

A Hash Based Visual Cryptography Scheme for Image Authentication

Gonela Shiva

M.TECH(CNIS),Dept. of IT
Sreenidhi Institute of Science & Technology
Hyderabad, Telangana, India
shivagonela342@gmail.com

CH. Samson

Associate professor & Associate Head Dept, of IT
Sreenidhi Institute of Science & Technology
Hyderabad, Telangana, India
samchepuri@gmail.com

Abstract — In this paper we have proposed a Hash based visual cryptography scheme for image authentication. The secret image to be transmitted is encoded into two shadow images called user share and key share. The Hash cryptographic algorithm is applied on each share, and the resultant Hash codes are concatenated with the shares, and sent to communication participants. The same Hash is used to verify the sender at the receiving end. Then the shares are stacked together to recover the original secret image. From the results obtained in our analysis, we conclude that the proposed scheme provides not only confidentiality but also image authentication.

Keywords- Visual Cryptography; user share; key share; hash; image Authentication.

I. INTRODUCTION

Visual Cryptography is a cryptographic technique which allows visual information such as text, pictures and images to be encrypted. An image is divided into n shares so that stacking of n shares will reveal the original image with loss of quality. Visual Cryptography is introduced by Moni Naor and Adi Shamir in 1994 [1]. They 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, no $n-1$ shares would reveal the original image.

Each pixel of the image divided into smaller blocks. There are always the same number while (transparent) and black blocks. If a pixel is divided into two parts, there is one white and black block. If the pixel is divided into four equal parts, there are two white and two black blocks.

Text based passwords attacks have become common now a days there are different text based password attacks. So new schemes of authentication are been in research. One such Method is Visual cryptography which is used to generate different unidentified shares so that these shares can be shared between two or more parties so that stacking of these shares will help in identifying the original image message. Using the Hash of images will help in generating the hash of a secret image so that it is impossible to get the secret image back from hash code. This paper presents a method of using Visual Cryptography and Hashing to Store and authenticate the user.

II. RELATED WORK

Many authors published different Visual Cryptography Schemes for different applications. Each scheme has its own advantages and disadvantages. Naor and Shamir [2] have worked on Basic Visual Cryptography scheme. Ateniese et al. [3] have worked on Elegant Visual Cryptography scheme for general access structure based on the cumulative array method. Naor and Pinkas [4] have worked on methods of authentication and identification between two participants. Yang et al. [5] have worked on Cheating method against some Visual Cryptography scheme were discussed.

The existing methods propose different authentication mechanism using visual cryptography where the generate images shares are stored in the database so that when the user insert the this secret share the system will retrieve the server share and stack both the shares, finally this stacked image is compared to the original image in database than user will be authenticated. This method degrades the performance of the system and increase the memory size of database as images take more memory.

This method also suffers from the regular attacks if the attacker compromises the database server all the user credential will be stolen, the server shares can be used to guess the user share according to Yang et al. [5].

The rest of the paper is organised as follows. In Section II, the related work is mentioned. Section III describes the proposed approach. Section IV deals with the implementation results obtained in our analysis. Finally in Section V, we draw conclusions from the results obtained from our approach and mention future scope for the possible enhancement.

III. PROPOSED APPROACH

In order to overcome the above mentioned drawbacks we proposing a Hash based methodology using visual cryptography. The proposed approach consists of four phases as follows.

A. Registration Phase

In this phase, the user is asked to provide the information about the username, email-id and image that is wants to use for authentication. The system uses the visual cryptography technique to generate the image shares. It generates two secured shares using a system generated key string.

B. Generating Image Shares

The system uses the visual cryptography technique to generate the image shares. It generates two secured shares using a system generated key.

C. Generating Hash Values of Shares

Now the hash value of server share is calculated by using any hashing method we have used MD5 hash to generate the hash value of server share. This hash value is stored in the database of the server so that even if the database is compromised or information is stolen the attacker cannot guess the user image by any of the method as adding the secure salt to the server share will provide security against the feature dictionary attacks on images.

