User Authentication Using Image Processing Techniques

Dr. Nagabhushana
Department of Computer Science & Engineering, S.J.M.I.T Chitradurga, Karnataka-577501
Email: hod.cse@sjmit.ac.in
Dr. Aravinda T V
Department of Computer Science & Engineering, S.J.M.I.T Chitradurga, Karnataka-577501
Email: arvind_cta@yahoo.co.in
Nataraja B S
4th Semester, M.Tech., Department of Computer Science & Engineering, S.J.M.I.T Chitradurga.
Email: nataraja.bs@gmail.com

---ABSTRACT---

Conventional password transformation plot for client authentication in order to provide access to the system is to change password into some form of hash esteems. These secret word plans are nearly straightforward as well as quick in light of the fact that those depend on content and famed cryptography. In any case, those can be presented to digital assaults using secret key by cracking device or hash-breaking on the web locales. Assailants can altogether make sense of a unique secret word from hash esteem if it is generally basic and clear. Therefore, numerous hacking mishaps are happening transcendentally in frameworks receiving these hash oriented plans. This project recommends an upgraded secret word preparing plan in view of picture utilizing visual cryptography (VC). Not the same as the customary plan in light of hash and content, the proposed system changes a client identification word of plain text type into 2 pictures encoded by Visual Cryptography. The server just saves client identification word and one of the pictures rather than secret key. At the point when the client sign in and upload the other picture, then server extracts client identification word by using OCR (Optical Character Recognition). Thus, it confirms client through contrasting extricated ID and spared one. This proposed system has bring down calculation, counteracts digital assault went for hash splitting, and underpins confirmation not to uncover individual data, for example, ID to assailants.

Keywords **- Visual cryptography, user authentication, password processing, hash, OCR, multimedia.**

Date of Submission: June 28, 2018 Date of Acceptance: July 30, 2018

I. INTRODUCTION

Secure Information Storage and Communication assumes a fundamental part in the digital Age. All the Financial and Banking applications were moving towards cashless exchanges. In this way the information, passwords, reports and other essential data must be secured from exposure. PCs and mobiles are being utilized for information handling, stockpiling, recovery and communication of data.

This proposed system suggests user authentication using image processing techniques based on VC encrypted image. This image consists of the user authentication information.

Thinking about password as a mystery picture, it is partitioned into two shares utilizing anyone of the Visual cryptography methods. As both the shares look as irregular pixels, they can be covered up in a cover picture and imparted to the authenticated user. At the collector side, the shares can be extracted from the cover picture and consolidated to get back the original picture secret key. It is discovered that the Visual Cryptography is unbreakable [1]. Thus it assures the security of the password in the form of shares from the intruders. As a visual cryptography technique is used, if the cover file is captured by the intruder, it is difficult to suspect the hidden data [2].To authenticate the user this scheme user OCR [6] to extract the hidden data inside the image. The intention of this proposed system is to prevent cyber attack and support more secured user authentication and preserve the privacy of user personal data.

II. LITERATURE REVIEW

A. Visual Cryptography [1]

Naor and Shamir proposed the VC in 1994, which is a kind of image cryptography having little calculation. The VC method creates two images from unique image which contains the secret information by changing over every pixel. The newly created images look like a noise or gray. Instead of the Original picture, the VC encrypted images are shared to others. In the event that you again need to see unique picture, you assemble and stack up the VC encrypted images, at that point we can get the original picture. Unmistakably it has brought down computational cost of encryption compared to other cryptography techniques. Decryption technique does not need any calculation since it is reliant just without hesitation of human.

B. OCR: Optical Character Recognition [9][10]

OCR is the technique used to convert the printed or composed text into editable text. It is largely used in broad daylight workplaces, for example, banks, polices, hospitals, and so on. Individuals can perceive the content from the image, yet really the brain that performs procedure to translate the image read by eye. There are few OCR algorithms to make use of this in machine.

