MULTI-MODE DATA SECURITY FOR SECRET COMMUNICATION

Candida Paulette Alphonso[1], Maruska Mascarenhas[2]

[1]Computer Engineering Department, Goa College of Engineering, Goa, India
[2]Computer Engineering Department, Goa College of Engineering, Goa, India

Abstract

Data Security in the current digitized era determines the ability of the system to protect, manage and distribute sensitive information. Privacy is the right of authorized users to ensure that confidential information maintained is being controlled and protected from unauthorized access or distribution. The major goals of data security are Confidentiality, Integrity, and Authentication. Text based passwords are the most common methods used for authentication. But these textual passwords are vulnerable to dictionary attacks, eves dropping and shoulder surfing. To address this problem, an approach for image based authentication has been proposed to authenticate a valid user with regards to enhancing the security of textual passwords which can be easily compromised. In this paper, algorithms for Image Cryptography, Image Steganography and Knowledge based Image CAPTCHA have been proposed to provide a one time communication. The image will be encrypted into two image shares at the server during password generation and the share returned to the client will be used as a token during authentication. At no time the entire password will be transmitted over the network or stored on any system during authentication. This hybrid multi-mode approach attempts to lessen the attacks towards password security thereby minimizing the risks of user impersonification and providing efficient means to transfer secret data using images. The proposed approach is well suited for private networks to transfer confidential messages without compromising the integrity of data.

Keywords*—authentication; visual cryptography; password; steganography; CAPTCHA*

--***--

1. INTRODUCTION

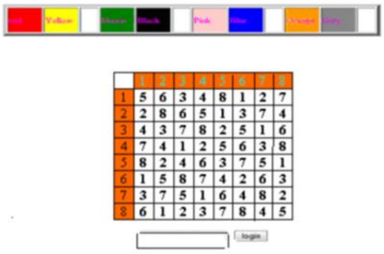
With the rapid advancements in technology, improvements in the methods for authentication have given way to more sophisticated means of attacking a user's privacy. Textual passwords can be easily compromised with brute force attacks, even to crack encrypted passwords. Military and defense organizations cannot tolerate leakage of any sensitive data in a secret communication. The confirmation of a user's claimed identity is a crucial step before exchanging any confidential data between the two parties. The transfer of any sensitive data or passwords should be shielded from snooping attacks.

In order to conquer the limitations of text-based passwords, we propose a hybrid multi-mode authentication to strengthen text passwords by combining them with images for increased security. The proposed method uses Image Steganography to prevent eavesdropping during transmission of password. An algorithm for Image Cryptography is proposed to encrypt the image into two shares. A Knowledge based Image CAPTCHA will further authorize a valid user.

2. RELATED WORK

2.1 Authentication Scheme for Generating Session Passwords using Color and Images

The authentication technique explained in [1] is based on color and textual passwords for generating a different password for every login session. Such a technique is resistant to dictionary attack and shoulder-surfing. In order to generate a password during registration, the user rates the given colors. During login, a random color grid of 4 pairs of color is displayed along with a random number matrix in Fig 1. Each pair of color represents the row and the column of the grid. Depending on the ratings given to the colors during registration, the user is expected to select the numbers from the matrix to generate the session password. The drawback in this hybrid approach lies when a hacker makes a number of attempts to login in order to guess and learn the color rating pattern.



	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Fig. 1 Matrix Grid for Generating Session Passwords [1]

2.2 Multi Dimensional Password Generation Technique

A strong password generation technique explained in [2] was proposed for cloud computing where an authorized user can use the services on the cloud. This technique aims at generating a multidimensional password based on the input parameters provided by user, using text and images. The system reads the text and extracts features from the given input images and generates textual password which is a sequence of the input parameters. Such passwords are lengthy and difficult to remember.

2.3 Authentication Using Persuasive Cued Click-Points

A Cued Click-Point technique explained in [3] allows the user to select one point in each of the random N images presented to user during password generation. A click on an image would generate the next image. During authentication, the user is expected to remember the points clicked on those images to generate the same series of images shown in Fig. 2.

