RESEARCH ARTICLE OPEN ACCESS

An Efficient General Access Structure Based Multiple Secret Visual Cryptography

S.A.Ayswaria, Guided by: Mrs.A.M.Asbel Shiny
M.E-CS, Dept of ECE, Arunachala College Of Engineering For Women.
Dept of ECE, Arunachala College Of Engineering For Women.

Abstract –
Information, image and media encryption is a method for preventing misuse of adversaries. Because encryption and decryption normally need too complex computation. Visual cryptography is a method in which decryption is performed with used via human visual system. A conventional threshold (k out of n) visual secret sharing scheme encodes one secret image P into n transparencies (called shares) such that any group of k transparencies reveals P when they are superimposed, while that of less k than ones cannot.We define and develop general constructions for threshold multiple-secret visual cryptographic schemes (MVCSs) that are capable of encoding s secret images P_1,P_2…Ps into n shares such that any group of less than k shares obtains none of the secrets, while each group of shares k,k+1,..n reveals P_1,P_2…P_S , respectively, when superimposed.Thus by this scheme we can improve the security of the user through images without using by cryptographical strategies.When secret information is managed by individuals, there exist potential treats of interruption, interception, modification and/or fabrication owing to inadequate management, natural disasters or human attacks. Thus, the design of secret sharing approaches that allow the secret to be shared among a group of participants has become a significant and vital research topic in modern security. Here linear programing is done.This construction is novel and flexible. They can be easily customized to cope with various kinds of MVCSs.

Index Terms — Linear programming, multiple secrets, pixel expansion, threshold visual secret sharing.

I.INTRODUCTION

WHEN secret information is managed by individuals,there exist potential treats of interruption, interception, modification and/or fabrication owing to inadequate management,natural disasters or human attacks (by malicious intruders or unfaithful individuals). Thus, the design of secret sharing approaches that allow the secret to be shared among a group of participants has become a significant and vital research topic in modern security.

Visualcryptography 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.When secret information is managed by individuals, there exist potential treats of interruption, interception, modification and/or fabrication owing to inadequate manage-ment, natural disasters or human attacks (by malicious intruders or unfaithful individuals). Thus, the design of secret sharing approaches that allow the secret to be shared among a group of participants has become a significant and vital research topic in modern security.Visual cryptography (VC), first proposed in 1994 by Naor and Shamir [1], is a secret sharing scheme, based on black- and-white or binary images. Secret images are divided into share images which, on their own, reveal no information of the original secret. Shares may be distributed to various par- ties so that only by collaborating with an appropriate number of other parties, can the resulting combined shares reveal the secret image. Recovery of the secret can be done by super- imposing the share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is of particular interest for security applications based on biometrics [2]. For example, biometric information in the form of facial, finger- print and signature images can be kept secret by partitioning into shares, which can be distributed for safety to a number of parties. The secret image can then recovered when all parties release their share images which are then recombined.

A basic 2-out-of-2 or (2, 2) visual cryptography scheme produces 2 share images from an original image and must stack both shares to reproduce the original image. More generally, a (k, n) scheme produces n shares.With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want .To deal with the security problems of secret images, various image secret sharing schemes have been developed.To prevent digital contents from being intercepted by unauthorized parties is a critical demand in information security. With the increasing popularity of the Internet, which makes possible the instant access or distribution of digital contents, such a demand becomes even more significant.

Traditional crypto- graphic skills recommend plenty of solutions by encrypting the digital data into some cipher text that cannot be recognized by illegal intruders. Yet the decryption of the protected cipher text needs computations. Generally speaking, the cost or efficiency of the software performing the decoding computations is mostly proportional to the security of the encryption algorithm.

