Research Inventy: International Journal of Engineering And Science
Vol.4, Issue 5 (May 2014), PP 16-20
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Doubly Secured Authentication Scheme using RKO technique of Visual Cryptography

[1]Mrs. Moushmee Kuri, [2]Dr. Tanuja Sarode
[1](Assistant Professor, Computer Department, W.I.E.E.C.T/ Mumbai University, India)
[2](Assistant Professor Computer Department, T.S.E.C/ Mumbai University, India)

ABSTRACT - *Authentication using passwords has become old and is not reliable with respect to security. Passwords if too simple can be easily cracked and if too complex it's difficult to remember them. Password storing and matching use different hashing/encryption techniques. However they require complex algorithms for encryption and decryption, Visual cryptography is a technique which provides confidentiality without any cryptographic knowledge or complex computations. Visual information such as photo and signature can be encrypted by decomposing it into several images, called shares; in such a way that decryption can be done by human visual system with stacking of the shares. The RKO technique which is a hybrid technique of VC divides the image into two shares, one random share and one key share. When these two shares are XORed pixel by pixel the generated is same as the original image in terms of quality. In this paper we propose a doubly secured authentication scheme which uses RKO technique to login. This scheme creates shares of photo and signature image and uses these shares to login the system. This scheme improves the security level of the existing schemes.*

Keywords *- Visual Cryptography, Authentication, Shares, Bank login, Image Encryption, RKO technique.*

I. INTRODUCTION

With everything becoming online there is an urgent need to ensure information security. Nowadays almost all banks have gone online. With the increasing use of network banking there is an utmost need to secure the customer information and free him from any kind's of cyber frauds. Most of the banking applications have a user id and a password to login. This system is not that much reliable as passwords can be cracked. In this paper a doubly secured authentication scheme is proposed where instead of making use of the conventional encryption techniques we make use of the visual cryptography techniques. The disadvantage of conventional cryptographic methods is that they need a lot of time and computation power
for performing encryption and decryption. In addition to that, these methods are susceptible to many security attacks. So, some new scheme should be looked forward to, which can provide confidentiality with simpler techniques. attacks. So, some new scheme should be looked.

In 1994, Naor and Shamir [1] proposed a new cryptographic area called visual cryptography based on the concept of secret-sharing. It divides an image into a collection of shares and requires threshold number of shares to retrieve contribution of the paper. the original image. The decrypted message is obtained from stacking of the shares. The most notable characteristic of this scheme is to have a computation-less decryption.
The hybrid method of Visual Cryptography called RKO technique which creates two shares: one random share and second key share can be used to make the information security more reliable.

II. REVIEW OF LITERATURE

Various methods have been employed for maintaining secrecy and confidentiality of images.

A. Image Encryption (using keys):

This approach is basically similar to the conventional encryption methods which involve using an algorithm (and a key) to encrypt an image. Some of the proposed techniques for encrypting images use "Digital Signatures" , "Chaos Theory" , "Vector Quantization" etc. to name a few. There are some inherent limitations with these techniques; they involve use of secret keys and thus have all the limitations as regards key management. In addition, in some cases the available keys for encryption are limited (restricted key space). Also high computation involved in encryption as also weak security functions are also an issue. However the greatest strength of most of these schemes is that the original image is recovered in totality [5].

B. Visual Cryptography (Image Splitting)

The idea of Image splitting more often referred to as Visual Cryptography Schemes (VCS) involves splitting a secret image into n random shares such that these shares individually reveal no information about the secret image (but for its size) but a qualified subset of the shares(as specified by the encrypter) when stacked up reveal the secret image. The random image shares (qualified set) are merely printed on transparencies and stacked up revealing the original image). The major issues which restrict its employment is the poor quality of the recovered image limited color representation.

C. Hybrid Approach

In this approach the RKO technique can be implemented which splits the image into two shares. The first share is the random share and the second share is the key share. These two shares have no resemblance to the original image. When the two shares are combined using XOR it reveals the original image. The quality of the image revealed is same as the original image. This algorithm has perfect reconstruction property and there is no loss of picture quality. This algorithm can also be used on gray scale images without any loss of image quality.

III. PROPOSED AUTHENTICATION SYSTEM

The proposed system aims to improve the security of the traditional authentication systems where signature can be forged or passwords can be cracked. The system can be used in banks or any organization where you need to prove your identity to carry out the transactions. The system uses a customer photo which is a color image and his signature which is a black and white image.

