# AUTHENTICATION FRAMEWORK USING VISUAL CRYPTOGRAPHY

**Megha B. Goel[1], Vaishali B. Bhagat[2], Veena K. Katankar[3]**

[1, 2, 3]*Lecturer, Information Technology, SRMCEW, Maharashtra, India*
***megha.bgoel@gmail.com**, **bhagat.vaishali14@yahoo.in**, **katankar_veena@yahoo.com***

## Abstract

*Now a days, when we login in the website for eg. yahoo.com, gmail.com and filpkart.com we have to enter the username & password. But password is in the form of text & many users create password by combining various personal details so it is possible to forge that password. This paper proposed a new approach for providing secured authentication using visual cryptography & stenography. In the proposed work, first user has to select one cover image (secret image). Then user has to create one secret question & also has to provide the answer of that secret question. The answer of that question is hiding in the cover image (using steganography) which is selected by the user. Then we will create the shares of this cover image through visual cryptography. The process of share generation is done at the server, during this process two shares are generated & one share is given to the user & another is stored in the server. During transmission if attack is performed on the share than it is not possible to recover any information from the single share. When the user want to login, user has to provide the username & in place of password, user has to upload the share, which is provided to him/her after the registration, than at the server side both share are superimposed, one which is provided to the user & another which is stored in the server, this superimposing or stacking will reveal the cover image (secret image). From this cover image we will extract the answer of secret question. Then we will ask the user to answer the secret question & in the last we will match both answer of secret question, one which is provided by the user & another which is extracted from the cover image, if both answer are matched than only we will authenticate the user otherwise not.*

***Keywords:*** *Visual Cryptography, Stenography, Authentication*

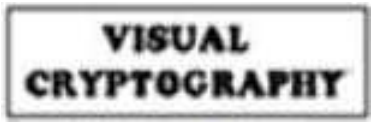
----------***----------

## 1. INTRODUCTION

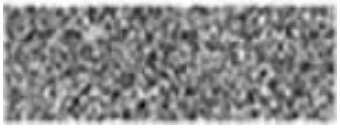
Now a day the transmission of data through computer is increasing rapidly. So the security of transmitted data becomes mandatory. Cryptography is the desired technique to provide security of the transmitted data. There are two processes in cryptography: Encryption & Decryption. Encryption is the process in which the plain text is converted into cipher text. Decryption is the process in which cipher text is converted into plain text. To encrypt data we apply an encryption algorithm at the sender side & to reveal the data at the receiving end we apply a decryption algorithm.

In 1994 Naor & Shamir [1] proposed a new cryptography area called visual cryptography. In visual cryptography visual information (i.e. image, text) is encrypted using encryption algorithm but here there is no need of decryption algorithm to reveal the visual information. It means that visual cryptography recover data with the aid of human visual system without any complex computation.

Visual cryptography schemes hide the secret image into two or more images which are called shares. The secret image can be recovered simply by stacking the shares together without any complex computation involved. The shares are very safe because separately they reveal nothing about the secret image. Simple visual cryptography is insecure because of the decryption process done by human visual system.

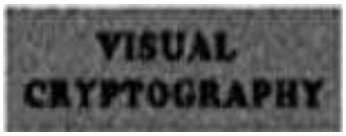



Original Image



Share 1
+

Share 2
=




Decoded Image

**Fig -1**: Working of (2, 2) Visual Cryptography scheme

The basic model of visual cryptography proposed by Naor and Shamir accepts a binary image 'I' as the secret image, and divides it into 'n' number of shares. Each pixel of image 'I' is represented by 'm' sub pixels in each of the 'n' shared images. Stacking of shares reveals the secret image but increases the size by 'm' times. The various black and white visual cryptography schemes can be summarized as follows:

1) 2 out of 2 scheme*:* In this, the secret image is distributed on two shares which are both required for the decryption process. This is depicted in Figure 1.

This scheme can be realized by using either 2 sub pixels or 4 sub pixels to represent each pixel of the secret image as explained below.

a) 2 sub pixels*:* Each pixel is subdivided into one black and one transparent (white) sub pixel as shown in Figure 2.

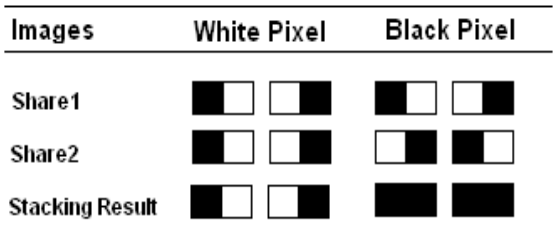



**Fig -2**: (2, 2) 2 Sub pixels

b) **4 sub pixels:** Each pixel is subdivided into four sub pixels, two black and two transparent (white) ones as shown in Figure 3.