With such an interesting feature that no computing device is required but only transparencies superimposition and human visual perception in the decoding process, visual cryptography has attracted much attention since the introduction by Naor and Shamir. Consider a secret binary image P shared in a (k,n) threshold structure. A feasible (k,n)-VCS encodes each pixel p in P into m sub pixels, referred to as the pixel expansion, in each of the s shares such that the superimposed result of k (or more) shares reveals to our eyes (even though it results in a loss of contrast be- tween the reconstructed white and black pixels), while that of less than k ones only reveals a seemingly random picture. In general, the pixel expansion and the contrast in the reconstructed result be- come the most critical measurements for evaluating the quality of a (k,n) -VCS. We expect a smaller pixel expansion to reduce the share size/resolution and ease the carry (or transmission via communication channels) of the shares; or a larger contrast to en-hance the recognition of our visual perception. The optimal pixel expansion of an (n,n)-VCS was proved to be $m_{(n,n)} = 2^{n-1}$ with a contrast of by Naor and Shamir [18], that of a $(2,n)$-VCS was found by Eisen and Stinson [12], and that of a general (k,n) -VCS was explored by Shyu and Chen [23]. For further related studies, please refer to [11], [16], [18], [26] on the essential concepts of (k,n)-VCSs, [1] on the VCS with extended capabilities where the shares may be meaningful (instead of seemingly random) pictures, [2], [3] on the VCS with general access structures, [10], [15], [20], [29] on color VCSs, [5], [7], [12], [14] on the contrast of VCSs, on the pixel expansion of VCSs, and so on.

All of the a fore mentioned studies focused on the sharing of one secret image. Due to the flexibility in practical applications and complexity in theoretical interests, the sharing of multiple secret images, in which different combinations of shares recon- struct different secrets, becomes a significant research topic. The related studies in the literature can be classified into two categories in terms of the decoding processes:

(1) direct superimposition only, where the shares are stacked directly onto each other; and
(2) allowing additional operation(s) before superimposition, where at least one of the shares is allowed to take one or more operations (such as flipping or rotation) before stacking onto others.

Cryptography, or encryption, refers to the encoding messages so that they can only be decoded, and read, by specific individuals. Traditional cryptographic methods typically involve a set of instructions, known as an algorithm, and a secret key ,a word, phrase or string of numbers -- that is known only to the sender and the intended recipient of the message.It provides better security than anyother cryptographical methods.Simple to implement.Decryption algorithm does not required(use a human visual system)so a person unknown visual cryptography can decrypt the message.We can send cipher text through FAX or EMAIL.Lower computational cost since the secret message is recognized only by human eyes and not cryptographically computed.

Visual cryptography is a secret sharing scheme with many applications. some of them include Biometric security, Watermarking, Steganography, Printing and scaning applications, Bank customer identification, Security puposes.

II.REVIEW OF EXSISTING METHOD.

The concept of threshold secret sharing was first proposed by Shamir [19] and Blakley [4] independently in 1979. A threshold (k out of denoted as (k,n)) secret sharing scheme encodes a secret s into n shares, which are distributed to the n participants, such that only any group of k (or more) participants can decode using their shares, while that of less than k ones cannot in an information-security concern. Therefore, the secret is not only safeguarded from all groups of less than shares, but also tolerant of a loss of up to n – k ones.

Visual cryptography (VC, for short) was first proposed by Naor and Shamir at Eurocrypt‟94 [18]. A visual secret sharing (or visual cryptographic) scheme (denoted as (k,n)-VCS) deals with the visual version of secret sharing where the shared secret is in the form of an image, the encoded shares are printed on transparencies (also called shares), and the decoding process becomes the human visual recognition to the superimposed transparencies. Any group of (or more) transparencies reveals the secret image to our eyes when they are superimposed, whereas that of any group of less than k ones only reveals a seemingly random picture from which no information of the secret can be obtained.

Tzeng and Hu [16] introduced another model in which the revealed foreground may be darker or lighter than the background and the secret is only recovered by stacking any two (but neither one nor more than two) shares, denoted by (2,n) -rVCS (for the capability of the reversible foreground and background). The optimal pixel expansion of a (2,n)-rVCS was later proposed by Blundo et al. [3]. Regarding , no result of the minimum pixel expansion in any (k,n)-rVCS has ever been studied.

