Share data using Face Authentication

Swati D. Gaikwad[1], Prof. Venkat Ghodke [2]

[1]*Department of Electronics and Telecommunication, ME(DS), GSMCOE Balewadi Pune, Savitribai Phule Pune University, Maharashtra, India*
[2]*Department of Electronics and Telecommunication, AISSMS Institute of Information Technology Pune, Savitribai Phule Pune University, Maharashtra, India*

Abstract - *The sharing data has become a part of our life. We are surrounded with the data sharing. To and fro of digital data is moving all over through mobiles, laptop etc. The data can be shared within a fraction of second. Which comforts our life, but our data is insecure. What we share personal, confidential and lot many is unprotected. We are unable to provide the hundred percent assurances. Hence, highly confidential data needs a security and a proper feedback. So that one can assume that the data which is send is secured. we are going to apply a cryptography on a confidential data which will provide us (2,2) shares, the share1 is send to server and other share2 will undergo by the procedure of stenography with the stego key given by sender. The stego share2 is send on the electronic mail of the desired person. He will prove his face authentication after that he con login to account. The share2 he receives via mail and other share1 from the server as his authentication is proved. The share2 via mail requires the stegokey to destegnograph then share2 and share1 are decryptograph to form the original confidential data. This was the case when the face authentication was proved, in the another case in which the face authentication is not proved then the share1 from the server is deleted and the sender is informed by the mail directly that unauthorized person is trying to retrieve this information.*

Key Words: cryptography, stegnography,data sharing, face authentication, shares, face detection.

1. INTRODUCTION

The digital imaging tools may come in handy in throwing more light in this field. Visual cryptography (VC) is a technique that encrypts a secret image into *n* shares, with each participant holding one or more shares. Anyone who holds fewer than *n* shares cannot reveal any information about the secret image. Stacking the *n* shares reveals the secret image and it can be recognized directly by the human visual system. Secret images can be of various types: images, handwritten documents, photographs, and others. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme. The original motivation of VC is to securely share secret images in non-computer-aided environments. However, devices with computational powers are ubiquitous (e.g., smart phones). Thus, sharing visual secret images in computer-aided environments has become an important issue today.

Internet is one of the most popular communication channels but it is insecure. As it is an open and insecure medium, malicious users can intercept data. The fast growth of online applications results in the data security problem. In order to achieve data security, users need secure communication methods for transmitting secret messages over the internet. Due to unauthorized access of images the cyber-crime is increasing day by day. Hence the secrecy should be maintained in sharing information. So there should the provision to provide security for sending the confidential data.

In this paper, we tried to keep the data secured. Even if the intruders or the malicious user tried to retrieve the confidential data, they will not be able to do so. Here in this paper, we are going to use the face authentication for the security purpose. As initially we are going to do the registration of the clients (who are participated in sending or receiving data). Which will consists of their username, password, contact details, address, electronic mail id and finally with the image of their own face. This all details will complete the first phase will can be called as the phase of registration.

Secondly, we are going to login with authenticated client's username and password, for sharing a confidential data to the other client. Similarly the other client should also posses with the registration process (username, password, e-mail id, contact details, address and face image). Now the confidential data which is to be send is loaded in the account.

Thirdly, encryption process is done on the data which as a result creates (2,2) shares of the image. We call these shares as share1 and share2. Share1 which is send directly to the server and the share2 which is send via mail after the process of stegnography. Now we successfully generate two shares, share1 and share2 respectively. We applied the stegnography to the share2, along with the stegokey (this is the key or code which is use to stegnograph the image and same key or code is used to

© 2015, IRJET.NET- All Rights Reserved

destegnograph the image.) and later on we are able to get the new image which is stegnpgraphed.

Finally, the client is selected from the list of the registered clients and the stegnographed share2 image is send on respective clients mail. The share1 is send to the server and the client1 (sender) can now logout from his account. Now at the side of the client2 (receiver), initially he need to be login into his account. Client2 finds a mail received that he has received a share2 on his e-mail account. Then client2 has to download the share 2 from his mail apply the stegokey to destegnograph the share2. Also have to prove his face authentication and then and only then able to get share1 from the server. After receiving both the shares, share1 and share2 the original image (confidential data) is recovered.

