# VISUAL CRYPTOGRAPHY SCHEME USING GRAY CODE AND XOR OPERATION

Deepika M P[1], Dr. A Sreekumar[2]
[1]Research Scholar, CUSAT
[2]Associate Professor, DCA, CUSAT

**Abstract**

**Today digital media has replaced almost all forms of communication, information preservation and processing. Security in digital media has been a matter of serious concern. This has resulted in the development of, what we call cryptography. Secret sharing schemes and Visual secret sharing schemes, (aka visual cryptography schemes (VCS)) form parts of this large study. "Secret" means something that is kept or meant to be kept unknown or unseen by others. Some time secret is thought to be secure in a single hand and at other times it is thought to be secure when shared in many hands. A secret sharing scheme is a method of dividing secret information into two or more pieces called shares, distributing these shares among communication parties and retrieving the information by combining all or predefined sub collection of the shares. In this paper we will provide the readers an overview of the basic visual cryptography scheme constructions, in addition, we have proposed a visual cryptographic scheme based on Gray coding and XOR operation. Here the secret image is shared using Gray code and reconstructed by using the XOR operation. The proposed method is for the gray scale images. The proposed scheme doesn't have pixel expansion. The original secret image, shares and the reconstructed secret image are in same size. So the scheme is a lossless scheme.**

**Keywords: Visual cryptography (VC), secret sharing schemes, Gray code, XOR operation**.

## I. INTRODUCTION

Visual cryptography [1] is very special data security method which provides a very powerful technique by which one secret can be distributed into two or more shares. When shares on transparencies are super imposes exactly together, the original secret can be discovered without any complicated algorithm or computer participation. Visual cryptography scheme (VCS) is an encryption method that uses combinatorial techniques to encode secret written materials. The idea is to convert the written material into an image and encode this image into *n* shadow images. The decoding only requires only selecting some pre defined subset of these *n* images or all n shadow images, making transparencies of them, and stacking them on top of each other. Cheating [29] is possible in visual cryptography because protection of secret sharing participants is not the main concern. Since there is no restriction on the behavior of the participants, any participant, called a cheater, can reveal a forged share on purpose, and there by cheat other participants.

In this paper, some important and related works in visual cryptography are included as the next section. After that the proposed scheme is explained.

## II. RELATED WORKS

Visual cryptography is paradigm of cryptography which allows visual information (e.g. images, printed text and handwritten notes) to be encrypted in such a way that its decryption can be done by the human eye, without the aid of computers. It avoids the need of complex mathematical computations during decryption and the secret image can be reconstructed using stacking (OR operation).

Visual cryptography (VC) [1] was originally invented and pioneered by Moni Naor and Adi Shamir in 1994 at the *Eurocrypt* conference. Visual cryptography is a “new type of cryptographic scheme, which can be decoded concealed images without any cryptographic computation. As the name suggests, VC is related to human visual system. VC is a cryptographic technique which allows visual information (picture, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system. When shares are stacked the human eye do the decryption. This allows anyone to use the system without any knowledge of cryptography and without performing any computations whatsoever. This is the main advantage of VC over the other popular conditionally secure cryptography schemes. The mechanism is very secure and very easy to implement. There are diverse visual cryptography schemes based on the factors such as pixel expansion, contrast, security, meaningless or meaningful shares, type of secret image (either binary or color) and the number of secret images encrypted (single or multiple secret) etc.

The following are the diverse visual cryptography schemes:

1. Traditional Visual Cryptography
2. Extended Visual Cryptography
3. Halftone Visual Cryptography
4. Recursive Threshold Visual Cryptography Scheme
5. Random Grids based Visual Cryptography
6. Color Visual Cryptography Schemes
7. Probabilistic Visual Cryptography
8. Region Incrementing Visual Cryptography
9. Progressive Visual Cryptography
10. Segment based Visual Cryptography Scheme
11. Cheating Immune Visual Cryptography Schemes
12. Size Invariant Visual Cryptography
13. User-friendly Visual Secret sharing scheme
14. Dynamic Visual Cryptography
15. OR and XOR Visual Cryptography

Naor and Shamir’s [1] traditional visual cryptography scheme , the very initial implementation assumes that the image or message is a collection of black and white pixels (means, binary images), each pixel is handled individually and it should be noted that the white pixel represents the transparent colour. One disadvantage of this is that the decryption process is lossy. The main area that suffers due to this lossy process is the contrast. One of the very important attribute in visual cryptography is the contrast of the recovered images, because it determines the clarity of the recovered secret by human visual system. The relative difference Hamming weight between the representation of white and black pixels signify the loss in contrast of the recovered secret. The newer schemes deal with gray scale and colour images which attempt to minimize the loss in contrast by using digital half toning.

