ISSN: 2456-9348
Vol (02) _Issue (04) Impact Factor: 4.520

iJETRM

International Journal of Engineering Technology Research & Management

REMOTE AUTHENTICATION USING FACE RECOGNITION WITH STEGANOGRAPHY

Nishant Kaushik[1],
Dr. Parveen Sultana H [2]
[1,2]Vellore Institute of Technology, Vellore
[1]nishant1796@gmail.com
[2]hparveensultana@vit.ac.in

ABSTRACT

In today's world securing data from the hackers and other unauthorized attackers is a critical task. Almost all the system has some kind of authentication which allows the user to access their data. Most of these system are limited to one layer of security like textual passwords. The authentication using textual password is famous as it is straightforward. But the simplicity comes at the cost of vulnerability. These authentication methods are prone to spyware and dictionary attacks. As the systems are becoming more powerful than ever, it is easy to launch a dictionary attack. Another form of attack is to monitor the request and response between the client and server. It is possible when the attacker has gained physical access to the communication medium. Intruder just has to analyze the packets to figure out the delicate information such as password. There are many networks that cannot afford any kind of breach. Steganography, the art of hiding the existence of message by embedding the secret message into another medium, can be exploited in authentication system. Steganography has emerged as technology with various application which introduced steganalysis, the process to detect the hidden information. The user has to undergo face recognition as well as textual authentication. Since any of the request and response between server and client will not have password in plain text form, it is not possible to breach the password. The system is combination of face recognition and steganography.

Keywords:
Remote Authentication, Steganography, Cryptography

INTRODUCTION

The digital world is evolving rapidly. This means that people are finding new ways to doing old task efficiently and creatively. Although it seems boon but we should not forget that people won't stop using technology to their own advantage. This makes the world more vulnerable as it grows. The authentication systems are the ones which require immediate attention.

Authentication has three major factors namely knowledge, ownership and inherence. The knowledge is the usual password or PIN that needs to be entered by user. The ownership includes anything that user possesses like ATM card, Mobile or software OTP. These two are quite vulnerable as they are accessible to hackers/attackers. The inherence factors includes the personal traits of an individual. These could be fingerprint, retina pattern, etc.

Nowadays the applications tends to use two or more of the factors for authenticating users. E.g. Gmail offers two step authentication and gives alert every time user logs in with a new device.

Another new kind of authentication coming into picture is the biometric authentication. This kind of authentication uses the third factor i.e. inherence. During the enrollment time, the user is supposed to register using their unique biometrical characteristic like fingerprint, face, etc. Hence, every time user tries to login they are expected to present these characteristics. The base principle behind this type of authentication is the digitalization of analog data.

Steganography (Greek word *steganos* meaning "covered" and *graphie* or "writing") is used to hide messages into more complex type of information such as images, audio or videos. These are called mediums. Steganography takes advantage of the fact that the minor changes in the medium cannot be noticed by humans.

Terms related to steganography:

- Secret data: The data that needs to send covertly from one place to another.
- Cover Medium: It refers to the medium which is used to cover the secret data.
- Stego Object: It refers to the cover medium once the secret has been successfully embedded.

- Stego Key: This key defines how the data is embedded into the cover medium. This is used at both the embedding and retrieving process.
- Imperceptibility: It defines the quality of stego object. The imperceptibility is nothing but the undetectable nature of the cover medium once the secret data is embedded.
- Capacity: It the amount of data that can be embedded into the cover medium and stego object remains undetectable at the same time.

A steganographic system is comprised of two algorithms, the first is for hiding and the second is for retrieving. The hiding process is concerned with embedding data within the cover medium. Therefore, this process should be constructed carefully to be sure the stego object is identical to the cover medium as possible which makes sure that the existence of message is undetectable. Therefore, basically the components of the embedding process system consists of a secret message and a cover medium as inputs, a steganography algorithm as the method of hiding and a resulting stego object as the output. Also a secret key can be used for hiding the data as a third input to increase the robustness and security of the hidden data, such that there is no way the data is retrieved in the absence of the secret key even though the algorithm of hiding is known.

