Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Visual Pixel Expansion of Secret Image

By Velmurugan.N, Vijayaraj.A
Saveetha Engineering College, Thandalam

Abstract - Two common drawbacks of the visual cryptography scheme (VCS) are the large pixel expansion of each share image and the small contrast of the recovered secret image. In this paper, we propose a step construction to construct VCSOR and VCSXOR for general access structure by applying (2,2)-VCS recursively, where a participant may receive multiple share images. The proposed step construction generates VCSOR and VCSXOR which have optimal pixel expansion and contrast for each qualified set in the general access structure in most cases. Our scheme applies a technique to simplify the access structure, which can reduce the average pixel expansion (APE) in most cases compared with many of the results in the literature. Finally, we give some experimental results and comparisons to show the effectiveness of the proposed scheme.

Keywords : *Average pixel expansion (APE), VCSOR, VCSXOR, Visual Cryptography Scheme (VCS), Share image, Secret image.*

GJCST Classification : *I.4.6*

Strictly as per the compliance and regulations of:

Visual Pixel Expansion of Secret Image

Velmurugan.N [α], Vijayaraj.A [Ω]

Abstract - Two common drawbacks of the visual cryptography scheme (VCS) are the large pixel expansion of each share image and the small contrast of the recovered secret image. In this paper, we propose a step construction to construct VCSOR and VCSXOR for general access structure by applying (2,2)-VCS recursively, where a participant may receive multiple share images. The proposed step construction generates VCSOR and VCSXOR which have optimal pixel expansion and contrast for each qualified set in the general access structure in most cases. Our scheme applies a technique to simplify the access structure, which can reduce the average pixel expansion (APE) in most cases compared with many of the results in the literature. Finally, we give some experimental results and comparisons to show the effectiveness of the proposed scheme.

Keywords : Average pixel expansion (APE), VCSOR, VCSXOR, Visual Cryptography Scheme (VCS), Share image, Secret image.

I. Overview of the Paper

In this project, there is a secret image which is encrypted into some share images. The secret image is called the original secret image for clarity, and the share images are the encrypted images. When a qualified set of share images are stacked together properly, it gives a visual image which is almost the same as the original secret image or recovered secret image. In the case of black and white images, the original secret image is represented as a pattern of black and white pixels. Each of these pixels is divided into subpixels which themselves are encoded as black and white to produce the share images. The recovered secret image is also a pattern of black and white subpixels which should visually reveal the original secret image if a qualified set of share images is stacked. This paper will focus on the black and white images, where a white pixel is denoted by the number 0 and a black pixel is denoted by the number 1. Using these 0's and 1's the XOR and OR operation takes place to recover the original secret image.In a traditional VCS, each participant takes one share image and all the share images have the same pixel expansion. However, in proposed construction of this paper, each of the participants may take multiple share images with different pixel expansions. So, in the following part, list the pixel expansions of all the share images for each participant. We compute the average pixel expansion (APE) as well, where the APE is defined as the average value of the total pixel expansions of the share images that each participant holds. Quantum key distribution protocol which works on network security by the use of key agreement. Secret Key is used by each user in the network. Each user has unique Secret Key and will be shared by each user to Trusted Center. In Trusted Center we have to generate a Key for network Security with the Help of Algorithms and Quantum Mechanics. Through that we have to prove how secure the data has been transmitted over network to receiver.

Author α : Assistant Professor, Department of MCA, Saveetha Engineering College, Thandalam, Chennai-602 105.
E-mail : velmurugann@yahoo.com
Author Ω : Associate Professor, Department of IT, Saveetha Engineering College, Thandalam,Chennai-602 105.
E-mail : satturvijay@yahoo.com

II. Existing System

In 2008 an algorithm for visual cryptography has been developed by Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, and L. M. Patnaik for Banking Applications. The aim of the algorithm was to design an efficient technique for checking authenticity of the customer in corebanking and internet banking applications. In 2008 Avishek Adhikari and Bimal Roy have proposed On some Constructions of Monochrome Visual Cryptographic Schemes, which is a (2, n) visual cryptographic scheme.Data hiding in halftone images using conjugate ordered dithering (DHCOD) algorithm is an existing algorithm which is used for visual cryptography scheme. In this algorithm let X is the cover image and H is the image to be hidden i.e. secret image.

