Distributing Confidentiality to a Visual Secret Sharing Scheme

Neethu T. Sunil, V. Tharmalingam

Abstract – A Visual Secret Sharing (VSS) scheme is one realization of secret sharing schemes without using computation which distinguishes VSS from ordinary cryptography. In a typical VSS scheme (normally called a (k, n) –threshold VSS scheme), a dealer encodes a secret image in to 'n' shares each of which reveals no information regarding the secret image. In this system ,the secret image can be reproduced only by stacking n number of shares in the correct order. The reproduced images will be clearer (larger contrast) and with small pixel expansion compared to Unconditional security VSS scheme. This security notion is effective when attackers cannot use computers since it may take much time to analyze combinations of sub pixels exhaustively.

Index Terms – Visual secret sharing, Weaker security sharing, halftone technique, visual cryptography.

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer.

In one of the demonstrated visual secret sharing scheme developed by Monsignor and Adi Shamir, an image was cut down into n shares so that only someone with all n shares could decrypt the image, while below the threshold shares revealed no information about the original image. Decryption was performed by overlaying the share images. When proper shares were aligned, the original image would appear .The general idea behind "secret sharing" is to distribute a secret to n different participants , any k participants can reconstruct the secret .Any k-1 or fewer participants cannot reveal anything about the original image.

First the secret image is encrypted into 'n' meaningless share images and it cannot leak any information of the shared secret by any combination of the n share images except for all sharing scheme is necessary. VSS is less complex and cheap compared to other data transmission techniques.

Ordinary VSS schemes have some minor cons, so it would be useful if we can find some alternative to those minor disadvantages and develop a better VSS scheme would help in attaining more security for data transmission at a much lesser cost. The proposed idea comes from the fact that VSS schemes need no computation in decryption. In such a scenario, it may be difficult to analyze every share exhaustively without computers, for instance, they would not investigate combinations and/or statistical data of pixels in shares.

Manuscript received on April, 2013.

Neethu T. Sunil, Computer Science and Engineering, Annai Mathammal Sheela Engineering College, Namakkal District, Tamil Nadu, India.

V.Tharmalingam, Computer Science and Engineering, Annai Mathammal Sheela Engineering College, Namakkal District, Tamil Nadu, India.

Based on this observation, they can relax the unconditional security notion of -threshold VSS schemes to a weaker notion in such a way that it is secure if the image obtained by stacking or fewer shares seem to be a random dot image. We say that such VSS schemes are weakly secure VSS schemes or simply WS-VSS schemes hereafter. On the other hand, we abbreviate the unconditionally secure VSS scheme as US-VSS schemes in this paper. We note here that, in several previous studies on VSS schemes for black–white binary secret images, the weak security notion was implicitly used in their constructions of US-VSS schemes without sufficient security analyses. Hence, it is important to discuss the security of WS-VSS schemes not only in terms of minimizing the pixel expansion but also to evaluate the security of these previous studies in VSS schemes. We define a WS-VSS scheme and give its security analysis inspired by the above background.

II. LITERATURE SURVEY

The following are some of the important concepts in the major papers that were reviewed during the literature survey to get an idea of the different systems existing in the relevant area.

A. How to Share a Secret

In this paper they show how to divide data D into' n' pieces in such a way that D is easily re constructible from any k pieces but even k - 1 pieces reveals no information about D. This method allows the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces.

This paper they generalize the problem to one in which the secret is some data D (e.g., the safe combination) and in which non mechanical solutions (which manipulate this data) are also allowed.

Such a scheme is called a (k, n) threshold scheme. For managing the cryptographic keys, powerful threshold schemes can be helpful keys. To protect the data we can encrypt it .But to protect the encryption key we need a different method (further encryptions change the problem rather than solve it).

B. Secret Sharing Schemes

A secret sharing (SS) scheme is a method to encrypt secret information S into n pieces called shares V1, V2…Vn, each of which has no information about the secret S, but S can be decrypted by collecting several shares. For example, consider a (k; n)-threshold SS scheme illustrated in Figure 1. In this SS scheme, any k out of n shares can decrypt secret S but any k -1 or fewer shares do not leak out any information of S. Hence, even if n - k shares are destroyed by any enemies, we can recover S from the remaining k shares.