Registration and Hash generation process are depicted in Fig 1.

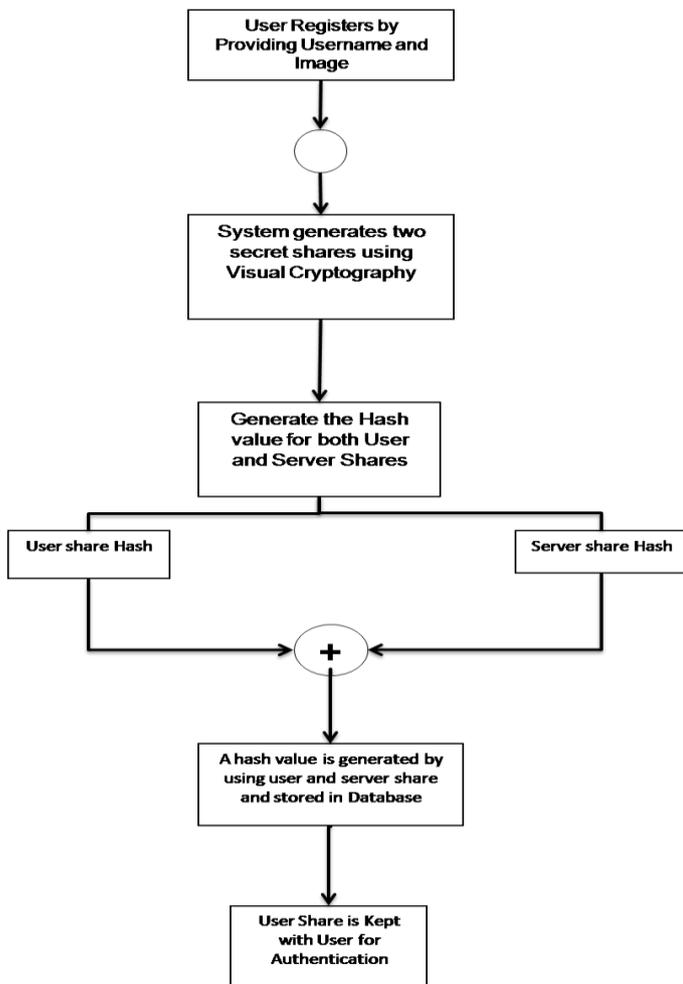


Fig 1: Flow diagram representing A, B, C Phases

D. Authentication Phase

The user enters the username and inputs these share for authentication. The system will generate the hash code of user share by appending the secured random Salt to the share image and calculates the hash.

Now the server image share hash value and user image share hash values are concatenated and final hash value is calculated which is then compared to the server hash if both hash values are matched the user is authenticated provided access to the use services otherwise the service is not accessible and user is not authenticated.

