Available online at www.ijiere.com

International Journal of Innovative and Emerging Research in Engineering

e-ISSN: 2394 - 3343 p-ISSN: 2394 - 5494

Digital Image Sharing with Security

Swati D. Gaikwad 1[a], Dr. Anil S.Hiwale 2[a]
[a]M.E (appeared) 1, Pune, India
[b]Ph.D (E&TC) 2, Pune, India

ABSTRACT:
The internet is ruling over the world in 21st century. The data can be shared within a fraction of second. As it makes our life simpler so also there are chances of occurring some problems. These are lot many ways to hide the confidential data such as cryptography, visual secret sharing schemes, addition of noise images, steganography etc. But, then also, there are chances of leaking data. Failure of the essential security. Hence, highly confidential data needs a security and a proper feedback. So that one can assume that the data is which is send is secured. This can be done in such a manner that the data which is to be send is hidden by using cryptography as well as steganography and send to the receiver side. During this process a fifty percent of security is maintained. The remaining security can be achieved due to authentication. In this paper the face recognition is used for authentication purpose. This technique will result out the real or fake receiver. According to that, system will provide the response. If the receiver is authenticated then the sender will get the autoreply as the data is delivered successfully. In case if the receiver is unauthenticated then the data will be in a stand-by mode and also will inform to sender through a feedback message.

Keywords: Image sharing, visual cryptography, steganography, security, face authentication and recognition.

I. INTRODUCTION

The era of digital communication has become very fast. The information can be transferred within no time. As these are some benefits of digital communication there are some demerits also. We the human, cannot ignore such drawbacks. The life has totally encircled with the communication. Also the confidential data are used to transfer over the internet which provides a scope for the malicious user who are intended to receive the secret data. There are also some techniques to hide the data. Such as cryptography, steganography, visual cryptography and watermarking.

A. Background

There are lot of technologies come into existence which provide security and keep the data confidential. But there are such intruders who attack despite of preventive measures. In cryptography, the plaintext or original data to be secured is transferred (or encrypted) it into a cipher text (which is in an unreadable format) this process is done on the basis of a secret key. A person who has the cipher text as well as the same secret key which was used before, can only decipher (or decrypt) the original data i.e the plaintext. But the cipher text may achieve the attention of the intruders. In the steganography technique the file, image or message is embedded with another file, image or message. It also provide some level of security but not highly secured. Hence, these both cryptography and steganography have low level of security so in combination they are used together to provide high level of security. In order to protect the secret data from the intruders.

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

In visual cryptography technique, the secret image or secret data is converted into (k,n) visual cryptography scheme where the n is the number of total shares and k is the minimum number of shares which are required to retrieve the secret image. It can be written in the form as $(2 \leq k \leq n)$.in the visual secret sharing scheme secret image is converted into the number of shares which can be expressed as (n, n) it means that there are total n number of shares and to recover the secret image n number of shares are required. Here even if (n-1) shares will be unable to recover the image. The image is first of all encrypted by the visual cryptography using the natural visual secret sharing scheme (NVSS) then we cover the secret image using any printed image or any content such as photographs, portraits, landscape, hand-printed, scenery and flysheets.[4]

With the help of this visual cryptography, the secret data can be hidden but then also the authentication is required. There are lot many authentications available but biometric technology is used to authenticate the identity of person which uses physiological and behavioral characteristics.

B. Motivation

The secret image shared with the visual cryptography and visual secret sharing scheme. The secret data should be protected under any circumstances and the secret information should be put on in the secure hands. So for which the authentication is necessary[6].

C. Objective

This papers main objective of the project is to send the message in the form of the image, which is hidden in the another image. The original image is converted into the n number of shares where the original secret image can be retrieved back only if the person possess with the n number of shares. The image in which the secret image is embedded is called as the cover image. Here the cover image can be any printed image, flysheet, scenery etc. this all process covers the visual secret sharing scheme and the visual cryptography. Then the secret image is present to the receiver with the cover image and now he needs to be retrieved it . the secret image is received via electronic mail and for that the person requires username and the password which will prove his basic authentication. Later after signing into the mail inbox he will have to prove his second authentication i.e face recognition, if he proves himself to be authenticated then he will have the secret image in front of his eye. But in case, if he fails to prove his identity then at that moment the source image will be deleted. On the contrary the sender will have a feedback message by means of a graphical user interface (GUI).