Extended VC [2] takes the idea of visual cryptography further by creating shares which are meaningful to anyone who views them. This helps to alleviate suspicion that any encryption has taken place and also presents visually pleasing shares which incorporate all the previously mentioned features of VC. Extended visual cryptography schemes allow the construction of visual secret sharing schemes within which the shares are meaningful as opposed to having random noise on the shares. After the sets of shares are superimposed, this meaningful information disappears and the secret is recovered. This is the basis for the extended form of visual cryptography. Meaningful shares avoid attention of hacker considering the security issues over the communication channels. An extended visual cryptography scheme (EVCS) proposed by Ateniese et al.[3] is based on an access strucrture which contains two types of sets , a qualified access structre and a forbidden access structure 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. However , for any set which is a member of the forbidden access structure and has no information on the shared secret, meaning that no useful information can be revealed from stacking the shares of participants. The first paper to consider image size invariant VC was proposed by Ito et al.[4] . The traditional VCS employ pixel expansion. In pixel expansion, each share is *m* times the size of the secret image, where *m* refers to the number of pixels in the generated shares that represents a pixel of the original input image. Thus, it can lead to the difficulty in carrying these shares and consumption of more storage space. Ito’s scheme removes the need for this pixel expansion. That is, the reconstructed image is identical to the original image. There are also some other studies which focus on the methods without pixel expansion [5][6][7]. In a general halftone visual cryptography framework [8][9], where a secret binary image is encrypted into high- quality halftone images or halftone shares. In particular, the proposed method applies the rich theory of blue noise halftoning to the construction mechanism used in conventional VC to generate halftone shares, while the security properties are still maintained. The same contrast is obtained over the whole decoded image. The halftone shares carry significant visual information to the viewers, such as landscapes, buildings, etc. The visual quality obtained by this method is significantly better than that attained by extended VC or any other available VC method known to date. Halftone VC is built upon the basis matrices and collections available in conventional VC.

A recursive [10][11][12] style of secret sharing takes into account a set of two shares which contain more than one secret. Recovering this secret requires rotation or shifting of the share to different locations on the corresponding share. In recursive hiding of secrets, the user encrypts additional information about smaller secrets in the shares of a larger secret without causing any expansion in the size of the latter, thereby increasing the efficiency of secret sharing. The idea here is to double the secret size at every step and so increases the information that every bit of share conveys to (n-1)/n bit of secret i.e. almost 100%.

Random Grids[13][14][15][16] extends the solution to the secret sharing problem by implementing a collection of 2-D transparent and opaque pixels arranged randomly which reveals the secret to the Human Visual System(HVS) when being superimposed. Unlike other visual cryptography approaches, random grid does not need the basis matrices to encode the shares. Pixel expansion is disallowed which is therefore a great advantage of using Random Grids. Also, the sizes of secret image and the shares are identical to each other.

Sharing Single Secret until the year 1997 visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg [17]. Colored secret images can be shared with the concept of arcs to construct a colored visual cryptography scheme. In c-colorful visual cryptography scheme one pixel is transformed into m subpixels, and each subpixel is divided into c color regions. In each subpixel, there is exactly one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacked subpixels.

For a colored visual cryptography scheme with c colors, the pixel expansion m is c× 3. Yang and Laih [18] improved the pixel expansion to c ×2 of Verheul and Van Tilborg. But in both of these schemes share generated were meaningless. For sharing a secret color image and also to generate the meaningful share to transmit secret color image Chang and Tsai [19] anticipated color visual cryptography scheme. Sharing Single Secret and Multiple Secrets is possible through color VCS. Hou, [20] proposed a VCS for color images .His methods are based on Halftone technique and color decomposition. Basic Terminologies used in encrypting Colored Images via Visual Cryptographic method are discussed below.

