A Novel Mathematical Model for (*t*, *n*)-Threshold Visual Cryptography Scheme

B.Padhmavathi [#1], Dr.P.Nirmal Kumar [*2]

[#] *Research Scholar, JNTUH, Kukatpally Hyderabad, Andhra Pradesh*

[*] *Associate Professor, Department of ECE, College of Engineering, Guindy, Anna University, Chennai*

***Abstract*—As technology is progressing and more and more personal data is digitized, there is even more need for data security today than there has ever been. Protecting this critical data in a secure way against the unauthorised access is an immensely difficult and complicated research problem. Within the cryptographic community, many attempts have been in this regard. In visual cryptography, secret sharing offers a similar scheme, where a secret *S*, encoded into an image is shared among a group of *n* members, each of them holds a portion of the secret as their secret shares. The secret can only be retrieved when a certain number of *t* members *(where $t \leq n$)* combine their shares together. And while any combination with fewer than *t* shares have no extra information about the secret than 0 shares. This kind of secret sharing system is known as *(t, n)* - threshold scheme or *t*-out-of-*n* VC scheme. In this paper, we discuss various types of visual cryptographic schemes emphasizing on improving the efficiency and capacity of the original schemes. An analysis on the optimal contrast of the recovered secret, the robustness and security issues of technique is also presented. This paper attempts to develop a mathematical model based on interpolation for visual cryptography. Such a model using Lagrange's formula is implemented and experimental results are verified.**

***Keywords*—Threshold scheme, Visual Cryptography, Mathematical Model, Lagrange Interpolation**

I. INTRODUCTION

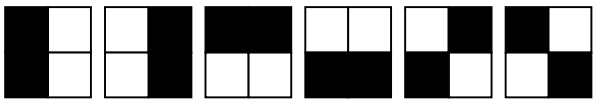
A secret is something which is kept from the knowledge of any but the initiated or privileged. Secret sharing defines a method by which the secret is distributed among a group of participants and each participant is allocated a piece of the secret. This piece is known as secret share. The original secret can only be reconstructed when a sufficient number of shares are combined together. While the shares are separate, no information about the secret can be accessed. That is the shares are completely useless while they are separate.

This above problem can be generalised and formulated as a definition of (k,n) - threshold scheme. The definition can be explained as follows: Let S be the secret to be shared among n parties. $A(k,n)$ – Threshold scheme is a way to divide S into n pieces s_1, s_2, s_3, s_n that satisfies the following conditions:

1. Knowledge of k or more s_i pieces makes S easily computable.
2. Knowledge of any $k-1$ or fewer s_i pieces leaves S completely undetermined.

Visual cryptography is a cryptographic technique that also attempts to solve the secret sharing problem. But VC uses the idea of hiding the secrets within the images. Later these images are encoded into multiple shares to be distributed among participants. In (k,n) image sharing, the image that carries the secret is encrypted into n shadow shares and the decryption is totally unsuccessful unless at least k pieces are collected for reconstruction. Visual cryptography is a desirable scheme as it embodies both the idea of perfect secrecy using a onetime pad algorithm and a very simple mechanism for decoding the secret.

Visual cryptography was introduced in [1] to protect secret images. The major contribution of their approach is that in visual cryptography, people can use their eyes (rather than the computer's computation) to recover a secret image by simply stacking the two corresponding transparencies, while any transparency alone cannot reveal the given secret image. To know about the simplest design of VC, readers may inspect Fig.1 to find some very simple patterns of blocks repeatedly used to decompose a black-and-white secret image. Note that each pixel of the secret image yields a 2-by-2 block in transparency 1 and another 2-by-2 block in transparency 2. In fact, for every pixel of the secret image, according to whether the pixel is black or white, we can just use Fig. 1 to randomly choose a pair of 2-by-2 blocks (related to that pixel's brightness) to paint the corresponding position in transparencies 1 and 2. Notably, after stacking, if all four elements in the resulting 2-by-2 stacked block are black, then the input pixel of the secret image must be a black pixel; on the other hand, if just two of the four elements in the resulting stacked block are black, then the input pixel must be a white pixel. Therefore, the resulting recovered image (2×2=4 times larger than the original secret image) can be utilized to trace back the original secret image with its original size easily. This is the original (2, 2) visual cryptography scheme. Here the total number of participants are 2 and both the shares are needed to reconstruct the original secret and the size of the shares, recovered image is 2 or 4 times larger than the original image.



