IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012
ISSN (Online): 1694-0814
www.IJCSI.org

182

Design and Implementation of a Novel Authentication Algorithm for Fool-Proof Lock-Key System Based On Visual Secret Sharing Scheme

Harinandan Tunga[1] and Soumen Mukherjee[2]

[1] Department of Computer Sc. & Engineering
RCC Institute of Information technology
Kolkata, West Bengal, India

[2] Department of Computer Application
RCC Institute of Information technology
Kolkata, West Bengal, India

Abstract

The paper aims at creating an authentication algorithm using visual cryptography that creates a fool-proof lock-key mechanism wherein a lock can be opened by its paired key only and the key cannot be duplicated. In our proposed mechanism we uses a lock and a key, both is one part of given secret image. Every lock-key pair has one associated unique image. The lock is just like a safe door which has a memory and that can be used to transmit and receive signals like the key. Another part of the mechanism is that the lock and the key can change the pixel distribution of the some parts of the secret image when unauthorized access is going on.

Keywords: *Fool-Proof Lock-Key, Visual Cryptography, Visual Secret Sharing Scheme (VSSS), Secret Image, Sub pixel.*

1. Introduction

Security is one of the most important needs of human being today. Reports of thefts have become so common that we have almost accepted them as a part of the society. This calls for the need of secure systems that safeguard our homes, lockers, safes etc. The designed system should therefore provide a level of security that would guarantee complete security to its users. Cryptography (or cryptology; from Greek kryptos, "hidden, secret"; and gráph, "writing", respectively) is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Cryptography can be defined as the conversion of data into a scrambled code that can be sent across a public or private network and deciphered by the intended receiver.

2. Related Patents and Publication Works

In this portion we discuss some of the related works and patent. The Patent number: 6989732 [1], describes improved electronic lock system is provided for use with real estate lock boxes where there is the need for many people to access the secured compartment of the lock box in a controlled manner. The Patent Application number: 11/842,138 [3] talks of a secure computation environments are protected from bogus or rogue load modules, executables and other data elements through use of digital signatures, seals and certificates issued by a verifying authority. The Patent Application number: 12/652,663 [4] is an invention which deals with the application of visual cryptography to check and authenticate votes. Rao et. al. [5] talks of a fingerprint authentication system. Hegde et. al. [6] applies visual cryptography to banking applications. Hu et. al. [7] describes the cheating prevention using visual cryptography. Fang et. al. [8], used a technique of reversing secret images, a novel multi-secret visual cryptography scheme is presented in this paper. During the secret sharing process, the correlative matrices are designed to encode multiple images into two ring shares. Compared with the previous works, the proposed scheme makes the number of secret images not restricted and has obviously improved the pixel expansion and the relative difference. However, none of the prior art attempts, individually or collectively, proposed the system and embodiments indicated and disclosed (later) by the present invention.

3. Extended Visual Cryptography Based on VSSS

Extended Visual Cryptography is a kind of cryptography that can be decoded directly by the human visual system without any special calculation for decryption. There are three input picture one of them is secrete which is embedded on both Fig.1 and Fig.2. As shown in the Fig. 1, Fig. 2 and Fig. 3 below, the system takes two pictures stacked together and generates the third one as output. This type of visual cryptography, which reconstructs the image by stacking some meaningful images together, is especially called Extended Visual Cryptography.

Fig. 1 Embedded image 1   Fig. 2 Embedded image 2

Then stacked one over the other, the following image is revealed –

Fig. 3 Output secrete image

This is the secret image that was to be transmitted. The basic model of the visual cryptography consists of a several number of transparency sheets. On each transparency a cipher text is printed which is indistinguishable from random noise. The hidden message is reconstructed by stacking a certain number of the transparencies and viewing them. The system can be used by anyone without any knowledge of cryptography and without performing any cryptographic computations. Naor and Shamir [14][15] have developed the Visual Secret Sharing Scheme (VSSS) to implement this model. In k out of n VSSS (which is also called (k, n) scheme), a binary image (picture or text) is transformed into n sheets of transparencies of random images. The original image becomes visible when any k sheets of the n transparencies are put together, but any combination of less than k sheets cannot reveal the original binary image.