C. Persuasive Text Passwords [3]

Text-based secret key is generally considered as the most universal confirmation conspires in PC frameworks these days. In any case, content based passwords are helpless against a few assaults, for example, brute-force assault and dictionary-based assault. Thusly, many have concentrated on improving the security quality of Text-based secret word. The persuasive Text password (PTP) is a strategy to enhance secret word quality by adding some irregular characters to client's secret word. This method contrast PTP and some basic secret key arrangements. On account of this, a few imperfections of PTP are resolved. A change of PTP is proposed to reduce its disadvantages. The change is actualized by joining PTP with a secret word approach. The test comes about demonstrate that the new form of PTP is superior to the first form in both security and ease of use.

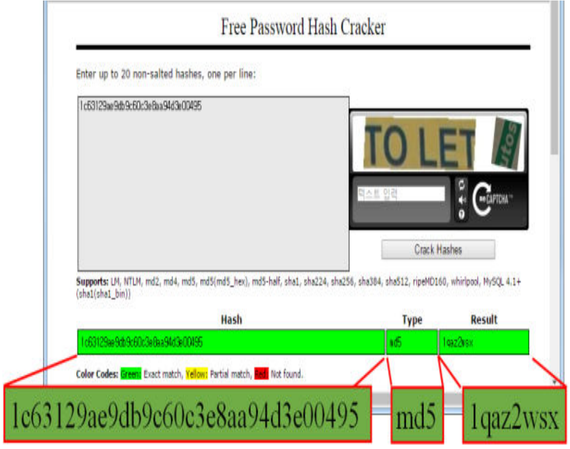
III. EXISTING SYSTEM

The list of existing user authentication methods is as follows:

- An ID (Identification)/Password: To Open a session on a computer or to authenticate on internet, the authentication is done by verifying whether the password matches with the user name stored in the database.
- A PIN (Personal Identification Number) Code: Here a unique PIN number is assigned to users. That is matched with the user credentials stored in the database.
- An RFID Card: Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. The tag contains electronically-stored information.
- A Fingerprint: Fingerprint recognition refers to the automated method of identifying or confirming the identity of an individual based on the comparison of two fingerprints for authentication on computerized system.
- A Facial Recognition system with a Webcam: Facial recognition is also a form of biometric authentication; face recognition algorithms identify facial features by extracting points of interest, or highlights, from a picture of the subject's face.
- A One Time Password Token: OTP Verification module verifies Email Address/Mobile Number of users by sending verification code (OTP) during registration. It removes the possibility of a user registering with fake Email Address/Mobile Number.

The most common and followed method is text based An ID (Identification)/Password, which works as follows.

User authentication by and large frameworks have continued fundamentally through check of the user ID and his/her password. This traditional method, to send and check password, uses a hash-based password conspire that changes original password to hash value by some functions. The Advantages of this system are that it is easy to fit in the system and processing speed is fast because of the text based processing of the hash functions like MD5, SHA256. Be that as it may, it is helpless against attacks, for example, dictionary-based attack or brute force attack clearly by secret key cracking tool or hash-cracking on the web locales. Accept that somebody have the secret word "1qaz2wsx" in a framework. On the off chance that an assailant knows hash value "1c63129ae9db9c60c3e8aa94d3e00495", the value can be adequately split essentially by free break site as shown in **figure 1**. Even though the attacker doesn't have any knowledge about hash function utilized in the system, he or she can easily figure out which kind of hash function is used in the system. As the outcome, the attacker can make auxiliary harm to the system.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

1c63129ae9db9c60c3e8aa94d3e00495

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin))

Hash	Type	Result
1c63129ae9db9c60c3e8aa94d3e00495	md5	1qaz2wsx

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Fig 1: "crackstation.net" used to crack password.

