k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence

Shyamalendu Kandar
Department of Computer Sc. & Engineering
Haldia Institute of Technology
Haldia, India

Bibhas Chandra Dhara
Department of Information Technology
Jadavpur University
Kolkata, India

ABSTRACT
Visual cryptography is a special type of encryption technique where visual information (Image, Text etc) gets encrypted in such a way that decryption can be performed by Human Visual System with a computation free decryption process. The beauty of the visual secret sharing scheme is in its decryption process where without any complex cryptographic computation encrypted data is decrypted using Human Visual System (HVS). But the encryption technique needs cryptographic computation to divide the image into a number of parts let n such that at least a group of k shares out of n shares reveals the secret information, less of it will reveal no information.

In this paper we have discussed a technique called random sequence which needs very less computation for k-n secret sharing.

Keywords: Visual Cryptography, Secret Sharing, Random Sequence

1. INTRODUCTION
Visual cryptography is a cryptographic technique where visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the human visual system without aid of computers [1].

Image is a multimedia component sensed by human perception. Pixel is the smallest unit constructing a digital image. Each pixel of a 32 bit digital color image are divided into four parts, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency. If all bits of Alpha part are '0', then the image is fully transparent.

A 32 bit sample pixel is represented in the following figure [2] [3].

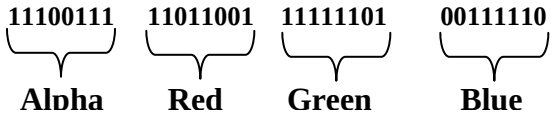


Figure 1: Structure of a 32 bit pixel

Human visual system acts as an OR function. If two transparent objects are stacked together, the final stack of objects will be transparent. Changing any of them to non-transparent, the final stack of objects will be non-transparent.

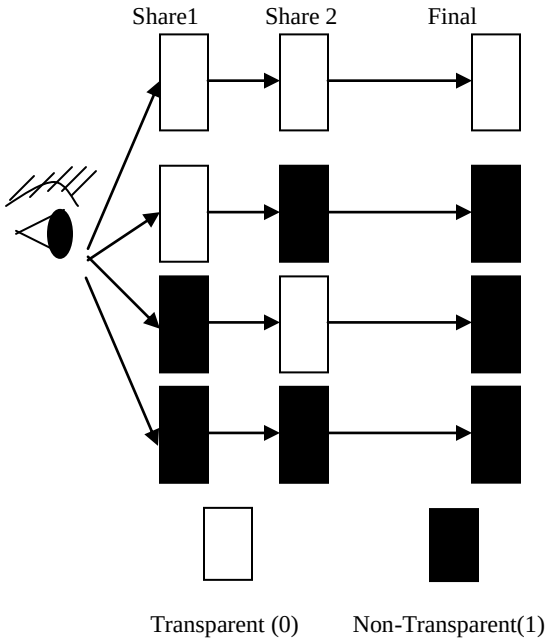


Figure 2: Human Visual system as OR Function

In this paper we have proposed a secret sharing algorithm to divide a digital color image into n number of shares where minimum k numbers of shares are sufficient to reconstruct the image. To achieve this, following condition must be fulfilled. If there is '1' in certain position of a pixel, there must be '1' in that position of that particular pixel in (n−k)+1 number of shares generated from the original image. In the remaining shares in that position of the particular pixel there is 0. In an earlier attempt [4][5][6] we proposed a scheme of generating (n-k) +1 discrete random numbers within 1 to n to divide an image into n number of shares. But that needs to perform a number of looping operations for each position of each pixel of each n number of shares if a '1' is found in that position. In this current work we have proposed a scheme called random sequence which is more generalized and gives relief from too many looping operation.

The organization of the paper is as follows. The already existing secret sharing schemes are described in section 2. Description of proposed Random Sequence based secret sharing is given in section 3. The visual cryptography process using random

sequence is described in section 4. Experimental results are shown in section 5. Future scopes are given in section 6. Finally, conclusions are made in section 7.

2. EXISTING SECRET SHARING SCHEMES

The idea of secret sharing was separately proposed by Adi Shamir [7] and G. Blakley [8] in 1979. In 1983 another method of secret sharing was proposed by Asmuth and Bloom [9]. Shamir' scheme is based on Polynomial Interpolation; Blakley scheme is based on hyper plane geometry where as Asmuth-Bloom scheme is based on Chinese Remainder theorem.

a) Shamir's Secret Sharing Scheme

This scheme divides a secret data S into n number of shares let $S_1, S_2 \ldots\ldots S_n$ such that

i) Knowledge of k or more shares among S_i ($i \leq n$) can reveal the secret information.

ii) Knowledge of less than k shares reveals no information about the secret share.