Vertical Shares Horizontal Shares Diagonal Shares

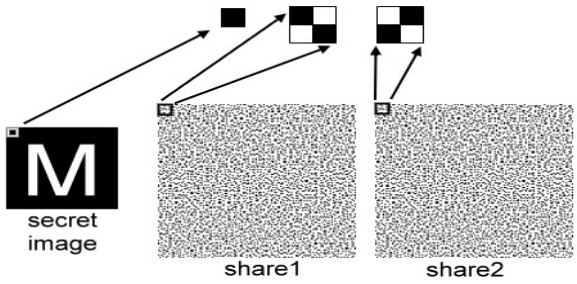


Fig. 1 An Ordinary (2, 2) Visual Cryptography scheme

Although number of variant visual cryptography techniques were introduced later to create size invariant shares, (k,n) -threshold methods, access structure based share groups, Random grid based shares etc, almost all methods suffered from image quality and contrast factors. If quality and contrast are given priority then the size of the shares would increase considerably. Also the number of shares needed to produce the original secret would also increase.

In the next section a brief survey of various VCS techniques would be discussed and analysed for the above factors. This analysis leads to the design of a mathematical model. The fourth section describes the mathematical model and the experimental results would prove various benefits.

II. Related Work

In this section, various VCS techniques are reviewed. An extended visual cryptography scheme (EVCS) proposed in [2] based on an access structure which contains two types of sets, a qualified access structure T_{qual} and a forbidden access structure T_{forb} in a set of n participants. The technique encodes the participants in that if any set, which is a member of the qualified access structure and those sets are superimposed, the secret message is revealed. Where as members of the forbidden access structure have no useful information and they can't reveal the secret.

Ito's scheme [3] proposes a size invariant scheme with no pixel expansion and also use a (k,n) scheme with the help of a Boolean n -vector $V=[v_1,v_2,v_3..v_n]^T$, where each v_i represents the colour of the pixel in the i^{th} shared image. The most important part of any scheme is the contrast as it is hard to visually recover the secret. In this scheme the contrast is based on the probabilities with which a black pixel on the reconstructed image is generated from a white and black pixel on the secret image. This is because the pixels of the respective shares are combined by a Boolean OR operation.

A probabilistic method to deal with the size invariant shares is proposed in the paper [4]. Here the frequency of the white pixels is used to show the contrast of the recovered image. Aspect ratio invariant secret sharing is presented in [5].This scheme drastically reduces the number of extra sub pixels needed in constructing the secret. The share size is equal to the secret size and aspect ratio is maintained thus avoiding the distortion while reconstructing the secret.

Recursive style of secret sharing is based on the concept of an image with multiple secrets. Recovering the secrets involves rotation or shifting of the shares to different locations on the corresponding share. Random grid algorithm uses a common random share using which corresponding secret shares are generated for different user secrets. Hence for every user secret, (2, 2) scheme is applied.

Similarly different VCS schemes were developed for different types of secret images like for colour images, half-tone images etc leading to various applications. Each method has its own advantages and drawbacks. But none of these schemes are based on a mathematical model. Hence this paper proposes a mathematical model for secret sharing schemes which guarantees a perfect (k,n) -threshold visual cryptography.

III. PROPOSED WORK

Secret sharing is a very important embranchment of the modern cryptography. Secret sharing is a technique for sharing a secret to a group of participants, each of which holds a portion of the secret. The secret can be retrieved when a certain number of t members combine their shares together, while any combination with fewer than t shares has no extra information about the secret than 0 shares.

We begin this section by explaining what threshold scheme of secret sharing as given in is ([6]-[7]). Then we apply this scheme to (k,n) -threshold visual cryptography Scheme. This mathematical approach involves Lagrange's interpolation over a Galois field mod p. When applied to an image, it is observed that size invariant n secret shares are generated and any of the t shares can be used to reconstruct the original secret. The recovered secret is perfect in its quality in terms of contrast, resolution and size.

A. Shamir's Threshold Secret Sharing Scheme

The basic idea of Shamir's scheme is based that two points are needed to determine a line, three points to determine a quadratic and so on.

Suppose we have a prime p , which is larger than the entire possible message and also larger than n number of participants. All the calculations are carried out mod p. Here, we can also use a composite number n , however, it will guarantee the solution finally. Suppose we want to share a secret message M , represented as a number mod p. There are n persons who have shared the secret and when any t persons get together, they can retrieve the secret by their shared parts.

