ISSN: 2321-8169
168 – 172

A Visual Cryptography Scheme for User Authentication

Miss.Vaishali Bhagat
Asst. Professor, Dept. of Information and Technology,
S. R.M.C.E.W.
Nagpur, India
bhagat.vaishali14@gmail.com

Rida Ansari
Dept. of Computer Science and Engineering
S. R.M.C.E.W.
Nagpur, India
ridaansari24@gmail.com

Roshani Thakre
Dept. of Computer Science and Engineering
S. R.M.C.E.W.
Nagpur, India
roshanithakre77@gmail.com

Neha Patiye
Dept. of Computer Science and Engineering
S. R.M.C.E.W.
Nagpur, India
neha.patiye3oct1995@gmail.com

Snehal Kolte
Dept. of Computer Science and Engineering
S. R.M.C.E.W.
Nagpur, India
snehal.kolte95@gmail.com@gmail.com

Latika Chaudhari
Dept. of Computer Science and Engineering
S. R.M.C.E.W.
Nagpur, India
latikachu1995@gmail.com

Abstract— A new scheme for user authentication is proposed using visual cryptography and invisible digital watermarking. Visual cryptography which allows visual information to be encrypted in such a way that decryption becomes the job of the person to decrypt via a sight reading. In the proposed work, user signature will be embedded within the cover media. It may be text, images, audio, video etc. Here we used cover image for embedding data by using a single bit LSB watermark insertion algorithm. After that the image will be split into two shares. Shares will be later encrypted by using a Column Shift Permutation algorithm. Receiver will decrypt the shares using Column Shift Permutation algorithm. Shares are collected and stamp together by receiver to get cover image. Then signature will be de-embedded from the cover image. Data will be transfer using communication media. Image will be passed in more secure manner without any distortion. This method is very efficient and effective .The method can be implemented with minimum processing. This application used in customer identification in bank and in online voting.
Keywords- *Visual Cryptography, least significant bit (LSB) algorithm, Column Shift Permutation algorithm, embedded shares, encryption and decryption.*

*****

I. INTRODUCTION

In the ever change in global data communication, inexpensive Internet connections, and fast-paced software development , security is becoming more and more of an issue. Security is now a basic requirement because global computing is inherantly insecure. As your data goes from point A to point B on the internet, for example, it may pass through several other points along the way, giving other users the apportunity to intersect, and even alter it. It does not nothing to protect your data center, other servers in your network, or malicious user with physical access to your EnGarde system.

Consider the range of types of security techniques which are relevant to the provision of the types of security features like, Encipher Technique for providing confidentiality features, Integrity Technique for providing data integrity features and as a building block in authentication exchange, Digital Signature Technique for providing data integrity and non repudiation features, Hash Function Technique used in conjunction with digital signatures and also as a means of building integrity techniques and authentication exchange for providing entity authentication features.

Visual cryptography which allows visual information to be encrypted in such a way that decryption becomes the job of the person to decrypt via a sight reading. Visual cryptography is the art of encrypting visual information such as handwritten text, images etc. The encryption takes place in such a way that no mathematical computations are required in order to decrypt the secret data. The original information to be encrypted is called as secret. Fundamental idea behind visual cryptography is to share the secret data among group of n participants. In order to share the secret, it is divided into n number of parts called shares. These shares are distributed among the participants.

Secret sharing has been a serious concern even before the digital era. One can find a lot of method and practices which shows the application and demand of technique historically. Sending information without lickage, without tampering, without noise to the intended recepient is the biggest challenge in IT now. The field of secure messaging can be broadly classified into two cryptography and stegnography.

ISSN: 2321-8169
168 – 172

Cryptography is the art of secure messaging. Stegnography, is the hiding of secrete message within an ordinary message and the extraction of it at its destination. Stegnography takes cryptography, a step further by hiding an encrypted message so that no one capture it existance. Ideally anyone scanning your data will fail to know its contains encrypted data.

Two level security is provided to data by using embedding and encryption method. User signature will be embedded into cover image by using single bit LSB watermark insertion algorithm and then image will be split into two shares. After that shares will be encrypted using Column Shift Permutation Encryption Algorithm. Receiver will decrypt the shares using Column Shift Permutation Decryption Algorithm. Shares are collected and stamp together by receiver to get cover image. Then signature will be de-embedded from the cover image.