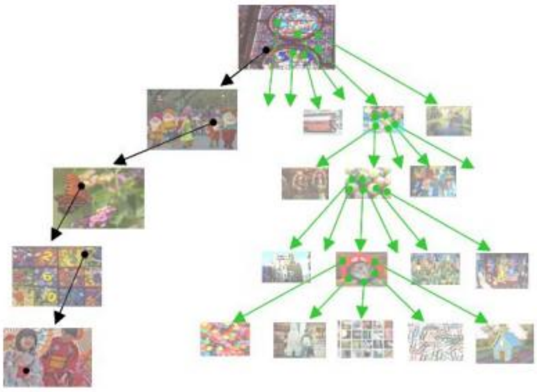


Fig. 2 Cued Click Points [3]

In the Cued Click-Point technique different users seldom selected the same predictable points and anyone could easily crack the password. A technique called Persuasive Cued Click-Point explained in [3] was suggested with regard to this, where the system randomly selected a viewport area on the image and the user was asked to select points within the viewport. Such a feature encourages users to select less predictable passwords. The limitation of using a click point technique requires storing multiple images to authenticate a single user.

2.4 Image Based Authentication using 3-Level Security System

The technique mentioned in [4] uses a 3-level security system which is a text based authentication at first level, image based authentication at second level followed by generation of one time password for every session at level three .The one time password is sent on the email id of the authorized user. Once a text password was matched at level one, the user was asked to click points on the image in level two. If a hacker was trying to login he would have successful attempts during the first two levels, if he knew the text password and image click points. But his attempt would fail when he would be asked to enter the one time generated session password sent on the authorized user’s email id. Remembering the click points for different images is a difficult task.

2.5 Biometric Authentication System

Biometrics verify a person's uniqueness by analyzing his physical features which include facial analysis, fingerprint, hand geometry, retinal analysis or behaviors like signature, key stroke, and voice. Biometric recognition systems mentioned in [5] work in two modes: Enrollment mode where the system captures the biometric trait into the database, and authentication mode where the system verifies a person's claimed identity from his earlier enrolled pattern. Biometric authentication may fail in cases of damage or changes in the physiological characteristics of a person in cases of accidents.

2.6 Visual Cryptography

Visual Cryptography was introduced in 1994 by Noar and Shamir mentioned in [6] is scheme to secure images by encrypting the images into shares so that it is unreadable for an intruder. The image shares are created from the original image which are garbled or encrypted such that the overlapping of the shares would reveal the secret image. The overlaid shares are decrypted by the human visual system.

The various techniques for Visual Cryptography are mentioned below:

2.6.1 Visual Cryptography for Monochrome Images

Visual Cryptography for monochrome images was divided into a number of schemes mentioned in [7] are as follows:

- (2, 2) Visual Cryptography Scheme: Encrypts original image into two shares and secret image is revealed when both the shares are stacked.
- (2, n) Visual Cryptography Scheme: Encrypts the secret image into n shares and secret image is revealed when any two shares are stacked.
- (n, n) Visual Cryptography Scheme: Encrypts the secret image into n shares and secret image is revealed only when all n shares are stacked.
- (k, n) Visual Cryptography Scheme: Encrypts the secret image into n shares and secret image will be revealed only when any group of at least k shares are overlaid.

In these schemes, every pixel in the original secret image is replaced by a 2* 2 block of four pixels [8]. These scheme lead to pixel expansion and therefore the image shares created would be larger than the original image shown in Fig. 3.And hence the revealed secret image wouldn’t be the of the same size as that of the original image.

