International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 7 (2014), pp. 727-732

http://www. irphouse.com

Two Step Share Synthesized Image Stamper Algorithm for Secure Visual Sharing

C Chandrasekar[1] and K E Narayana[2]

[1, 2] *Department of Computer Science And Engineering,*
[1, 2] *Indira Institute Of Engineering And Technology,*
Tiruvallur – 631203, Tamilnadu, India

ABSTRACT

Visual cryptography (VC), allows the encryption of secret information in the image form. By applying the concept of secret sharing, a secret image can be encrypted as different share images printed on transparencies, which are then distributed to participants. By stacking transparencies (shares) directly, the secret images can be revealed and visually recognized by humans without any computational devices and cryptographic knowledge. On the other hand, any one share or a portion of shares can leak nothing related to the secret image. VC is a very good solution for sharing secrets when computers cannot be employed for the decryption process. VSS schemes generate noise-like random pixels on shares to hide secret images. In this manner, the secret can be perfectly concealed on the share images. However, these schemes suffer from a management problem—dealers cannot identify each share visually. Each share constitutes some information and when k shares out of n stacks together the secret will reveal. However less than k shares will not work. The advantage of the visual secret sharing scheme is its decryption process i.e., to decrypt the secret image information using human visual system without any computation. The Traditional Visual Cryptography approach suffers from share identification problem. This problem can be solved by this system thereby incorporating the concept of image stamping that adds a meaning full cover image in each share. The existing scenario for general access structures also suffer from pixel expansion problem when rejoining the image share in other end, hence in our proposed approach we are trying to enhance the image by reducing the grayscale in order to acquire the image as in the original before transmission.

Keywords—Extended visual cryptography (EVC), general access structures, optimization, Average pixel expansion (APE), visual secret sharing scheme.

1. INTRODUCTION

Visual cryptography (VC), allows the encryption of secret information in the image form. By applying the concept of secret sharing, a secret image can be encrypted as different share images printed on transparencies, which are then distributed to participants. By stacking transparencies (shares) directly, the secret images can be revealed and visually recognized by humans without any computational devices and cryptographic knowledge. On the other hand, any one share or a portion of shares can leak nothing related to the secret image. VC is a very good solution for sharing secrets when computers cannot be employed for the decryption process. VSS schemes generate noise-like random pixels on shares to hide secret images. In this manner, the secret can be perfectly concealed on the share images. However, these schemes suffer from a management problem dealers cannot identify each share visually. Hence, researchers have developed the extended visual cryptography scheme (EVCS) also known as the friendly VC scheme which adds a meaningful cover image on each share to address the management problem.

In this project of propose a two phase encryption algorithm of EVCS for general access structures to overcome with the pixel expansion problem. The proposed algorithm is applicable to binary secret/cover images, and no computational devices are needed during the decryption phase. In order to avoid pixel expansion, we do not adopt the traditional VC-based approach to encrypt secret images. The encryption process can be divided into two phases. The first phase of the algorithm, which uses optimization techniques for a given access structure, constructs a set of noise-like shares that are pixel-expansion-free.

The main approach is that the participants can take multiple share images for sharing one secret image. Based on their idea, an access structure can be partitioned into several independent access structures to reduce the average pixel expansion (APE). This phase aims to construct a pixel expansion- free VCS for a given access structure .The main idea behind the solution approach is as follows. A security system employs different keys to protect a secret and distributes these keys to participants. Each key may be duplicated and will be distributed to at least one participant. Each participant is allowed to hold at least one key.

Our proposed algorithm can totally remove the pixel expansion. The proposed stamping algorithm may result in some dim traces of cover images on the recovered images. There are three ways to remove or conceal the traces to promote the display quality for recovered images. First, use graphs drawn by lines be the cover images, for example, the cover images. Second, adjust the density of cover images as low as possible. Finally, adopt a pair of complementary images to be the cover images in each qualified set.

