Remote Authentication using Face Recognition with Steganography

Nishant Kaushik, Parveen Sultana H, Senthil Jayavel

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 applicationwhich 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

I. 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.

Revised Version Manuscript Received on 25 November 2018.

Nishant Kaushik, VIT University, Vellore Tamil Nadu, India.
Parveen Sultana H, VIT University, Vellore Tamil Nadu, India.
Senthil Jayavel, Kumaraguru College of Technology, Tamil Nadu, India

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 stegnographic 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.

II. LITERATURE SURVEY

Theremote authentication can be improved by not passing the information directly. The steganography is being used a lot for that. The steganography is been in the digital world for a long time.

Over the years it has been used significantly to transfer secret data in digital communication channels covertly. Since the data should not be exposed to unauthorized users, it is utmost priority that the very existence of the data The data that needs to be hidden is embedded into another medium like images, text, audio and video, etc. The resource in which the data is hidden is known as cover medium, and the resulting object is called the stego medium (for instance if we use image the object is called stego image). The process of trying to find the hidden information in a cover medium is known as steganalysis. Many steganography algorithms have been developed trying to make it difficult to breach using steganalysis techniques.

Just like steganography is trying to hide the existence of secret message, cryptography is concerned with protecting the data by ciphering it. Hence, steganography and cryptography mostly goes hand in hand. So the encrypted data does not make sense to anyone but the meant parties after they decrypt it (Dunbar, 2002; Eloff, & Olivier, 2005). Encrypted data could be vulnerable because intruders are aware of its existence (Jain &Boaddh, 2016). And since attackers have the chance attack the data, then it is possible to break down the security system (Al-Mohammad, 2010). Thus hiding the communication is important than trying to protect it.

Karim, Rahman and Hossain (2011) proposed a solution of inserting data bits into the cover image randomly. To decide the places of hiding, in addition to the secret key they utilized the red channel of the cover picture. They found out the value of XOR of red bit with current bit if the value is 0, then the secret bit is embedded over the LSB of the blue color of that pixel. Otherwise it is embedded into the green pixel. In this way, it difficult to retrieve the secret data using steganalysis without the secret key. The algorithm is robust but it enters the data into the pixels sequentially from starting to end. Another problem is the capacity of the data that can be entered is not efficient as it uses 24 bytes for each byte of data. In 2013 Rivest Cipher 4 Algorithm was proposed by Akhtar, Johri and Khan. They used stego-key to randomly embed the secret data all over the image. They also used bit inversion technique to improve the quality of the image

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.

III. METHODOLOGY

This paper is refinement of the previous paper published by me i.e. “Remote authentication using face recognition with Steganography”. In this paper a modified LSB algorithm is suggested which will increase the PSNR value of the stego-image after embedding the secret message.
The modified algorithm makes the use of pseudo random number generator to find the random pixels.

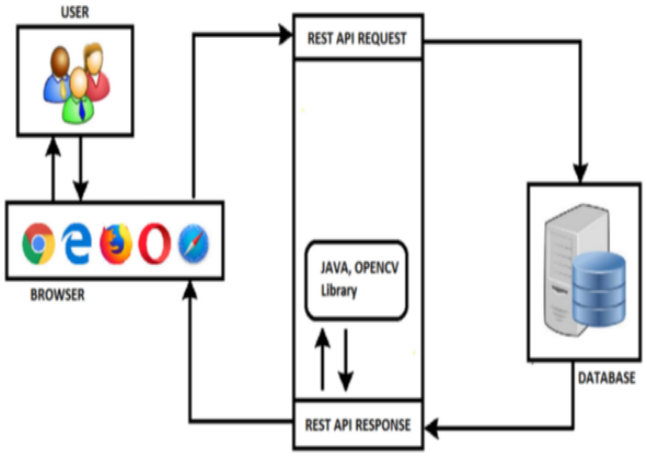


Fig. 1: Architecture of Proposed System

Encryption First we concatenate the username and password using a delimiter.

In the previous paper we used the LSB technique in which we made use of the unchanged bits of each pixel to identify how the secret data should be embedded into that bit. We used the last three bit to store the data. The other bits which are not used were 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 was be used to check which of these three is being used to embed secret data into the pixel byte.

We follow the same algorithm but instead of using secret key to find whether we push the bits front or back, we make the use of pseudo random generator to find the pixel locations. This introduces much more randomness as compared to the previous technique which only inserts the modified pixel either front or back.