Users have the responsibility on this kind of attacks [3]. At the point when a researcher asked to numerous individuals about secret key management practices, a great many people reacted with the accompanying five adverse behaviors:[4]

1. Picking a PC secret key out of the blue.
2. Barely changing a secret key.
3. Letting another person utilize claim secret key.
4. Writing their secret key next to the PC.
5. Offering a secret word to family, companions or collaborators.

Another significant cause is utilizing of simple passwords. For security of passwords the contributing factors includes length of password, reuse of password, changing frequency of password, entropy level and uniqueness of the password. The **figure 2** shows how users deal with the password over fulfilling the above mentioned factors.

First graph (a) indicates 45.16% (14 of 31) of people replied with reuse of own password. Graph (b) shows the length of passwords used by the people. Graph (c) shows how user makes out password and Graph (d) shows the password change frequency.

Significantly those practices end up frail point and influence entire framework. Numerous researchers have enhanced hash based secret word conspire into the blend of watchword and a few salts in the hash function. But these enhanced methods also didn't prevent the password hacking attacks like birthday attack [5]. In see not quite the same as text-based plan, we propose upgraded user authentication scheme in light of an image made by VC. This image contains user secret information.

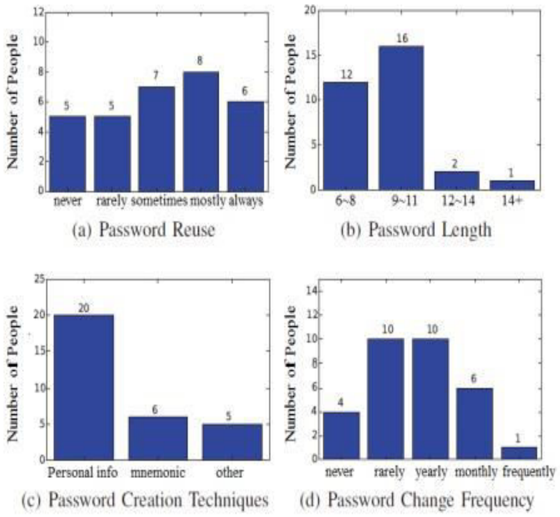


Fig 2: Survey result about password security factors [4]

A. *Visual Cryptography Phase*

The binary password image is taken. Using conventional visual cryptographic technique, it is divided into two shares with pixel expansion.

This method is as follows:

S0 = all the matrices obtained by permuting the columns of $\begin{bmatrix}1 & 0 & 1 & 0\\ 1 & 0 & 1 & 0\end{bmatrix}$ Thus

S1= all the matrices obtained by permuting the columns of

$$\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\end{bmatrix}$$

S0 represents sub pixels of a white pixel and S1 represents sub pixels of a black pixel. One of the matrixes S0 or S1 is selected, depending on the pixel value of the source image. Each row data is put as 2X2 matrix form in the generated share. The number of rows indicates the number of shares to be divided and number of columns indicates the pixel expansion (Here 4.i.e, 2X2)[8].

A cover image of size twice of the image share is taken. The first share is placed in the least significant bit plane and the second share is placed as continuation in the least significant bit plane of the cover image. The receiver gets the cover image.

Figure 3 gives a clear picture of Phase 1 and **Figure 4** gives the process of extraction of password.