1. Add some noise to the secret image i.e. H. Let us call it as H1.It introduces some stochastic factors between the original multi-tone images and final share. This step is very important to break the direct correlation between multi-tone and share images.
2. Convert the noisy secret image i.e. H1 into binary image. Let us call it as H2.
3. Generate the first share X1: X1 will be nothing but a dithered halftone image generated by the cover image X. We can use dithering technique to generate the halftone image.The error diffusion technique spreads the quantized error in neighboring pixels which can affect in halftoning of that pixel and we might get wrong value for e.g. a pixel which should be a black one can turn to a white pixel. While in ordered dithering we deals with individual pixels and it is takes less computation to generate the halftone image. Since this work is completely based on pixel by pixel manner so it is better to use ordered dithering with respect to error diffusion. We have also made a small change in the

revealing operation of DHCOD algorithm which shows a dramatically good result in the revealed image. If we change the revealing operation from "AND" to "XOR" then we get a very clear secret image without any cover image. But we cannot use this for visual cryptography since we are performing XOR operation and it does not work for stacking of shares. But it may be very useful in copyright protection and other cryptographic scheme.

Merits and Demerits of this Scheme

Proposed scheme provides a high-level security. First phase i.e. visual cryptographic encryption adds the advantages and security of basic schemes. Then phase two adds the advantage and security DHCOD algorithm. Here we get the shares with some information as some image can be shown in the shares with respect to completely black and white pixels in basic scheme. Since it provides better security so it is most useful in transmission of financial documents. More applications can also be developed which require a high level security. As we know no scheme can be perfect in all aspects. This scheme also has drawbacks as the quality of the revealed image is not rich. Since it uses second phase takes the input as the result of first phase i.e. visual cryptographic encryption so definitely it will have the low contrast and high pixel expansion.

III. Proposed System

To overcome the drawbacks of visual cryptography schemes we propose a step construction to construct VCS_{OR} and VCS_{XOR} for general access structure by applying (2,2)-VCS recursively, where a participant may receive multiple share images. The proposed step construction generates VCS_{OR} and VCS_{XOR} which have optimal pixel expansion and contrast for each qualified set in the general access structure in most cases. Our scheme applies a technique to simplify the access structure, which can reduce the average pixel expansion (APE) in most cases compared with many of the results in the literature. Finally, we give some experimental results and comparisons to show the effectiveness of the proposed scheme.

In a traditional VCS, each participant takes one share image and all the share images have the same pixel expansion. However, in proposed construction of this paper, each of the participants may take multiple share images with different pixel expansions. So, in the following part, list the pixel expansions of all the share images for each participant. We compute the average pixel expansion (APE) as well, where the APE is defined as the average value of the total pixel expansions of the share images that each participant holds.Particularly, for a set of participants A, we define the pixel expansion of A as the largest pixel expansion of the share images of A. If A is a qualified set, then define the contrast of A as the contrast of the recovered secret image after adjusting stacking.The participants may have multiple share images, and different qualified sets of share images may result in different contrasts. So, in this paper will focus pixel expansion as well as contrast of the secret image.

Data Flow Diagram

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system. A data flow diagram can also be used for the visualization of data processing (structured design). It is common practice for a designer to draw a context-level DFD first which shows the interaction between the system and outside entities. This context-level DFD is then "exploded" to show more detail of the system being modelled.

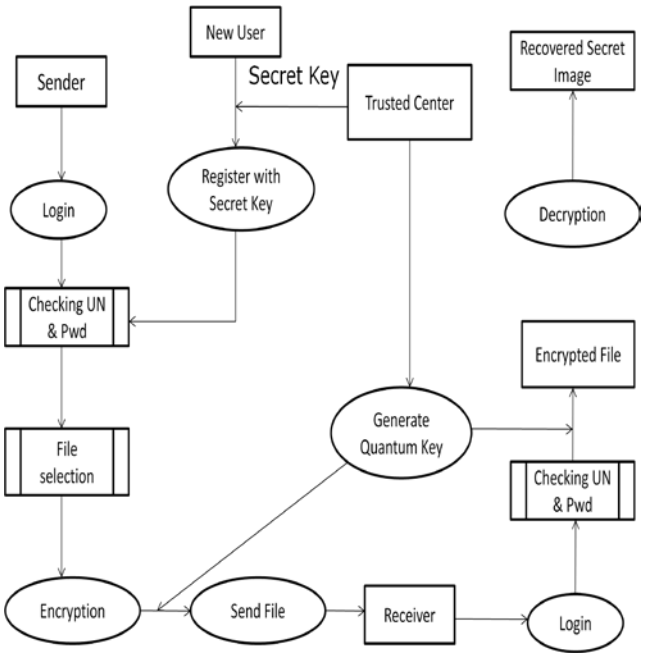

Fig : Data Flow Diagram

IV. Module Description

This includes three basic modules. They are

- Sender
- Trusted Center
- Receiver

SENDER

Getting Authorization is the first stage in sending phase. If a user wants to send a text to Destination user, he wants unique Identification. By using that Identification System knows that the person is an authorized person. This phase or Sender Module has Sub Modules. They are as:

- Registration

- Login
- Send Data

Registration is the Initial state for getting Authentication. By Providing username and Password user sets their Authentication. And System provides one more credentials that is Secret key which is generated by the system for each user. By using username, Password and Secret key system will identify the Authorized person. These credentials are provided to user for the login purpose. These values are stored in the Database. The Database access will be through the registration form in the project. A user wants to send a file means, he/she must log in by using his/her authentication credentials. In this module we have to give username, password and Secret key which was generated by the system.If the user does not provide proper information or the given information is mismatched with database then our system shows Exception message immediately.If the user's details are verified and matched with the existing database then our system allows the person to transmit the file.