II. RELATED WORK

Ratheesh V. R.,Jogesh J.,Jaymohan M., [1] in this paper ,made an attempt to apply visual cryptography scheme with meaningful shares along with digital watermarking for user authentication. Nayan A.Ardak, Prof.Avinash Wadhe, [2] in this paper, visual cryptography technique are used for privacy protection such as Expansion less share, Image captcha Base authentication technique, Compression random share and error diffusion for visual quality improvement. Praveen Kumar.P,Sabitha.S ,[3] user authentication is an important phase in most of the communications through public network. Visual cryptography provides a new way of performing encryption which requires less computing. Chandrashekhra And Jagdisha, [4] in this paper, uses color image visual cryptography for password protection and it is not able to break this protection with combinatorial techniques to encode secrete written material. Sruthy K Joseph,Ramesh R,[5] in this paper, visual cryptography scheme that can generate non expanded share images. Since random grid method is used, the decoded secrete will be of the same size as that of the secrete image.

III. PROPOSED SYSTEM

Authentication is a process in which the legal patent provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. Authentication is done to confirm real identity of the data, image or whatever entities. It is mainly done to ensure that it came from the real user. Here authentication is mainly done for the security purpose at both the sender as well as the receiver for secure communication. The data hiding key provided to the receiver acts as a tool for authentication.

In this scheme, authentication is provided by embedding and encryption of image. The size of original image after embedding is remains unchanged so that hacker cannot recognize the image will be stegoimage. For that user signature will be embedded within the cover media. The signature will be embedded into the cover image by using a single bit LSB watermark insertion algorithm. Stegoimage will be generated and then it is split into two shares. Share will be encrypted by using a Column Shift Permutation encryption algorithm. Encrypted share will be send to the receiver. Instead of using key for encryption as well as decryption, here seed matrix is used at sender and receiver side for encryption and decryption to provide more authentications.

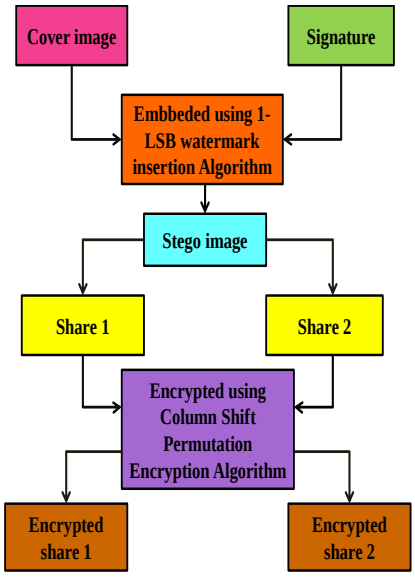


Fig 3.2.1 Creation of StegoImage and Generations of Shares

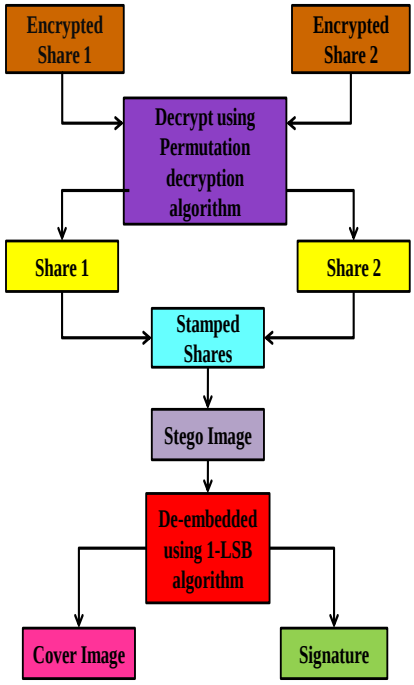


Fig.3.2.2 Retrieval of Secret Image

Visual cryptography can be use as a means for transfering a secret image to the authorised person. In proposed work secret image is embedded into a cover image and the embedding that can be done by using watermark insertion algorithm. After the steno image that will be generated. This steno image will be split into two shares. Both the shares that contain secret image that is to be embedded behind the cover image. These shares will be encrypted by using a column shift permutation encryption algorithm. After this both encrypted share send to the receiver.