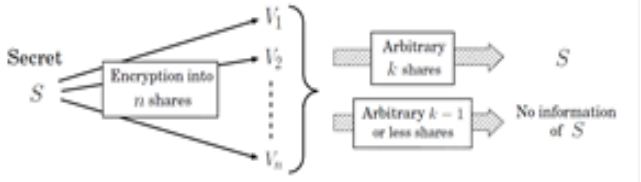

Fig.No.1 A (k, n) –threshold secret sharing scheme

C. *Extension of Threshold secret sharing schemes*

The original SS scheme by Shamir and Blakely is a (k; n)-threshold SS scheme. But, it can be extended in two ways.
1. Perfect S2.3 Extensions of Threshold Secret Sharing scheme.
2. Ramp SS Schemes.
In the case of threshold access structure, we assume that every share is equally important, but there are cases such that we want to make some shares more important than the others.
As another extension of (k; n)-threshold SS schemes, ramp SS schemes were proposed independently by Blakely-Meadows and Yamamoto in 1984. A ramp SS scheme is a SS scheme with intermediate properties between qualified sets and forbidden sets.

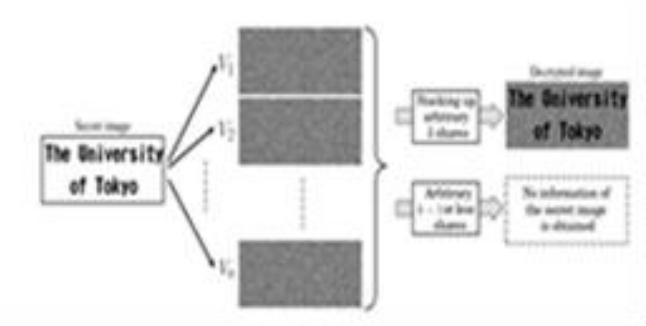

Fig. No .2 An example of a (k; n)-threshold VSS scheme

D. Trivial Secret sharing schemes

There are several (t, n) secret sharing schemes for t = n, when all shares are necessary to recover the secret:
Encode the secret as an integer s. Give to each player i (except one) a random integer ri . Give to the last player the number Failed to parse (Cannot write to or create math output directory): (s - r_1 - r_2 - ... - r_ {n-1}). The secret is the sum of the players' shares .When space efficiency is not a concern, we can reveal a secret to any desired subsets of the players simply by applying the scheme for each subset.

E. *Computationally Secure Secret Sharing Schemes*

The disadvantage of unconditionally secure secret sharing schemes is that the storage and transmission of the shares requires an amount of storage and bandwidth resources equivalent to the size of the secret times the number of shares. If the size of the secret were significant, say 1 GB, and the number of shares were Γ0, then Γ0 GB of data must be stored by the shareholders. Alternate techniques have been proposed for greatly increasing the efficiency of secret sharing schemes, by giving up the requirement of unconditional security.

F. *Visual Cryptography*

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. In 1994, one of the best-known techniques has been developed by Moni Naor and Adi Shamir. They demonstrated a visual secret sharing scheme, where an image was cut down into n shares so that only someone with all n shares could decrypt the image, whereas any information about the original image cannot revealed by n-1 shares. Decryption was performed by overlaying the shares. The original image can be recovered by overlaying all n shares together.

Fig. No.3 Visual Cryptography Example –Shares

Fig .No . 4 Visual Cryptography Example-Output

In this example, the Wikipedia logo has been split into two share images. Here, each of the white pixel in the original image is split into two of the same small blocks that have full black and white pixels. The result is a light-colored block when these two blocks are overlaid exactly .Each black pixel in the original logo is split into two complementary small blocks. The result is a completely black block when these two blocks are overlaid.

G. *Integer programming*

There are many important practical problems that can be formulated as integer programs. In fact, the whole class of NP-complete problems has such a formulation. This means that we cannot expect polynomially fast algorithms to exist for integer programming. Nevertheless, important theoretical advances, coupled with fast computer processors, have opened up new possibilities for finding optimum solutions via integer programming.

III. EXISTING SYSTEM

Here discusses the methods followed by the existing systems. It also gives an idea about the existing system, its limitations, proposed system and its advantages.
In a typical VSS scheme, called a (k, n) -threshold VSS scheme, a dealer encodes a secret image into n shares, each of which reveals no information regarding the secret image. The secret image can be reproduced by stacking k out of n shares in an arbitrary order. Hence, no computation is required in decryption for VSS schemes, which distinguishes VSS schemes from ordinary cryptography. In addition, unconditional security is guaranteed in VSS schemes, which means that every color on the secret image seems to be equiprobable (and hence, no information is obtained) from k-1 or fewer shares no matter they are investigated.
Several secret sharing schemes are said to be information theoretically secure, whereas the unconditional security for improved efficiency maintaining enough security to be considered as secure as other common cryptographic primitives.
For example, they might allow secrets to be protected by shares with 128-bits of entropy each, since each share would be considered enough to stymie any conceivable present-day adversary, requiring a brute force attack of average size 2127.

A. Disadvantages of Existing System

A drawback exists in VSS schemes. That is, we must expand the original pixels on the secret images in encryption, which makes lower level of contrast of the reproduced images. Hence, many efforts have been devoted to minimizing the pixel expansion and to maximize the contrast of reproduced images. As a result, tight lower bounds for pixel expansion were derived for several VSS schemes.