Visual cryptography operates on binary images, it can be applied to grayscale images by using a halftoning algorithm to first convert the grayscale image to a binary image [5]. This allows for use of visual cryptography schemes to biometric images which are naturally and meaningfully grayscale, such as facial images. Hence, using halftoning techniques to convert grayscale images to binary images is a useful pre-processing step for visual cryptography. However, the halftoning process applied to a grayscale image results in a reduction of the image quality and since visual cryptography schemes also result in a reduction in image quality, mitigating image degradation becomes an important objective in a visual cryptography scheme. Previous schemes integrating halftoning and visual cryptography have suffered from issues such as image expansion (that is, requiring significantly more pixels for the shares and/or recovered secret image) [6] and compromise of the security of the scheme.

III.PROPOSED METHOD.

1.The Basic Colored VSS Scheme

If the smallest graphic unit in a color picture is called pixel, the key concept of colored VSS scheme is to transform the pixel to b sub pixels of color 0, 1,..., c − 1. The infrastructure of colored sub pixels.A circle sub pixel with a sector of angle 2π/c is called a color i sub pixel where the sector has color i and the other part in the circle is black. Of course the color black might be one of the c colors, but it is always distinguishable from the c colors. Figure 1(b) shows that "OR" of elements equals color i , if all elements are color i , otherwise it equals color black. For a colored (k, n) VSS scheme, the dealer produces n transparencies and each pixel in transparency contains b sub pixels. The color of one pixel in stacked transparencies is dependent on the interrelation between the stacked (or "OR") sub pixels. If all sub pixels are of color i , then one sees color i , otherwise one sees black color. Next we use the Definition 6.1 in [9] to show the formal required conditions of a colored (k, n) VSS scheme.

Definition 1 :

A k out of n c-color VSS scheme
S = (C0 , C1 ,..., Cc−1), consists of c collections of n × b q-ary matrices, in which the c colors are elements of the Galois field GF (q). To share a pixel of color i, the dealer randomly chooses one of the matrices in Ci . The chosen matrix defines the color of the b sub pixels in each one of the transparencies. The solution is considered valid if the following three conditions are met for all 0 5 i 5 c − 1:

1. For any S in Ci , the "OR" v of any k of the n rows satisfies zi (v) = h, where v isa vector with coordinates in c colors and black color, and zi (v) denotes the number of coordinates in v equal to color i.
2. For any S in Ci , the "OR" v of any k of the n rows satisfies z j (v) 5 l , for j 6= i.
3. For any i1 < i2 < ... < i S in {1, 2,..., n} with s < k, the collections of s × b matrices Dj , for j ∈ {0, 1,..., c − 1} obtained by restricting each n × b matrix in C j to rows i1 , i2 ,..., i S are indistinguishable in the sense that they contain the same matrices with the same frequencies. Note that h > l and b is the block length of a colored VSS scheme. The cardinalities of the Ci are denoted as r and must coincide. The first two conditions can be called color ensuring that stacking k transparencies will reveal the original color of the pixel. The last condition is called security implying that k − 1 or fewer transparencies give absolutely no information about the shared secret. The value of h and l determines how good the revealed secret image is, and the value of b determines the resolution of the original picture.

2.A Colored k out of n VSS Scheme

we show a method to construct the (k, n) colored VSS scheme. Our scheme uses the different infrastructure of colored sub pixels. When considering the implementation of a colored VSS scheme, our infrastructures of sub pixels is suitable and ready for the image editing package. Note that color i circle sub pixel with a sector or color i and the other sector of black color cannot be directly used in the image editing package. The infrastructure of our color sub pixels is shown below.