II. Literature Survey

There are several methods and devices used to guide visually impaired persons. Several research works are being performed by many institutions throughout the world to offer the best navigational robot in terms of cost effectiveness. This section gives a brief review on various navigational aids for blind individuals.

From many years security has been a major issue. For personal identification the biometric technology plays a very important role. A biometric system operates by capturing and storing the biometric information and then comparing the scanned biometric with what is stored in the repository There are very different applications where personal identification is required such as in banking sector, in computer, at airports, electronic mail, mobile phones etc. It is very hectic to remember the different codes and passwords for different application. The biometric receives much more attention in today’s busy life. There are lot many biometric techniques such as iris, fingerprint, palm print, ear, hand vein, eye vein, key stroke, voice, hand geometry, signature, face, retina. Among these all techniques face authentication is one of the best techniques which proves more reliable, uniqueness, noninvasive and stable.

The iris has many features that can be used to separate one iris from another. One of the primary visible feature is the trabecular meshwork, a tissue which provide the appearance of dividing the iris in a radial fashion. This feature is permanently formed by the eighth month of gestation. During the development of the iris, there is no genetic influence on it, a process known as “chaotic morphogenesis” that occurs during the seventh month of gestation, which means that even identical twins have differing irises. The iris is protected because of eyelid, cornea. There isnot any effect of age on the iris which means it remains in a stable form an individuals’ birth to the death.

Palm vein is used with the palm prints to increase the robustness. When the veins are imaged they possess the deoxidized hemoglobin in the veins which absorbs the 760nm wavelength of light. Hence when the palm is illuminated by the means of infra red light, due to the deoxidized hemoglobin the dark pattern is observed in the palm print.

For fingerprint eighteen different type of local ridge has been observed. Ridge ending and ridge bifurcation which are called as minutia are the two main types. From the input finger print image the minutia is detected and the minutia pattern which matches the to minutia pattern results the identity of the fingerprint. In the face authentication the skin colour pixel play a very important role and which provides the decimal value for the pixel in the range of 120 to 140.

The face recognition are based on the location and the shape of the facials parts such as chin, nose, lips, eyebrows, eyes and their facial relationship. Weighted combination of the canonical faces is the overall identification of the face. Also the face is changeable on the basis of the expression.

In the hand vein authentication process, the individuals have the different shape and the vascular pattern at the back of the hand which is different from person to person. Also along with that temperature, humidity and state of the skin which directly effects on the vein image. when the individual grows the shape of the dorsal hand remains unchanged, which is also a noninvasive technique

III.Proposed Work

System consists of the two main parts sender side and the receiver side. But for both of them the initial process is the same.