To achieve this aim, we need the following steps:

1. Select $t-1$ *integers* mod p randomly, represented by

$$s_1, s_2, \ldots . s_{t-1} \quad (1)$$

Create a polynomial

$$s(x) = M + s_1 x + \cdots + s_{t-1} x^{t-1} \pmod{p} \quad (2)$$

2. Select n different integers $X_1, X_2, X_3, \ldots X_n \pmod{p}$ and $x_1, x_2, x_3, \ldots x_n \pmod{p}$ for n participants, and calculate the corresponding values $S(X_1), S(X_2), S(X_3), \ldots S(X_n)$. Then each participant is assigned a pair (x_i, y_i) with

$$y_i \equiv s(x_i) \pmod{p} \quad (3)$$

3. Keep the polynomial as a secret and publish p.

So far, the generation of Shamir's secret is described. Next the secret recovery scheme will be presented. Now suppose t Persons want to recover the secret and their pairs are $(x_1, y_1) \ldots (x_t, y_t)$.

- Create t equations according to the pairs as following :

$$y_k \equiv M + s_1 x_k^1 + \cdots + s_{t-1} x_k^{t-1} \pmod{p}, 1 \le k \le t \quad (4)$$

- Rewrite these equations into a matrix equations as :

$$\begin{pmatrix} 1 & x_1 & \cdots & x_1^{t-1} \\ 1 & x_2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & x_t & \cdots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{t-1} \end{pmatrix} \equiv \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix} \pmod{p} \quad (5)$$

Where s_0 is equal to Secret M. If the determinant of the left matrix is a non zero mod p, this equation always has a unique solution mod p.

- If we get solution to this equation, then we can obtain the secret $M = S_0$.

Instead of finding the Inverse of the matrix, we can try an alternate approach to recover the secret. First, let

$$l_k(x) = \prod_{\substack{i=1 \\ i \ne k}}^{t} \frac{x - x_i}{x_k - x_i} \pmod{p} \quad (6)$$

By using the method of fractions mod p, we can get

$$l_k(x_j) = \begin{cases} 1 & if \quad k = j \\ 0 & if \quad k \ne j \end{cases} \quad (7)$$

Finally, we can obtain the Lagrange Interpolation Formula,

$$p(x) = \sum_{k=1}^{t} y_k l_k(x) \quad (8)$$

Which satisfies the requirement $p(x_j) = y_j$ for $1 \le$ message, we can simply calculate $p(x)$ and evaluate formula for any secret message M as the following

$$M \equiv \sum_{k=1}^{t} y_k \prod_{\substack{j=1 \\ j \ne k}}^{t} \frac{-x_j}{x_k - x_j} \pmod{p} \quad (9)$$

Based on the above Shamir threshold scheme, the Secret image sharing scheme will be presented in the next subsection.

B. (t, n)- *Threshold Secret Sharing Scheme for Gray Scale Images*

Suppose we can split a secret image I into n different shadow images $(s_0, s_1, s_2, \ldots s_{n-1})$. Then the original image can only be recovered by the combination of t different shadow images. To accomplish this goal, the polynomial in Shamir threshold scheme is employed. In Shamir threshold scheme, the coefficients $(s_0, s_1, s_2, \ldots s_{n-1})$ are randomly selected from integers less than p. However, in the secret image sharing scheme, values of each pixel are used as these coefficients.

Since the value of a gray image is between 0 and 255, the prime number p =257 is selected as the closest prime number to 255.Then the image with the size $H \times W$ is divided into m parts and each part contains t pixels. For example, if the size of an image is 256 × 256 and t =4, we will get m -16384 parts. For each part k, a polynomial

$$s_k(x) = s_0 + s_1 x + \cdots + s_{t-1} x^{t-1} \pmod{p} \quad (10)$$

is defined, where $(s_0, s_1, s_2, \ldots s_{n-1})$ correspond to the values of each pixel in part k.

According to this polynomial, we can get an array A_x containing m values $S_1(x), S_2(x), \cdots S_m(x)$ for a given X. If we reshape this array A_x into $a \times b$ matrix, a shadow image will be obtained. Moreover, if we choose n different x – values, we can get n different shadow images. In this scheme, the number t must be selected appropriately, so that m is an integer and can be represented as $a \times b$ Matrix.

C. *Image Recovery Based on Shadow*

Suppose n different shadow images are obtained from a (t, n) secret image sharing scheme. Then any combination of t different shadow images will yield a recovered image. We define an array to store the value of x for the selected t shadow images. The recovery scheme will be presented in the following steps:

1. Reshape all the t shadow images from $a \times b$ matrix into arrays with m length.
2. Read the i^{th} element of each array as $S_i(X_1)$ where l indicates the index of different arrays and X_1 corresponds to the l^{th} element of the array X. Then we get the t values as

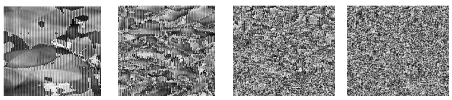
3. By using these t values, we can get the following equations,

Solve these equations together, we can get the values of the pixels at the i^{th} rows of the reshaped original image.