This technique is called (k, n) secret sharing. The technique is described with an example in the following section.
The (k, n) secret sharing comes from the concept that k points are necessary to define a polynomial of degree (k−1). To construct the polynomial, (k−1) coefficients $a_1, a_2 \ldots a_{k-1}$ are required. Here a_0= S, the secret data. The polynomial $f(x) = a_0 + a_1x + a_2x^2 + \ldots..+a_{k-1}x^{k-1}$ is constructed from the coefficients. Total n points let i=0…..n are taken and corresponding f(x) are also calculated. From these values n number of pairs (i, f(i)) are constructed. The original coefficients are retrieved by interpolation method from at least k numbers of these pairs.

Example:
Let the secret information is 2134. Let we want to implement a (k, n) secret sharing where k=3 and n=4. Let (k−1) that is 2 coefficients are 145 and 70. The polynomial is

$f(x) = 2134 + 145x + 70x^2$.

Let the four points are 1, 2, 3, 4. The corresponding 4 pairs (i, f(i)) renamed as (x_i, y_i) are (1, 2349), (2, 2704), (3,3199) and (4, 3834).

From these pairs minimum 3 pairs are required to find the original coefficients.

Let take 3 pairs (1, 2349), (3, 3199) and (4, 3834). Using Lagrange Interpolation l_0, l_1 and l_2 are found as $(x^2-7x+12)/6$, $(x^2-4x+4)/-2$, $(x^2-4x+3)/3$.

From these three pairs, f(x) is calculated as

$f(x) = \sum y_j l_j \quad 0 \leq j \leq 2$. Which produces the original polynomial $f(x) = 2134 + 145x + 70x^2$.

b) Blakley Secret sharing scheme

Blakley secret sharing is based on hyper plane geometry. It is a general true that non-parallel planes intersect at a specific point. This secret sharing scheme says that

i) Secret is point in *m*-dimensional space

ii) Share corresponds to a hyper plane

iii) Intersection of threshold planes gives the secret

iv) Less than threshold planes will not intersect to the secret

c) Asmuth-Bloom secret sharing scheme

This technique is based on Chinese Remainder theorem. This technique takes a sequence of pair wise co prime positive integers $p_0, p_1, \ldots..p_n$ such that

$$p_0 \cdot \prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i.$$

where $n \geq 2$ and $2 \leq k \leq n$.
The working principle of the scheme is as follows

i) The secret S is chosen as a random element of the set Z.

ii) A random integer α is chosen such that

$S + \alpha p_0 < p_1p_2 \ldots p_k$. The reduction modulo m_i of $S + \alpha p_0$ for all $1 \leq i \leq n$ are calculated. These are represented as shares $I_i = (S_i, p_i)$

iii) From given k distinct shares $I_{i1}, \ldots, I_{ik}$, the following set of equations are formed

$$\begin{cases} x \equiv I_{i1} \bmod p_{i1} \\ \vdots \\ x \equiv I_{ik} \bmod p_{ik} \end{cases}$$

As $p_{i1}, p_{i2}, \ldots p_{ik}$ are pairwise co-prime, by Chinese remainder theorem the system has a unique solution S_0 modulo $p_{i1} \ldots p_{ik}$. The secret S is the reduction modulo p_0 of S_0

3. RANDOM SEQUENCE

In k-n secret sharing scheme an image is divided into n number of shares in such a way that the original image is retrieved by stacking atleast k number of shares, where $k \leq n$. If k number of shares are taken from n number of shares, the remaining shares are (n−k). The condition of placing '1' in the particular bit position of a pixel in (n−k+1) shares must be fulfilled if the original image contains '1' in the particular bit position of the pixel. If seen from one side to the stacked shares, the bit sequence for a particular bit position of a pixel contains (n−k+1) number of '1' s and (k −1) numbers of '0's if the original image contains '1' in the particular bit position of the pixel. In this context this combination of '0' and '1' is taken as sequence. If a particular bit position contains '1', the sequence will be one of ${}^nC_{k-1}$ different sequences.

If in a certain bit position '1' is found, a random number generator will generate number from 1 to ${}^{n}C_{k-1}$. This is called random sequence. This is denoted in Fig. 3.

If a particular secret information is to be divided into n number of shares where k number are sufficient to retrieve the original, then n number of shares with all 0 in bit positions are created. As described, ${}^{n}C_{k-1}$ different sequences of 0 and 1 are generated.