. Halftoning: This method uses the density of the net dots to simulate the gray level is called Halftone and transforms an image with gray level into a binary image before processing.

. Color Decomposition: In this, every color on a color image can be decomposed into three primary colors: C, M ,Y (if subtractive model is used) or R,G.,B(if additive model is used).This method expand every pixel of a color secret image into a 2x2 block in the sharing images and keep two colored and two transparent pixels in the block.

. Pixel expansion: Pixel expansion m refers to the number of subpixels in the generated shares that represents a pixel of the original input image. Smaller pixel expansion results in smaller size of the share. It represents the loss in resolution from the original picture to the shared one.

In [21] the authors proposed a model where the pixel expansion *m* is 1, that is, there is no pixel expansion. The reconstruction of the image however is probabilistic, meaning that a secret pixel will be correctly reconstructed only with a certain probability. However, while in the deterministic model the reconstruction of an approximation of the secret pixel is guaranteed, in Yang's probabilistic model the secret pixel is correctly reconstructed with some probability. Yang's aim is to provide schemes with no pixel expansion, which are obviously desirable. However the quality of the reconstructed pixel depends on how big the probabilities are of correctly reconstructing secret pixels.

Progressive Visual Cryptography [22] takes into consideration the premise of perfect secret recovery and high quality secret reconstruction. Many of the schemes do require computational effort in order to perfectly reconstruct the secret. A new sharing concept emerged known as Progressive Visual Cryptography which revealed the secret image progressively as more and more number of shares were stacked together. Traditional visual cryptography schemes were based on pixels in the input image. The limitation of pixel based visual cryptography scheme is loss in contrast of the reconstructed image, which is directly proportional to pixel expansion. Bernd Borchert proposed [23] a new scheme which is not pixel-based but segment-based. It is useful to encrypt messages consisting of symbols represented by a segment display.

For example, the decimal digits 0, 1 , …. 9 can be represented by seven-segment display. The advantage of the segment based encryption is that, it may be easier to adjust the secret images and the symbols are potentially easier to realize for the human eye and it may be easier for a non expert human user of an encryption system to understand the working. The secret, usually in the form of digits is coded into seven segment display before encrypted. Two random share images will be generated during encryption. Decryption process involves the stacking of these two share images.

Ran-Zan Wang developed a scheme Region Incrementing Visual Cryptography for sharing visual secrets of multiple secrecy level in a single image [24]. In this scheme, different regions are made of a single image, based on secrecy level and different encoding rules are applied to these regions.

Ito's scheme [4] removes the need for this pixel expansion. The scheme uses the traditional (k, n) scheme where m (the number of sub-pixels in a shared pixel) is equal to one. The structure of this scheme is described by a Boolean n-vector V = $[v_1. . . v_n]T$ , where $v_i$ represents the color of the pixel in the i-$^{th}$ shared image. If $v_i = 1$ then the pixel is black, otherwise, if $v_i = 0$ then the pixel is white. The recovered secret can be viewed as the difference of probabilities with which a black pixel in the reconstructed image is generated from a white and black pixel in the secret image. Three major size invariant visual cryptography schemes are: random grid, probabilistic and multi-pixel encoding.

The core idea behind dynamic visual cryptography [25] is increasing the overall capacity of a visual cryptography scheme. This means that using a set of two or more shares, we can potentially hide two or more secrets. Multiple secret sharing is very useful when it comes to hiding more than one piece of information within a set of shares. Chen and Tsao [26] [27] proposed a novel random grid based visual secret sharing scheme that has been skillfully designed to produce meaningful (user-friendly) share images without pixel expansion. It explains a procedure with different light transmissions based on the share images and the logo image (cover image) used to make the shares user-friendly. Usually all the conventional visual cryptography schemes (VCS) uses OR operation for stacking operations and so it is also called OR-based VCS. But it offers a poor visual quality image during decoding (stacking). XOR based VCS [28] uses the properties of Contrast and Security Advantage XOR-based VCS (XVCS), which uses XOR operation