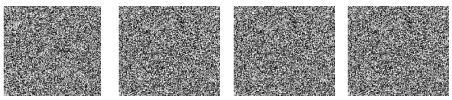
4. Repeat steps 2 & 3, until all the elements of each array have been calculated. Then we can get the whole reshaped image.

5. Reshape and reorder the image thus obtained from $m \times t$ into $H \times W$. Thus we will get the recovered image.

Fig. 2 Secret image



Shadow1 Shadow 2 Shadow 3 Shadow 4



Shadow 5 Shadow 6 Shadow 7 Shadow 8

Fig. 3 Shares created

Fig. 4 Reconstructed secret image

D. Analysis of Security

Suppose we want to recover an image from (t,n) secret image sharing scheme, then we need to construct

$$m = \frac{H \times W}{t} \tag{11}$$

Polynomials, such as,

$$s_i(X_0) = s_0^i + s_1^i X_0 + \cdots + s_{t-1}^i X_0^{t-1} (\text{mod } 257) \tag{12}$$

For an image size $H \times W$. For each of those polynomials, there are t unknown coefficients. Suppose we have only $t-1$ shadow images, then we construct only $t-1$ equations.

$$\begin{aligned} s_i(X_0) &\equiv s_0^i + s_1^i X_0 + \cdots + s_{t-1}^i X_0^{t-1} (\text{mod } 257) \\ s_i(X_1) &\equiv s_0^i + s_1^i X_1 + \cdots + s_{t-1}^i X_1^{t-1} (\text{mod } 257) \\ &\vdots \\ s_i(X_{t-2}) &\equiv s_0^i + s_1^i X_{t-2} + \cdots + s_{t-1}^i X_{t-2}^{t-1} (\text{mod } 257) \end{aligned} \tag{13}$$

In this situation, there are t unknowns and $t-1$ equations, which means we cannot know exactly the t^{th} root. The probability, one can guess the correct value is $1/256$. Therefore, the probability, one can recover the whole image without errors is $(1/256)^m$. For this reason, it is impossible to recover an image with the combination of $t-1$ or less shadow images.

IV. Conclusions

In this paper, a novel mathematical model for the threshold visual cryptography for secret image sharing is presented. Firstly, we review the development of visual cryptography secret sharing schemes and analyse the shortcomings of each scheme. It was obvious that each scheme was application specific and does not provide a generalized mathematical proof. This leads to the necessity that any secret sharing or distribution scheme must be general and highly secure. Hence based on the Lagrange Interpolation formula, a secret image was shared among n participants as shadow images. With any combination of t shadow images where $(t \le n)$ the original image was reconstructed. The experimental results show that the quality of the restored secret is perfect in terms of contrast, resolution and size.

References

[1] M. Naor and A. Shamir, "Visual cryptography", Advances in cryptology Eurocrypt'94, pp.1-12, Springer Berlin Heidelberg, 1995.

[2] K.H. Lee and P.L. Chiu, "An Extended Visual Cryptography Algorithm for General Access Structures", IEEE Transactions on Information Forensics and Security,vol.7,no.1, Taiwan.

[3] R. Ito, H. Kuwankada and H. Tanaka, "Image size invariant visual cryptography", IEICE transactions on fundamentals of electronics, communications and computer sciences,vol.82, no.10,pp.2172-2177, 1999.

[4] S.J Lin and W.H Chung, "A Probabilistic model of (t,n) Visual Cryptography Scheme with Dynamic group", IEEE transactions on information forensics and security, vol.7, no.1, February 2012.

[5] C.N Yang and T.S Chen "Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion", Pattern recognition Letters, vol.26, no.2, pp.193-206, 2005.

[6] A Shamir, "How to share a secret", Communications of the ACM, vol.22, no.11, pp.612-613, 1979.

[7] G. R. Blakley "Safe guarding Cryptographic Keys", International Workshop on Managing Requirements Knowledge, pp. 313-313. IEEE Computer Society, 1899.

[8] C.C. Chang, J.C. Chuang, P.Y. 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. vol. 2, pp.300-304.

[9] S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, vol. 40, no 12, pp.3633 - 3651, 2007.