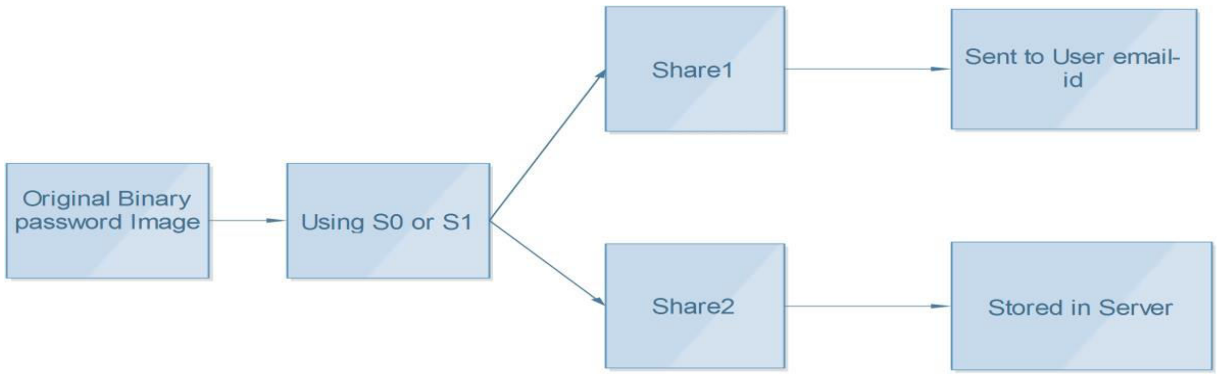


Fig 3: Division and embedding the image shares in the cover image

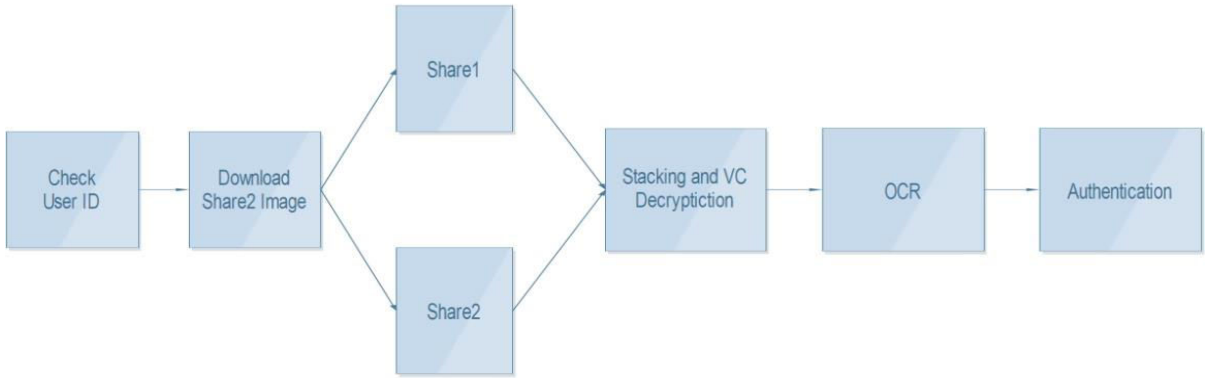


Fig 4: Extraction of Embedded image shares and then password image

B. OCR Phase: Recovery/ Extraction of password

At the beneficiary end, the bits of the LSB plane of the cover picture are extricated into 2 shares. OR operation is performed on the separated shares and complemented. The secrete key is recouped. In any case, according to the calculation 50% of the white pixels in the first secret word picture will be turned to grey.

The Objectives of the proposed method are:

1. Provide Secure user authentication
2. Prevent cyber attack and support privacy of personal information.

V. IMPLEMENTATION

Firstly, the admin has to register the user to server system. For that, admin has to construct an original image which has white background and black letters. During registration the Server create Share1 and share2 images from Original password image using SEED function of VC encryption methods. Then share2 image is saved in server and share1 image is sent to the user mail-id. During login the user sends ID of text type and the share1 image instead of password to the server. The server stacks up the stored share2 image and the user input share1 image, to obtain the original image [7]. Then OCR operation is performed to obtain the text stored in the image. If the extracted text matches with the saved user Id then the user is securely authenticated. Otherwise authentication is unsuccessful.

The user registration process follows the following algorithm:

Step 1: Input user profile Information.
Step 2: If new user then
Server creates the Original password image and stores it.
Else go to step 1.
Step 3: Server create Share1 and share2 images for Original password image using VC Encryption.
Step 4: Send the share1 image to the user and save share2 image in server.
Step 5: return user registration successful.

