A Protocol for Secret Sharing using Segment Based Visual Cryptography

[1]Sesha Pallavi Indrakanti, [2]Avadhani P S

[1]Dept. of Computer Applications, GVP Degree College (Autonomous), Visakhapatnam, AP, India
[2]Dept. of Computer Science and Systems Engineering, Andhra University College of Engineering (Autonomous), Andhra University, Visakhapatnam, AP, India

Abstract

Security is playing a vital role in the life of information. Security has become a requirement in the digital world for maintaining the secrecy of the information. Lots of techniques have been proposed for textual data. Maintenance of secrecy of pictorial data is also equally important.

Most of the pictorial hiding goes with pixel based, here a version of Visual Cryptography is presented which is segment-based instead of pixel based. The message which is in the form of numbers is converted into segment based encrypted into two random shares. The decryption process involves the stacking of the two shares.

A protocol for encrypting the secret message in to shares using a 7-segment display and 16-segment display is proposed which will enhance the clarity of the decrypted image. It is easier to view the secret images with the human eye by stacking the transparencies.

Keywords

Secret Sharing, Encryption, Decryption, Segment Based

I. Introduction

Secure distribution of a secret in an insecure channel has got significant priority in the current communication technology era. The rapid growth of computer networks and communication technologies, large amounts of digital data has been transmitted over the internet. However, secret data transmission over an open channel can be easily interfered, forged, or attacked by intruders. For the sake of security, secret data is often encrypted before transmission.

This secure distribution of secret between two parties can be achieved either through symmetric key encryption or asymmetric key encryption. Symmetric key encryption employs only one key with both the users where as asymmetric key encryption employs two keys for communication. The encryption techniques require key distribution protocols for key exchange and key establishment; they are the most fundamental cryptographic primitive in all kinds of applications where security is a concern.

The advances in technology are demanding more robust and less complex security schemes. Other then these traditional symmetric and asymmetric encryption techniques there are secret sharing techniques that have gathered greater prominence. Secret sharing refers to a method of distributing a secret amongst a group of participants, each of which is allocated a share of the secret. Secret sharing was proposed by both Adi Shamir [1] and George Blakley [2] independently of each other in 1979. Their schemes propose that a secure secret sharing scheme distributes shares so that anyone with fewer than t shares has no extra information about the secret than someone with 0 shares. The traditional cryptography schemes encrypted only textual information, where as visual secret sharing schemes encrypted visual information. In order to protect the security of data, in 1994, Noar [3] proposed a new field of cryptography called Visual Cryptography (VC). Visual Cryptography Scheme (VCS) is a kind of secret sharing scheme which allows the encryption of a secret image into n shares that are distributed to n participants.

A secret sharing scheme can be evaluated by its (a) security (b) reconstruction precision (contrast or accuracy), (c) computation complexity and (d) storage requirement (pixel expansion) [4]. The first criterion is satisfied if each share leaks no information from the original image and the original image cannot be reconstructed if there are fewer than k shares collected. The second criterion is considered to be the quality of the reconstructed secret image. The computational complexity concerns the total number of operators required both to generate the shares and to reconstruct the original secret image. The last criterion, which affects data transmission speed, is also called the share size. A large share size implies high transmission and storage cost. An ideal VSS scheme must satisfy high security, high accuracy, low computational complexity, and small share size.

Chen and Wu [5] proposed a (2,2)-threshold visual secret sharing scheme for two secret images. The first secret image is decrypted by only stacking two share images and the second secret image is decrypted also by stacking two share images and one share image rotated. To overcome the angle restriction of Chen and Wu's scheme, Hsu et al [6] proposed another scheme to hide two secret images in two share images with arbitrary rotating angles. Their scheme rolls up the share images to become rings so that it becomes easy to rotate the share images at any desired angle.

Secret sharing techniques belong to the larger area of information hiding that includes watermarking [7-8]. VSS schemes [9] -[14] have come forth by concentrating on processing of binary secret images and have been extended to processing gray level [15] and color image secret sharing[16-18]. I.S.Pallavi et al [19] in 2007 proposed Secure Visual secret sharing scheme in which meaningful shares are used to hide the colored secret image, which is split in to two parts which also reduces the threat of vulnerability.