TRUSTED CENTER

This module provides the path for the data transfer from the sender to the receiver. This will also generates and verifies the generated key simultaneously.

Verify the secret key received from the user and authenticate the corresponding user for secure transmission. It is shared secret key which is used to for encryption and decryption. The size of session key is 8 bits. This session key is generated from pseudo random prime number and exponential value of random number.

RECEIVER

Getting Authorization is the first stage in receive phase. If a user wants to receive a text from source user, he wants unique Identification. By using that Identification System knows that the person is an authorized person. Verifying the credentials provided, it will allow the user to receive the data. The data given are stored in the database. Similarly there will be secret key generation. In the receiver there will be decryption module. This phase or Receiver Module has Sub Modules. They are as:

1. Registration
2. Login
3. Receive Data

Registration is the Initial state for getting Authentication. By Providing username and Password user sets their Authentication. System provides one more credentials that is Secret key which is generated by the system for each user. By using username, Password and Secret key system will identify the Authorized person. These values are stored in the Database. A user wants to send a file means, he/she must log in by using his/her authentication credentials. In this module we have to give username, password and Secret key which was generated by the system.If the user does not provide proper information or the given information is mismatched with database then our system shows Exception message immediately.After login the TCP program calls i.e. our Trusted Center program starts listen the client or sender. Through Login we send the sender's secret key for Identification. If the given credentials provided matches the data in the database then it allows the transaction. If improper it declines the transaction and identifies that it is an unauthorized user. Here, the receiver waits for the sender request to send the data.

The main aim of this module is to decrypt a file. Decryption will happen only if the system gets a key from Trusted Center (TC). So after verification of user identification system will send the current user's name and his/her secret key to Trusted Center (TC).

V. Implementation

Implementation is the most crucial stage in achieving a successful system and giving the user's confidence that the new system is workable and effective. Implementation of a modified application to replace an existing one. This type of conversation is relatively easy to handle, provide there are no major changes in the system. Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user. And so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly.

MAINTENANCE

The software will definitely undergo change once it is deliver to the customer. There can be many reasons for this change to occur. Change could happen because of some unexpected input values into the system. In addition, the changes in the system could directly affect the software operation. The software should be developed to accommodate changes that could happen during the post implementation period.

VI. Conclusion

In this paper, the step construction of VCS for general access structure which improves the pixel expansion and contrast properties compared with many of the known results in the literature. According to the step construction proposed in this paper, the VCS with general access structure can be constructed by only applying (2, 2)-VCS recursively, regardless of whether the underlying operation is OR or XOR, where a participant may receive multiple share images. This result is most interesting, because the construction of

XOR for general access structure has never been claimed to be possible before. Using Cryptography scheme, image is transferred in a secure mode through the trusted center. Simultaneously, the quantum key is generated in the trusted center and it is distributed to the sender and the receiver. By, this authentication the third party cannot interfere in the middle during the data transfer. The proposed construction can generate optimal OR and XOR for each qualified set and our schemes can also reduce the APE in the most cases compared with the known results in the literature.

References References Referencias

1. M. Naor and A. Shamir, "Visual Cryptography," in EUROCRYPT'94, Berlin, 1995, vol LNCS 950, pp. 1-12, Springer-Verlag.
2. E. Bihman and A. Itzkovitz, "Visual Cryptography with polarization," in RUMP Session of CRYPTO'98, 1997.
3. S. Droste, "New results on visual cryptography," in CRYPTO'96, 1996, vol. 1109, pp. 401-415,Springer-VerlagLNCS.
4. C. Blundo, A. De Santis, and D. R. Stinson, "On the Contrast in visual cryptography schemes," J. Crypotology, vol. 12, no. 4, pp. 261-289, 1999.
5. C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett., vol. 25, pp. 481-494, 2004.
6. S. Cimato, R. De Prisco, and A. De Santis, "Probablistic visual cryptography schemes," Computer J., vol. 49, No. 1, pp. 97-107, 2006.
7. X. M. Chen, "On the simplification of the acces: structure secret sharing schemes(in Chinese), "China Sci. Bulletin, vol. 15, pp. 1599-1603,1999.
8. C. N. Yang and T. S. Chen, "Size –adjustable visual secret sharing schemes," in ASIA CRYPT'2002, 2002, vol. 2501, pp. 328-345, Springer-VerlagLNCS.