On the other hand if the client2 is unable to provide his authentication, then the share1 from the server will be get deleted and he will not be able to retrieve the original data from a single share2. Simultaneously the client1 will receive the message as unauthenticated person tried to get the data.

2. LITERATURE SURVEY

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. Hierarchical model of six layer for information security application. On layer 6, several popular security applications have been listed such as: secure e-mail, digital cash, e-commerce, etc. Those applications depend on the implementation in layer 5 of secure authentication protocols like SSL/TLS, IPSec, IEEE 802.11, etc. However, those protocols cannot be put in place without implementing layer 4, which consists on customary security services such as: authentication, integrity, non-repudiation and confidentiality. The underlying infrastructure for such security services is supported by the two pair of cryptographic primitives depicted in layer 3, namely, encryption/decryption and digital signature/verification. Both pair of cryptographic primitives can be implemented by the combination of public-key and private key cryptographic algorithms, such as the ones listed in layer 2. Finally, in order to obtain a high performance from the cryptographic algorithms of layer 1, it is indispensable to have an efficient implementation of arithmetic operations such as, addition, subtraction, multiplication, exponentiation, etc. The whole concept was initially presented by Moni Naor and Adi Shamir in visual cryptography [1].

In visual secret sharing scheme the images can be shared via heterogeneous carrier. The hand printed images are used for image sharing scheme. Method to store the noise share has been developed by the Kai-Hui Lee and Pei-Ling Chiu. a VSS scheme, (*n, n*)-NVSS scheme, that can share a digital image using diverse image media. The media that include *n*1 randomly chosen images are unaltered in the encryption phase. Therefore, they are totally innocuous. Regardless of the number of participants *n* increases, the NVSS scheme uses only one noise share for sharing the secret image. Compared with existing VSS schemes, the proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness, both for shares and for participants. There are four major contributions. First, this is the first attempt to share images via heterogeneous carriers in a VSS scheme. Second, to introduce hand-printed images for images-haring schemes. Third, it proposes a useful concept and method for using unaltered images as shares in a VSS scheme. Fourth, a method to store the noise share as the QR code. The method and concept for using unaltered images as shares in the visual secret sharing scheme [2].

The combination of both the steganography and the visual secret sharing scheme which in result provides the high level of the security to the information which is being to be transmitted. Visual cryptography is that current space of analysis wherever heap of scope exists. In the existing VC schemes no security is provided to the secret shares and intruder can alter its bit sequences to create fake shares. A steganography, visual secret sharing scheme and the combination of both. Therefore it provides higher levels of security to the information being transmitted. That is the intruders cannot easily break the system. Even if they realize the existence of a secret data they cannot easily recognize the data, since data is hidden in two ways. Shruthi, Ranjan and Prasanna propose the new image compression and encryption technique. This system cannot be broken easily by the intruders [3].

Performance on visual cryptography schemes depends such as security, accuracy, contrast, computational complexity type, share generated of secret image. visual cryptography techniques is applied to protect face template in the database as well as providing extra layer of authentication to the existing face based authentication system. In order to hide the secrecy expansion and increasing of the number of shares, but this affects the resolution. Therefore an optimum number of shares are required to hide the secrecy. At the same time security is also an important issue. Hence research in visual cryptography is towards maintaining the contrast at the same time maintaining the security. In visual cryptography, here during encryption part actual image is decompose in to three shares this can be done for more

© 2015, IRJET.NET- All Rights Reserved

number of share generation in future so that security will enhance [4].

An improved (3, 3)-visual secret sharing scheme, which can be used to embed three secret messages into three shares and improve security. First of all, the fist main share image is resulted randomly and other two share images are based on the first share image and the two coding tables are designed[6].