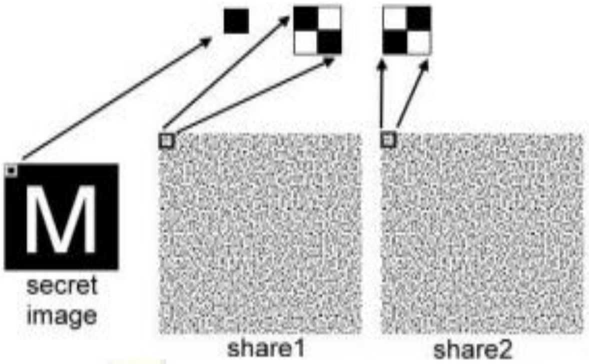
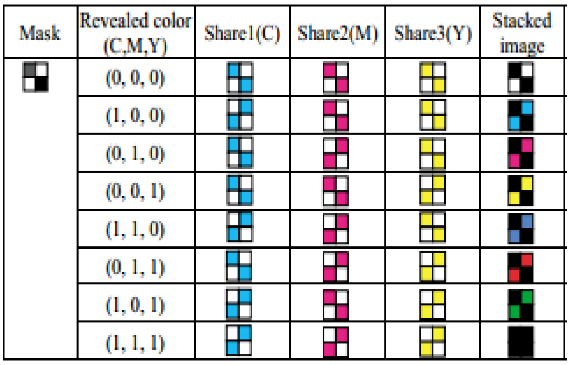


Fig. 3 (2, 2) Visual Cryptography Scheme [8]

2.6.2 Visual Cryptography for Colored Images

Hou had proposed a Visual Cryptography scheme for colored images explained in [9]. This scheme transforms the colored image to CMY color model. Fig. 4 shows the color scheme where a mask is set .For every color component not present in the revealed color; the share was created in the orientation based on the mask set. The original pixel is decomposed into CMY shown in Fig. 5. For each decomposed pixel, 2*2 block shares are created based on the color scheme. Then the blocks $C1_{ij}$, $M1_{ij}$ and $Y1_{ij}$ were combined to form Share 1. Similarly the blocks $C2_{ij}$, $M2_{ij}$ and $Y2_{ij}$ were combined to form Share 2.Later, Share 1 and Share 2 were combined to reveal the secret image.

In colored image visual cryptography, the computational complexity increases because the process for revealing the secret image involves creating more number of shares at various levels as shown in Fig. 5.The revealed secret image has undergone expansion and is not the exact copy of original image.



Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image
	(0, 0, 0)				
	(1, 0, 0)				
	(0, 1, 0)				
	(0, 0, 1)				
	(1, 1, 0)				
	(0, 1, 1)				
	(1, 0, 1)				
	(1, 1, 1)				

Fig. 4 Color Scheme [9]

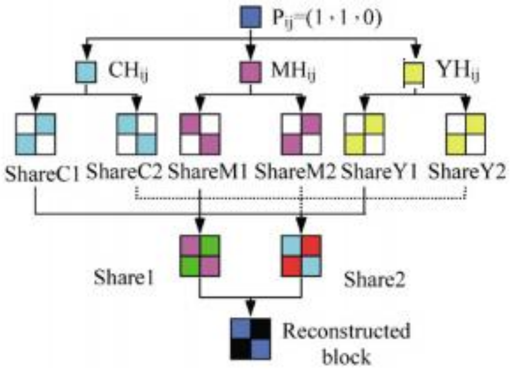
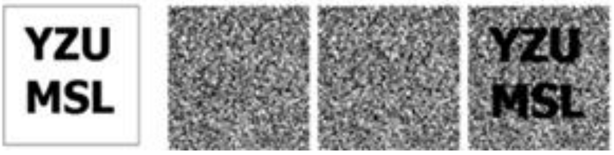


Fig. 5 Color Visual Cryptography [9]

2.6.3 Expansionless Visual Cryptography for Binary Images

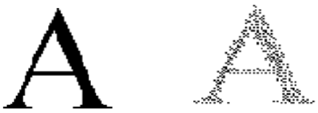
A Visual Cryptography scheme is mentioned in [10] using random grids for binary images. The shares are created without any expansion. The algorithm generates a random grid G1 (share 1) which has the same dimension as that of original image. If a pixel p in the original image is a black then copy the corresponding pixel of G1 to the corresponding pixel of G2 (share 2). If p is a white pixel, assign the complement value of the corresponding pixel of G1 to the corresponding pixel of G2 (share 2). When both shares are overlaid, the pixels that are identical in both grids would look grey, and the shares with opposite states will be black. The resultant image was of the same size as that of the original image shown in Fig. 6.The only limitation was that the revealed secret image had a greying effect.