## III. PROPOSED METHOD

### VCS USING GRAY CODE AND XOR OPERATION

The proposed scheme is based on the Gray code and XOR operation. The proposed method is for the gray scale images. Using this method we can construct two variant VCS, one is 7-out-of-7 scheme, VCS (7, 7) and the second is 3-out-of-7 scheme, VCS (3, 7). For this, two sets of shares are generated, Qualified set of shares (Q-set) and Forbidden set of shares (F-Set).The Q-set contain 3 shares among 7 shares that are generated and F-set contain 4 shares among 7 shares that are generated. From the secret image these two sets of shares are constructed using the Gray code. The reconstruction of secret image is simply by XORing the shares. For reconstruction there are two separate algorithms based on the schemes that we are following. The Algorithm.1 gives the share construction and A*lgorithm.2.1 and Algorithm 2.2* give the two variant procedures for reconstructing the secret image. The *Algorithm.2.1* is about the secret image reconstruction from Q-set of shares. *Algorithm 2.2* is about the secret image reconstructed from both the Q-set and F-set.

**Algorithm 1.** Share construction is as follows:

```
Input:  The secret image, SI, with dimension NxM
Output: Seven shares; $S_1$, $S_2$, .... $S_7$ ; Each of dimension NxM

[For constructing shares 5 pixels are considered at a time.]

Step1: For i= 1 to N
Step2: Select the 5 pixel at a time from the ith raw of the secret image.
Step3: Convert each pixel value to its corresponding binary value.
Step 4: Divide the binary value into 8 blocks each having 5 bits in length.
        Step 4.1:  Let n = Number of 5 bits
                   block.(that is 8)
        Step 4.2: For j=1 to n
        Step 4.3: $M_j$ =  $j^{th}$ 5 bits block
        Step 4.4: For k=1 to 7
        Step 4.5: Convert 5 bits block, say $M_j$ into
                   the corresponding Gray value, say
                   G
        Step 4.6: Save $S_k$= G.
        Step 4.7: if i%2= =0 then save $S_k$ in
                  Qualified set say Q-Set
        Step 4.8: Update $M_j$ =G
        Step 4.9: End if (k).
        Step 4.10: End if (j).
Step 5: Divide the shares $S_1$ through $S_7$  into 5 blocks each having 8 bits in length.
Step 6: Convert the shares $S_1$ through $S_7$  into the corresponding decimal values.
Step 7: Stop
```

**Algorithm 2.1.** Reconstruction of secret from Qualified set of shares(Q-Set) is as follows:

```
Input: Qualified set of shares;  $S_2$, $S_4$, $S_6$ ; Each of dimension NxM

Output: The secret, SI, with dimension NxM

Step1: For i= 1 to N
Step2: For j=2, 4, 6
        Step2.1: Select the 5 pixel at a time from the
                 $i^{th}$ raw of the $j^{th}$ share.
        Step2.2: Convert each pixel value to its
                 corresponding binary value.
        Step 2.3: Divide the binary value into 8
                  blocks each having 5 bits in
                  length.
        Step 2.4: Perform block by block XOR on
         the  shares.
        Step2.5:convert the result into
        corresponding  decimal value.
        Step2.6: Save the result as the  5 pixel
        information of the secret image
Step 3: Stop.
```

**Algorithm 2.2.** Reconstruction of secret from all seven shares is as follows:

```
Input: Seven shares; $S_1$, $S_2$, .... $S_7$ ; Each of dimension NxM

Output: The secret, SI, with dimension NxM

Step1: For i= 1 to N
Step2: For j=1 to 7
        Step2.1: Select the 5 pixel at a time from the
                 $i^{th}$ raw of the $j^{th}$ share.
        Step2.2: Convert each pixel value to its
                 corresponding binary value.
        Step 2.3: Divide the binary value into 8
                  blocks each having 5 bits in
                  length.
        Step 2.4: Perform block by block XOR on
         the  shares.
        Step2.5:convert the result into
        corresponding  decimal value.
        Step2.6: Save the result as the  5 pixel
        information of the secret image
Step 6: Stop.
```

EXAMPLE

Suppose the first 5 pixels of the Secret Image is ; **205, 163, 191, 240, 254**

The participant-shares are generated using Gray code of the secret image. Initially the pixel values are converted into the binary form and divided into 5 bits blocks.

