Data security for Image Shares by 2- Level Authentication in Visual Cryptography

[1]T Dinesh Babu, [2]G Sujatha

Information Security and Computer Forensics, SRM University
[1]dinesh.tatapagari@gmail.com, [2]sujatha.g@ktr.srmuniv.ac.in

***Abstract*- In today's world Information security is one of the most important solutions in the computing environment. Cryptography and Steganography are the most widely used techniques to overcome threats to data. By using this cryptography scheme we can save the images or text in database in the form of shares. The secret images can be restored by stacking operation. This property makes cryptography useful especially for the low computation load requirement. A secret message/image transmission will be done through (2, 2) visual cryptographic shares which are transmitted so that a potential eavesdropper won't be able to know the data that is transmitted or stored. This paper examines the need of developing a methodology which would help the user to represent the resultant message/image in the same size as the original secret image. Also, this paper puts forward a tool which would help the user with a 2 level authentication by password protection.**

I. INTRODUCTION

Information security is vital for protecting the confidentiality, integrity and availability of resources, and data. Without confidentiality, trade secrets or personally identifying information can be lost. To ensure the security of a particular data different techniques are used. Cryptography ensures conversion of a readable format into an unreadable cipher which is understood only after decryption. Steganography on the other hand embeds message into a cover media and hides its existence. Neither of them alone is secure enough for sharing information over an unsecure communication channel and is vulnerable to intruder attacks. Our proposed technique which involves steganography using Visual Cryptography is an efficient way of sharing & storing information. In this paper a secret message/image transmission technique has been proposed through (2, 2) visual cryptographic shares which are transmitted so that a potential eavesdropper won't know the data that is transmitted or stored.

II. RELATED WORK

2.1visual Cryptography

Visual cryptography is a cryptographic technique which allows visual information (pictures, text) to be encrypted in such a way that decryption can only be carried out if all the threshold images (Shares) are obtained. One of the best-known techniques has demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. (2,2) Visual Cryptography Encodes secret image in threshold images (shares). These Shares are represented on transparencies. Secret Image/Text is reconstructed visually. Each participant gets one share k out of n, participants are needed to combine their k shares and see secret image. Every single pixel is split into sub pixels. Human vision still perceives them as one pixel.

2.2 Visual Cryptography Goals

Confidentiality - Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear, and by restricting access to the places where it is stored. Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

Integrity - In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified, unauthorized, or undetected. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

Availability - For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

Authenticity - In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be.

Non-repudiation - In law, non-repudiation implies one's intention to fulfil their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Electronic commerce uses technology such as digital signatures and public key encryption to establish authenticity and non-repudiation. Thus using this technique of Visual Cryptography helps us to achieve a more reliable and secure means of communication & storage of data.

III. METHODOLOGY

Experiment Setup and Methodology Used The main objective of this project is secure transmission & storage of secret message in the image file by splitting the images in to shares.

The hardware and software requirements for Visual cryptography are as following.

Hardware/software Requirements

Hardware

- Processor: Preferably 1.0gHz or Greater
- Ram:512 MB OR Greater
- Hard Disk:40GB
- Monitor:15vga colour

Software

- Platform : java
- Operating system: windows xp/7/8.
- Tools: IDE Net Beans 5.0 and above.

This paper provides solution for secure transmission & storage of secret message in the image file by splitting the images in to shares using (2,2) VC scheme and secure random password**.**

In this paper they are mainly five architecture modules they are as follows

1. Login
2. Encryption
3. Decryption
4. Password generation

3.1 Login

In login the user need to enter the password provided by the Administrator. Unless the user enters the password he/she cannot use the product. By this login module it protect from unauthorized user's usage. If the user enters the proper password he will be redirected to the encryption and decryption modules.

3.2 Encryption

The user needs to enter the password in order to use the system. After entering the valid password the user is able to see the encryption and decryption tabs. Encryption module gets the secret image that has to be encrypted and generate shares and random password. The shares and the password have to be stored in database. Hacker unless he has the two particular shares and the password he couldn't able to decrypt the secret image.

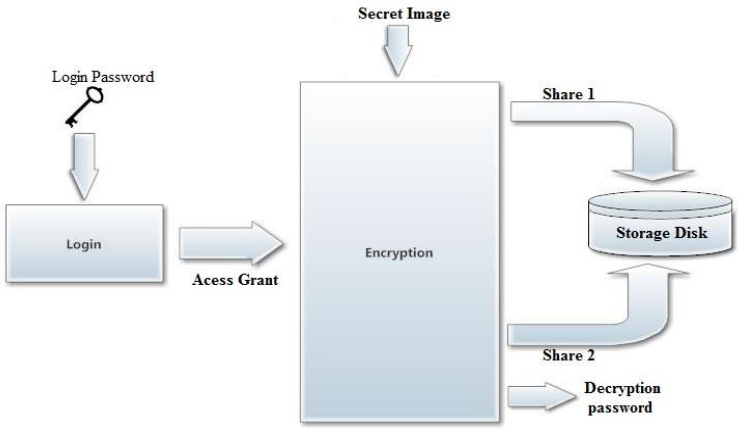


Fig 1 Encryption Process

Encryption (2,2) visual cryptography scheme The corresponding matrices are as follows:

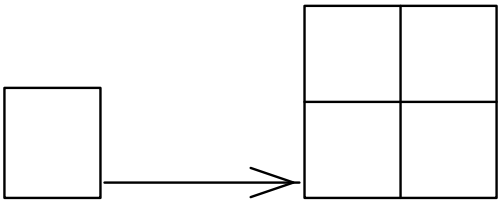
$$C_0 = \{ \begin{pmatrix}0011\\0011\end{pmatrix}, \begin{pmatrix}1100\\1100\end{pmatrix}, \begin{pmatrix}1010\\1010\end{pmatrix}, \begin{pmatrix}0101\\0101\end{pmatrix}, \begin{pmatrix}0110\\0110\end{pmatrix}, \begin{pmatrix}1001\\1001\end{pmatrix} \}$$

for white pixel and

$$C_1 = \{ \begin{pmatrix}0011\\1100\end{pmatrix}, \begin{pmatrix}1100\\0011\end{pmatrix}, \begin{pmatrix}1010\\0101\end{pmatrix}, \begin{pmatrix}0101\\1010\end{pmatrix}, \begin{pmatrix}0110\\1001\end{pmatrix}, \begin{pmatrix}1001\\0110\end{pmatrix} \}$$

for black pixel.

One pixel is divided into four sub pixel.
Pixel Conversion:



The user is first asked to select the secret image he wants to encrypt. The fileChooser() predefined method allows us to choose the appropriate image we want. After choosing the image when the user clicks on the ENCRYPT button the Crypting.loadAndCheckSource() method is called, this method checks if the image is smaller than the minimum possible size, it is resized if required. This method also checks if it is a valid source file. The image file is assumed to be a PNG file, if it is not it is converted into the PNG format. The PNG image allows only ARGB format, so initially it first checks for ARGB color space converts it if it isn't already.

BufferedImage.TYPE_INT_ARGB property used to carry out this operation. The method checks if image contains only black + transparent or white pixels. The colored pixels get converted to either black or transparent. This is determined by knowing brightness of the image. The brightness of the image is calculated by Euclidian formulae equation. Depending on the brightness it is converted into either black or transparent.

Euclidian formulae:

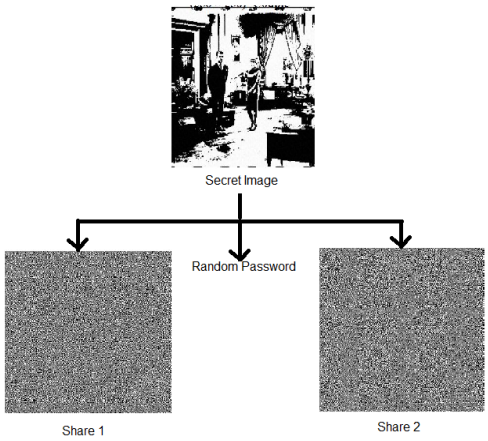
Brightness = (0.2126 * r) + (0.7152 * g) + (0.0722 * b)

Depending on the height and width values the shares are generated using the predefined class called Secure Random which generates random pixels. Each 2x2-pixel-pack has 2 randomly set pixels. The share 1 is generated using the Secure Random class. The share 2 is then generated depending on the share 1 and the secret image. The two shares are then displayed in Scroll panes respectively. The Buffered Image, Graphics2D predefined class are used to store the generated shares. We can also save the shares which will be used in the Decryption.

The Encryption functionality also incorporates a dual password mechanism for more security. This password is generated using the various different regions of the images; the password is generated and displayed in the textbox which is known only to the sender and receiver.

For generating the password during encryption, regions of the staked images are selected. For black pixel value is set to 0, If white then value is set to 1.This value is then converted to hexadecimal for easily remembering the password, Integer.toHexString () method is used to display the value in hexadecimal. This password is used for authentication of receiver side.

Encryption result



3.3 Password Generation

Password generation module will be handled by the administrator. The administrator generates different passwords for the users. Using the password provided by the administrator user can login to the system. Our system incorporates a password mechanism for better security and a more efficient way of user authentication. In the first interface of password generation, when user clicks on the generate method, an 8 digit password is created.

First 4 digits of the password is generated randomly and the other four digits of the password are generated with logic of combination of two digits to get sum of 9. The String Builder class is used to append these values of the password and another method converts it into the string and it is displayed in Textbox to the user. Only with respective shares and the password, user will be able to decrypt the secret image.