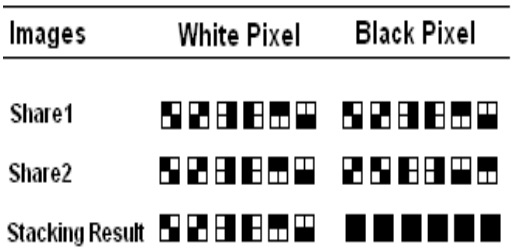


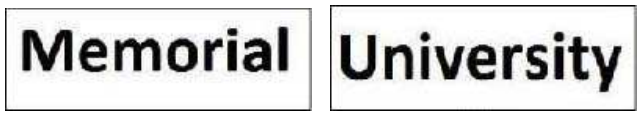

**Fig -3**: (2, 4) 2 Sub pixels

2) n out of n scheme*:* In an n out of n scheme the secret message is distributed on n transparencies. Superimposing I transparencies with i < n will not reveal any information of the secret image. There exist two possible ways to construct an n out of n scheme by using $2^n$ sub pixels or $2^{n-1}$ sub pixels.

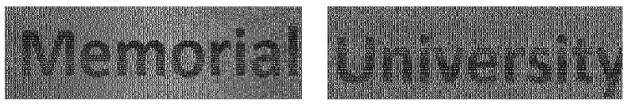
3) k out of n scheme: Splitting of the secret message into n shares out of which any k shares are required for decryption. Contrary to the n out of n scheme, not all n transparencies are required for the decryption in this case k < n.

In 1996, Ateniese, Blundo, & Stinson [2] proposed extended visual cryptography schemes in which shares contain not only the secret information but are also meaningful images.


Secret Image




First Cover Image Second Cover Image




Share 1 Share 2


Recovered Secret Image

**Fig -4**: Example of (2, 2) EVC Scheme

## 2. Existing System

In the existing system there are two steps for Authentication
1) Registration Phase
2) Login Phase

### 2.1 Registration Phase

For e.g., suppose following is the registration or sign up form of any website


**Fig -5**: Registration Phase


**Fig -6:** Login Phase

The disadvantage of existing system is that we have to remember many passwords for different websites. Second is that it is very easy to forget password.

## 3. PROPOSED SYSTEM

Proposed system will overcome the disadvantage of existing system.

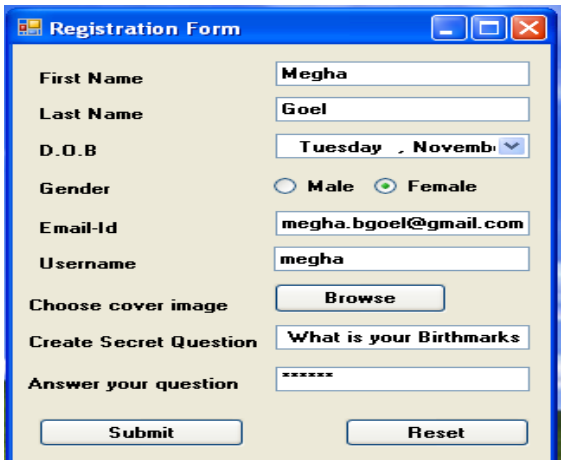



**Fig -7:** Registration Phase


**Fig -8:** Login Phase

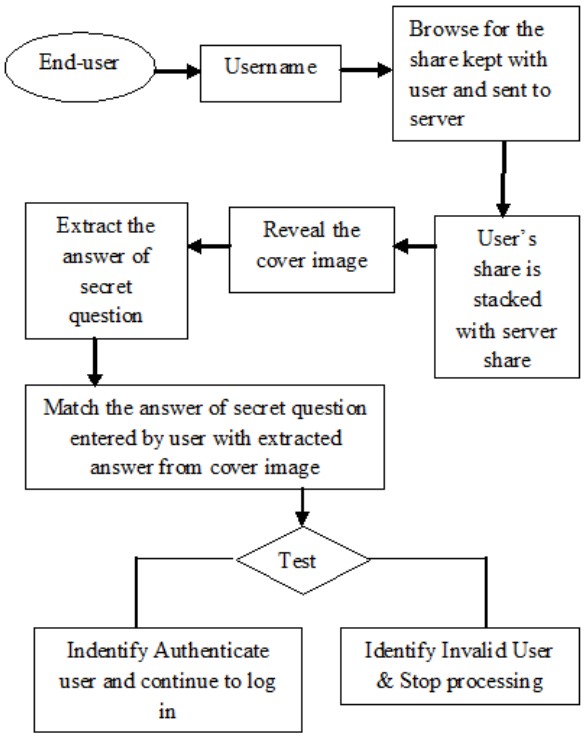



**Fig -9:** Proposed System

## 4. WORKING

Here in the proposed system instead of password we use the concept of visual cryptography. In the registration phase, user has to choose one secret or cover image. Then user has to create one secret question & also provide the answer that question.