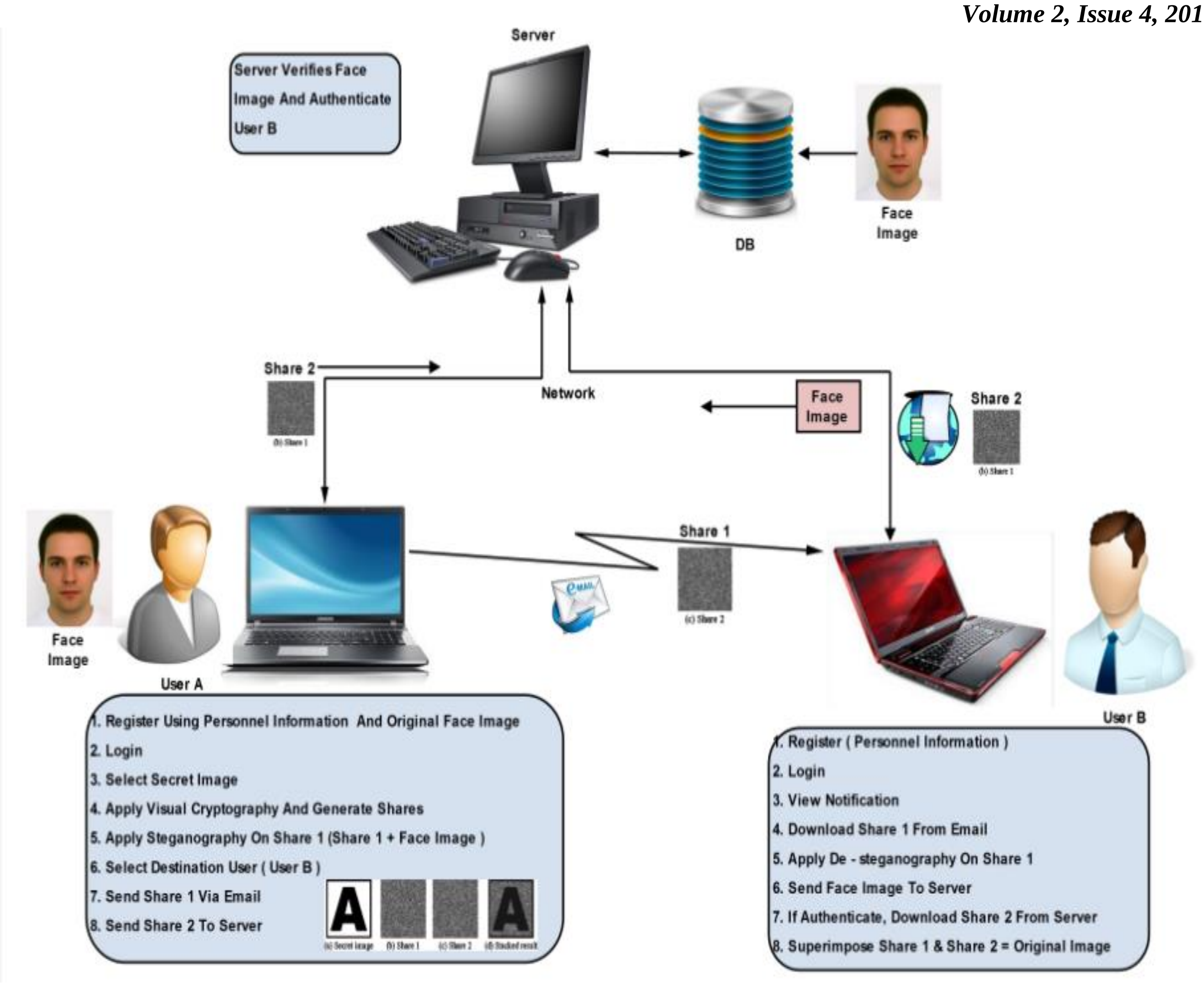
Server
Server Verifies Face Image And Authenticate User B
DB
Face Image
Share 2
Network
Face Image
Share 2
Share 1
Face Image
User A
User B
1. Register Using Personnel Information And Original Face Image
2. Login
3. Select Secret Image
4. Apply Visual Cryptography And Generate Shares
5. Apply Steganography On Share 1 (Share 1 + Face Image)
6. Select Destination User (User B)
7. Send Share 1 Via Email
8. Send Share 2 To Server
1. Register (Personnel Information)
2. Login
3. View Notification
4. Download Share 1 From Email
5. Apply De - steganography On Share 1
6. Send Face Image To Server
7. If Authenticate, Download Share 2 From Server
8. Superimpose Share 1 & Share 2 = Original Image

Figure 1: Sharing data.

A. REGISTRATION

In this paper the process of registration is similar to that of creating graphical user interface by creating the login identification and the password. As well as the images of the original face has to be stored in the database which is at the server side. So that now it can be considered that the stored image is of the authorized person and images other than that will be considered as unauthorized.

B. LOGIN

By entering login identification and password one can login. In this paper the graphical user interface be created separately so that it can linked with the server for face recognition. Both the login and the face if recognized then after that only the person has the authority to send the confidential data. In the similar way the person on the receiver side has to prove his both the identification the and then only he will be able to retrieve the secured data.

C. SELECTING SECRET IMAGE

Once after the login sender can send the data to the user. The image which contain the confidential data is selected and send to the various user.[5]

D. APPLY VISUAL CRYPTOGRAPHY

The main part of this paper is to create the shares by using the visual cryptography. The shares are created in such a way that one share will contain the data and the other share will contain the face image. So that even if one share is retrieved no information is going to leak. The user should posses with the both shares either of them is of no use.[2]

E. APPLY STEGANOGRAPHY

The steganography is applied over the confidential image as well as the face image so that they get hidden in it and to get it back one require to de-stegnograph it. The process of the steganography shuffles the pixels in the image according to the steganography key. After applying the same key one can de-stegnograph the the image.