The system has two phases: Registration and Login.

Phase 1: Registration Phase: Any new user has to first register himself in the system. To register he needs to submit his personal details and a photo and signature. Once he is registered a account number will be send to his registered email id along with his photo share and signature share. These shares he need to present at the time of login.

The communication steps involved in registration are:

Step 1: Enter name, age, address.
Step 2: Enter the email id to which account number and the two shares have to be send.
Step 3: Submit the user photo.
Step 4: Submit the user signature.

After submitting the above details the customer will be registered in the system. He will be assigned an unique account number. A random share and key share will be generated for his photo and signature image using the RKO technique. The account number, the random share for photo and signature image will be send to his registered email id. The key share for photo and signature image along with the account number and other details will be stored in the database for further use.

Phase 2: Login Phase: Already registered user can login the system provided they have a account number, a photo share and a signature share. The system prompts the user to enter the account number, load his photo share and his signature share. Using RKO technique the shares are overlapped and the photo and signature are regenerated. The generated photo and the signature are displayed on the bank side along with the original photo and signature image. If both match then allow him the access or else deny access.

The communication steps involved in login are:

Step 1: Enter the account number.
Step 2: Submit the signature share received through mail.
Step 3: Submit the photo share received through email.
Step 4: Overlap the signature share with the bank signature share and photo share with bank photo share.
Step 5: Display the resultant images.

If the resultant photo matches with the original photo and the resultant signature matches with the original sign then only the customer will be allowed to access his bank details. Else the customer will be denied access.

No intruder can enter the system because no fake share other than the actual share can overlap with the bank share to generate the original image. And since both the shares are send to the customer email id no intruder can capture the actual shares.

Fig 1. Shows the architecture of the system.(RS : Random Share, KS: Key share)

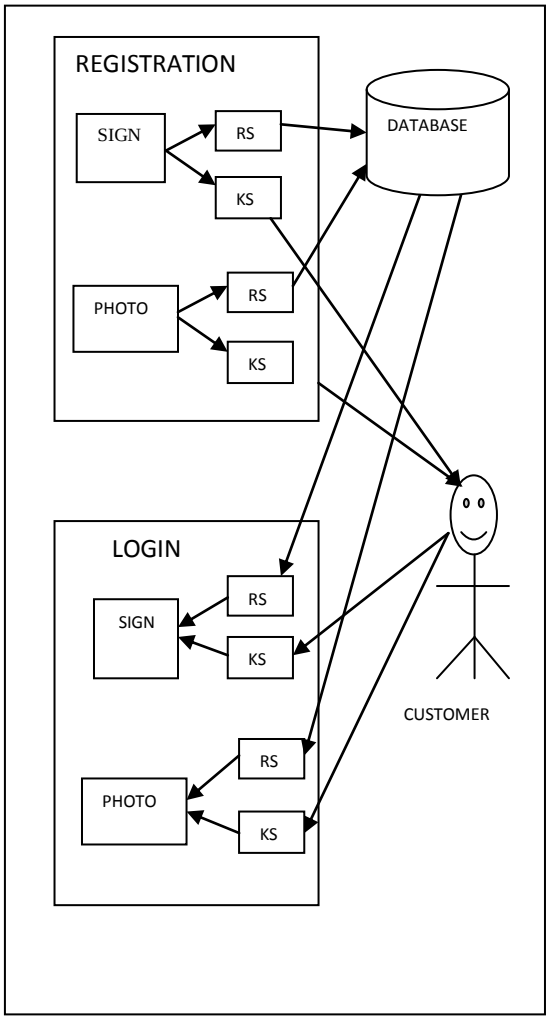

Fig 1. Architecture of the system

The advantages of the proposed architecture are:

1. The proposed system employs photo as well signature image check to improve the security over the existing authentication methods.

2. The use of RKO technique of hybrid visual cryptography makes it difficult for the intruder to enter the system as shares generated by him will never match the bank share.

3. Even if the shares are stolen the generated photo will not match the intruder face. So it cannot be misused.

IV. IMPLEMENTATION DETAILS

The system was implemented in JAVA by using the RKO [15] technique to generate the photo share and the signature share. The key shares were stored in the Oracle database and the random shares were sent to the customer. While matching the share from the customer are matched with the shares stored in the Oracle database on the bank side. If the shares match then only the generated photo is exact replica of the submitted photo and generated signature is exact replica of the submitted signature.