We now describe the construction based on the new infrastructure of colored sub pixels. Based on the new definition of colored sub pixels, the optimal construction of black and white (k, n) VSS scheme in [1], [2], [4]–[7] can be used to design a colored (k, n) VSS scheme. Our scheme has the block length b = c × m, where c is the number of colors and m is the share size of the used black and white (k, n) VSS scheme.

THEOREM 1:

The scheme from Construction 1 is a colored (k, n) VSS scheme with "c" colors and the parameters are b = c × m, h = m − l ,„ l = m – h‟.

3.A Colored VSS Scheme with General Access Structure

The authors have presented visual cryptography schemes for general access structures, where an access structure is a specification of all qualified and for- bidden subsets of participants. Any qualified sets can share the black & white secret image. A general colored VSS scheme can also be constructed on such black and white general scheme. We herein use Ateniese et al‟s (0Qual , 0Forb , m)-VCS (visual cryptography scheme) [2] to design a colored VSS scheme for any access structure, where 0Qual and 0Forb are the sets of non-empty subsets of {1, 2,..., n} to define which combinations shall reveal a picture and m is the share size. Any set X = {i1 , i2 ,..., i p } ∈ 0Qual can reveal the shared image, but any set X = {i1 , i2 ,..., i p } ∈ 0Forb has no information on the shared image.

4.An Improved Pre-Processing Scheme

The novel aspect in this approach is to perform the block replacement such that there is a better balance of white and black in the processed secret image. We shall refer to blocks of two white and two black pixels as candidate blocks. In the BBR approach, we balance white and black in the processed image by assigning some candidate blocks to black and others to white. better visual results can be achieved using an intelligent block replacement approach that considers the characteristics of the original image in determining whether a candidate block should be assigned to black or white. The block replacement approach proposed here tries to keep the local ratio of black to white pixels in the processed image close to the local ratio of black to white pixels in the original halftone secret image. Therefore, the resulting recovered image is closer in quality to the original grayscale image.

5.Threshold Visual Cryptographic Scheme

Let $H(V)$ denote the Hamming weight (the number of black subpixels) of a binary vector V . The definition of a (k,n) VCS proposed by Naor and Shamir [18] .

6.Threshold Multiple-Secret Visual Cryptographic Scheme

A conventional (k,n) -VCS shares one secret image among participants following the (k,n) access structure. Here, we con- sider the sharing of multiple, say s , secret images among n par- ticipants. The formal problem specification of a (k,n,s)· -MVCS is presented. The general construction of our scheme is introduced. The definition and construction of the more general (k,n,s,R) -MVCS are presented.

IV.CONCLUSION

We give formal definitions to threshold multiple-secret visual cryptographic schemes, namely (k,n,s) MVCS and (k,n,s,R) MVCS, using only superimposition without any additional operation in decoding process. General constructions for both schemes are designed using the skills of linear programming in which the objective functions are to minimize the pixel expansions with the constraints satisfying the revealing, concealing and security conditions in the corresponding definitions. The minimum pixel expansions obtained by lp_solve for both schemes under different problem scales are summarized and reported, which have never been discussed before in the literature.

The proposed definitions are innovative and significant in revealing the research of visual multiple-secret sharing using only superimposition. The design of the integer linear programs for (k,n,s) -MVCS and (k,n,s,R) -MVCS is novel and flexible to be applied to various types of VCSs. For instance, the reversible VCS (where the revealed foreground may be darker or lighter than the background) proposed in [8] and followed in [23] can be easily dealt with by modifying the revealing condition (from the less than " < " to greater than " > " relation, or simply using the inequality "$\neq$" relation). Even though the proposed constructions are focused on binary secret images, they are applicable to color secret images by exploiting the skills of halftoning, color decomposition, color combination, and so on [15], [20]. It is noticed that the pixel expansion reported are of theoretical interest, yet, some of them, especially when n or s or grows larger, lose the practicability due to the large pixel expansion and degraded contrast. We would not suggest applying the proposed MVCSs for such cases in practical applications.The basis matrices constructed are uniform and canonical (totally symmetric). Concerning the goal of maximal contrast in VCS, Blundo *et al.* [7] have ever discussed the relationship between a canonical scheme and the maximal contrast. Thus, we may utilize their findings to work on the topic of maximizing contrast in visual multiple-secret sharing.