a) Original Image b) Image Shares c) Revealed Image

Fig. 6 Color Visual Cryptography [10]

A novel idea of hierarchical visual cryptography stated in [11] is an expansion less scheme for binary images. The idea is that the shares are produced in levels. The shares are generated using the 2*2 block replacements. Two shares (S1, S2) are produced at this level, which is level one. Each share is then divided into two shares by the same methodology to (S11, S12), (S21, S22). This is level two where four shares are produced. Any three shares are collectively taken combined using inference rules [11] to form the key share. The key share was than stacked on the remaining share. The greying effect is completely removed in the revealed secret image. The concentration of white and black pixels in the revealed image is different from that of the original image shown in Fig. 7.



a) Original Image b) Revealed Image

Fig. 7 Hierarchical Visual Cryptography [11]

2.7 Image Steganography

2.7.1 Least Significant Bit Substitution

Image Steganography using Least Significant Bit Substitution mentioned in [12] focuses on substituting the secret information bit into the least significant bit of each pixel of the image .If an image is 24 bit image, made of three components: red, green and blue, then each of them will constitute of 8 bits. The data to be embedded will be substituted onto the least significant bits of each 8 bit RGB representation. LSB substitution is an inefficient method for hiding data in binary images as it would be easily detectable.

2.7.2 Edge based Detection for Image Steganography

Image Steganography based on edge detection explained in [13] focuses on detecting the edges of a particular image for inserting the secret data. A contour is traced at the edges to find the orientation or edge direction. Based on the direction, the location for embedding the secret would be known. The yellow colored pixel indicates the data carrying pixel Fig. 8. The drawback is that any edge base detection technique can be easily traced to get the information.

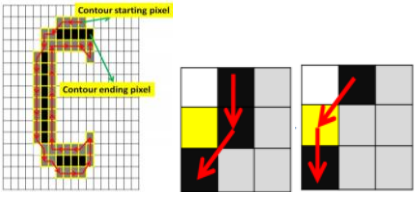


Fig. 8 Steganography using Edge Detection [13]

2.7.3 Parity Checker for Image Steganography

Image Steganography technique mentioned in [14] uses parity checker for individual pixels for inserting in the least significant bit.

The algorithm is as follows:
Step 1: Do not modify pixel with all 0s or 1s
Step 2: Embedding data:
a) To insert 0 into a pixel, check pixel parity
i) If odd parity do nothing
ii) If even parity, then make pixel parity odd by substituting 0 or 1 onto the LSB
b) To insert 1 into a pixel, check pixel parity
i) If even parity do nothing
ii) If odd parity, then make pixel parity as even by substituting 0 or 1 onto the LSB
Step 3: Extraction of data:
For every pixel of the stegged image, check the parity
i) If odd parity, then bit is 0
ii) If even parity, then bit is 1

2.8 CAPTCHA

CAPTCHA (Completely Automatic Public Turing test) to tell Computers and Humans Apart was introduced to improve information security. A CAPTCHA system must satisfy the following three conditions: (1) Humans should recognize the contents and pass it easily. (2)It is invoked to prevent robots to pass the system or to prevent attacks from unauthorized access. (3)It should be generated easily and quickly

The different types of CAPTCHA explained in [15] are as follows: 1) Text-based CAPTCHA; 2) Image-based CAPTCH; 3) Audio-based CAPTCHA 4) Mathematical and Knowledge Based CAPTCHA.