The binary equivalent of the pixel values are;

11001101 10100011 10111111
11110000 11111110

The 5 bit blocks are;

11001 10110 10001 11011
11111 11100 00111 1111

Apply the steps *4.1* to *4.10* of the *Algorithm 1*.The first 5 pixel of the first share is generated from the initial binary form of the pixel values.

The first 5 pixel of the second share is generated from the first share. Likewise first 5 pixel values of the 7 shares are generated. TABLE. 1 shows the seven shares related to the example that we have considered here

| *Sl No* | *SHARES (in Binary form)* | *SHARES (in Binary form)* |
|---|---|---|
| 1 | 10101 11101 11001 10110 10000 10010 00100 10001 | 175 115 104 079 145 |
| 2 | 11111 10011 10101 11101 11000 11011 00110 11001 | 152 235 220 110 217 (Q- set) |
| 3 | 10000 11010 11111 10011 10100 10110 00101 10101 | 134 191 058 088 181 |
| 4 | 11000 10111 10000 11010 11110 11101 00111 11111 | 197 225 175 116 255 (Q- set) |
| 5 | 10100 11100 11000 10111 10001 10011 00100 10000 | 167 049 120 204 144 |
| 6 | 11110 10010 10100 11100 11001 11010 00110 11000 | 244 169 204 212 210 (Q- set) |
| 7 | 10001 11011 11110 10010 10101 10111 00101 10100 | 142 232 042 220 180 |

TABLE.1 Seven Shares

SECRET RECONSTRUCTION FROM QUALIFIED SET:

In secret reconstruction from qualified set, 3 out of 7 share scheme, as mentioned above in the Algorithm .1 the shares in Qualified Set (Q-Set) are just XORed.

```
11111  10011  10101  11101  11000  11011  00110  11001  ⊕
11000  10111  10000  11010  11110  11101  00111  11111  ⊕
11110  10010  10100  11100  11001  11010  00110  11000  ⊕
______________________________________________________
11001  10110  10001  11011  11111  11100  00111  11110
```

The result is; 11001101 10100011 10111111 11110000 11111110 (in 8 bit blocks ;)
**205, 163, 191, 240, 254** (in decimal form; the original secret)

SECRET RECONSTRUCTION FROM ALL SEVEN SHARES:

As mentioned above in the Algorithm, the secret reconstruction from all seven shares; 7 out of 7 share scheme, all shares are just XORed.

```
10101  11101  11001  10110  10000  10010  00100  10001   ⊕
11111  10011  10101  11101  11000  11011  00110  11001   ⊕
10000  11010  11111  10011  10100  10110  00101  10101   ⊕
11000  10111  10000  11010  11110  11101  00111  11111   ⊕
10100  11100  11000  10111  10001  10011  00100  10000   ⊕
11110  10010  10100  11100  11001  11010  00110  11000   ⊕
10001  11011  11110  10010  10101  10111  00101  10100   ⊕
_________________________________________________________
11001  10110  10001  11011  11111  11100  00111  11110
```

The result is; 11001101 10100011 10111111 11110000 11111110 (in 8 bit blocks ;)
**205, 163, 191, 240, 254** (in decimal form; the original secret)

## IV.SECURITY ANALYSIS

The security wise analysis in this case shows that, if the algorithm is known then the reconstruction of the secret will be easy. By just performing the repeated binary code generation from one of the share, the secret information can be reconstructed. That is there is no need of the collusion of either the shares from the Qualified Set or all seven shares. From the secret reconstruction algorithm it is clear that, the maximum steps that we need to perform the binary code generation to reconstruct the secret is 8.In order to avoid this situation, the blocks (5 bits blocks) are shuffled in shares. The thing that should be ensured in the shuffling is, it should be done separately among Qualified sets (Q-Set) and Forbidden sets (F-Set). Now, if the previously mentioned attack is applied on any of the shares, the secret will not be reconstructed in any of the stage.