REFERENCES

[1] G. Ateniese, C. Blundo, A. De. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," Theoretical Computer Sci., vol. 250, pp. 143–161, 2001.

[2]. G. Ateniese, C. Blundo, A. De. Santis, and D. R. Stinson, “Visual cryptography for general access structures,” Inf. Computat., vol. 129, pp. 86–106, 1996.

[3]. G. Ateniese, C. Blundo, A. De. Santis, and D. R. Stinson, “Constructions and bounds for visual cryptography,” Lecture Notes Computer Sci., vol. 1099, pp. 416–428, 1996

[4]. G. R. Blakley, “Safeguarding cryptographic keys,” in Proc. Nat. Computer Conf., 1979, vol. 48, pp. 313–317.

[5]. C. Blundo, A. De. Santis, and D. R. Stinson, “On the contrast in visual cryptography,” J. Cryptology, vol. 12, pp. 261–289, 1999.

[6]. C. Blundo, P. D‟Arco, A. De. Santis, and D. R. Stinson, “Contrast optimal threshold visual cryptography schemes,” SIAM J. Discrete Math., vol. 16, pp. 224–261, 2003.

[7]. C. Blundo, S. Cimato, and A. De Santis, “Visual cryptography schemes with optimal pixel expansion,” Theoretical Computer Sci., vol. 369, pp. 169–182, 2006.

[8]. C. Blundo, A. De Bonis, and A. De Santis, “Improved schemes for visual cryptography,” Designs, Codes and Cryptography, vol. 24, pp. 255–278, 2001.

[9]. M. Bose and R. Mukerjee, “Optimal (k , u) visual cryptographic schemes for general k ,” Designs, Codes and Cryptography, vol. 55, pp. 19–35, 2010.

[10]. S. Climato, R. D. Prisco, and A. De. Santis, “Optimal colored threshold visual cryptography schemes,” Designs, Codes and Cryptography, vol. 35, pp. 311–335, 2005.

[11]. S. Droste, “New results on visual cryptography,” Advances in Cryptography-CRYPTO’96, Lecture Notes in Computer Science, vol. 1109, pp. 401–415, 1996.

[12]. P. A. Eisen and D. R. Stinson, “Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels,” Designs, Codes and Cryptography, vol. 25, pp. 15–61, 2002.

[13]. Free Software Foundation, lp_solve Reference Guide Menu [Online]. Available:http://lpsolve.sourceforge.net/5.5, since Feb. 1999

[14]. T. Hofmeister, M. Krause, and H. U. Simon, “Contrast-optimal k out of n secret sharing schemes in visual cryptography,” Lecture Notes in Computer Sci., vol. 1276, pp. 176–185, 1997.

[15.] Y.-C. Hou, “Visual cryptography for color images,” Pattern Recognit,, vol. 36, pp. 1619–1629, 2003.

[16]. T. Katoh and H. Imai, “An extended construction method for visual se- cret sharing schemes,” Electron. Commun. Jpn. (Part III: Fundamental Electronic Science), vol. 81, pp. 55–63, 1998.

[17]. H. Koga, “A general formula of the (t,n) -threshold visual secret sharing scheme,” Lecture Notes in Computer Sci., vol. 2501, pp. 328–345, 2002.

[18]. M. Naor and A. Shamir, “Visual cryptography,” Adv. Cryptography: Eurocrypt’94, Lecture Notes in Computer Sci., vol. 950, pp. 1–12, 1995, Springer. [19]. A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, pp. 612–613, 1979.

[20]. S. J. Shyu, “Efficient visual secret sharing scheme for color images,” Pattern Recognit., vol. 39, pp. 866–880, 2006.