At the receiver side this encrypted share is decrypted by using same permutation decryption algorithm. Both the decrypted share are collected and its stamp together to form

ISSN: 2321-8169
168 – 172

the stego image. This stego image is de-embedded by using the same single least significant bit watermark insertion algorithm. Finally, we get the separate cover image and secret image.

VI. PHASE IMPLEMENTATION

Phase I. Authentication:

Authentication is done to confirm real identity of the data, image or whatever entities. It is mainly done to ensure that it came from the real user. Here authentication is mainly done for the security purpose at both the transmitter as well as the receiver for secure communication. The data hiding key provided to the receiver acts as a tool for authentication.

Phase II. Embedding

An embedding is one instance of some structure contained within another instance. Here a secret image and cover image is taken. The secret image is hiding behind the cover image using single bit least significant watermark insertion algorithm and stego image will be generated. Both files are saved with their respective extension.

Phase III. Share Generation

The stego image will be split into two parts. The share having same size and blur shares will be generated.

Phase IV. Encryption

In cryptography, encryption is the process of encoding message or information in such a way that only authorized parties can access it. In an encryption scheme, the intended information or message, referred to as simple image, is encrypted using an encryption algorithm, generating encrypted image that can only be read if decrypted. Both generated shares will be encrypted by using Permutation encryption algorithm. Then the shares will be sending to the receiver.

The purpose of encryption is to ensure that only somebody who is authorized to access data (for ex. A text message, image or a file), will be able to read it, using the decryption key.

Phase V. Decryption

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to text and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically it may also be perform with a set of key or password. At receiver side, both encrypted shares will be received by the receiver and decrypt it by using Permutation decryption algorithm.

Phase VI. Stamping of shares

Stamping is the process of placing an image, text or any data into a surface which can be image or any data. After decryption both shares will be stamp together and recover the steno image.

Phase VII. De-embedding

De-embedding is the process of eliminating the influence. Here the secret image which is hidden behind another image is subtracted or eliminated. Stego image will be de-embedding by using 1 bit least significant bit watermark insertion algorithm and the signature and cover image will get separately.

V. ALGORITHMS USED FOR IMPLEMENTING PROPOSED METHOD

Algorithm for Generation of Stego image

Start

Step 1-Take cover image and secret image

Step 2-Loop for embedding

a. Get a pixel from SI (Secret Image)

b. Convert it into Binary which is of 8 bit

c . Extract 1-LSB from green plane of cover image and 1-LSB from secret imaged. Perform addition of last bits of both images

Step 3- Stego image will be generated

Stop

Algorithm for Share Generation

Start

Step 1- Take Stego image as input

Step 2- Convert it into 8-bit binary format

Step 3- Separate the even-odd bit of image

Step4- Fill the even-odd blank position with padding 0 bit

Step 5- Share 1 and Share 2 generated

Stop

Algorithm for encryption of share

Start

Step 1-Take Share 1(S1) and Share 2(S2)

Step 2- Represent it into matrix form

Step 3-Take seed matrix R

Step 4- RS1=R - S1 or RS2= R - S2

Step 5- Apply column shift and transposition on RS1 and RS2

Step 6- Encrypted shares are formed

Stop

To recover the cover image and secret image the reverse procedure of algorithm will be followed.

ISSN: 2321-8169
168 – 172

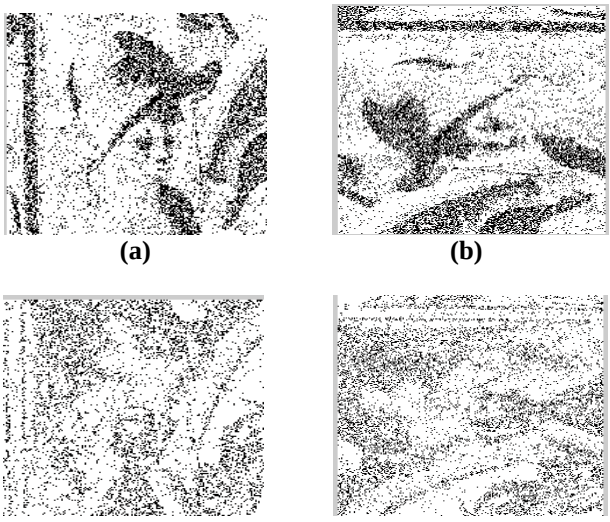
VI. RESULTS

This system is implemented in MATLAB (R2010a) using windows 7 operating system. The experimental result is carried out on cover image and secret image.