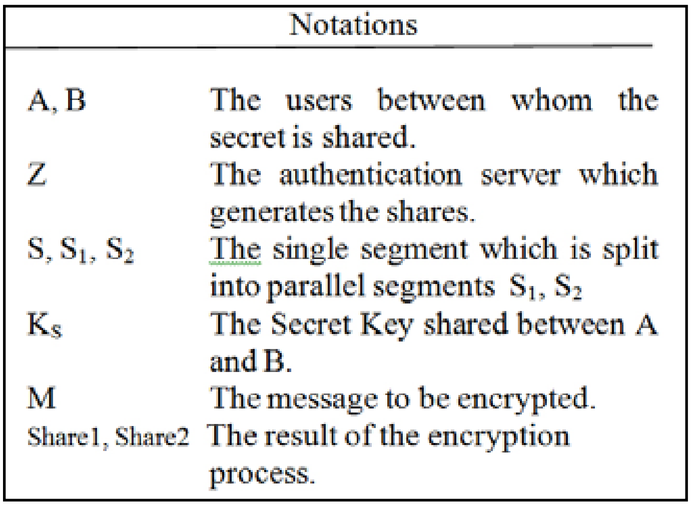
I.S.Pallavi et al in 2011 [20] proposed "Multiple Image Secret Sharing Scheme", which handles the present trend of encrypting multiple secret images. This scheme handles encryption by bisecting the secrets and managing the bisections using the concept of Visual Cryptography. I.S.Pallavi [21] et al in 2011 proposed "A Novel Multiple Visual Secret Data Hiding Scheme" which handles three secrets into 4 shares and further obtain 3 meaning full secrets. There is also a temporary share which helps in the recovery of the secrets. I.S.Pallavi [22] et al in 2011 proposed "Permutation based Image Encryption Technique" in which a secret is encrypted into meaningful shares and a key is constructed based on the encryption. The uniqueness here is that the key is constructed after the encryption process.

However, these earlier works result in a decrypted image of reduced quality. The proposed technique handles segments as the smallest unit of encryption based on visual cryptography to enhance the clarity of the decrypted image. It also satisfies the constraints of an ideal VSS scheme like security , high accuracy, low computational complexity, and small share size.

II. Notations

The following are the notations that are used throughout the protocol.

Table.1: Notations



Notations	
A, B	The users between whom the secret is shared.
Z	The authentication server which generates the shares.
S, S_1, S_2	The single segment which is split into parallel segments S_1, S_2
K_S	The Secret Key shared between A and B.
M	The message to be encrypted.
Share1, Share2	The result of the encryption process.

III. Protocol

An efficient protocol for secret sharing using segment based visual cryptography has been proposed. This is a two out of two visual cryptography technique based on segment display The protocol uses two variants of segment display, seven segment display and sixteen segment display.

A paper by Bernd Borchet [23] in 2007 has proposed a different variant of visual cryptography, i.e. instead of taking pixels as the smallest units to be encrypted, segments of a segment display are encrypted. A paper on Segment based visual cryptography for Key Distribution proposed by Sesha Pallavi Indrakanti and Avadhani P S [24] in 2012 has taken a seven segment display and applied it key distribution which has numerical and this technique is appropriate for maintaining secrecy of the initial exchange of key. The restriction being the non usage of alphabets as they cannot be properly represented using seven segments. For unambiguous representation using segment display a sixteen segment display with visual cryptography has been used for privacy preserving [25].

The proposed protocol involves two users A, B, and an authentication server Z. The authentication server does the process of generating the shares from the secret supplied by the initiator, and distributes the shares to the valid users. The users superimpose the shares to see the secret. The protocol is used for dual applications. One application is used for generating shares from a secret key KS. The other application is an encryption technique which generates the shares of the secret which is in the form of a plain text message M. The protocol in has two processes, one is the share generation process which is the encryption process and the other is the secret reconstruction process that is decryption.

A. Share Generation Process

The process of share generation is the key factor in encryption and key sharing process. The shares are generated taking the segment as the smallest unit instead of pixel. Two types of segment displays have been adopted for the security purpose, which are seven segment display and sixteen segment display. A different variant of segment display is used based on the type of technique used. The secret key constituted of only numbers is generated into shares using seven segment display where as a sixteen segment display is used for encrypting a secret with alpha numeric and special character combination. The process involved in shares generation is the same but the representation of segment display involved varies with the type of the technique.

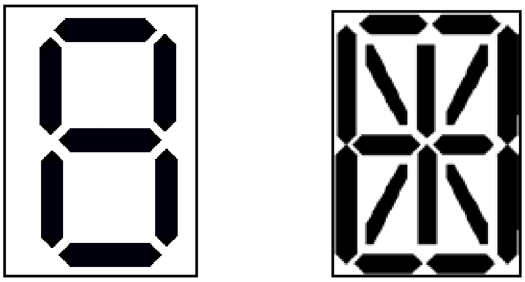


Fig. 1: Seven Segment and Sixteen Segment Displays

The process generating parallel segment depends on the type of character and any character that is taken is converted into either seven segment or sixteen segment display. The variants of segment displays used are shown in fig. 1.