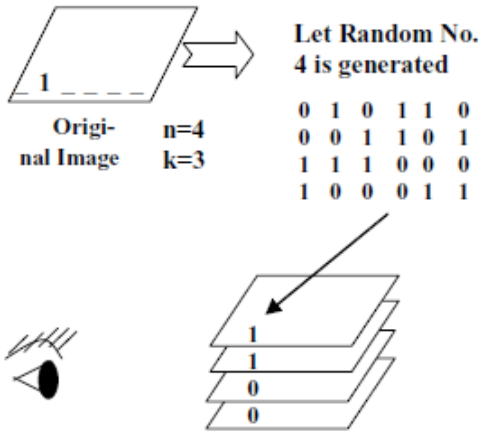


Figure: 3: Random Sequence

If in the original information in a certain bit position '1' is found a random number generator will generate number from 1 to ${}^{n}C_{k-1}$. OR operation is performed between the i^{th} bit of S_j share (where $1 \leq j \leq n$) with the j^{th} bit of the sequence generated by random number.

Example:
Let the secret information is 2134. The binary representation of it is 100001010110. Let k=3, n=4.
4 shares of each bit position 0 is constructed

000000000000 -------Share 1

000000000000 -------Share 2

000000000000 -------Share 3

000000000000 -------Share 4

The sequences are (Column wise)

0	**0**	**1**	**1**	**0**	**1**
0	**1**	**1**	**0**	**1**	**0**
1	**0**	**0**	**0**	**1**	**1**
1	**1**	**0**	**1**	**0**	**0**

First bit position contains '1'. For this, let the sequence chosen by random number is 3. So, 1100 is ORed with the '0' bit sequence for bit position 1. By this process let the final bit pattern of the shares become

000001000010 = 66

000000010110 = 22

100000000100 = 2052

100001010000 = 2128

Among these if any three are taken and bitwise OR operation is performed then the secret information 2134 is generated.

4. VISUAL CRYPTOGRAPHY SCHEME USING RANDOM SEQUENCE

The Visual Cryptography scheme consists of two steps,

a) k-n secret sharing of the original image using random sequence
b) Decryption using Human Visual System.

The two processes are described below.

4.1 k-n secret sharing of the original image using random sequence

Step I: The original image (I_{w*h}), number of shares to be divided (n) and number of shares needed (k) to retrieve the original image are taken as input

Step II: The number of sequences (ns) of (n−k+1) number of '1's and (k −1) numbers of '0's i.e. ${}^{n}C_{k-1}$ is calculated. Subsequently the sequences Sq_1, Sq_2, ….Sq_{ns} are constructed.

Step III: Let the shares of I denoted by S_1, S_2,…, S_n, each of size w X h. Shares are generated using the following logic.

i) Initialize all the bit positions of S_t by 0, for $1 \leq t \leq n$

ii) if (i^{th} bit value of I_{enc} is 1){

Generate a random number 'r' in the range 1 to ns.

Perform OR between the ith bit of S_j share
(where $1 \leq j \leq n$) with the j^{th} bit of the sequence Sq_r ,
($1 \leq r \leq ns$).
}

4.2 Decryption using Human Visual System.

It is already discussed that Human Visual system acts as an OR function. It is also mentioned that decryption in Visual cryptography is done by stacking k number of shares out of n shares generated. For computer generated decryption process we have used OR operation. The algorithm is described below.

Step I: Take s number of shares ($s \geq k$) out of n number of shares generated.

Step II: for (i=1 to s)
{
perform OR operation among the j^{th} bit of each share, where $1 \leq j \leq w*h$, to produce the final image.
}

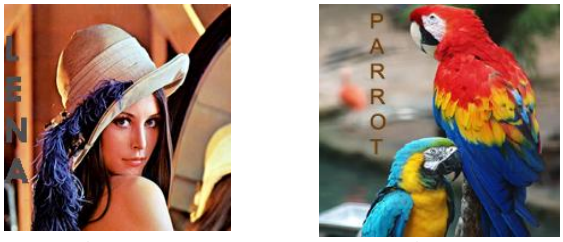
5. EXPERIMENTAL RESULT

Two images named 'Lena' and 'Parrot' are taken. Each of size 200 X 200.

The images are to be divided into 4 shares where 3 shares are sufficient to reconstruct the image. Here n=4 and k=3.