Pseudo random number generator is not entirely random because they make use of the mathematical formulas to compute the number. In general, to anyone who tries to find a pattern it will appear random but since it is generated using equations after a certain period it will repeat the order of output numbers. As we only use the pseudo random number generator (PRNG) to hide the username and password,

which won't be very long usually so we can safely make use of the PRNG.

The 16 bit secret key is used to generate random numbers using LFSR algorithm. Based on the algorithm we find the order of location of the pixels in which we hide the secret message. Since we are using 320 * 240 face images we need the random number between (and including) 0 and 76,799.

For example, random number generated based on 16 bit key [0 1 0 0 1 1 0 0 1 1 1 1 0 1 0 1]

1014 31073 25170 63879 2346

56369 18055 68702 24921 6941

50939 36243 20270 60350 10641

11189 26655 2212 61172 29400.... And so on

Now we use these numbers to find the pixel value.

Decryption

While decrypting we use the same 16 bit key [0 1 0 0 1 1 0 0 1 1 1 1 0 1 0 1] to find the pixel positions and follow the decrypting steps as follows.

1. Find the next random number using the secret key.
2. Find using the indicator bit of the pixel whether a secret message bit is hidden in the pixel or not.
3. If not, go to step 1.
4. If yes, find using the size bit of the pixel to get the number of secret pixel hidden.
5. Concatenate the secret bits in the secret message extracted.
6. Convert the binary string to the ASCII values and then ASCII value to the original message.

We used a delimiter to separate the username and password. Note that delimiter should not be allowed in username, so that we can find the first occurrence of the delimiter to separate the username and password.

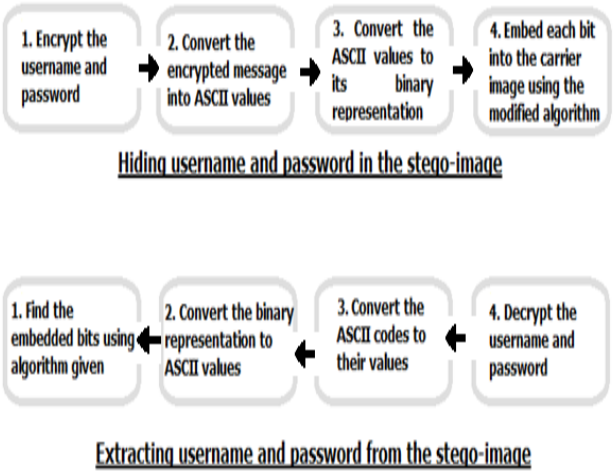
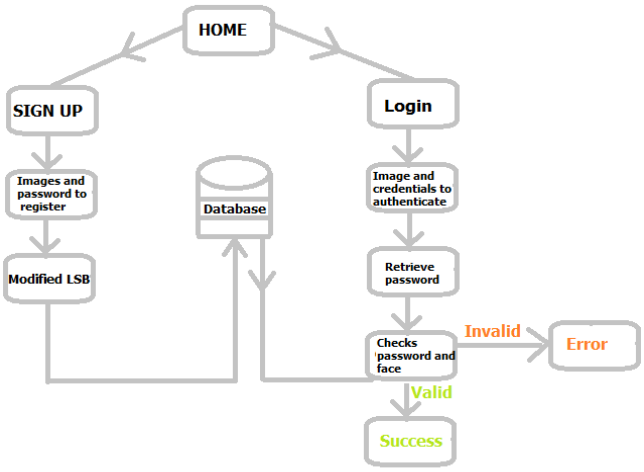


Fig. 2: The Flow of Data in the Process

As 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.

IV. 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.



V. 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

VI. 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 LSB algorithm is modified using PRNG which makes the application more robust. 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.

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. SnehaBansod and GunjanBhure, "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, "Image based steganography using LSB insertion technique", IEEE WMMN, pp. 146-151, January 2008.
4. DushyantGoyal and Shiuh - Jeng Wang, "Steganographic Authentications in conjunction with Face and Voice Recognition for Mobile Systems".
5. JasleenKour ,DeepankarVerma , " Steganography Techniques – A Review Paper" International Journal of merging Research in Management &Technology ISSN: 2278 - 9359 (Volume - 3, Issue - 5) May 2014.
6. SumeetKaur, SavinaBansal, 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.
8. NishantKaushik and Dr. Parveen Sultana. "Remote Authentication Using Face Recognition with Steganography". Vol (02) _Issue (04) April 2018.