Our Proposed system involves an automatic segregator of images which is a two-step process of converting any images into the required Visual cryptography formatted images (Converting the mode of the image and size of the image). After getting the exact image, the images will be bifurcated into various shares depends on the access structure. In our project, we have a secret image which needs to be encode into N shares printed on transparencies. Option of providing decision of the number of shares to the user is the new feature introduced. The shares of the images appear

random and contain no decipherable information's about the underlying secret image. Still, , if any 2 or more (Based on access structure) of the shares are stacked on top of one another the secret image becomes decipherable by the human eye. Once the shares were taken the shares needs to be stamped with the help of "Block-Based cipher Algorithm".

So that, a clear picture of segregating the images based on the viewable identifiers. Our project involves two step process of removing the stamp and de-cipher the logic behind the share spread and everything will be decided based on the underlying access structure. Enhancing the clarity of the image before processing for shares and after stamping is an important feature and provides added advantage while extracting and deciphering. The secret shared images will be stored in the database.

In our Project, providing a multiple shares based on the access structure with stamping concept is one of the runtime decisions taken in our system. The shares were stored in the DB repository for future references. Storing the shares in a safe repository is one the major advantages of the project. We are utilizing Microsoft's latest concept of storing the data in the format of File Stream in the database. Enhancing the visual clarity of the image before processing the images is one of the major advantage of our system.

2. PREVIOUS STUDIES

A) Reviews VCS/EVCS for GASs

1) Ateniese's VCS/EVCS for GASs: Ateniese's VCS approach for GASs also suffers from the pixel expansion problem. It will expand the size of shares 2–8 times for strong access structures on at the most four participants [10]. Moreover, their extended method for -EVCS will introduce extra pixel expansion that will enlarge the size of the shares and decrease the contrast of the recovered images.

There are other drawbacks of Ateniese's approach: black secret pixels cannot be completely recovered the aspect ratio of the recovered image cannot be maintained; the hyper graph coloring problem, which is NP-hard, needs to be solved; this approach needs a sophisticated codebook design; and the solution approach has to rely on the basis matrices of the existing VCSs cannot be generalized.

2) Liu's VCS for GASs: Liu claimed that his approach could improve the average pixel expansion and contrast properties as compared with Ateniese's approach. However, a comparison with the conventional VCS showed that Liu's approach had some additional drawbacks: first, the participants may take multiple share images with different pixel expansions for one secret image. This differs from conventional VC schemes and will increase administrative inconvenience and difficulty. Second, the decryption process is more complicated than conventional VCSs and needs the help of other devices. For example, for the VCS, the participants need to first enlarge the smaller share to the other larger shares. This will lead to an alignment problem while shares were printed on transparencies. Finally, recovered images cannot maintain the same aspect ratio as the original secret image.

3. PROPOSED SCHEME

In this section, we develop an algorithm based on the simulated annealing (SA) approach to solve the proposed mathematic optimization formulation for the GAS problem. We transform and relax the original mathematical model for the GAS solver to simplify solution procedures. Our solution approach adopts an iterative improvement framework. The share constructor consists of two modules the encryptor and the share synthesizer. We have proposed a stamping algorithm to stamp cover images on I-shares, which were produced in the first phase. There are two major differences between our approach and the existing research for the EVCS. The stamping algorithm tries to add black cover-pixels on the same coordinate of each I-share to reduce the overall number of extra cover-pixels in the recovered image.

3.1 Visual Binary Algorithm

The image is encoded in n number of shares and the message can be revealed by stacking/embedding k of those n shares. However, if k - 1 shares are stacked together, the encoded message cannot be seen to the user. A share generation scheme corresponding to n = 2. This is applied to a binary image by assigning the corresponding sub pixel grouping to the pixels throughout the image. This results in two random shares where the message cannot be identified.

3.2 Block Based Cipher Algorithm

The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbors. In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. At the receiver side, the original image can be obtained by the inverse transformation of the blocks.

4. IMPLEMENTATION

The user will be given a secure login and provide all the necessary details. Multiple users will be created in a hierarchical manner. So that, the owner of the data will login and an automatic bifurcation of images will happen based on the logged in users sub child. The information about the hierarchy needs to be given to the GAS system.