Ramp schemes in VSS schemes were studied in, in which a secret image is partially reproduced when the number of shares is below the threshold. Unfortunately, however, this may sometimes make it easy to guess whole secret images from a partial image since the secret is an image in VSS schemes. This fact suggests that it is difficult to apply the original concept of ramp schemes in secret sharing schemes directly to VSS schemes. Hence, it is necessary to introduce another approach to extend VSS schemes into ramp schemes. VSS schemes need no computation in decryption.

The main disadvantages summarized below:-

• A secret image is partially reproduced when the number of shares is below the threshold.

• It easy to guess whole secret image from a partial image since the secret is an image in VSS schemes.

• Confidentiality is also less.

IV. PROPOSED SYSTEM

The proposed idea comes from the fact that VSS schemes need no computation in decryption and the generic idea behind the proposed system is to introduce security to a weakly secure visual secret sharing scheme. That is, it is possible to assume in VSS schemes that we do not have (or it is a bother to use) computers in decryption. In such a scenario, it may be difficult to analyze every share exhaustively without computers, for instance, we would not investigate combinations and/or statistical data of pixels in shares. Based on this observation, we can relax the unconditional security notion of (k ,n) -threshold VSS schemes to a weaker notion in such a way that it is secure if the image obtained by stacking k-1 or fewer shares seems to be a random dot image. We say that such VSS schemes are weakly secure VSS schemes , or simply WS-VSS schemes hereafter. On the other hand, we abbreviate the unconditionally secure VSS scheme as US-VSS schemes in this paper. We note here that, in several previous studies on VSS schemes for black–white binary secret images, the weak security notion discussed above was implicitly used without sufficient security mechanisms in their constructions of US-VSS schemes.

Hence, it is important to discuss the security of WS-VSS schemes not only in terms of minimizing the pixel expansion but also to evaluate the security of these previous studies in VSS schemes. Motivated by the above background, we formally define a WS-VSS scheme and give its security analysis.

A. Advantages of Existing System

Advantages are: Security, Confidentiality, less time complexity and less need of storage area.

V. SYSTEM IMPLEMENTATION

A. Color Halftone Image Transformation

Halftone is the reprographic technique that simulates continuous tone imagery through the use of dots, differing either in size, in space or in shaping .The image that is produced by the half toning process is also known as "halftone". We can use the halftone process to decrease the visual reproductions to a binary. This binary reproduction relies on a basic optical illusion—that the human eye can blend the tiny halftone dots into smooth tones.

We apply color halftone transformation to produce color halftone images out of CA, CB and SI. Thus, CA, CB and SI are transformed into color halftone images CA', CB' and SI', respectively. The translation procedure is shown in below figure.

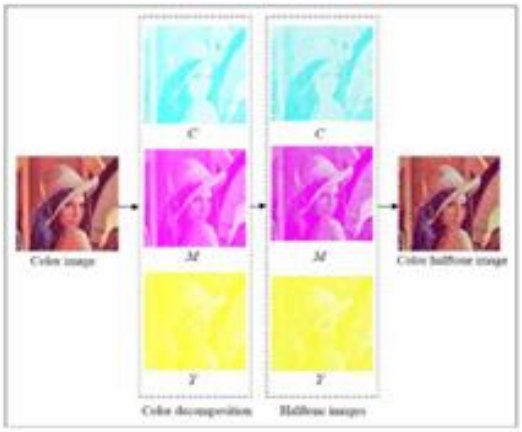

Fig .No. 5 Color halftone image transformation

In our project the color image is transformed to a color halftone image.

The steps involved in this process are:

1) Decompose the color secret image into three separate images that are respectively colored cyan (C), magenta (M) and yellow (Y).
2) The halftone technique is used to translate the three color images into halftone images.
3) By combining the three halftone images, a color halftone image can be generated.

Color halftone image

Extracted image

B. Pixel Extraction Process

Pixel extraction process, extracts pixels from the color halftone image. The following process must be done for each pixel of the color halftone image. According to Share 1, First, 2×2 blocks are built and the four pixels C, M, Y and W are randomly permuted .The number of blocks is also calculated for Share 2 according to the color ratio of the four pixels with the coding tab.