(a) (b)

(c)

Fig .1 Embedding: (a) Cover Image, (b) Secret Image, (c) Stego Image



(a) (b)

(c) (d)

Fig.2 Encryption: (a) Share 1, (b) Encrypted Share 1, (c) Share 2, (d) Encrypted Share 2

Fig (1) shows embedding and Fig(2) shows encryption of secret image by using 1-LSB watermark insertion algorithm and Column Shift Permutation Algorithm.Encrypted shares will be received and decrypted image is given below.

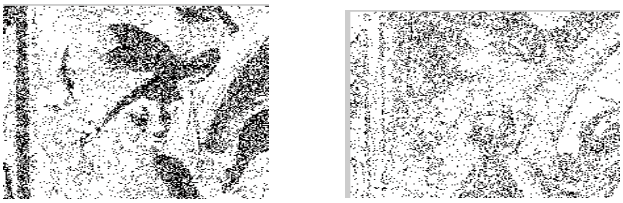


Fig 3: Decrypted shares

Fig 4: Stego image obtained after stamping

Collect the decrypted shares and stamping is performed to get stego image.De-embedding perform on stego image and reveal the secret image and cover image.

(a) (b)

Fig5: Reconstructed Image (a) Decoded Cover Image (b) Decoded Secrete Image

```
Mean Squared Error (Cover Image) = 0.096939
Peak Signal to Noise Ratio with LSB Encoding = 58.2658

Mean Squared Error (Secret Image)= 0
PSNR with LSB Decoding = Inf
```

Fig 6: PSNR and MSE ratio of secret image and cover image

VII. CONCLUSION AND FUTURE SCOPE

This system is developed for securing the image/data by using Matlab technology. In which securing the image is successfully tested with sample data/image and as the experimental result shows. This system fullfill the aim and objective of the project. This system uses color image visual cryptography technique for image/data protection and it is not able to break this protection with present technology.This visual cryptography technique are used for privacy protection such as expansionless shares image captch base authentication technique and error diffusion are used for visual quality is to be improved.

This is a technique for securing the data transmission. The sender will send secure data to the receive in less time delay. These scheme will be implemented in another application for secure communication.

ISSN: 2321-8169
168 – 172

REFERENCES

[1] Ratheesh V.R., Jogesh J., Jayamohan M.," **A Visual Cryptographic Scheme For Owner Authentication Using Embedded Shares**", Indian Journal of Computer Science and Engineering (IJCSE) Vol.5, No.5, Oct-Nov, 2014.

[2] Nayan A. Ardak," **Visual Cryptography Scheme for Privacy Protection**", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014.

[3] Praveen Kumar. P," **User Authentication using Visual Cryptography**", 2015 International Conference on Control, Communication & Computing India (ICCC) ,19-21 Nov,2015.

[4] Chandrashekhara and Jagdisha," **Secure Banking Application Using Visual Cryptography Against Fake Website Authenticity Theft**", Vol. 2,Issue -2,2013.

[5] Sruthy K Joseph, Ramesh R," **Random Grid Base Visual Cryptography Using A Common Share**", Conference of computing and network communication (CoCoNet'15), Dec.16-19,2015.

[6] Ziya Arnavut t, Meral Arnavut*, Basar Koc+, Hiiseyin Ko$\diamond$ak+ ,* SUNY Fredoniat*," **Investigation of Rowand Column Permutations for Lossless Compression of Images**", 978-1-5090-3784-1/16/$31.00.

[7] Patel Roshni, Prof. Aslam Durvesh, Prof. Aslam Durvesh,Patel Urvisha," **Lossless Method for Data Hiding In Encrypted Image**", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15.

[8] Shruti M. Rakhunde, Archana A. Nikose," **New Approach for Reversible Data Hiding Using Visual Cryptography**", 2014 Sixth International Conference on Computational Intelligence and Communication Networks.

[9] Long Bao, Yicong Zhou* and C. L. Philip Chen," **A lossless (2,8)-chaos-based secret image sharing scheme**", 2014 IEEE International Conference on Systems, Man, and Cybernetics October 5-8, 2014, San Diego, CA, USA.