Logging into this system is enable with MD5 algorithmic security. Then the images will be uploaded by the data owner. An automatic recognizer in turn our GAS will take care of analyzing the general access structure inside the system and based on that, the images will be segregated. In VC scheme each pixel ‘p’ of the secret image is encrypted into a pair of sub pixels in each of the two shares. If ‘p’ is white, one of the two columns under the white pixel is selected. If p is black, one of the two columns under the black pixel is selected. In each case, the selection is performed randomly such that each column has 50% probability to be chosen. The above points is valid for the system which has only two shares. Whereas in our system, the GAS solver will identify the number of shares automatically. Based on the number of shares, the pixel will be subdivided and ready to share to the end user.

The major drawback of the system is to identify the shares if the shares get collapsed. We don't have a proper system to identify such kind of pictures. That's why, to overcome such kind of problem. We are proposing a system which has a stamping system. Our stamping system involves stamping of a picture on top of the other images.

This is one of the most complex part in the system. Once the images were provided by the user. The images were validated. An automatic Image synthesize system will validate the images and it will be merged. In case, the images were not in a good shape. An automatic indication of the image not available will be given to the system.

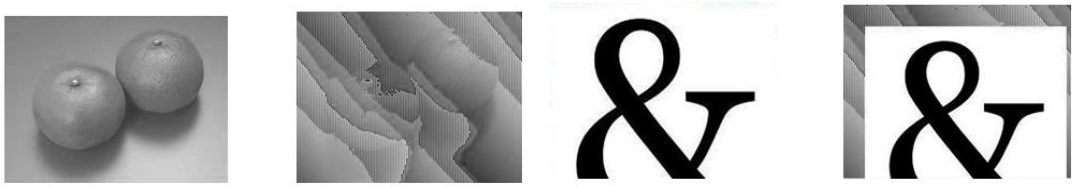

Fig. 4.1 Implementation results for stamping a cover image.

The use of the stamping algorithm reduces only slightly the contrast of the recovered images. This degradation is proportional to the parameter regardless of the VCS's access structure. This verifies the effectiveness of the proposed stamping algorithm.

5. CONCLUSION

In this project by proposing a two-phase algorithm for the Extended Visual Cryptography Scheme for general access structures. Our method guarantees the blackness of black secret pixels for VCSs and improves the display quality of the worst-case image which overcomes the pixel expansion problem. Our approach has better performances than those proposed in previous research in terms of the display quality of the recovered image, which includes contrast, perfect reconstruction of black secret pixels, and maintenance of the same aspect ratio as that of the original secret image. Network security in terms of information passing using secret image has a wide vision in the recent computer technology. The cryptographic means of the proposed system by means of secure image passing can also be extended by the incorporating the same ideas for audio and video information. Biometric Authentication for Banking and Financial Systems.

6. REFERENCES

[1] M. Naor and A. Shamir(1994), "Visual cryptography, " in Proc. Advances in Cryptology (Eurprocrypt'94), pp. 1–12.

[2] E. R. Verheul and H. C. A. v. Tilborg(1997), “Constructions and properties of k-out-of-n visual secret sharing schemes, ” Designs Codes Crypto., vol. 11, pp. 179–196.
[3] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography, ” Theor. Comput. Sci., vol. 250, pp. 143–161, 2001.
[4] H. Koga(2002), “A general formula of the (t, n)-threshold visual secret sharing scheme, ” in Proc. Advances in Cryptology (Asiacrypt), pp. 328–345.
[5] A. Adhikari and S. Sikdar(2003), “A new (2, n)-visual threshold scheme for color images, ” in Proc. INDOCRYPT 2003, Berlin, Germany, pp. 148–161.
[6] C. Blundo, P. D’Arco, A. D. Santis, and D. R. Stinson(2003), “Contrast optimal threshold visual cryptography schemes, ” SIAMJ Discrete Math., vol. 16, pp. 224–261.
[7] C. N. Yang(2004), “New visual secret sharing schemes using probabilistic method, ” Pattern Recognit. Lett., vol. 25, pp. 481–494.
[8] F. Liu, C. Wu, and X. Lin, “Step construction of visual cryptography schemes, ” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 27–38, Mar. 2010.