The user Authentication process follows the following algorithm:
Step 1: Check User Id.
Step 2: Input share1 and share2 images.
Step 3: Stack Up Share1 and share2 images and Perform VC Decryption.
Step 4: Perform OCR to extract string (User ID) from new image.
Step 5: If extracted ID corresponds with saved ID then
Return Authentication successful
Else
Return Authentication successful.

The **figure 5** and **figure 6** shows the Flowchart of the User registration process and User Authentication process respectively.

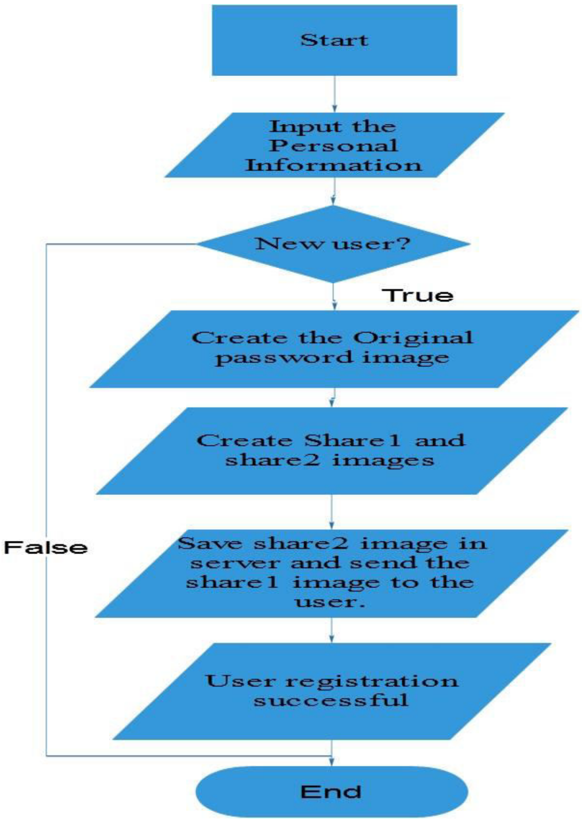

Start
Input the Personal Information
New user?
True
False
Create the Original password image
Create Share1 and share2 images
Save share2 image in server and send the share1 image to the user.
User registration successful
End

Fig 5: Flowchart of User Registration Process

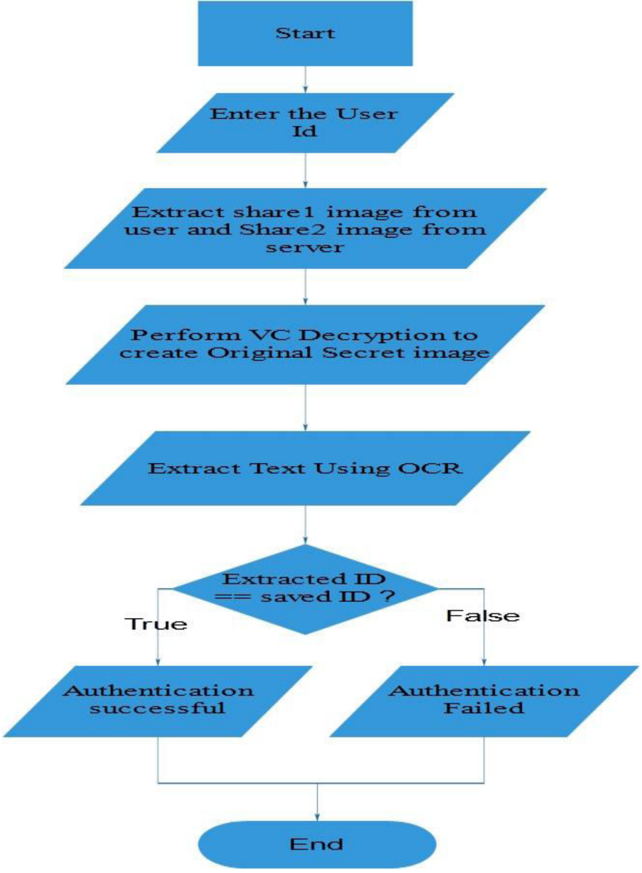
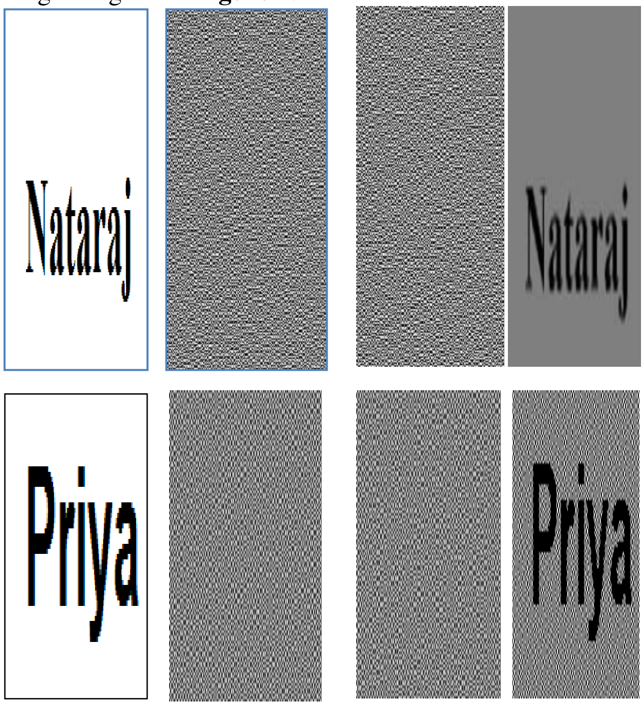