Principal component analysis (PCA) was invented in 1901 by Karl Pearson. PCA is a variable reduction procedure and useful when obtained data have some redundancy. This will result into reduction of variables into smaller number of variables which are called Principal Components which will account for the most of the variance in the observed variable. Problems arise to perform recognition in a high-dimensional space. Goal of PCA is to reduce the dimensionality of the data by retaining as much as variation possible in our original data set. On the other hand dimensionality reduction implies information loss. The best low-dimensional space can be determined by best principal components. The major advantage of PCA is using it in eigen-face approach which helps in reducing the size of the database for recognition of a test images. The images are stored as their feature vectors in the database which are found out projecting each and every trained image to the set of Eigen faces obtained. PCA is applied Eigen face approach to reduce the dimensionality of a large data set.[9]

3.SENDING AND RECEIVING DATA PROCESS WITH AUTHENTICATION

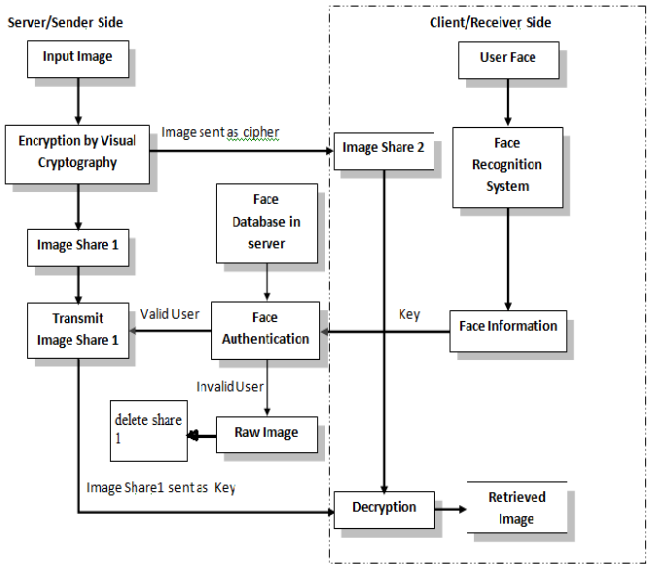

Fig 1: Block Diagram for Digital Image Sharing with Authentication.

4. PERFORMANCE ANALYSIS

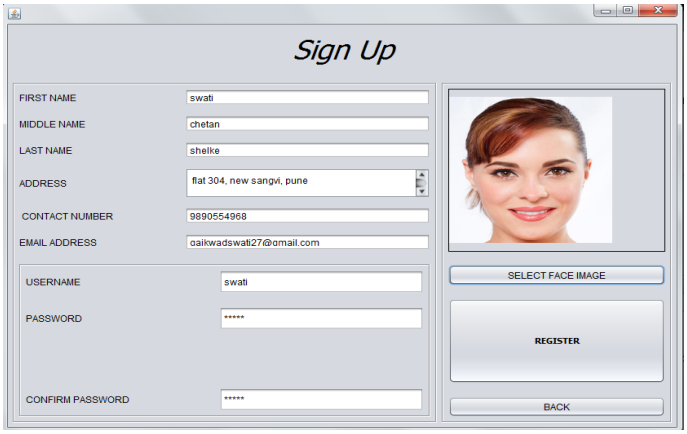

Fig 2: Registration information filling page.

In this paper, From the above Fig 2. It is cleared that the information of the person is gained. We are using here java as a tool which easily provide the platform for the application developing. This panel is a registration panel here we obtain the information from the person which after successful registration will be so called as a client. We initially take the personal information such as first name, middle name, last name, address, contact number, e-mail address, username, password, confirmation of the password and finally the image of the face. When all this information is gained after that the button for registering purpose is kept. Which will take two decision as whether this username already exists or not. If not then it will register this user or else it will provide with a message as this username exists.

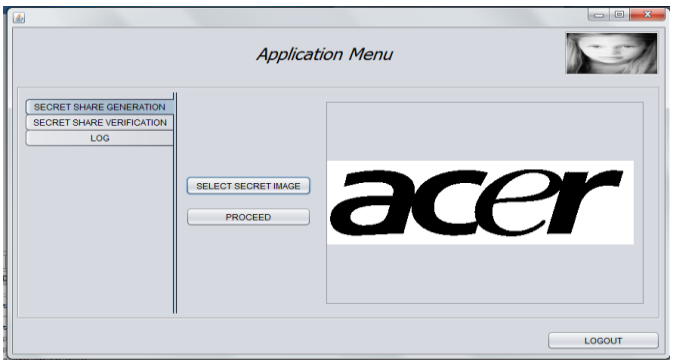

Fig 3: Application menu

After the login page, there a client requires a username and password to login. The same which he had used during the time of registration. After successful login the new panel will be generated called as the application menu. From the Fig 3. We can accurately observe three labels on the left side they are, secret share generation in this label we are able to select the secret data or secret image by clicking on the button by name select secret image. For example, we have taken the image of 'acer'. After the successfully uploaded the proceed button can be clicked to enter into new panel.