Each segment S in the figure is converted into parallel segments S_1, and S_2. Parallel segments are generated by drawing two segments S_1, and S_2, drawn in white on black backgrounds which are close and parallel as shown in fig. 2. The number of segments required to represent a parallel seven segment display are 14 where as the number of parallel segments required to represent a sixteen segment are 32.

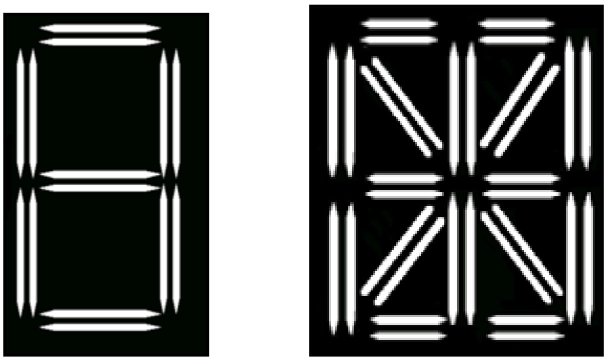


Fig. 2: Parallel Seven Segment and Sixteen Segment Displays

The share generation process is illustrated step wise in the fig. 3. An initiation request and an input from the initiator will result in the generation of the segment display and further the formation of shares 1 and 2. These shares are distributed to the users securely.

Table 2: Share Generation Algorithm

Step	Authentication Server (Z)	Users
1	Accept/ Generate a random KEY (KS) or a secret Message (M) ←	Initiator
2	Authentication server Z generates the segment display based on the below condition: If the type of input is a secret key KS use seven segment display Else If the type of input is a secret message(M), composed of alpha numeric and special characters use sixteen segment display	

3	Z generates a parallel segment S1, and S2 of the above secret in segment representation.	
4	The parallel segment display is now split into share1 and share2 based on the character. The shares are generated Z using parallel segment. at most one of the parallel segment is chosen randomly, depending on the symbol, to generate the share.	
5	Share 1 →	A
6	Share 2 →	B

B. Secret Reconstruction Process

The process of secret reconstruction of secret requires the shares to be stacked on each other to reveal the secret. The shares that are overlaid result in the formation of segments with two colors that are black and white.

The segments bright white in color form the character and the other segments are kept grey in color which is called black. The above scheme satisfies the basic security requirements of secret sharing scheme as follows: (1) with knowledge of both the share, it is easy to reconstruct the secret; and (2) with knowledge one shares, it is impossible to reconstruct the secret. Shamir's scheme of information being is theoretically secure as it satisfies these two requirements without making any computational assumption. The secret reconstruction process does not involve any computational complexity as it is based on the concept of visual cryptography.

IV. Security Analysis and Conclusion

An Attack on confidentiality and integrity of data are the emerging current trends. An attacker can try to recover the secret message or key belonging to a group that the outsider is unauthorized to know. This attack is related to the confidentiality of secret. This protocol concentrates on preserving the confidentiality aspect. The proposed protocol achieves the primary goal of security like confidentiality.

The proposed protocol is immune to brute force attack. This type of attack is utilized when it is not possible to take advantage of other weaknesses in an encryption system. This attack involves systematically checking all possible combinations until the correct key is found. Every character in the share that is generated looks like a seven or a sixteen segment display. The attacker cannot guess the character from the shares.

An attacker cannot guess what the secret is by capturing a single share. For him to learn what the secret is he has to have both the shares. At any point of time if he captures both the shares, it still does not help him obtain the previous session's secret.

An open distributed system in which the users access services on application servers is discussed here. A protocol for preserving the privacy of a secret using visual cryptography and segment display is presented here.

References

[1] A. Shamir,"How to share a secret", Communications of the ACM 22, 1979, pp. 612-613.

[2] Blakley, G. R.,"Safeguarding cryptographic keys", Proceedings of the National Computer Conference, pp: 313–317, 1979.

[3] M. Noar, A. Shamir,"Visual cryptography", A. De Santis (Ed.), Advance in Cryptography: Eurpocrypt'94, Lecture Notes in Computer Science, Vol. 950, pp.1-12, 1994.

[4] D. Wang, L. Zhang, N. Ma, X. Li,"Two secret sharing schemes based on Boolean operations", Proceedings of Pattern Recognition. Published by Elsevier Science Ltd., pp. 2776-2785, 2007.