V. EXPERIMENTAL RESULTS

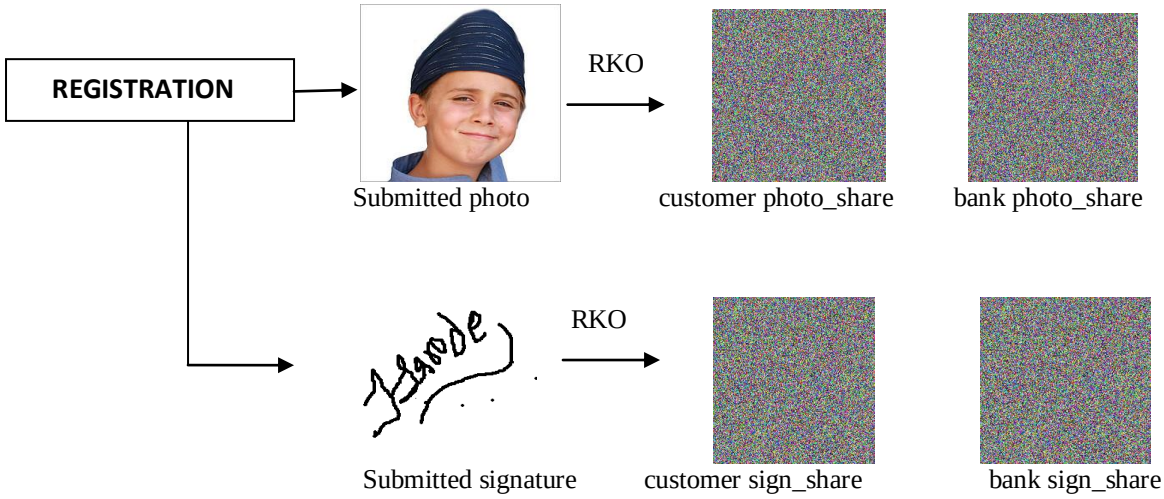

Fig 2. Registration process

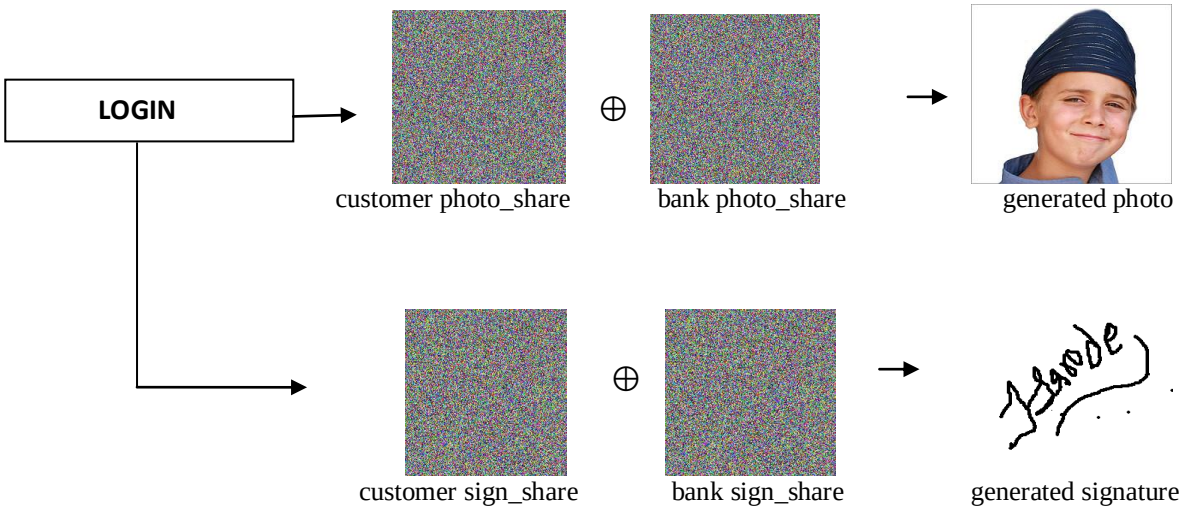

Fig 3. Login process

In our proposed scheme the generated image is an exact replica of the submitted image and the generated signature is the exact replica of the submitted signature as no data is lost during the RKO operations. The results were validated using Normalized Correlation (NC). NC is used to measure the correlation between the original secret image and the recovered images from the random shares.