3. PROPOSED METHOD

The proposed model focuses on a framework for authentication using binary images for securing text passwords. Performing attacks on images is comparatively difficult than text, therefore the risks on data can be minimized. Least Significant Bit Steganography in black and white images can be easily detectable. Also Edge Detection Steganography can be detectable easily with edge detection algorithms. Therefore a random image mask based algorithm is proposed for embedding text in binary image. The above related work on Visual Cryptography cannot be used in the proposed methodology since the decrypted image reveals the secret image but the concentration of white and black pixels vary from original image. The proposed algorithm for Image Cryptography requires the revealed image to be an exact match of the original image without expansion to secure the text embedded. The authentication also supports knowledge based image CAPTCA.

The process for password generation in the proposed approach starts at client side. The user needs to select an image and enter alphanumeric text password. The system will convert the image into a bitmap lossless binary image format. A binary image that is fully white or fully black will not be considered and will be notified to the user to select another image. A complete black or complete white image is not supported by the proposed algorithm for Image Steganography. The symmetric secret key will be exchanged prior to the password generation between the client and the server. This key will be exchanged using any existing key exchange algorithm and will further be used along with text password to generate the actual text password that will be sent across to the server. For secure password transmission, the system then performs Steganography on the image using the below proposed algorithm. The server splits the image into two shares using the algorithm mentioned below for Image Cryptography. One share is saved on the server while the other is sent to client. An image share which is sent to the client by the server will be directly saved in a directory on the client’s system and later notifying the client about the saved image path in the system files.

During authentication the client needs to select the image share sent to him earlier with the text password he had typed during password generation. The image share and the text password are sent to the server for authentication only after the user is validated for entering the knowledge based image CAPTCHA correctly. Now the server will generate the actual text password using the secret key and the password sent by user during authentication. The client share is stacked over the server share at the server. The text extracted from the stacked image should match the actual text password generated at the server to authenticate the valid user. Both the image shares have to be of the same corresponding image, generated during password generation for a valid authentication to take place.

The proposed approach for Password Generation is shown in Fig. 9.

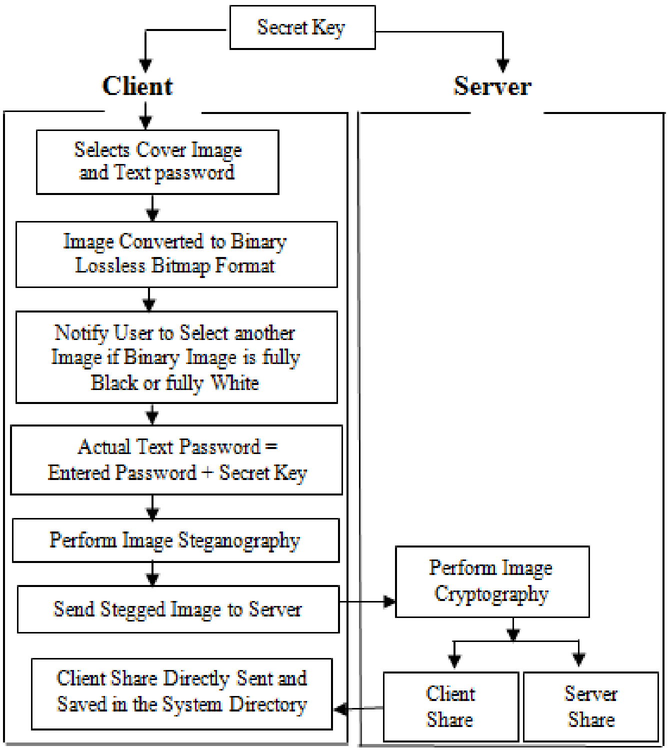

Secret Key
Client
Server
Selects Cover Image and Text password
Image Converted to Binary Lossless Bitmap Format
Notify User to Select another Image if Binary Image is fully Black or fully White
Actual Text Password = Entered Password + Secret Key
Perform Image Steganography
Send Stegged Image to Server
Client Share Directly Sent and Saved in the System Directory
Perform Image Cryptography
Client Share
Server Share

Fig. 9 Proposed Password Generation

The proposed approach for Authentication is shown in Fig. 10.