Literature Survey

Table 1: Problems noticed with other authentication systems

Method	**Gaps observed**
Triple password to prevent replay password attack	The users has to login three times just to use the service once. It is difficult to remember three passwords
Smart card based authentication	Fingerprint-Based Remote User Authentication Scheme Using Smart Cards it requires additional resources like smart cards which adds to the cost of the system, not to mention the issues created when the user may lose the cards.
Using key with random number	Generating random numbers helps to stop the users from accessing application services, but it does not help much in preventing password attack
Authentication based on dynamic password	At a time only one mobile application can be registered per user. Subject to the signal, power and security issues of the mobile. This creates a secondary dependency.

METHODOLOGY

The methodology adopted in this paper is an intensive literature review on the various methods for the authentication. The authentication system proposed uses modified LSB algorithm in conjunction with face recognition.
The system is developed using Java 8 as backend language, AngularJS as front-end and tomcat server is used. The following diagram gives a brief idea about the proposed system.

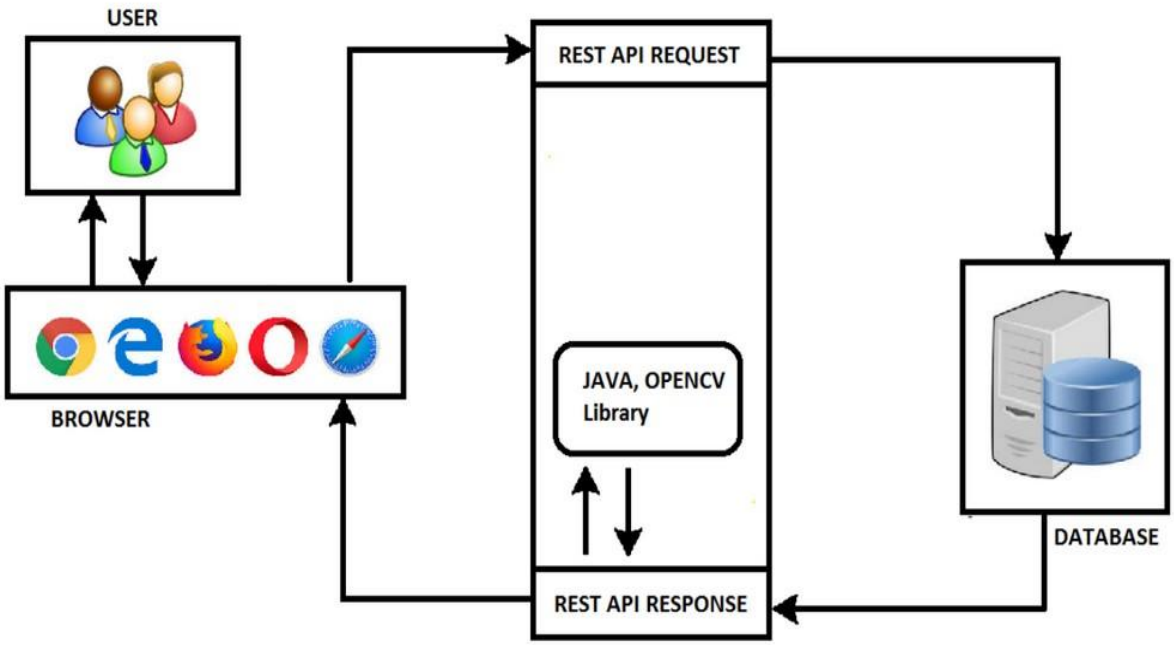

Fig. 1: Architecture of proposed system

It makes use of the unchanged bits of each pixel to identify how the secret data should be embedded into that bit. We make use of the last three bit to store the data. The other bits which are not used will be classified as indicator bit and size bit.
The indicator bit will identify whether we are supposed to use that particular bit or not. And size bit will be used to check which of these three is being used to embed secret data into the pixel byte.
Moreover we use a secret key. The data will be entered using two positions called front and back. The secret key is used to XOR with the current pixels indicator bit. If the value is 0 we insert value at back and increment front and back. Otherwise we embed value at front and increment front. This makes the system more robust as it introduces randomness into the embedded bits position.