Fig. 4 Visual Secret Sharing Scheme (VSSS) to implement the model

In the scheme, one pixel of the original image is reproduced by m sub pixels on the sheets. The pixel is considered "on" (transparent) if the number of transparent sub pixels is more than a constant threshold, and "off"(opaque) if the transparent sub pixels is less than a constant lower threshold, when the sheets are stacked together. The contrast α is the difference between the on and off threshold number of transparent pixels. Ateniese et al. [18] has extended the (k, n) VSSS to general access structures where senders can specify all qualified and forbidden subsets of n participants. Droste et. al. [16] considered the problem of sharing more than one secret image among a set of participants, and proposed a method to reconstruct different images with different combinations of sheets. Hofmeister et. al. [17] has discussed to maximize the contrast α using linear programming in the cases of k   {3, 4, n}. Visual cryptography is based on Boolean operations. Therefore half toning is necessary for applying visual cryptography to grayscale images. The proposed mechanism makes some consideration on the average transparency of a pixel in the context of half toning techniques.

4. Proposed Mechanism for Fool-Proof Lock-Key System

4.1 Proposed Algorithm

This proposed mechanism describes a safety mechanism based on visual cryptography. The mechanism described here is a lock-key based mechanism that uses the VSS Scheme to increase its security. This essentially consists of a lock and a key. Every lock-key pair has a unique image associated with it, unknown even to the owner of the same. The image is stored in the internal memory of the lock. This secret image is divided into two parts (hence forth referred to as L2SI_1 and L2SI_2 i.e. 2nd secret image part 1 and part 2 respectively). One of the parts is stored in the lock while the other is stored in the key. The lock, attached to the safe or the door consists of a power source. The lock also has a memory and can transmit and receive signals (passwords) to and from the key respectively. It also has a mechanism that can change the pixel distribution of the parts of the secret image, thus, storing different images in the lock and the key although the secret image remains the same i.e. only the division changes. The lock also consists of the 2nd part of the 1st secret image. The key contains a power port that gets automatically connected to the lock's power source once the key is inserted into the lock. It consists of the second of the first secret image and can send and receive passwords to and from the lock respectively. Another

IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012
ISSN (Online): 1694-0814
www.IJCSI.org

184

secret image is used for the combination. It is divided into two parts too and the 1st part (L1SI_1) is printed on the lock. The other and the complete image are stored in the lock. The proposed authentication algorithm for Fool-Proof Lock-Key System is given bellow. First we discuss the mechanism followed after inserting a key.

Step 1. L1SI_1 is read by the lock, put on LSI_2 and matched with L1SI.
Step 2. If matched, go to 6.
Step 3. The user is intimated of a level-1 breach of security. Lock is not sealed.
Step 4. Procedure ENDS.
Step 5. The password is sent to key by the lock.
Step 6. Key matches it, if matched then it sends L2SI_1 to lock.
Step 7. If no image is received by the lock, GO TO 11.
Step 8. Lock accepts image puts it on L2SI_2 and matches with L2SI.
Step 9. If matched go to 13.
Step 10. Pixel distribution of L2SI_2 changes.
Step 11. The user is intimated of a level-3 breach of security. Lock is sealed automatically.
Step 12. Procedure ENDs.
Step 13. The lock opens.
Step 14. The procedure ends.

The lock's safety is controlled and governed by the two secret images. The only situation that opens the lock is when both the images get successfully matched to the original one. Flow Chart of this algorithm given below:
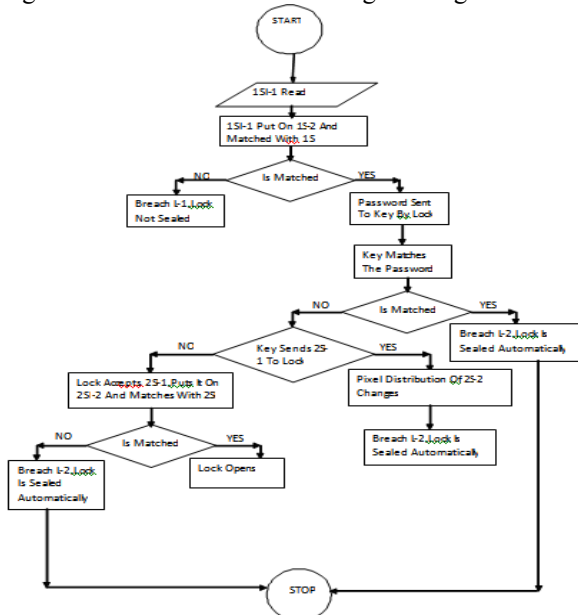

Fig. 5 Flow Chart of Authentication Algorithm for Fool-Proof Lock-Key System

4.2 Fraud Detection

There are two cases of Fraud Detection of a lock key system.

