Novel Authentication System Using Visual Cryptography

[1]Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana
[1]Symantec Software India Pvt. Ltd., India
Indian Institute of Technology Roorkee, India
{jaya.im.k, siddharthmalik76, abhinav6891}@gmail.com, anjalisardana@ieee.org

Abstract—An array of encryption techniques has been proposed for providing data security. However, most of the traditional cryptography methods require complex algorithms for encryption and decryption. Visual cryptography is a technique which provides confidentiality without any cryptographic knowledge or complex computations. Visual information (e.g. printed text, hand-written notes, pictures, etc.) is 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. Some important goals while developing a Visual Cryptography scheme is to have (i)optimum number of shares, (ii)good quality of reconstructed image and (iii)keeping the size of share small. This paper aims to provide a comparative study of various Visual Cryptographic schemes based on pixel expansion, no of shares, size and quality of reconstructed image, etc and some real-life applications of visual cryptography. A new authentication system has been proposed which uses the technique of visual cryptography to improve the security level of existing schemes. The application of the system in financial domain is discussed.

Keywords-visual cryptography schemes (VCS); share; pixel expansion; contrast; stacking.

I. INTRODUCTION

With network growing rapidly, there is an urgent need to ensure information security in the present era of electronic commerce. Internet has become the primary source of transmitting confidential data such as military information, financial documents, etc. Currently many security providing tools are used to make the communication reliable over network. Cryptography is one of the tools. It is not just a set of encryption-decryption algorithms but also applies to message integrity and authentication. 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.

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 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. It can also be used for applications which do not want to trust every participating entity in the process, using General Access Structure scheme. Another interesting extension of the original model is to generate innocent-looking shares so that attacker cannot get doubtful by looking at the random pattern of the share. Visual Cryptography is expanded to encode multiple secret images together so that overhead of keeping too many shares can be reduced. One other advancement in this field has been done to encode multi-pixels at once in order to reduce the share size and make the performance better.

In this paper, we propose a novel authentication system using Hou's [3] third algorithm for color images. The method proposed by Hou uses the technique of image-halftoning prior to applying basic VCS. This method is fairly simple and produces image with good quality.

The paper is organized as follows: Section 2 compares and analyzes the performance of various VCS. Section 3 contains some real-life applications of visual cryptography. Section 4 presents a proposed authentication system based on VC. Section 5 extends the proposed system for online applications.

II. COMPARISON

There are various parameters which can be used to compare the performance of visual cryptography schemes. Some of them are pixel expansion and contrast. It can be easily observed that as pixel expansion increases, we get more number of black subpixels for a white pixel in the reconstructed image and hence it corresponds to the loss in resolution. It also adds to larger size of the shares. So, m should be as small as possible. Contrast enables us to differentiate between a black and white pixel clearly

978-1-4673-0125-1 ©2011 IEEE

and thus corresponds to the quality of the reconstructed image.

Some other measures are computational complexity, number of colors supported, quality of reconstructed image, security of the method and generation of meaningful shares. Computational complexity deals with the time taken in encoding-decoding process and the nature of the algorithms used in the scheme. A VCS is more general and can be applied in many real world scenarios if it supports color images. Quality of reconstructed image should be good enough so that it can be applied in situations which demand crisp and clear output such as transmission of financial documents. Security means that the shares should not reveal any information about the secret image until threshold-amount of shares is stacked. Naor and Shamir [1] also suggested that random pattern of shares may attract attackers and hence meaningful shares should be produced to enhance the security of the scheme. Droste [16] proposed to share more than one secret among a set of shares to reduce the overhead of generating and transmitting numerous shares. Hou [9] suggested to encode more than one pixel for each encoding run to improve the performance, known as multi-pixel encoding .

The basic (2,2)-method can be used in electronic voting purpose and banking application. Schemes discussed in [11, 3, 4, 6 and 8] can be applied in situations which require color details such as person identification application. Applications which are more vulnerable to attackers can use schemes proposed in [1, 7, 4 and 5] which generate meaningful shares to fool the attackers. Multi-secret sharing methods [16, 13, 14 and 15] are useful in having less overhead of maintenance and transmission. The approach developed in [9 and 10] provide efficient methods to generate shares with no pixel-expansion and produce good-quality reconstructed image. These schemes can be used for applications which have a need of less storage, high-speed computation and fast transmission.