© 2015, IRJET.NET- All Rights Reserved

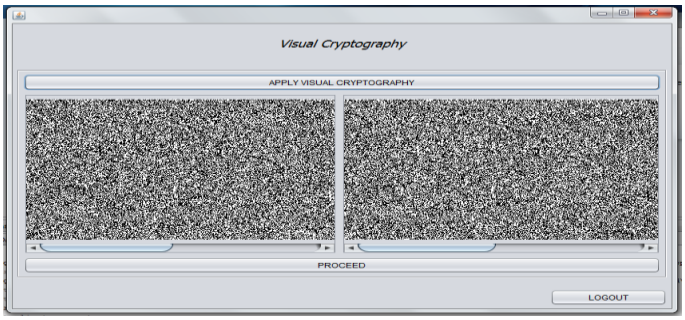

Fig 4: Visual Cryptography on Original image

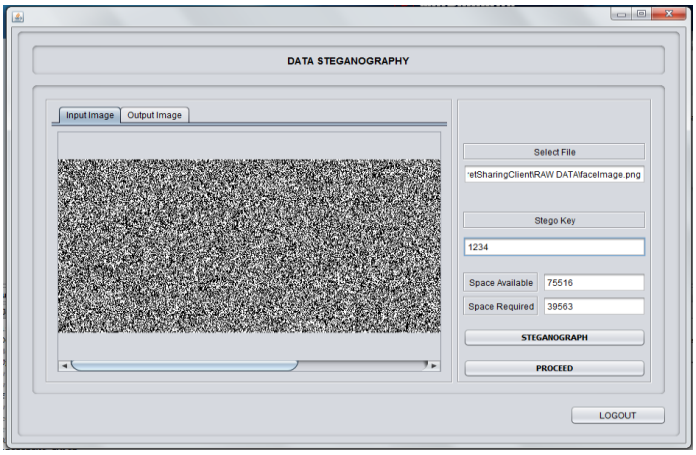

Fig 5: Apply Data Stegnography on Share.

From the above Fig 4 and Fig 5 the encryption and the stegnography is done then by using the stegokey the process of stegnography is completed successfully. Also in the above panel we have provided an output image which will be generated after stenograph.

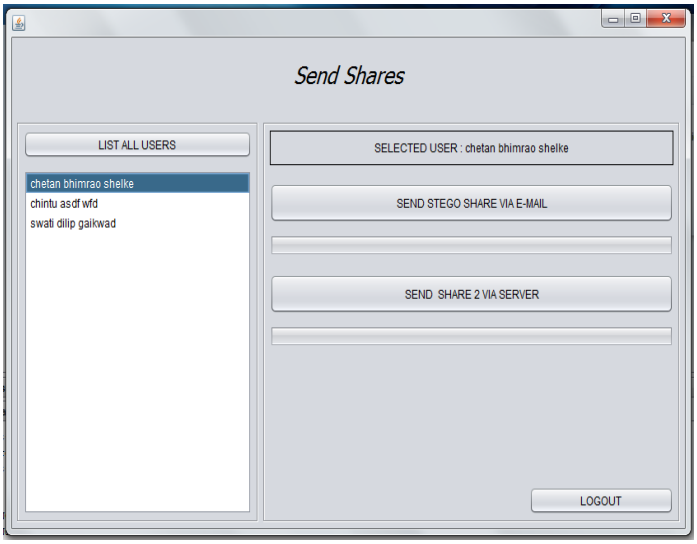

Fig 6: Selection of Sender and Sending of the shares.

In the above Fig the list of all available clients are provided out of which we can select our desired client.and can send the share via email and to the server.