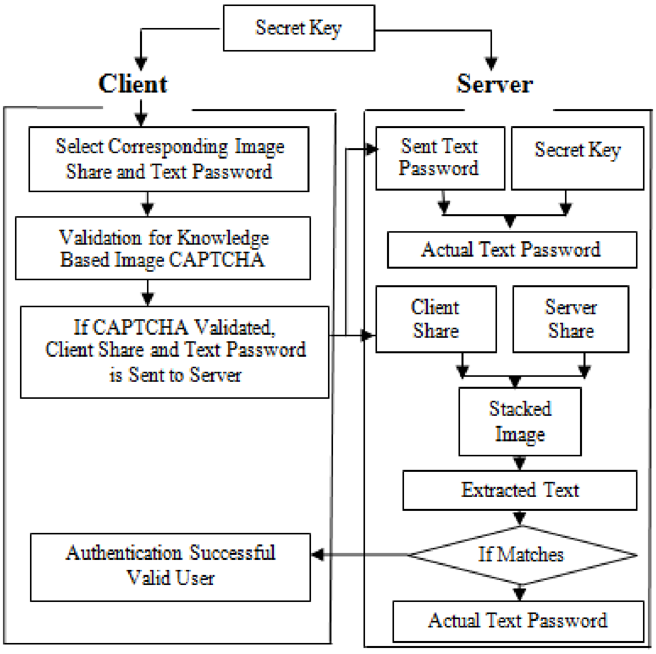

Secret Key
Client
Server
Select Corresponding Image Share and Text Password
Validation for Knowledge Based Image CAPTCHA
If CAPTCHA Validated, Client Share and Text Password is Sent to Server
Authentication Successful Valid User
Sent Text Password
Secret Key
Actual Text Password
Client Share
Server Share
Stacked Image
Extracted Text
If Matches
Actual Text Password

Fig. 10 Proposed Authentication

3.1 Generation for Actual Text Password

The client and the server will have a shared secret key exchanged using any Key Exchange Algorithm. This key will be XOR'ed with text password entered by user and later truncated to garble the actual password to be inserted. An example is shown below:

Consider: Entered Password: pswrd123; Secret Key: qkn32
X-OR of q: 01110001 with p: 01110000 is 00000001
X-OR of k: 01101011 with s: 01110011 is 00011000
X-OR of n: 01101110 with w: 01110111 is 00011001
X-OR of 3: 00110011 with r: 01110010 is 01000001
X-OR of 2: 00110010 with d: 01100100 is 01010110
X-OR of q: 01110001 with 1: 00110001 is 01000000
X-OR of k: 01101011 with 2: 00110010 is 01011001
X-OR of n: 01101110 with 3: 00110011 is 01011101

The Actual text Password is obtained after truncating the common bits from the XOR'ed result. .By scanning the bits horizontally the total length of Actual Text Password is 56 bits. The length of the actual text password generated will vary for every password generation.

3.2 Proposed Algorithm for Image Steganography

Encoding Algorithm:

Step 1: Divide the binary image into non-overlapping blocks equal to the total number of bits in the Actual Text Password.
The creation of blocks for every image will be randomized based on the length of the Actual Text Password.

Step 2: Let n be the number of blocks with fully black or fully white pixels. No insertion will be done in such blocks. Scanning from the start, alternate bits (odd/even) have to be omitted for insertion n number of times from the password to form the new Actual Text Password.

Step 3: Insertion of message bits

For Each Block

If pixels are all white or all black

Then skip the block for bit insertion

Else

Find parity (count) of the black pixels in the block

a) To insert bit "0"

i) If odd parity then skip the block and the bit

ii)If even parity, then make pixel parity as odd by changing a pixel within the block

b) To insert bit "1"

i)If even parity then skip the block and the bit

ii) If odd parity, then make pixel parity as even by changing a pixel within the block

Step 4: To change a bit, find a location within the block. Consider a 3*4 block B to insert bit "0". Block B has even parity, so we need to change the pixel parity to odd. If we randomly select any location in block S, we can easily detect the changed bit shown highlighted in Fig. 11.