Rijmen and Preneel [11] first proposed a method to encode color images. But it supported only 3-bit color images. Hou[3] proposed three methods to encode true-color images. The third method is used for the proposed authentication system for its simplicity and good image quality.

Table 1. Comparison of various VCS

Author	Encryption/ decryption	Pixel exp-ansion (m)	Decoding time	(n,n) scheme support	Decrypted image size	No of secret image	Share type	True color support	Security enha-ncement	Additional data structure	Meaningful shares	Multi-pixel encoding
Naor and Shamir [1], 1995	An original pixel divided into 255 sub-pixels.	255	NA	Yes	255 times	1	Rectangle	No (grey level)	No	No	No	No
Rijmen and Preneel [11], 1996	Each pixel expanded to 2 x 2 block.	4	NA	No	4 times	1	Rectangle	No (3-bit color)	No	No	No	No
Verhuel and Tilborg [12], 1997	Each subpixel takes one of grey-levels of 0,1,.., g-1 (g is no of grey levels)	Variable	NA	Yes	At least g^(k-1) times	1	Rectangle	No (grey level)	No	No	No	No
Chang et al. [4], 2000	With a predefined color index table, secret is hidden into 2 cover images.	529	more	No	m times	1	Rectangle	No	No	Yes	Yes	No
Chang-Yu [5], 2002	Based on modified visual cryptography. Decoding by XOR.	9	more	Yes	9 times	1	Rectangle	No	No	No	Yes	No
Lin and Tsai [2], 2003	After dithering of secret image, basic VC can be applied.	variable	NA	Yes	m times	1	Rectangle	No (grey level)	No	No	No	No
Hou's scheme 1 [3], 2003	After dithering, one black mask and 3 primitive color shares are generated.	4	NA	No	4 times	1	Rectangle	Yes	No	No	No	No
Hou's scheme 2 [3], 2003	After dithering, 3 primitive color shares are generated.	4	NA	No	4 times	1	Rectangle	Yes	No	Yes	No	No
Hou's scheme 3 [3], 2003	After dithering, 3 primitive color shares are generated (better quality than second)	4	NA	No	4 times	1	Rectangle	Yes	No	No	No	No

Wu et al. [6], 2004	Quantized-embeded image is divided into n shadows.	4	more	Yes	About 1/n times	1	Rectangle	No	Permutation	Yes	Yes	No
Wu and Chang [13], 2005	share *B* generated a/c to distribution of 2×2 extended block of share *A* at relative position. Decryption by rotation at 90 degree.	4	more	No	m times	2	Circle	No	No	No	No	No
Hou and Tu [9], 2005	r successive pixels of same color are taken as a unit of encryption (fixed encoding length)	1	NA	Yes	Same	1	Rectangle	Yes	No	No	No	Yes
Shyu et al. [14], 2007	n secrets can be obtained by stacking first share and rotated second shares with *n* different angles.	2*n	NA	No	NA	n>=2	Circle	No	No	No	No	No
Feng et al. [15], 2008	A stacking relationship graph of secret pixels and share blocks is generated to indicate encryption functions. A set of visual patterns is defined to produce 2 shares.	9	NA	No	3n times	n>=2	Rectangle	No	No	No	No	No
Zhang et al. [10], 2008	Encoding length in one run is equal to no of successive pixels of same color (variable encoding length)	1	NA	Yes	Same	1	Rectangle	Yes	No	No	No	Yes
Tsai et al. [8], 2009	Size of secret image is shrinked before encoding.	9	more	Yes	9 times	1	Rectangle	Yes	Permutation	Yes	Yes	No

III. APPLICATIONS

A. *Means of transmitting financial documents*

Hawkes et al. [17] proposed a technique which provides moderate degree of security to transfer financial documents over the internet securely, known as VCRYPT. VCRYPT is a simple, fast, visual cryptography technique, to provide privacy protection when transmitting sensitive data. When visual cryptography methods are applied to financial documents, it is often difficult to distinguish digits accurately because of containing an overall grey effect due to the leftover black subpixels from encoding which makes it an unattractive protection technique. VCRYPT evaluates every set of m subpixels corresponding to a pixel against the threshold; the pixel is black if the number of black subpixels is above the threshold value and white if it is below the threshold.