Start
Enter the User Id
Extract share1 image from user and Share2 image from server
Perform VC Decryption to create Original Secret image
Extract Text Using OCR
Extracted ID == saved ID ?
True
False
Authentication successful
Authentication Failed
End

Fig 6: Flowchart of User Authentication Process

The original password image and the shares of the image are given in **figure 7.**



A)Original Password

B)First Shared Image

C)Second Shared Image

D)Extracted Password Image

Fig 7: Results showing Original and share images

The eclipse tool is used for implementing the visual cryptography part by utilizing java programming language. And password hidden in the image is extracted using the open source OCR tool Tesseract.

VI. COMPARITIVE STUDY

The comparison of various User Authentication Methods with the proposed method in terms of time required for processing is shown in Figure 8.

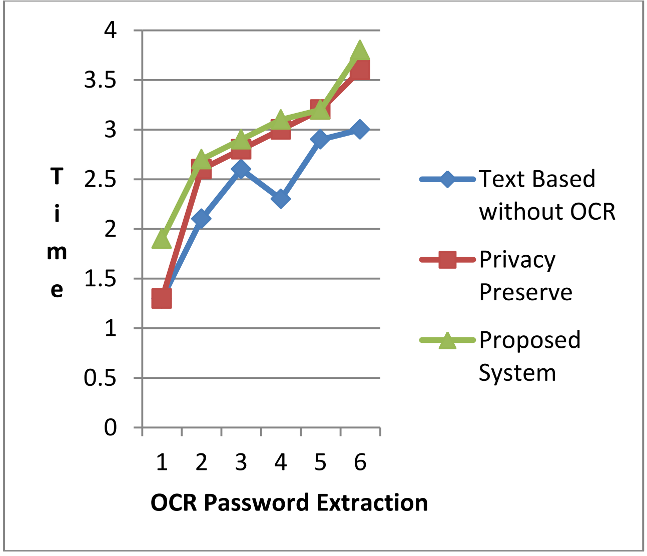


Fig 8: Graph showing comparison of various User Authentication Methods

When proposed method is compared with the existing systems in terms of memory consumption, both consume almost same amount of memory but the proposed method consumes slightly more because of the images involved in it rather than the text based password. The share2 image which is generated when user tries logs into the system is of no use after the user is successfully authenticated and is deleted. So there is not much of a difference with memory utilization. And regarding the accuracy, the proposed method is most accurate than the existing methods because it ensures that

- During user login time, login image is generated at the server and sent to the user's registered mail id.
- The server takes short span of time to deliver login image to the registered user and ensures the delivery of mail.