CASE 1: If a random key is used to open the lock – any other key but the original key doesn't have the unique 1SI-1 imprinted on it. When read and put on 1SI-2, the result doesn't match with 1SI and therefore the fraud is detected.

CASE 2: If 1SI-1 is copied on some other key – the key lacks 2SI-1 and therefore the lock gets sealed on such an attempt. The key transmits 2SI-1 if and only if the correct password is sent to it. Even if the password is recorded by a random key to reveal 2SI-1, the pixel distribution of 2SI-2 changes. Therefore 2SI-1 and the new 2SI-2 do not produce 2SI and the lock gets sealed.

5. Experimental Results

The paper was simulated and run on Mat lab. Code was written to generate shares from a grayscale image. They were then superimposed to generate the original image. Also, code was implemented to check two images, pixel by pixel to match them. A GUI was also developed so that the entire process can be carried out and demonstrated with considerable ease of use. The GUI lets the user behave as the key and the lock at different stages and allows providing different authentication messages. Both the levels of security, namely 1 and 2, were carried using several test images. The following portion includes the results and screenshots of the GUI developed for the purpose. The authentication mechanism worked successfully for the shares generated. When no image or an incorrect image was supplied to the lock by the key at the second stage of verification, pixel distribution of L2SI_1 changed. Therefore, the lock was sealed and protected from future attacks. No password but the one designated for the lock-key pair could cause the lock to reveal the contents of L2SI_2. No image but the shares could be used to provide successful access. The verification results are shown in the following tables.

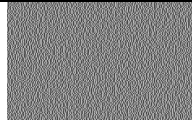Table 1: Experimental Result for verification number 1

IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012
ISSN (Online): 1694-0814
www.IJCSI.org

185
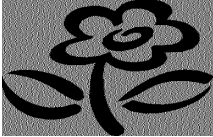
Verification Stage 1:	
Input Images	*Resultant Image*
Fig. 6 L1SI_1 image	Fig. 8 L1SI image
Fig. 7 L1SI_2 image	
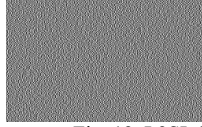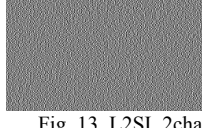
Table 2: Experimental Result for verification number 2

Verification Stage 2:	
Input Images	*Resultant Image*
Fig. 9 L2SI_1 image	Fig. 11 L2SI image
Fig. 10 L2SI_2 image	

Deterrence is the property which is used here for the information contained by the lock in the second stage of the verification is not static. If a random key is used to obtain information from the lock, then the pixel distribution of the image stored in the lock, namely L2SI_2 changes (referred to as L2SI_2changed). When the duplicated key is used to unlock the lock, it is rejected because –

$$L2SI\_2 + L2SI\_2changed \neq L2SI$$

Table 3: Experimental Result for verification number 3

Verification Stage 3:	
Input Images	*Resultant Image*
Fig. 12 L2SI_2 image	Fig. 14 L2SI image
Fig. 13 L2SI_2changed image	

6. Conclusions

Our proposed authentication algorithm has some advantages over the other systems using traditional lock-key based systems. Standard keys have a series of grooves on either side of the key (the key's blade), which limit the type of lock the key can slide into. As the key slides into the lock, the grooves on the blade of the key align with the wards in the key way allowing or denying entry to the cylinder. Then, a series of pointed teeth and notches on the blade allow pins or wafers to move up and down until they are in line with the shear line of the inner and outer cylinder, allowing the cylinder or cam to rotate freely inside the lock and the lock to open. Keys can be duplicated easily even without using the original key. This involves using a piece of soft iron which is inserted into the lock and rotated. The levers of the lock leave an imprint on the soft iron which is then shaped accordingly into grooves. Electronic lock key systems [1], [2], [3] describe systems or mechanisms which do not ensure the completion of a process that follows "handshake" protocol between the lock and the key. In these systems, the work done or the information contained by the lock does not change and therefore can be treated as static. In such a situation, a random key can be used to record the authentication message sent by the lock. Then, the same can be applied to the key to reveal its secret image/code/authentication message. Therefore, the key can be duplicated. Biometric Verification for Authentication using matching of fingerprints is becoming

slowly but gradually obsolete as the fingerprints of the owner can be easily obtained from various objects and picked by using Calcium oxide, Chalk, Haddonite White Lanconide, Mercury-chalk, Titanium dioxide or White tempera. We conclude that in such a system, the only way to open the lock is by means of the original key that is provided with the lock-key pair.

