop and incorporate biometric authentication techniques into practical applications[1].

This paper focuses on the principle to confront the problem of remote human authentication over wireless channels. It ensures security of the user, using his/her fingerprint image and an image of the user clicked by the webcam. The user's image and the fingerprint image will be steganographed and sent over the network for remote authentication. The rest of this paper is organized as follows: Section II focuses on the literature survey. In Section III a high level description of the proposed system is presented along with theoretical justification. Section IV focuses on hiding the face image and the user image using steganography. Section V includes description of the pattern recognition schemes. Section VI includes extended experimental results while Section VII concludes the paper. Section VIII includes the future work to be done for the proposed system.

2. LITERATURE SURVEY

In [1] Klimis Ntalianis and Nicolas Tsapatsoulis presented a robust remote authentication mechanism based on chaotic encryption, semantic segmentation and data hiding. The proposed human authentication scheme works over wireless channels and it provides robustness against deciphering and provides good encryption capacity. The proposed scheme provides security merits for the encryption module and also provides robustness to steganalytic attacks. According to the authors, the limitation of the proposed system is that Chaotic encryption is a new field for research and thus it will require a lot of time for its security mechanism to mature.

In [3] Vijay Kumar Sharma and Vishal Shrivastava have presented a steganographic algorithm for 8bit as well as 24 bit images based on logical operation. The proposed algorithm embeds n Most Significant Bits(MSB) of secret image in to Least Significant Bits(LSB) of cover image. With the help of this algorithm a great balance between security and image quality is obtained. An advantage of this algorithm is that this method is applicable for both grayscale as well as color images

In [4] authors have presented a new data - hiding technique where dark areas of the image are found out to hide the data using the least significant bit(LSB) technique. This method converts the image to binary image and labels each object of image considering 8bit connectivity. These images are then converted to RGB image to find dark places. 8 pixels of the dark places is considered as a byte and binary value of the secret data is inserted in the LSB of the dark places. High computation is required in this method to find the dark places. The hiding capacity of this method depends on the image texture.

In [5] authors have proposed a gray scale weighted average method to decrease the feature vector dimension which in turn will increase the overall performance of the system. The proposed approach gives better throughput than the color weighted average method. Benefit of using gray scale image that constitutes of intensity values is that it simplifies amount of information to be stored than three dimensional color images(true color images). The use of gray scale intensity values requires less space in memory.

In [6] Rishav Chakravarti and Xiannong Meng have described a novel approach that implements and tests search and retrieve algorithm based on simple color histogram for images. The algorithm proposed is easy to implement from a coding point of view.

In [7] Swapnalini Pattanaik and Prof.D.G. Bhalke have presented a paper that gives an overview of retrieving images from a large database. The system has used color histogram, color structure descriptor, color mean and texture for extraction of features. Euclidean distance is used for feature matching procedure.

3. PROPOSED METHODOLOGY

The proposed system is designed for Authentication of the user from a remote location using biometrics. It requires a database which stores the biometric signal as well as the image of the user. All this information is collected during registration of the user and stored it in the database. The architecture of the system is given in Figure 1.

All the components of the system are explained below in brief:-

- Input Biometric Signal:-This module shows the partial input taken from the user, that is, the biometric signal. The biometric signal considered for the proposed system is fingerprint. Fingerprints are very secure and cannot be easily forged, therefore their use makes the system more secure and safe.

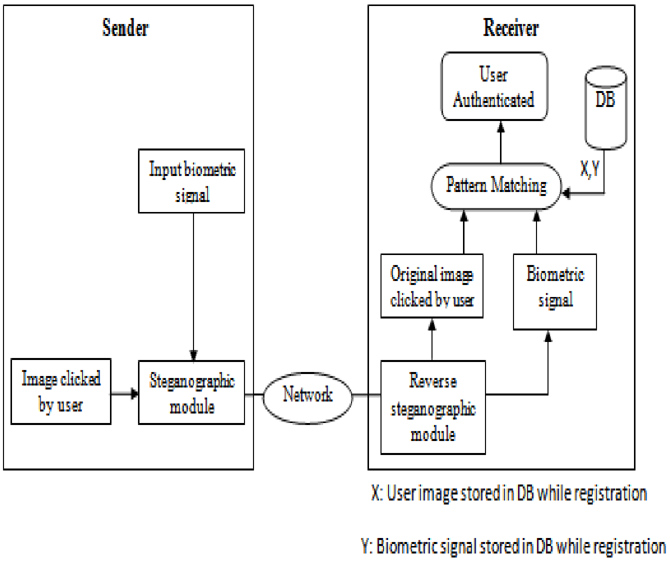
Sender
Input biometric signal
Image clicked by user
Steganographic module
Network
Receiver
User Authenticated
DB
X,Y
Pattern Matching
Original image clicked by user
Biometric signal
Reverse steganographic module
X: User image stored in DB while registration
Y: Biometric signal stored in DB while registration