F. SELECT DESTINATION

The destination is selected by means of user's email id so that sender can send the data to the as many user he can. Sender has to send only share one to the user and share two to the server. So that each of the user will posses with the single share on the basis of the primary authentication. Always the share two has to be send to the server and also retrieved from the server on the basis of the face recognition.[10]

G. SEND SHARE TO USER

The share one is send to the user by using the mail id. Also for the security purpose the share one and share two are send by the different path. The main moto of this paper is to keep separate the two shares so that the intruder even if tried to retrieve the data he will nat be able to do so. The share one on which the cryptography and after that the steganography is applied is send directly to the user.

H. SEND SHARE TO THE SERVER

The share two which is created by the same process of visual cryptography and steganography. The result of these two processes gives two shares out of which the second share is send to the server. And not to the client. On the client side he has to get the share one by using his user identification and password. But for the share two he has to send his the image of his face to the server. If the face image and the image stored in the database of the server is same then and then only the share two is send to the client. Now the client psses with both the shares, the share one and the share two. The process of the de-steganography is carried to retrieved the confidential data.[11]

But in case if the face image is of the intruder then in this condition the server will not send the share two to the client. And the share two which is present on the server side will be permanently deleted.

CONCLUSIONS

An attempt has been made to increase the security level for the highly confidential data. The sender and the receiver both are the aware of the sending and receiving of the confidential data. When the sender sends the data in this paper it is through email. The user login identification and password is required for the same so that initial authentication is completed with following the process of face recognition. This provides confirmation of the valid sender. By the process of the steganography and visual cryptography the shares of the confidential data is made and send through the wireless media. In the server the database is created which consist of the information of the authenticated user so that when receiver is going to retrieve the confidential data. Firstly by the user login identification and password and proceeded by the face authentication the shares are collected by the two different recognition. Until and unless total shares are collected one cannot retrieve the data. Both the authentication will provide the confidential data. In the negative case if unauthenticated person tries to retrieve the data then at the same time source file of the data will be deleted and sender will receive via mail that unauthorized person was going to retrieve the data. So that the necessary action can be taken.

REFERENCES

[1] Moni Naor and Adi Shamir, “Visual Cryptography”, department of applied math and computer science, Weizmann Institute, Rehovot,1995..

[2] Kai-hui lee and Pei-Ling chiu, “Digital Image Sharing by Diverse Image Media”, IEEE transcations on Information Forensic and security, vol 9, no 1, January 2014.

[3] Shruthi H.R, Ranjan Kumar H. S, Prasanna Kumar H.R, “ A Visual Secret sharing Technique for Secure and Fast Transmission”, Internationational Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 certified organization) Vol 2, issue 4, April 2014.

[4] Atul Sureshpant Akotkar, Chaitali Choudhary, “ Secure of Face Authentication using Visual Cryptography”, International Journal of Innovative Science and Modern Engineering (IJISME) ISSN 2319- 6386, Volume-2, Issue-5, April 2014.

[5] Zhimin Cao, Qi Yin, Xiaoou Tang and Jian Sun, “Face Recognition with Learning-based Descriptor”, National Natural Science Foundation of China Grant No.60553001, and the National Basic Research Program of China Grant Nos.2007CB8079002007CB807901

[6] Pei-Fang Tsai, Ming-Shi Wang, “An (3, 3)-Visual Secret Sharing Scheme for Hiding Three Secret Data” , downloaded from google on12, September 2014.

[7] Zhangquan Shen, Jiaguo Qi, and Ke Wang, “Modification of Pixel-swapping Algorithm with Initialization from a Sub-pixel/pixel Spatial Attraction Model”, the NASA Grant, at Michigan State University, National Technology Support Foundation of China, and Institute of Geographic Sciences and Natural Resources Research of the Chinese Academy of Sciences, China. 2009.

[8] Gunjan Dashore and Dr. V.Cyril Raj, “An Efficient Method for Face Recognition using Principal Componen Analysis (PCA)”, International Journal of Advanced Technology & Engineering Research (IJATER).

[9] Faizan Ahmad, Aaima Najam and Zeeshan Ahmed, “Image-based Face Detection and Recognition: State of the Art”, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 1, November 2012.

[10] Ms. R. Anitha, Dr. N. Sasirekha, “Image Securing Mechanism by Gradient Techniques”, International Journal of Computer Engineering and Applications, Volume VIII, Issue I, October 14.

[11] Rinki Pakshwar, Vijay Kumar Trivedi, and Vineet Richhariya, “A Survey On Different Image Encryption and Decryption Techniques”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013