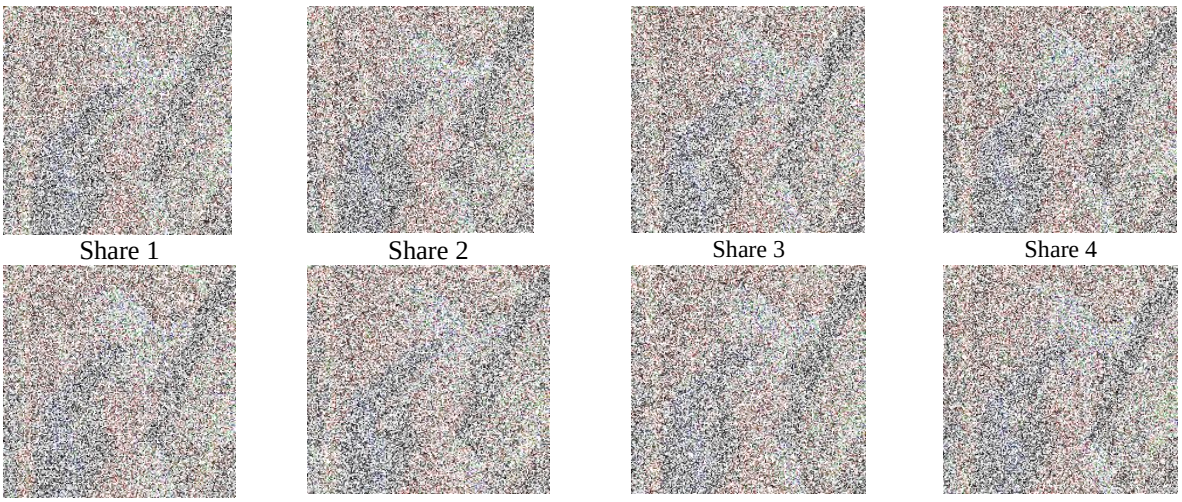
The source images are shown in Figure 4. The secret shares for image 4.i are shown in Figure 5 (i), and the shares for image 4.ii are shown in Figure 5 (ii).

In the decryption processes, let for the Lena image Share 1, 3, 4, 5, 7 and 8 are taken and for the parrot image Share 2, 3, 4, 6, 7 and 8 are taken. The decryption processes for the two images are shown in Figure 6 and Figure 7 respectively.