Figure -1: Proposed System Architecture

- Image clicked by the user:- This module shows the second input taken from the user, which is an image of the user clicked through the webcam. This image along with the fingerprint biometric is combined using a steganography technique.
- Steganographic Module:-Steganography is the hiding of a secret message within an ordinary message and the extraction of it at its destination. In this module the system hides the fingerprint biometric signal and the image clicked by the user. The technique that will be used here is Least Significant Bit (LSB) Steganography.
- Reverse Steganographic Module:- In this module the technique of reverse steganography is performed. After

performing reverse steganography, the original image clicked by the user and the fingerprint biometric signal are separated.

- Pattern Matching: - In this module, matching of the face image clicked by the user and the image stored in the database is done using CBIR(Content Based Image Retrieval). The biometric signal is matched with the one stored in the database using fingerprint matching device.
- User authenticated:-The pattern matching module gives the result of matching. If both the images in the pattern matching module are matched with that of those in the database then the user has been authenticated.

4. HIDING THE FACE IMAGE AND THE FINGERPRINT IMAGE USING STEGANOGRAPHY

The proposed system uses the technique of LSB Steganography for hiding the face image and the fingerprint image. The word steganography is the art of covered writing. In image steganography the information is hidden in images. Steganography is the process of writing hidden messages in such a way that no one except the sender and intended receiver, knows about the existence of the message[3].

In image steganography the proposed system hides an image in another image. LSB stands for Least Significant Bit. LSB embedding is a simple strategy to implement steganography. Like all other steganographic algorithms, LSB steganography hides the data into the cover image so that it cannot be detected by an observer. LSB technique works by replacing the LSB of the cover image with that of the secret image. Even though it is possible to embed data into an image in any number of bits, LSB embedding is performed on least significant bits. This reduces the variation in colors that the embedding creates. Steganography avoids showing as much variation as possible, to minimize the likelihood of detection.

LSB algorithms have a choice about how the data to be hidden is embedded. They can embed losslessly, keeping all information about the data intact, or the data may be generalized so that it requires less space.

The LSB steganography algorithm is used because it is easy to understand and also because of its high perceptual transparency.

The advantages of LSB steganography are:

- Easy to understand.
- High perceptual transparency.
- Low degradation in the image quality.

The disadvantages of LSB steganography are:

- Low robustness to malicious attacks.
- Vulnerable to accidental or environmental noise.
- The size of information to be hidden depends on the size of the cover- image[8].

The block diagram for LSB steganography is drawn below:

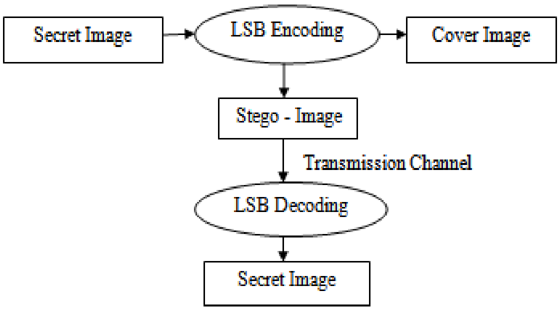

Figure -2: Block Diagram for LSB Steganography

5. PATTERN MATCHING SCHEMES

The proposed system uses CBIR(Content Based Image Retrieval) technique for matching of the face image. "Content-based" means that the contents of the image like colors, textures or shapes are analyzed and not the metadata such as tags, keywords or descriptions of the image. The CBIR consists of two steps namely feature extraction and similarity matching[7].