[5] 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.

[6] C. C. Chang, J. C. 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.

[7] Mandhani, N., Kak, S.,"Watermarking using decimal sequences", Cryptologia, Vol. 29, 2005, pp. 50-58.

[8] Penumarthi, K., Kak, S.,"Augmented watermarking", Cryptologia, Vol. 30, 2006, pp. 173-180.

[9] Yang, C.N., Laih, C.S.,"New (k,k) Visual Secret Sharing schemes using hierarchical structure technique", International Computer Symposium. Proceedings (ICS'98), Workshop on cryptology and information security, pp: 148-154, 1998.

[10] Wu, H.C., Chang, C.C.,"Sharing visual multisecrets using circle shares", Computer Standards & Interfaces, Vol. 28, 2005, pp. 123-135.

[11] Fang, W.P., Lin, J.C.,"Visual Cryptography with Extra Ability of Hiding Confidential Data", Journal of Electronic Imaging, Vol. 15, No. 2, Aug 2006, pp.1530-1541.

[12] Yung-Fu Chen, Yung-Kuan Cha, Ching-Chun Huang, Meng-Hsiun Tsai, Yen-Ping Chu.,"A multiple-level visual secret-sharing scheme without image size expansion", Elsevier Vol. 177, Issue 21, 1 November 2007, pp. 4696–4710.

[13] Parakh, A., Kak, S.,"A recursive threshold visual cryptography scheme", Cryptology ePrint Archive, 2008, Report 2008/535.

[14] Sandeep, K.,"Recursive information hiding in visual cryptography", Cryptology ePrint Archive, 2010, Report 2010/283.

[15] Blude, C., De Santis, A., Naor, M.,"Visual cryptography for grey level images", Information Processing Letters, Vol. 27, 2000, pp. 255-259.

[16] Muecke, I.,"Greyscale and Colour Visual Cryptography", Thesis of degree of Master of Computer Science, 1999, Dalhouse University – Daltech.

[17] R. Lukac, K.N. Plataniotis,"Colour image secretsharing", IEE Electronics Letters, 40, 2004. pp. 529–530

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

[19] I.S.Pallavi, P.S.Avadhani.,"Secure Visual Secret Sharing Scheme", 10th world conference on Integrated Design and Process technology, Antalya, Turkey, pp. 323-325, 2007.

[20] Sesha Pallavi Indrakanti,Venkata Vinay Pragada, P.S.Avadhani,"Multiple Image Secret Sharing Scheme", 20th International Conference on Software Engineering and Data Engineering (SEDE-2011), Las Vegas, USA, on June 20-22. pp. 155-159, 2011,

[21] Sesha Pallavi Indrakanti, Avadhani P.S.,"A Novel Multiple Visual Secret Data Hiding Scheme", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 2 (4) , july-August'2011, pp. 1423-1426.

[22] Sesha Pallavi Indrakanti, Avadhani P S.,"Permutation based Image Encryption Technique", International Journal of Computer (IJCA) Applications (0975 – 8887) Vol. 28, No.

8, August 2011, pp. 45-47.

[23] Bernd Borchert, WSI-2007-04,"Segment-based Visual Cryptography", WSI-2007-04.

[24] Sesha Pallavi Indrakanti, P.S.Avadhani,"Segment Based Visual Cryptography For Key Distribution", International Journal of Computer Science and Engineering Survey (IJCSES), Vol. 3, No. 1, February 2012, pp.105-111.

[25] Sesha Pallavi Indrakanti, Avadhani P S.,"Privacy preserving through segment based visual cryptography", Advanced Computing: An International Journal (ACIJ), Vol. 3, No. 4, July 2012, pp. 95-103.

Sesha Pallavi Indrakanti received her M.Sc. degree from Andhra University 2002. She received her M.Tech. degree in Information technology in 2007 from Andhra University. She has an experience of 10 years in teaching and is presently working as Associate professor and Head of the Department of Computer Applications in G.V.P.Degree College (Autonomous),Visakhapatnam, India. She is pursuing her Ph.D. from Andhra University, Visakhapatnam, India. Her areas of interest are Network Security, Data communications & Networks and Operating Systems.

Prof. P.S.Avadhani did his Masters Degree and Ph.D. from IIT Kanpur. He is presently working as a Professor in the Department of Computer Science and Systems Engineering, Andhra University college of Engineering Autonomous), Visakhapatnam. He has more than 75 papers published in various national/ international journals and conferences. His research areas include Cryptography, Data Security, Algorithms, and Computer Graphics.