$$NC = \sum_{i=1}^{w} \sum_{j=1}^{h} \frac{\overline{(Sij \oplus Rij)}}{w \times h}$$

S represents the secret image and R the recovered image. w, h represents the width/height of the photographs and $\oplus$ represents the exclusive OR operator. We repeated the test over multiple images, the NC for all the recovered images was 1.000. A comparison of RKO scheme with similar other schemes is listed in Table II.

TABLE II, COMPARISON OF TECHNIQUES

SCHEMES				
FEATURES	**Kuri, Sarode RKO TECHNIQUE[15]**	**Tsai, Chen et.al. [12]**	**Lukac, and Plataniotis [13]**	**Chang and Yu's scheme [14]**
Noise Correlation	Always 1.000	Always< 1.000	1.000	Always< 1.000
Image delivery Transparency	No	Yes	No	Yes
Additional Data Structure	No	Yes AX, BX	No	Yes S-E table (Local)
Key Management	No	Yes S, BX have to be kept secret	No	No
Pixel Expansion (256 color, (n, n) scheme)	No expansion	1 : 9 expansion	1: $2^{(n-1)}$	1 : 529

VI. CONCLUSION

In this paper, a doubly secured authentication system is presented with the concept of RKO technique based on the hybrid Visual Cryptography schemes. The proposed system improves the security level of the authentication process by checking the reconstructed photo and the signature image. It implements a double level check as the photo as well as signature should match to login. Either of this does not match then the user will not be allowed to login the system. The shares are transferred to the customer through a secure channel. So there is no chance of the shares being stolen. A intruder cannot login the system with his own shares as they will never match the shares stored with the bank. The use of this system can be in banking applications. Overall this system is very suitable to meet today's authentication challenges

REFERENCES

Journal Papers:

[1] M. Naor and A. Shamir, "*Visual cryptography*," in Proc. *EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS*

[2] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, " *Novel Authentication System Using Visual Cryptography*", *in 2011 World Congress on Information and Communication Technologies.*

[3] F. Liu1, C.K. Wu X.J. Lin , "*Colour Visual Cryptography Schemes*", *IET Information Security, vol. 2, No. 4, pp 151-165, 2008.*

[4] Y. C. Hou, "*Visual cryptography for color images*," *Pattern Recognition, vol. 36, pp. 1619-1629, 2003.*

[5] Siddharth Malik, Anjali Sardana, Jaya "*A Keyless Approach to Image Encryption", 2012 International Conference on Communication Systems and Network Technologies*

[6] L. W. Hawkes, A. Yasinsac and C. Cline, "*An Application of Visual Cryptography to Financial Documents*," *Technical report TR001001,Florida State University, 2000.*

[7] George Abboud, Jeffrey Marean, Roman V. Yampolskiy, "*Steganography and Visual Cryptography in Computer Forensics*", *in 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering*

[8] A. Shamir, "*How to share a secret*," *Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.*

[9] H.-C. Wu, C.-C. Chang, "*Sharing Visual Multi-Secrets Using Circle Shares*", *Comput. Stand. Interfaces 134 (28) ,pp. 123–135, (2005).*

[10] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin , "*Sharing* A *Secret Two-Tone Image In Two Gray-Level Images*", *Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.*

[11] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "*Multiple-Image Encryption By Rotating Random Grids*", *Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.*

[12] Du-Shiau Tsai , Gwoboa Horng , Tzung-Her Chen , Yao-Te Huang , "*A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint*", *Information Sciences 179 3247–3254 Elsevier, 2009*.

[13] R. Lukac, K.N. Plataniotis "*Bit-level based secret sharing for image encryption", The Journal of Pattern Recognition Society, 2005*.

[14] C.C. Chang, T.-X. Yu," *Sharing a secret gray image in multiple images*", in: *Proceedings of First International Symposium on Cyber orlds, 2002, pp.230–240.*

[15] Ms. Moushmee Kuri, Dr. Tanuja Sarode, "*RKO Technique for Color Visual Cryptography*", in *: IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 89-93*