References

[1] Patent number: 6989732, Filing date: Oct 9, 2002, Issue date: Jan 24, 2006. Application number: 10/267,174.

[2] Patent number: 7193503, Filing date: Jul 29, 2005, Issue date: Mar 20, 2007. Application number: 11/193,932.

[3] Application number: 11/842,138, Publication number: US 2008/0033884 A1, Filing date: Aug 21, 2007.

[4] Application number: 12/652,663, Publication number: US 2010/0142005 A1. Filing date: Jan 5, 2010.

[5] Rao, Y.V.S.; Sukonkina, Y.; Bhagwati, C.; Singh, U.K, "Fingerprint based authentication application using visual cryptography methods (Improved ID card)," TENCON 2008 - 2008 IEEE Region 10 Conference.

[6] Hegde, C. Manu, S. Shenoy, P.D. Venugopal, K.R. Patnaik, L.M, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications," 16th International Conference on Advanced Computing and Communications, 2008. ADCOM 2008.

[7] Chih-Ming Hu and Wen-Guey Tzeng, "Cheating Prevention in Visual Cryptography," IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 16, NO. 1, JANUARY 2007.

[8] Li-Guo FANG, Ya-Min Li, Bin YU, "Multi-secret Visual Cryptography Based on Reversed Images," Third International Conference on Information and Computing, 2010.

[9] http://www.en.wikipedia.org.

[10] D.C. Lou, H.K. Tso, J.L. Liu, "A copyright protection scheme for digital images using visual cryptography technique," in Computer Standards and Interfaces, vol.29, no.1, pp.125-131,2007.

[11] M.Naor, A. Shamir, "Visual cryptography," Advances in Cryptology-EUROCRYPT'94, LNCS, vol.950, pp.1-10, 1995.

[12] D.Jin, W.Q.Yan, M.S.Kankanhalli, "Progressive color visual cryptography," Journal of Electronic Imaging, vol.14, no.3, 033019, 2005.

[13] S.J.An, "A new bayer matrix-based scheme of visual cryptography for grey level images," Jounal of System Simulation, vol.16, no.11, pp.2463-2466, 2004.

[14] M. Naor and A. Shamir, "Visual cryptography, advances in cryptology", Eurocrypt '94 Proceeding LNCS, 950:1–12, 1995.

[15] M. Naor and A. Shamir, "Visual cryptography ii: Improving the contrast via the cover base", Theory of Cryptography Library, (96-07), 1996.

[16] Stefan Droste , New Results on Visual Cryptography, CRYPTO 96, Proc. of the 16th Annual International Cryptology Conference, Santa Barbara, CA, August 18-22, 1996, pages 401-415.

[17] Thomas Hofmeister, Matthias Krause, Hans-Ulrich Simon: Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography. COCOON 1997, pages 176-185.

[18] G. Ateniense, C. Blundo, A. de Santis and D.R.Stinson (1996) Visual Cryptography for General Access Structures.

Harinandan Tunga is with RCC Institute of Information Technology Kolkata, India for last nine years. His present research interests include Bioinformatics and Network Security. He has done B.Tech in 2003, ME in 2006. He has four published papers in National & International conferences and Journals. He has supervised several undergraduate and postgraduate dissertations.

Soumen Mukherjee is with RCC Institute of Information Technology Kolkata, India for last eight years. His present research interests include Collaborative Learning, Network Security, Object Oriented Modeling and Signal Processing Architecture. He has done MCA in 2003, ME in 2006 and PGDBM in 2009. He has fifteen published papers in National & International conferences and Journals and ten international book contributions. He has supervised several undergraduate and postgraduate dissertations. He is a Life Member of CSI, IETE, ISTE, ISCA and FOSET.