i) Lena ii) Parrot

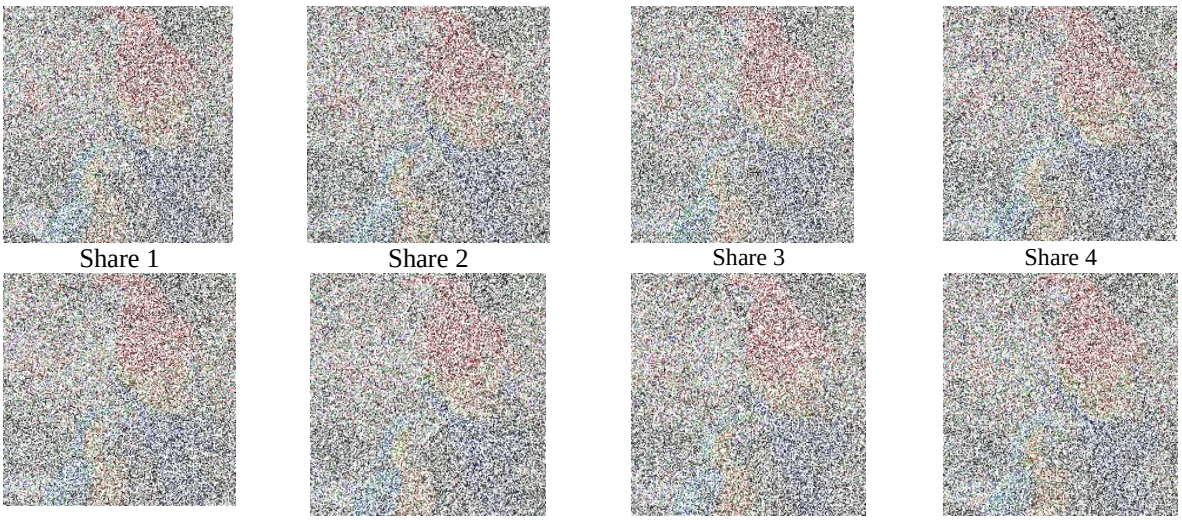
Figure 4: Source Images



Share 1 Share 2 Share 3 Share 4

Share 5 Share 6 Share 7 Share 8

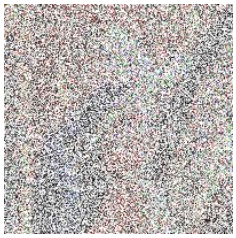
Fig 5.i: Secret shares for 'Lena' image

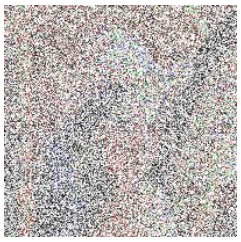


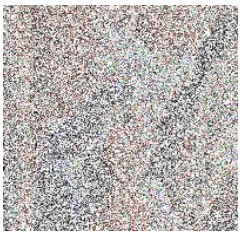
Share 1 Share 2 Share 3 Share 4

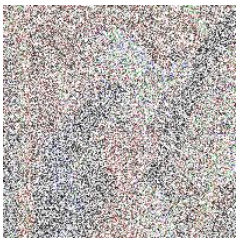
Share 5 Share 6 Share 7 Share 8

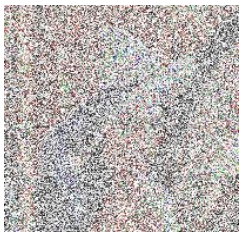
Fig 5.ii: Secret shares for 'Parrot' image


Share 1


Share 3


Share 4


Share 5


Share 7

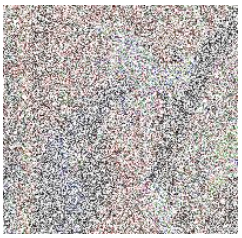
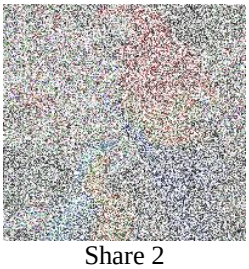
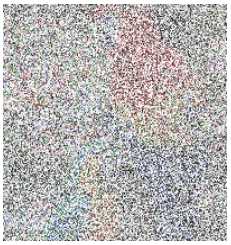

Share 8

Fig.6: Retrieval of Lena image


Share 2


Share 3


Share 4


Share 6


Share 7


Share 8

Fig.7: Retrieval of Parrot image

6. FUTURE SCOPE

Visual Cryptography technique is used to protect image-based secret information. In this scheme we have proposed a technique called random sequence to divide an image into n number of shares. The shares are sent through different communication channels from sender to receiver so that the probability of getting sufficient shares by the intruder minimizes.

But the distorted shares may arise suspicion to the hacker's mind that some secret information is passed. The original image can be encrypted using a key to provide more security to this scheme [5]. The key may be a text or a small image.

Steganography [10][11] can be used by enveloping the secret shares within apparently innocent covers of digital picture. This technique is more effective in providing security from illicit attacks.

7. CONCLUSION

Here we have proposed k-n secret sharing technique of color images using random sequence. This technique does not need complex mathematical calculation like the existing schemes [7][8][9][12][13][14]. In both secret share generation and decryption part, OR operation is used, which makes the scheme very simple.

But the main disadvantage of this scheme, like the other existing visual cryptography schemes is the security. Any person having sufficiently k number of shares can easily reconstruct the original image. In a future attempt we want to provide some security schemes to the proposed technique to make the scheme more secure.

8. REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt'94, pp. 1–12, 1995.

[2] Ranjan Parekh, "Principles of Multimedia", TMH, 2006

[3] John F Koegel Buford, Multimedia Systems, Addison Wesley, 2000.

[4] Kandar Shyamalendu, Maiti Arnab, "K-N Secret Sharing Visual Cryptography Scheme For Color Image Using Random Number", International Journal of Engineering Science and Technology, Vol.3 No. 3 March 2011, pp 1851-1857

[5] Kandar Shyamalendu, Maiti Arnab, "Variable Length Key based Visual Cryptography Scheme for Color Image using Random Number", International Journal of Computer Application, Vol. 19 No. 4, April 2011. pp34-39

[6] Kandar Shyamalendu, Maiti Arnab, Dhara Bibhas Chandra "Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking" International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011 pp543-549

[7] A. Shamir: "How to share a secret ?" Comm ACM, 22(11):612-613, 1979.

[8] G. Blakley : "Safeguarding cryptographic keys " Proc. of AFIPS National Computer Conference, 1979.

[9] C. Asmuth and J. Bloom "A modular approach to key safeguarding" IEEE transaction on Information Theory, 29(2):208-210, 1983.

[10] Hartung F., Kuttter M., "Multimedia Watermarking Techniques", 1999 IEEE

[11] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications. IEEE Journal on Selected Areas in Communications, 16(4):573–586, May 1998

[12] Nakajima M. , Yamaguchi Y., Extended visual cryptography for natural images. Journal of WSCG.v10 i2. 303-310.

[13] F. Liu, C. K. Wu, X.J. Lin, "Colour visual cryptography schemes" IET Information Security, 2008, Vol. 2, No. 4, pp. 151–165

[14] Kang InKoo el. at., Color Extended Visual Cryptography using Error Diffusion, IEEE 2010