3.4 Decryption

User needs to enter the password in order to use the system. After entering the valid password, the user will be able to see the encryption and decryption tabs. Decryption module gets the two share images of respective secret image and password. If password entered is valid then system displays the decrypted secret image. After entering the valid password, the system first generates the staked image using the shares that are uploaded. Staked image is then decrypted in to clear image which is secret image.

In the Decryption method the user is first asked to choose the two shares which were generated by the Encrypt functionality. Once the user clicks on the Decrypt button it calls the Crypting.loadAndCheckEncrFile() method. The two shares are validated using the StakedImageGeneration method which uses the method g.drawImage() to draw the first share and the second share is also drawn using the same method. Thus the two images are superimposed on each other. We display the stacked image and the secret image in the respective Scroll panes. The decryption mainly is carried out by the logic that each pixel contains a (2, 2) matrix and by OR operation we get the resultant colour. If all 2*2 matrices are black then it is black otherwise it is white.

The decryption method also includes the same password mechanism which was used in the Encryption method which is very vital for the security. The user is asked to type the password which was already generated in encryption if the password matches then only the operation is carried out else it displays a message Wrong password.

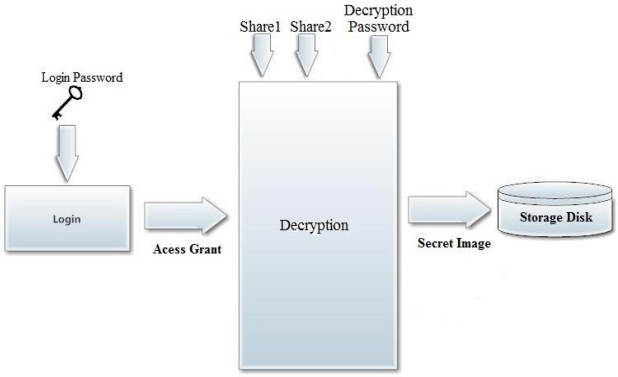


Fig 2

Decoding through (2,2)VCP

- Stacked version of authenticated image is regenerated by AND'ing each pixel position wise.
- Regenerating the original authenticated image from the stacked version by OR ing these four pixel values(ST(i)(j), ST(i)(j+1),ST(i+1)(j), ST(i+1)(j+1)).

Decryption result

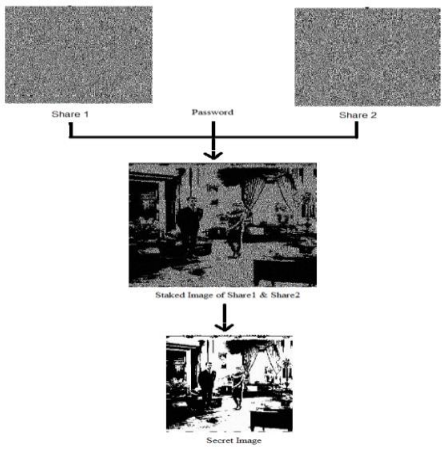


Fig 3

IV. FUTURE WORKS

Security of data is one of the crucial aspects of the current corporate world. Several challenges have to be faced in future for providing more security with the advanced technology. In future every job will be done remotely (work from home) so in order to provide security in remote based, project has to be extended to provide service in web based. On providing web based employee and employer can work in remote locations without any security issues. This concept can be implemented in RFID in order to authenticate multiple people in order to open locker or enter in to strong rooms of banks etc.

V. CONCLUSION

In this project, the concept of (2,2) Visual Cryptography Schema has been introduced. This helps in providing more security to image file that are stored in the data base. Detecting or guessing of share in order to find out the secret image is overcome by using 2nd layer password security. This project protect from unauthorized user by authenticating with password. So, the user with a valid password can only access the project tool. This project helps in providing authentication to different user with shares they have.

REFERENCES

[1] J.K. Mandal#1, S. Ghatak Secret Image / Message Transmission through Meaningful Shares using (2, 2) Visual Cryptography (SITMSVC), IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 978-1-4577-0590-8/11/$26.00 ©2011 IEEE MIT, Anna University, Chennai. June 3-5, 2011

[2] Jena, D., Jena, S.K.: A Novel Visual Cryptography Scheme. In: The 2009 International Conference on Advance Computer Control, pp. 207-211 (2009).

[3] M. Nakajima and Y. Yamaguchi. Extended visual cryptography for natural images. In WSCG Conference 2002, pages 303–412, 2002

[4] Naor, M., Shamir, A.: Visual Cryptography. In De Santis, A. (ed.) 1994. LNCS, vol . 950, pp. 1-12. Springer, Heidelberg (1995).

[5] S. Guha, S. Das, S. Sarkar and A. Chaudhury "Visual Cryptography using pixel filtering technique for continuous tone 24-bit image" Proc of National Seminar on Role of ICT in improving Quality of life Page 61- 72, 2010.

[6] http://www.oracle.com/technetwork/java/codeconvtoc-136057.html

[7] http://en.wikipedia.org/wiki/Visual_cryptgraphy

[8] http://stackoverflow.com