The CBIR approach in the proposed system firstly takes an image stored in the database during registration and converts it into a grayscale image. Then histogram equalization is done on this grayscale image to increase the contrast of the image[7]. Next step is to rescale the image into 300x300 pixels. The features will be 25 RGB regions in the image. For each of the 25 signature values, average the pixels around a central point and return the average as an instance of color. All the above steps are then repeated for the later image which is to be authenticated.

The Euclidean distance between the signatures of the two images is calculated[7]. The difference is calculated by, Difference = | distance of registered image - distance of image for authentication | . If the difference is less than the threshold value (1100 in this case), the two images are said to be matched.

The advantages of CBIR technique for face matching are:

- Automatic extraction of visual features
- Due to the use of gray scale images less memory is required to store pixel information[5].
- Easy to implement from coding point of view[6].
-

The disadvantages of CBIR technique for face matching are:

- The approach shows poor performance under different light conditions.
- Calculating the histogram is mathematically complex.

- The color analysis does not always relate to similarity of colors as recognized by the human eye[6].

6. EXPERIMENTAL RESULTS

In order to test the proposed system a database of 20 candidates(male and female) was used.

Table -1: Results for the given system

Number of users tested	Number of recognized users	Number of unrecognized users	Success Rate
20	17	3	85%

Success rate = (No. of users correctly recognized÷ Total No. of users in dataset) × 100

The success rate is calculated on the basis of the number of face images and fingerprint images that are matched. The proposed system could not match the face images under poor light conditions, use of sunglasses, presence of beard on the face of male candidates and other such factors. The fingerprint images were not matched in presence of scars, burns and other casualties to the finger. Overall, the system gave favorable performance and matched the users successfully with a success rate of 85%.

7. CONCLUSION

Biometric signals play an important role in our everyday lives, since governments as well as organizations resort to their use in major procedures such as citizen authentication. Thus there is an urgent need to integrate biometric authentication into our practical applications. This paper describes a novel approach that uses LSB Steganography and CBIR for face matching for remotely authenticating a user. The proposed system provides 85% accuracy when tested for a dataset of 20 users. According to the tests performed the system provides better efficiency under similar light conditions.

The application of the proposed system could be a smart interview system wherein a candidate can give an interview from a remote location using his face image and finger biometric.

8. FUTURE WORK

In future research, the effects of transmission of other hidden biometric signals (e.g., Palm print, voice or iris) can be examined. Also the effects of compression of the biometric signals should be studied. Another very important aspect for further research includes the study of the attacks on the wireless networks. Also video object extraction techniques should be studied and implemented.

REFERENCES

[1] 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, January 2015.

[2] Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and SalilPrabhakar, Member, IEEE, " Introduction to Biometric Recognition", IEEE transactions on circuits and systems for video technology, Vol. 14, No. 1, January 2004.

[3] Vijay Kumar Sharma,M.Tech. scholar, Arya college of Engineering & IT ,Jaipur , Rajasthan (India) and Vishal Shrivastava , Associate Professor Arya college of Engineering & IT, Jaipur, Rajasthan (India),Journal of Theoretical and Applied Information Technology," A Steganography Algorithm For Hiding Image In Image By Improved LSB Substitution By Minimize Detection", Vol. 36, No.1, 15th February 2012.

[4] H. Motameni, M. Norouzi, M. Jahandar, and A. Hatami,"Labeling Method in Steganography ", International Journal of Computer, Electrical, Automation, Control and Information Engineering, Vol:1, No:6, 2007.

[5] Kamlesh Kumar, Zain-ul-abidin, Jian-Ping Li and Riaz Ahmed Shaikh,"Content Based Image Retrieval Using Gray Scale Weighted Average Method", (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 7, No. 1, 2016.

[6] Rishav Chakravarti and Xiannong Meng, "A Study of Color Histogram Based Image Retrieval", 2009 Sixth International Conference on Information Technology: New Generations.

[7] Swapnalini Pattanaik and Prof.D.G.Bhakle," Beginners to Content Based Image Retrieval", International Journal of Scientific Research Engineering & Technology (IJSRET) Volume 1 Issue 2 pp 040-044 May 2012.

[8] Sneha Bansod and Gunjan Bhure, "Data Encryption by Image Steganography", International Journal of Information and Computation Technology, ISSN 0974-2239, Volume 4, Number 5, 2014.