C. Encoding

To generate the shares, two N×N cover images, named CA and CB, are used to encode the N×N secret image SI and make two 2N×2N shares called Share 1 and Share 2. Share 1 and Share 2 are meaningful shares. There are two coding tables referred to in the encoding procedure: cover coding table (CCT) and secret coding table (SCT). As the names suggest, CCT is responsible for the encoding of the cover image, and SCT, on the other hand, is used to encode the secret image .Cover coding and secret coding tables respectively given below:-

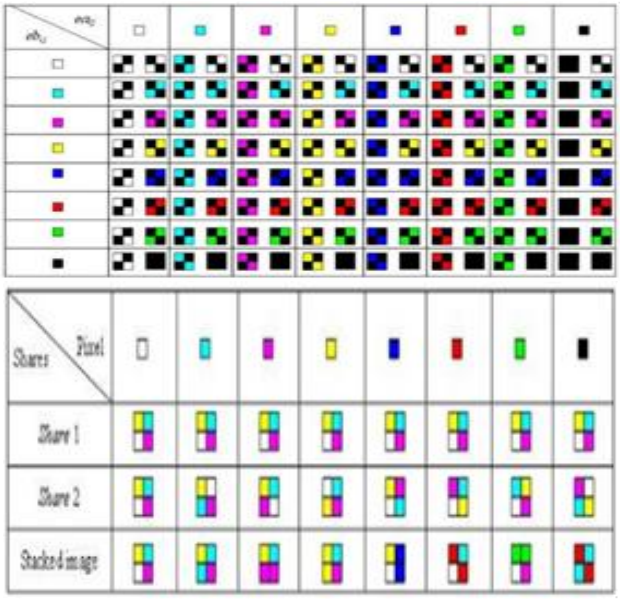

Fig.No.6 a)Cover coding table b)Secret coding table

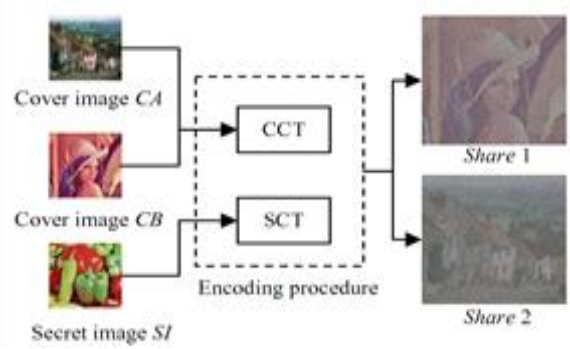

Fig .No. 7 Encoding procedure

D. Decoding

As shown in the Fig .No. 8, in the decoding procedure the secret image can be easily reconstructed by stacking the shares together.

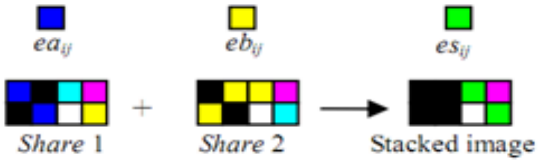

Fig .No. 8 Decoding by stacking n shares together.

In the decryption process, we stack Share 1 and Share 2 together to reconstruct the secret image (see above figure). Also, blocks representing eaij and ebij become black after the stacking, but will not affect the block which represents esij. Meanwhile, this can improve the contrast of the secret image and make the image clearer.

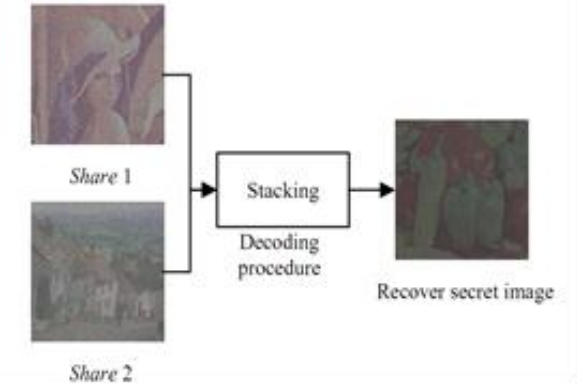

Fig .No. 9 Decoding procedure

VI. CONCLUSION

Based on the observation, we can relax the unconditional security notion of (k,n) -threshold VSS schemes to a weaker notion in such a way that it is secure if the image obtained by stacking k-1 or fewer shares seems to be a random dot image. We say that such VSS schemes are weakly secure VSS schemes or simply WS-VSS schemes hereafter.

REFERENCES

[1] A. Shamir, "How to share a secret"
[2] Mitsugu Iwamoto, "General Construction Methods of Secret Sharing Schemes and Visual Secret Sharing Schemes"
[3] M. Naor and A. Shamir, "Visual cryptography"
[4] www.wikipedia.com
[5] G. Ateniese, C. Blundo , A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures"
[6] C. Blundo, P. D'Arco, A. D. Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes".
[7] Pei-Fang Tsai and Ming-Shi Wang, "An (3, 3)-Visual Secret Sharing Scheme for Hiding Three Secret Data".
[8] Integer programming.
[9] Velmurugan and Vijayaraj, "Visual Pixel Expansion of Secret Image".