B=

1	1	0
1	1	0
1	0	0
1	0	0

S=

1	1	0
1	1	0
1	0	0
1	0	1

Fig. 11 Location for Pixel Parity Change

In order to get an efficient location to change a pixel, find neighboring pixels that will have same value after the pixel is changed within the block.Block B' gives the pixel neighbourhood correlation. Select the highest and the first correlation numeric to change bit in Block S' in Fig. 12. The highlighted area indicates the location to change the pixel bit. Block S' now has odd parity.

B'=

0	2	2
1	4	2
2	4	1
2	2	0

S'=

1	1	0
1	0	0
1	0	0
1	0	0

Fig. 12 Neighbourhood Pixel Correlation

Step 5: Continue the above step for all message blocks and send the stegged image to receiver.

Decoding Algorithm:

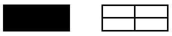
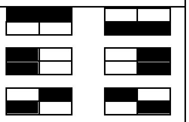
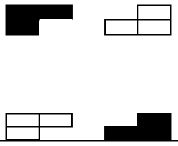
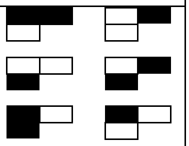
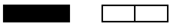
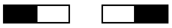
Step 1: Divide the image into blocks based on the Actual Text Password generated on the server.
Step 2: If all pixels in a block are white or all black, then no bit is extracted
Step 3: If odd parity in the block, then bit extracted is "0"
Step 4: If even parity in the block, then bit extracted is "1"

3.3 Proposed Algorithm for Image Cryptography

Encoding Algorithm:

Assumption: Black Pixel=Bit "1; White Pixel=Bit "0"
Step 1: Divide the image into 2*2 non-overlapping blocks.
Step 2: For every block, scan horizontally the pixels and group similar colour pixels together.

Table 1: Mask for Share Creation

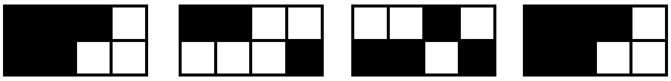
Count of Similar Color Pixels	**Block of Similar Pixels**	**Masks**
All Four Pixels		
Three pixels		
Two Pixels		
One Pixel		

Step 3: For every group of similar pixel, create shares using random masks shown in Table I. The masks for three pixels can be tilted as per the orientation of block of similar pixels.

Decoding Algorithm:

Step 1: A simple XOR operation is performed on the created shares for every pixel to reconstruct the original image.

The original image along with the shares created is shown in Fig. 12.The reconstructed image is same as original.



a) Original Image b) Image Shares c)Reconstructed Image

Fig. 12: Image Cryptography

3.4 Algorithm for CAPTCHA

The proposed work focuses on integrating two types of CAPTCHA i.e. Image and Knowledge based. The algorithm for Image based Knowledge CAPTCHA is as follows:
Step 1: The server generates a pseudorandom alphanumeric string along with a knowledge based question on the Sum of Subsets.
Step 2: The randomly selected alphanumeric string will be converted to a noise based colored image making it difficult for programs to identify the characters in the image. The characters will be tilted, distorted and overlapped. This will prevent the CAPTCHA from OCR attacks. Any program that tries to break the CAPTCHA has to first identify the characters from the noisy image, then analyze the question on sum of subsets and answer to it correctly. A robot will take more time to decode such a CAPTCHA than a human.
Step 3: The user will be asked to enter the two digits from the alphanumeric string that would form the requested sum sent from the server. If the answer is correct, the user will be considered valid user.

4. CONCLUSION AND FUTURE WORK

The proposed technique for password generation assures password confidentiality since a partial text password in an encrypted image share is saved on the systems. Any user trying to authentication himself using any image other than the required image share will not be authenticated. Any attack on the systems trying to snoop the password will be of no use as it would give an access only to a partial password. The proposed authentication framework can be used to transfer confidential messages. These secret messages will be never saved on any system. If an intruder has compromised the saved image shared on the system, then the authentication will fail. But since the authentication is based on a one time communication framework, such an attack will be useless, as the messages transferred earlier were never saved and no data would be lost. In such a situation the user can register him again.