We know that the human eye is more reactive to green and red as compared to blue. Also since we only need to store the credentials we don't require large capacity in the cover medium. Hence we only use blue color byte array to store the secret data. The better quality of the image compared to the original image keeps the high PSNR value.

Efficiency

The application uses many processes which may affect the efficiency. The modified LSB algorithm will not be cost expensive as it requires fixed amount of space and time due the fixed number of pixels in the image. The face recognition also depends upon the number of pixels linearly in the images as Haar image features in constant time. Hence, the quality of image is changed overtime then complexity will be affected. Thus we can say time and space complexity is O(n), n being the number of pixels in the image.

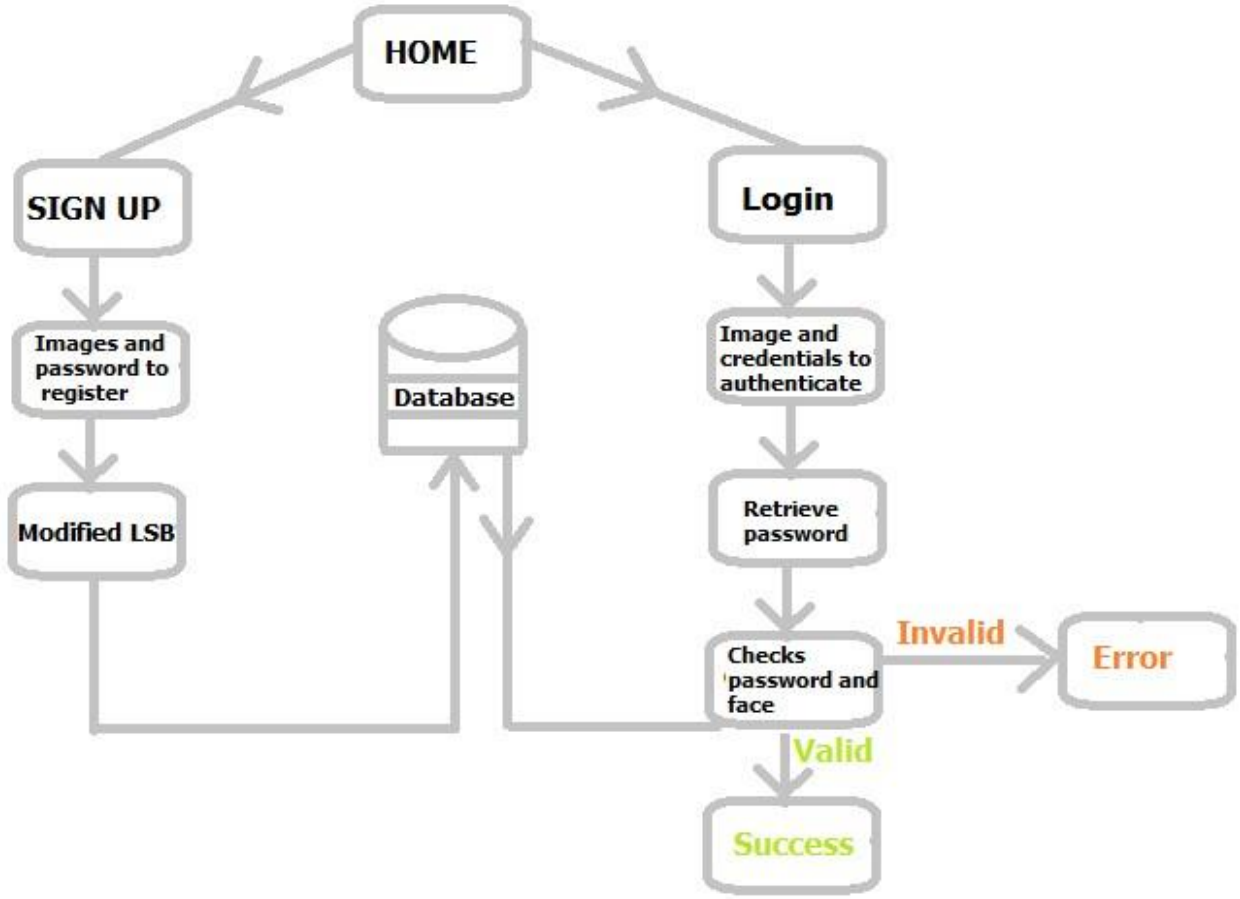

Fig. 2: Working of authentication system

Testing

The proposed system is tested under various cases to insure the correctness of the system. The following table summarizes the results. The system is able to pass most of the test cases.

.

Table 2: Test cases and results.

Test ID	Test case description	Expected Result	Obtained Result	Pass/Fail
1	Valid credentials with valid face image.	Should Authenticate correctly	Authenticated correctly	Pass
2	Invalid credentials with valid face image.	Should not Authenticate correctly	Not Authenticated	Pass
3	Valid credentials with invalid face image.	Should not Authenticate correctly	Not Authenticated	Pass
4	Valid credentials with blurred image of face.	Should Authenticate correctly	Not Authenticated	Fail

5	Valid credentials without face image	Should not Authenticate correctly	Not Authenticated	Pass
6	Valid credentials and low light image of face	Should Authenticate correctly	Authenticated correctly	Pass

CONCLUSION

The remote authentication process is the one which requires security and reliability. As discussed, many methods has been used to make the process secure. The product designed and developed here has met most of the requirements. It is not expensive to build or maintain, and doesn't require additional materials support to work. The modified LSB method has made the login and registration process much more robust and invulnerable to intruders. The GUI designed is user friendly so it's simple to understand for anyone. I will continue to work on this product and try to make the steganography process more efficient and robust.