VII. CONCLUSION AND FUTURE ENHANCEMENT

In this paper we presumed that online attacks have been expanded. Here user authentication using image processing techniques is implemented. The password picture is isolated into two shares utilizing the traditional visual cryptography method. The server just has client's ID and one of the pictures rather than secret key. When the client sign in and input other picture, the server separate ID by using OCR. Subsequently, it can verify client by obtained ID and the spared one. The proposed method has brought down computation, reduces cyber-attacks and supports secure user authentication.

FUTURE ENHANCEMENT

The future work is to implement user authentication by using coloured original image instead of the black and white this method used.

REFERENCES

[1] Noar M., Shamir A., Visual cryptography: Advances in Cryptography, Eurocrypt'94, Lecture Notes in Computer Science, vol. 950,Springer-Verlag. 1 – 12 1995.

[2] Bailey, K., and Curran, K., "An Evaluation of Image Based Steganography Methods", Journal of Multimedia Toolsand Applications, Vol. 30, No. 1, pp. 55-88, 2006.

[3] Nguyen, Thi Thu Trang, and Quang Uy Nguyen, "An analysis of Persuasive Text Passwords, "Information and Computer Science (NICS), 2015 2nd National Foundation for Science and Technology Development Conference on. IEEE, 2015.

[4] Tam, Leona, Myron Glassman, and Mark Vandenwauver, "The psychology of password management: a tradeoff between security and convenience, "Behaviour & Information Technology 29.3 (2010): 233- 244.

[5] Gauravaram, Praveen, "Security Analysis of salt|| password Hashes," Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on. IEEE, 2012.

[6] Dana Yang, Inshil Doh, Kijoon Chae, "Mutual Authentication based on Visual Cryptography and OCR for Secure IoT Service," Source of the Document 2016 6th International Workshop on Computer Science and Engineering, WCSE 2016, 2016, Pages 214-219.

[7] User athentication using visual cryptography. 2015 International Conference on Control, Communication & Computing India (ICCC) | 19-21 November 2015 | Trivandrum. Pages 647-652.

[8] Analysis and Extraction of Password Image using Visual Cryptography and Steganography International Journal of Advanced Research in Computer Science and Software Engineering. Volume 7, Issue 5, May 2017 Pages 321-325.

[9] Mori, Shunji, Ching Y. Suen, and Kazuhiko Yamamoto, "Historical review of OCR research and development," Proceedings of the IEEE 80.7 (1992): 1029-1058.

[10] Patel, Chirag, Atul Patel, and Dharmendra Patel, "Optical character recognition by open source OCR tool tesseract: A case study," International Journal of Computer Applications 55.10 (2012).

BIOGRAPHIES AND PHOTOGRAPHS

1. *Prof. Nagabhushana*

Prof. Nagabhushana is having around 14 years of experience in teaching field. Presently working as a professor and HOD in Computer science & engineering department, SJM Institute of technology, Chitradurga. He has published more than 8 national and international papers. He completed his Ph.D in CSE in the year 2015.

2. *Prof. Aravinda T V*

Prof. Aravinda T V is having around 14 years of experience in teaching field. Presently working as a professor in Computer science & engineering department, SJM Institute of technology, Chitradurga. He has published more than 8 national and international papers. He completed his Ph.D in CSE in the year 2015.

3. *Nataraja B S*

Nataraja B S pursuing M.Tech.(Computer Science and Engineering) in Shri Jagadguru Mallikarjuna Murugarajendra Institute Of Technology, Chitradurga, India. His area of interest encompasses Visual Cryptography, Digital Image Processing, and Web Applications Development.