This authentication framework can be extended for random key generation using the image share and image CAPTCHA to transfer the secret message intended to the recipient. The key would be generated by extracting features from the images. Every message sent will be encrypted and secured with a new and different key, as the image share would remain the same but image CAPTCHA would be different for every message transfer. Such randomness in the key would secure the secret message to be communicated.

REFERENCES

[1] M Sreelatha, M Shashi , M Anirudh ,MD Sultan Ahamer and V Manoj Kumar, “Authentication Schemes for Session Passwords using Color and Images,” in *International Journal of Network Security & Its Applications* , Vol.3, No.3, May 2011.

[2] Dinesha H A and Dr.V.K Agrawal, “Multi-Dimesional Password Generation Technique For Accessing Cloud Services,” in *International Journal on Cloud Computing: Services and Architecture* (IJCCSA), Vol.2, No.3, June 2012.

[3] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C.van Oorschot, “Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism,” in *Dependable and Secure Computing*, IEEE Transactions Vol. 9, No. 2, March/April 2012.

[4] Surabhi Anand, Priya Jain, Nitin and Ravi Rastogi, “Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication,” in *14th International Conference on Modelling and Simulation*, 2012.

[5] Smita S. Mudholkar , Pradnya M. Shende and Milind V. Sarode, “Biometrics Authentication Technique For Intrusion Detection Systems Using Fingerprint Recognition,” in *International Journal of Computer Science, Engineering and Information Technology* (IJCSEIT), Vol.2, No.1, February 2012.

[6] M. Noar and A. Shamir, “Visual cryptography,” in *Advances in Cryptology - EUROCRYPT'94*, pp. 1-12, 1995.

[7] Debasish Jena and Sanjay Kumar Jena, “A Novel Visual Cryptography Scheme” in *International Conference on Advanced Computer Control*, *IEEE*, pp. 207 – 211, 2009.

[8] Jagdeep Verma, Dr.Vineeta Khemchandani , “ A Visual Cryptographic Technique to Secure Image Shares,” in *International Journal of Engineering Research and Applications* (IJERA) , Vol. 2, Issue 1,Jan-Feb 2012, pp.1121-1125.

[9] Young-Chang Hou,*“*Visual cryptography for color images,” in Journal *of Pattern Recognition Society, Pattern Recognition*, pp 1619–1629,2003

[10] Ran-ZanWang , Yung-Ching Lan, Yeuan-Kuen Lee , Shih-Yu Huang , Shyong-Jian Shyu and Tsorng-Lin Chia , “Incrementing visual cryptography using random grids,” in *Elsevier, Optics Communications*, Jan 2010,pp 4242–4249.

[11] Pallavi Vijay Chavan, Dr. Mohammad Atique and Dr. Latesh Malik, “Design and Implementation of Hierarchical Visual Cryptography with Expansion less Shares,” in *International Journal of Network Security & Its Applications*, Vol.6, No.1, January 2014.

[12] Mr. Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi and Saurabh Singh Gangwar, “Image Steganography Using Least Significant Bit With Cryptography, in *Journal of Global Research in Computer Science*, March 2012,pp. 53-55.

[13] Krupali V. Deshmukh, and Prof. Gyankamal J. Chhajed, “A Steganographic Method for Data Hiding in Binary Image using Edge based Grids**,”** in *International.Journal of Computer Technology & Applications*,Vol 5 ,1369-1374.

[14] Rajkumar, Rahul Rishi and Sudhir Batra, “A New Steganography Method for Gray Level Images using Parity Checker,” in *International Journal of Computer Applications* (0975 – 8887) ,Volume 11– No.11, Dec 2010.

[15] Amalu James, Geo George and Asha Yeldose, “A Survey on Spelling Based CAPTCHA,” in International *Journal of Research in Computer and Communication Technology*, 2014.