B. *Electronic-Balloting System*

In a voting procedure, the machines require voters to trust them, without giving any proof that each vote was recorded correctly. Chaum [18] proposed a secret-Ballot Receipts system based on (2,2)-threshold binary VCS. It generates an encrypted receipt to every voter so that the election outcome can be verified. At the polling station, user will receive a double-layer receipt containing her voting decision. One of the layers is given to the voter and other one is destroyed immediately. The remaining one layer, the receipt, is an unreadable and seemingly random pattern of tiny squares. To make sure that the vote is not altered, serial number of the receipt can be used to check on the election Web site. This will return a posted receipt. Both the receipts must be identical and can be checked by overlaying the two receipts. The receipts also improve robustness, which currently is achieved by costly hardware redundancy in storing and transporting votes.

There are several advantages of this system. First, a receipt not posted properly can act as a physical evidence of the failure of the election system. Secondly, voters are ensured that no one can decode the receipt unless that person somehow knows the decryption algorithm and obtained all secret keys, each of which is held by different trustee. Third, it eliminates the need for trusted voting machines.

C. *Authentication in WiMAX*

Visual cryptography can also be used to enhance the security level and improve the resource utilization in case of wireless networks. Denial of Service (DoS) attacks are very dangerous in wireless network scenario. In WiMAX a large number of authentication requests sent to the Base Station (BS) by rouge Subscriber Stations (SSs) might lead to a DoS attack. Here BS allocates most of its resources for authentication process where certificates of both the parties are exchanged and checked.. A method for PKM-RSA proposed by Altaf et al. [19] uses visual cryptography as a pre-authentication tool to avoid DoS attacks caused by the large number of rouge requests. A simple XOR operation is used to check the validity of requesting SS and BS both, thus providing mutual authentication scheme. It adds another level of security and improves the resource utilization of BS.

IV. PROPOSED AUTHENTICATION SYSTEM

The proposed system aims to improve the security of traditional authentication systems where signature can be forged and code or password can be cracked. The system can be used for a physical bank or for credit card application, where card is used physically. The advantage of this scheme is that even if the customer's IC card is lost, it cannot be misused. A person authentication application can be implemented by applying the (2, 2)-threshold visual cryptography scheme for color images.

The system is designed to create two shares of customer image and signature. One image share and one signature share is printed on the IC card that is with the customer. The bank keeps remaining one image share and gives the second signature share to the central authority. The central authority (CA) is a trusted organization, and the bank and the customer can rely upon it for not manipulating or disclosing the share. Each customer is first validated against the reconstructed customer image for which the shares are with the user and the bank. If the generated image is identical to the user, next validation step is performed. If the validation fails, the customer is declared unauthenticated at this very step. This is the first level of security check. If the image is identical, bank sends the signature share of the user to CA. CA does not disclose its share. It sends a reply containing the generated image after stacking the signature shares. The person-in-charge checks the revealed signature against the signature produced. If they match, the user is authenticated. Thus the system provides two-level protection. There are some important points regarding the system architecture:

- CA is contacted only when the user passes first level of security check. This way the communication cost over the network is reduced.
- Even if bank data is manipulated somehow, the signature share is kept safe with CA and authentication process remains secure.
- CA sends the stacked signature image to the bank. This way, the code generation and decision making of authentication process remain isolated. So manipulation of CA data also cannot hamper the authentication process. Security is broken only when both the bank and CA data are compromised.

Figure 2 shows the system architecture. Here XOR operation can be used instead of OR to perform the decryption. It will improve reconstructed image quality significantly as XOR allows for perfect reconstruction of the pixels.

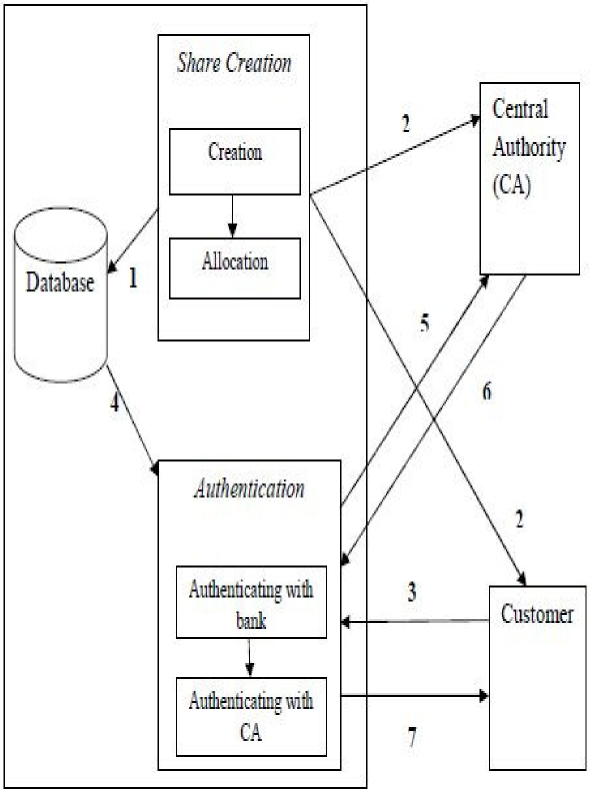

Figure 2: System Architecture

The communication steps are as follows:

1. Image and signature share creation
2. Share allocation to customer and CA
3. Customer requesting for authentication
4. Bank performing authentication with bank share
5. Bank requesting CA to send signature
6. CA replies with reconstructed signature
7. Bank declaring authentication result

The advantages of the proposed architecture are:

1. The proposed system employs two-level check to improve the security over the existing authentication methods.
2. The presence of a third organization, CA enhances the security further as more number of parties is involved in the process. The customer's satisfaction increases as it does not have to trust only the bank. Even if the bank data is compromised, any hacker cannot do the transactions as the signature share is kept with central authority.
3. Even if the card is lost, it cannot be misused.

V. METHOD EXTENSION

The above authentication system is proposed for a physical organization. But it can be extended for doing authentication over network too. Here the customer first sends the image share to the bank. Bank has the customer image and the signature/passcode in its database along with the second image share. Bank matches the reconstructed image with the customer image. If they match, second level of authentication is started. Now the customer sends the signature share to the bank. Bank transfers this share to the central authority. CA then sends the reconstructed image back to the bank. The bank verifies this image with the signature image and declares the authentication result.

A. *Security Threat*

The problem when sending the shares over the network is that they can be tracked by an attacker. The share is just a random pattern of black and white pixels. Though the attacker will not be able to decrypt the share, he will at least gain this information that some data has been encrypted here. With very high computation power and time, he may be able to gain some information about it. One improvement that can be done here is that the shares which are transferred over the network can be hid inside other cover image. Now the share will look like a valid image. One efficient technology for doing this is proposed by Jaya and Anjali Sardana [20]. This way the customer can send the shares to the bank in cover image, known as meaningful share. This is similar to other authentication methods but it improves the security by further hiding the original data.

B. *Drawback*

The drawback of this scheme is that it will take more time for transmitting the shares and taking the authentication decision by the bank. The shares need to be transmitted between the customer-bank pair and the bank-CA pair. So it will take more time for communicating over the network. The bank will have to match the reconstructed image with the images present in the database. This will need a pixel-by-pixel comparison and thus will take more time.

VI. IMPLEMENTATION AND RESULTS

A. *Implementation Details*

The scheme is validated by implementing prototype of customer image generation and reconstruction in Java. The bank already has copy of reconstructed images (kept before allocating the shares) and it can be easily verified by doing a pixel-by-pixel matching of the images produced. Since intermediate shares are meaningful, eavesdropper / sniffer would be unable to perceive the activity of secret being shared.

B. *Results*

The meaningful shares look exactly like the cover image and give no sign that some data has been hidden there. One share for both the images is given to the customer. Bank keeps the Customer share 2 and passes signature share 2 to CA.

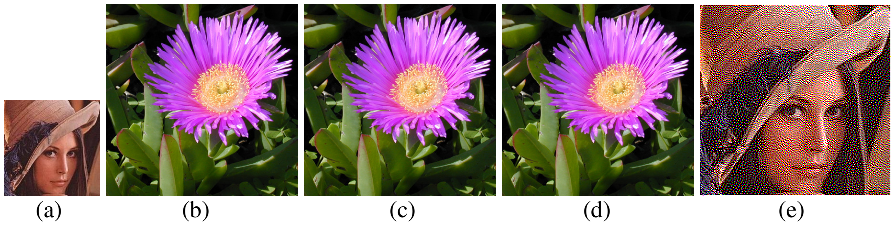

Figure 3: (a)Customer Image (b)Cover Image (c)Meaningful Share 1 (d)Meaningful Share 2 (e)Reconstructed Customer Image