By using steganography algorithm we will hide the answer of secret question in the cover image & then apply the visual cryptography schemes to create the shares of the cover image.

One share is given to the user other is stored in the server. Now we will use the share which is provided to the user for login instead of password.

The advantage of proposed system is that, user don't have to remember many passwords. But user have to carry this share (it is in the form of image) means user have to store it in his/her PC, pen drive or CD. Now here it is possible that anyone can steal this share but if user will choose meaningful cover image, for eg., image of itself, then anybody will think that this is simply a picture not a share. & in any case if share is stolen than there is a facility of secret question. This question is created by the user so only user has the knowledge about the question & answer.

### 4.1 Share Generation Process

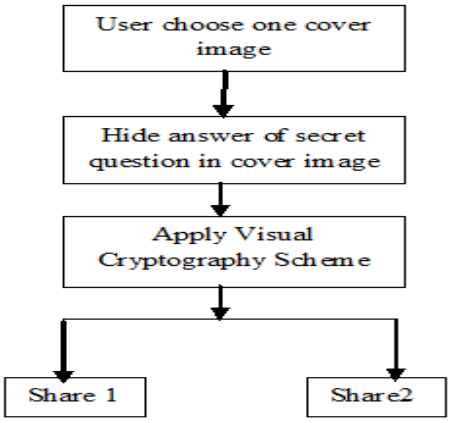



**Fig 10:** Share Generation Process

## CONCLUSIONS

Commonly used authentication schemes are vulnerable to attacks. Some authentication system traditionally use text password to verify user. Attackers can easily theft text password and capture confidential information of user. Valid as well as invalid user are easily identified using our proposed sysetm.The proposed methodology preserved the confidential information using 2 phases of security. In First phase, we ask the user to choose cover image and create secret question and answer that question. The answer is stored in encrypted form and hides in cover image and generates shares of it. Original answer is generated by stacking of two shares, one kept with user and other with server.

Second phase match the resulting share with share entered by user at the time of log-in. If match found then he is able to continue the next steps and identifies as authorized user otherwise identifies as unauthorized user. So this proposed system not letting unauthorized user to log-in into account.

## REFERENCES

[1]. M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.
[2]. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended Visual Capabilities for Visual Cryptography," Theoretical Computer Science, vol.250, pp.143-161, 2001.
[3]. Hsien-Chu Wu, Hao-Cheng Wang & Rui-Wen Yu, "Color visual cryptography scheme using meaningful shares", ISDA'08, Vol. 3, pp. 173-178, Nov. 2008.
[4]. F. Liu1, C.K. Wu X.J. Lin , "Colour Visual Cryptography Schemes", IET Information Security, vol. 2, No. 4, pp 151-165, 2008.
[5]. P.S. Revenkar, Anisa Anjum, W.Z. Gandhare, "Survey of Visual Cryptography Schemes", IJSIA, Vol. 4, No. 2, April, 2010.
[6]. E. Verheul and H. V. Tilborg,"Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes" Designs, Codes and Cryptography, 11(2) , pp.179–196, 1997.
[7] R.Youmaran, A. Adler, A. Miri , "An Improved Visual Cryptography Scheme For Secret Hiding", 23rd Biennial Symposium on Communications, pp. 340-343, 2006.
[8]C.C. Wu, L.H. Chen, "A Study On Visual Cryptography",Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C.,1998.

## BIOGRAPHIES

**Megha Goel** has received the B.E. degree in Information Technology from RTMNU, Maharashtra, India in 2008 & pursuing M. Tech in CSE from RTMNU. Since, 2010 she is working in the department of IT as a lecturer in SRMCEW, Nagpur, Maharashtra, India.

**Vaishali Bhagat** has received the B.E. degree in Information Technology from RTMNU, Maharashtra, India in 2008 & pursuing M. Tech in CSE from RTMNU. Since 2010, she is working in the department of IT as a lecturer in SRMCEW, Nagpur, Maharashtra, India.

**Veena Katankar** has received the B.E. degree in Computer Technology from RTMNU, Maharashtra, India in 2003 & obtained M.E. in WCC from RTMNU. Since 2010, she has been Asst. Professor in the department of CSE, SRMCEW, Nagpur, Maharashtra, India.