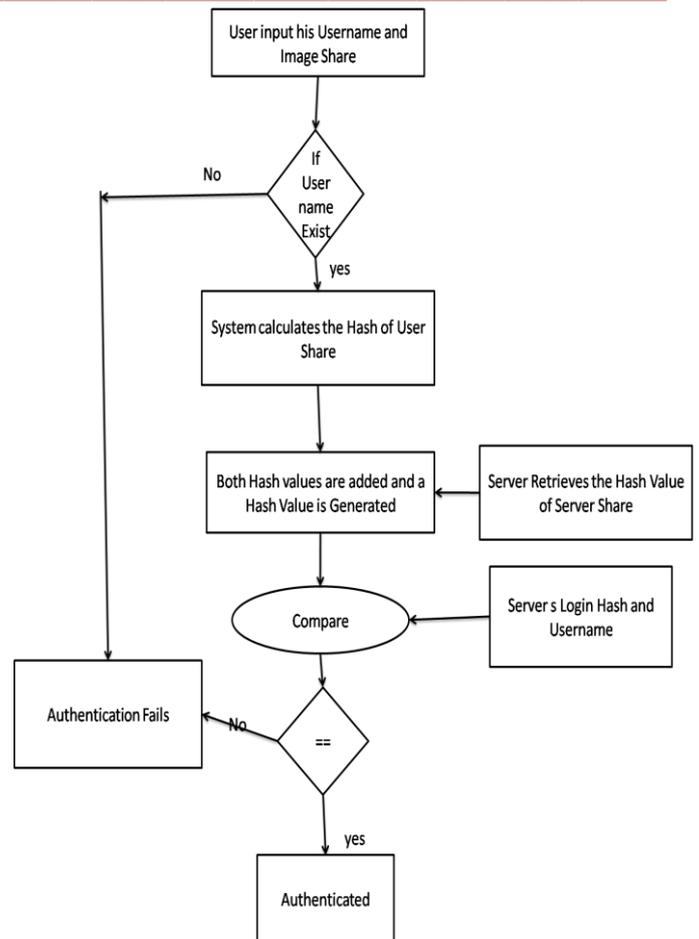


Fig 2: Flow diagram representing Authentication Phase

IV. RESULTS

In this paper, we have implemented a hash based visual cryptography scheme for image authentication. The secret image is shown in Fig 3. A key share/server share is chosen and is shown in Fig 4. On performing Exclusive XOR operation between the secret image and the key share, we obtain user share which is shown in Fig 5. We apply MD-5 on both user share and key share and from these two hash codes we obtain a resultant hash as shown in Fig 6.



Fig 3: Secret Image

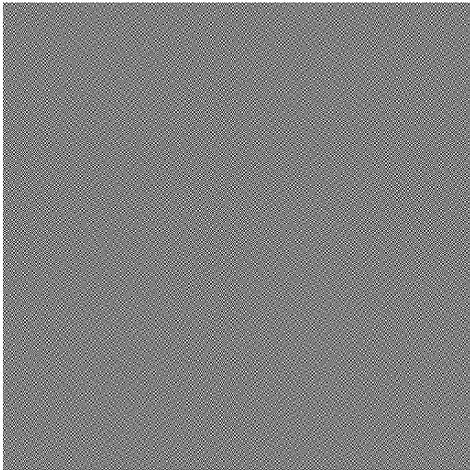


Fig 4: Key share/Server share

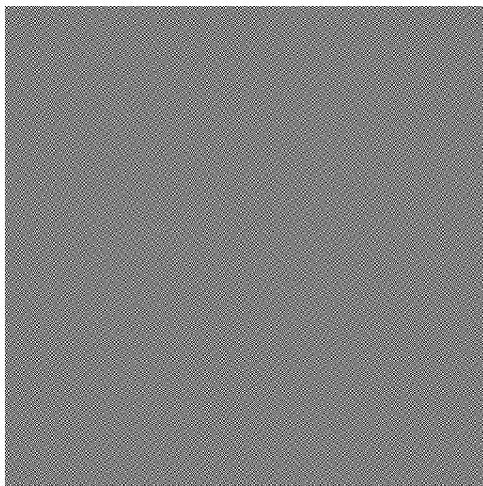
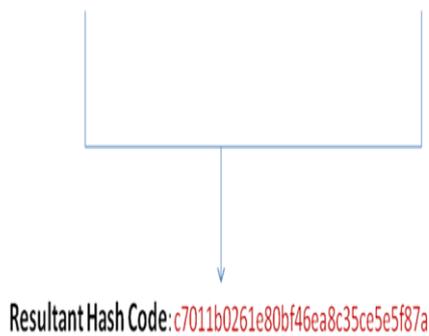


Fig 5: User share

USER SHARE HASH CODE: c518ae3702a0780c31fcd0132497e827
 KEY SHARE HASH CODE: e635094ba5c909df1ffe178e93200b94



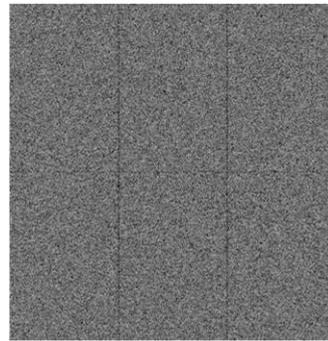
This Resultant Hash Code is Stored in Database for Authenticating

Fig 6: Hash code of user share, key share and resultant hash code

The below scenario shows the possible cases of authentication, if the user share is wrong, authentication fails

which can be shown in Fig 7. If the user share is correct then the user will be authenticated which can be shown in Fig 8.