This project is an open source project uploaded on GitHub (Front-end: https://github.com/n1sh/FaceSteg, Back-end: https://github.com/n1sh/FaceStegBackend), which makes it available for anyone to change, modify and improve. This application can be improved by using better face recognition techniques, improving the LSB algorithms by modifying it. Also people can add new modules to it to make it more applicable. As we know the security is very much in demand so it would behoove if improve the security in the authentication. Other than LSB, there are many algorithms and techniques to embedded data into the image.

.

ACKNOWLEDGEMENT

I take this opportunity to express my heartfelt gratitude to my guide Dr. Parveen Sultana, Assistant Professor, School of Computer Science and Engineering (SCOPE, VIT), whose able guidance helped me in the development of the proposed system for my problem statement. I would also like to extend my sincere gratitude towards VIT University for assistance in carrying out the research.

REFERENCES

[1] Vishnu S babu and Prof. Helen K J. "*A Study on Combined Cryptography and Steganography:*" International Journal of Research and Studies in Computer Science and Engineering Volume 2, Issue 5, May 2015, PP 45 - 49 ISSN 2349 - 4840 (Print) & ISSN 2349 - 4859(online).

[2] 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.

[3] Sutaone, M.S., Khandare, M.V, "I*mage based steganography using LSB insertion technique*", IEEE WMMN, pp. 146-151, January 2008.

[4] Dushyant Goyal and Shiuh - Jeng Wang, "Steganographic Authentications in conjunction with Face and Voice Recognition for Mobile Systems".

[5] Jasleen Kour , Deepankar Verma , " *Steganography Techniques – A Review Paper*" International Journal of merging Research in Management &Technology ISSN: 2278 - 9359 (Volume - 3, Issue - 5) May 2014.

[6] Sumeet Kaur, Savina Bansal, and R. K. Bansal., "*Steganography and Classification of Image Steganography Techniques*". International Conference on Computing for Sustainable Global Development.

[7] Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb "*A secure covert communication model based on video steganography* " 11331. 978 - 1 - 4244 - 2677 - 5 IEEE 2008.