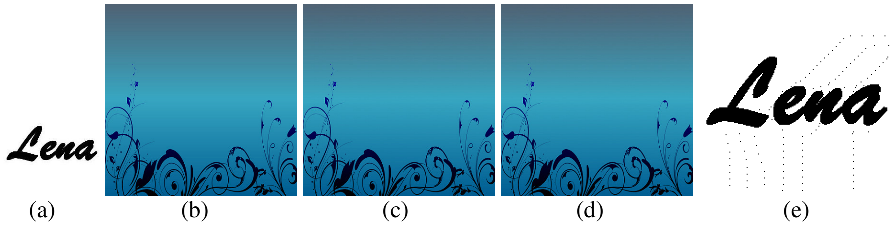

Figure 4: (a)Signature Image (b)Cover Image (c)Meaningful Share 1 (d)Meaningful Share 2 (e)Reconstructed Signature Image

CONCLUSIONS

In this paper, we have proposed an authentication system with the concept of color visual cryptography proposed by Hou. The proposed system improves the security level of authentication process by checking the reconstructed customer image and signature. The use of the system is discussed here in case of banking applications. But it can also be used in some other scenarios such as credit card applications. Overall, this system is very suitable to meet today's authentication challenges.

REFERENCES

[1] *M.* Naor and A. Shamir, "Visual cryptography, Advances in cryptology EUROCRYPT'94," in Lecture Notes in Computer Science. vol. 950, Springer, Berlin, 1995, pp. 1-12.

[2] C. Lin and W. Tsai, "Visual cryptography for gray-level images by dithering techniques," Pattern Recognition Letters, vol. 24, pp. 349-358, 2003.

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

[4] C. Chang, C. Tsai, and T. Chen, "A New Scheme For Sharing Secret Color Images In Computer Network," Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27, 2000.

[5] Chin-Chen Chang, Tai-Xing Yu , "Sharing A Secret Gray Image In Multiple Images," Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.

[6] Y.S. Wu, C.C. Thien, J.C. Lin, Sharing and hiding secret images with size constraint, Pattern Recognition, vol. 37, pp. 1377–1385, 2004.

[7] 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.

[8] D.-S. Tsai, G. Horng, T.-H. Chen, Y.-T. Huang , "A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint," Information Sciences, vol. 179, pp. 3247–3254, 2009.

[9] Y. C. Hou, S.-F. Tu, "A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method," Journal of Research and Practice in Information Technology, vol. 37, pp. 179-191, 2005.

[10] H. Zhang, X. Wang, W. Cao and Y. Huang, "Visual Cryptographic for General Access Structure by Multi-pixel Encoding with Variable Block Size," International Symposium on Knowledge Acqusition and Modeling, 2008.

[11] V. Rijmen and B. Preneel, "Efficient colour visual encryption for shared colors of Benetton," in Eurocrypto'96, Rump Session, Berlin, 1996.

[12] E. R. Verhuel and V. Tilborg, "Construction and Properties of k out of n visual secret sharing schemes," Designs, Codes and Cryptography, vol. 11, pp. 179-196, 1997.

[13] H.-C. Wu and C.-C. Chang, "Sharing visual multi-secrets using circle shares," Computer Standards & Interfaces, vol. 28, pp. 123- 135, 2005.

[14] S. J. Shyu, S.-Y. Huang, Y.-K. Lee, Ran- Zan Wang and K. Chen, "Sharing multiple secrets in visual cryptography," Pattern Recognition, vol. 40, pp. 3633-3651, 2007.

[15] J.-B. Feng, H.-C.Wu, C.-S Tsai, Y.- F.Chang, and Y.-P. Chu, "Visual secret sharing for multiple secrets," Pattern Recognition, vol. 41, pp. 3572-3581, 2008.

[16] S. Droste, "New results in visual cryptography," Advances in cryptology – CRYPTO '96, Lecture Notes in Computer Science, No. 1109, pp. 401–415, 1996.

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

[18] D. Chaum, "Secret-ballot receipts: True voter verifiable elections," IEEE Security and Privacy, vol. 2, pp. 38-47, 2004.

[19] A. Altaf, R. Sirhindi, A. Ahmed, "A Novel Approach against DoS Attacks in WiMAX Authentication using Visual Cryptography", The Second International Conference on Emerging Security Information, Systems and Technologies, SECURWARE, Cap Esterel, France 2008.

[20] Jaya and Anjali Sardana. "Multiple Secrets Sharing With Meaningful Shares," in International Conference on Advances in Computing and Communications (ACC 2011): 2011.Springer-Verlag Berlin Heidelberg , Part IV, CCIS 193, 2011, pp. 233-243.