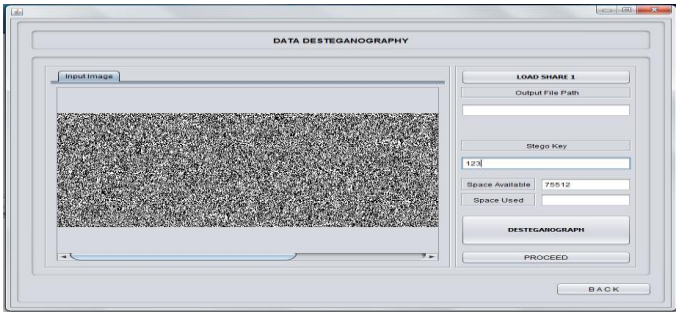

Fig 7: Destgnogaphy of the share

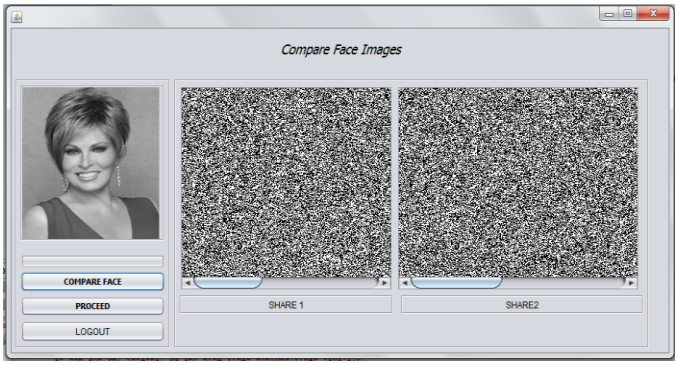

Fig 8: Comparing the face and downloading other share.

The destegnograph of the share is done by using the stegokey inFig 7. In Fig 8.the face of the client is compared and then after succeful comparison the share2 is downloaded.

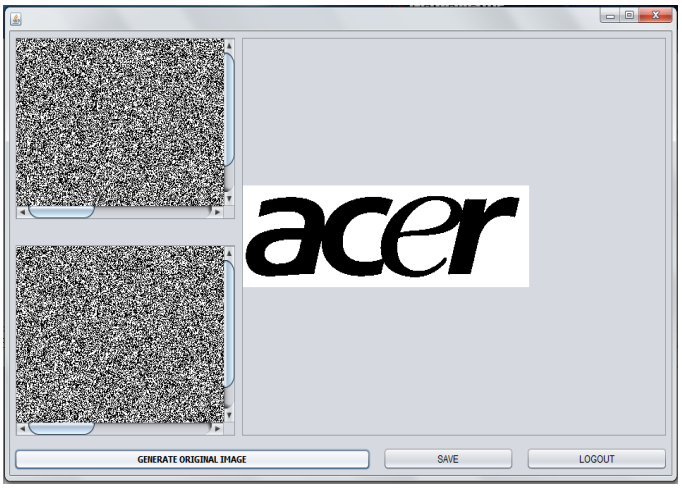

Fig 9: Original data is retrived successfully

In the Fig 9, both the shares are decrypted and the original secret image is achieved.

© 2015, IRJET.NET- All Rights Reserved

5. CONCLUSIONS

Secret data can be send to the confidential client only. With the process of visual cryptography and stegnography. In which we successfully obtain the two shares by using visual cryptography i.e/successful encryption is done, and also apply stegokey for the process of the stegnography i.e successful stegnography and de-stegnography is done. Also we are able to find that intruder who is trying to attack on the secret data. We are also able to protect our secret data from the malicious attackers. The sender is also informed by this situation.

ACKNOWLEDGEMENT

The authors would like to thank all the reviewers for their helpful comments and suggestions.

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.2007CB807900, 2007CB807901

[6] Pei-Fang Tsai, Ming-Shi Wang, "An (3, 3)-Visual Secret Sharing Scheme for Hiding Three Secret Data" , downloaded from google on 12, September 2014.

[7] Zhangquan Shen, Jiaguo Qi, and Ke Wang, "Modification of Pixel-swapping Algorithm with Initialization fr om 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 Component 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.

© 2015, IRJET.NET- All Rights Reserved