If Wrong User Share



HASH CODE: Oeedc7789f89340c6db2882b38f4c703
 Server Share/Key Share HASH CODE: e635094ba5c909df1ffe178e93200b94

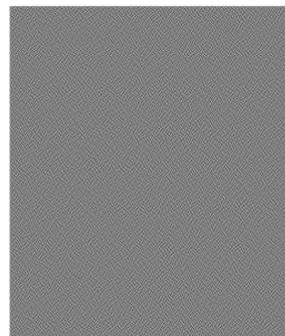
Resultant Hash Code: 984fcbf80af27db918ce1f159a8bec32



Original Resultant Hash Code: c7011b0261e80bf46ea8c35ce5e5f87a

Fig 7: Diagram for wrong user share is used, Authentication fails

If Correct User Share



HASH CODE: c518ae3702a0780c31fcd0132497e827
 Server Share/Key Share HASH CODE: e635094ba5c909df1ffe178e93200b94

Resultant Hash Code: c7011b0261e80bf46ea8c35ce5e5f87a



Original Resultant Hash Code: c7011b0261e80bf46ea8c35ce5e5f87a

Fig 8: Diagram for correct user share is used the user will be authenticated

V. CONCLUSION AND FUTURE SCOPE

The proposed hash based visual cryptography scheme for image authentication can overcome the cheating attacks of visual cryptography as proposed by Yang et al. [5]. This

approach reduces the size of database the process of retrieving and comparing become very fast when compared to retrieving the images from database.

This method can be used in biometric fingerprint scanning where the thumb image is captured and shares are generated by using the visual cryptography system [9].

This method can be used to produce the smart cards to the users, which can be used to authenticate the users for providing the services.

Using the proposed method the authentication becomes very fast when compared to the previous methods. This approach can be used with all applications of visual cryptography authentication system. We can develop separate authentication device for personal computer, so that every user will have smart card that contains a user share, when the user insert the smart card to that authentication device user will be authenticated. We hope to develop a full prototype of such method as our future work.

REFERENCES

- [1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.
- [2] Shamir, .How to Share a Secret., Communication ACM, vol. 22, 1979, pp. 612-613.
- [3] W.-G. Tzeng and C.-M. Hu, "Anew approach for visual cryptography," "Designs, Codes, Cryptog. vol. 27, no. 3, pp. 207– 227, 2002.
- [4] M. Naor and B. Pinkas, "Visual authentication and identification," in Proc. Advances in Cryptology, 1997, vol. 1294, LNCS, pp. 322–336.
- [5] C.-N. Yang and C.-S. Lai, "Some new types of visual secret sharing schemes," in Proc. Nat. Computer Symp., 1999, vol. 3, pp. 260–268.
- [6] W.-G. Tzeng and C.-M. Hu, "Anew approach for visual cryptography," "Designs, Codes, Cryptog. vol. 27, no. 3, pp. 207– 227, 2002.
- [7] W-Q Yan, D.Jin and M. S. Kakanahalli(ISCAS-2004).Visual Cryptography for Print and Scan Applications,. IEEE Transactions, pp.572-575.
- [8] M. Hu and W. G. Tzeng, .Cheating Prevention in Visual Cryptography,. IEEE Transaction on Image Processing, vol. 16, no. 1, Jan-2007,pp. 36-45.
- [9] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Syst. J., vol. 40, no. 3, pp. 614–634, 2001.
- [10] R. LuKac, K.N. Plataniotis"Bit-level based sharing for image encryption", The journal of Pattern Recognition Society, 2005.