## V.APPLICATION

PROPOSED SCHEME AS SECRET SHARING SCHEME:

Suppose the organization's structure is as shown in FIG.3; that is , A B and C is having equal high privileges and D,E,F and G is having same privileges which is lower than of A, B and C. Then the secret, if any, can be shared among them using the proposed system. Here the shares in the Q-Set should be shared among A, B and C. And the shares in the F-Set should be shared among D, E, F and G.

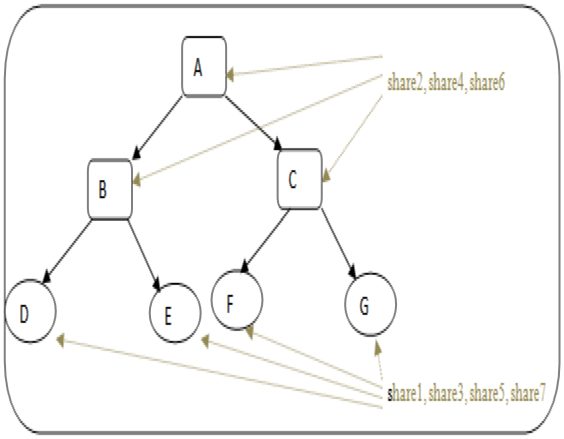


Fig 3: One Sample Organization Structure

PROPOSED SCHEME AS VISUAL DATA ENCRYPTION SCHEME:

The encryption scheme using the proposed system can be represented as bellow;

$$CI=E(SI,K)$$
$$SI=D(CI,K)$$

Where

SI is the secret image

CI is the cipher image

E is the encryption scheme; (The Gray code generation)

D is the decryption scheme; (The Binary code generation)

K is the key.

The encryption is the block processing. Here the block size is 5 bits. The process is as follows;

1. Consider 5 pixels from the secret image (SI) at a time.
2. Convert the pixel values into binary form.
3. Divide the binary value into 5 bits blocks; {8 blocks will be there}
4. Read 8 digit key; K. {each digit for each 5 bits block}.
5. Repeat the following steps until all the blocks are processed.
   4.1. Pick a block and its corresponding digit from the key
   4.2. Covert the block into the gray code, number of times the digit from the key is having.
6. Divide the resulting binary form into 8 bits block {5 blocks will be there}.
7. Convert the binary value into corresponding decimal value and save it as the 5 pixel values of the Cipher Image(CI)
8. Stop

Like encryption, the decryption is also blocking processing. The process is as follows;

1. Consider 5 pixels from the Cipher Image (CI) at a time.
2. Convert the pixel values into binary form.
3. Divide the binary value into 5 bits blocks; {8 blocks will be there}
4. Read 8 digit key; K. {each digit for each 5 bits block}.
5. Repeat the following steps until all the blocks are processed.
   4.1. Pick a block and its corresponding digit from the key
   4.2. Covert the block into the binary code, number of times the digit from the key is having.
6. Divide the resulting binary form into 8 bits block {5 blocks will be there}.
7. Convert the binary value into corresponding decimal value and save it as the 5 pixel values of the Secret Image(CI)
8. Stop

EXAMPLE

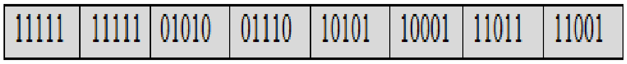
ENCRYPTION

Assume the pixel values; **255 212 234 199 121**

The binary equivalent is;

11111111 11010100 11101010 11000111 01111001

Divide the message into 5 bits block;



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 11111 | 11111 | 01010 | 01110 | 10101 | 10001 | 11011 | 11001 |

Now select a key K. The conditions are;

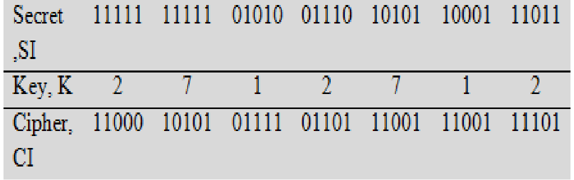
(a) Digits in the key should be less than or equal to the number of blocks in the message i.e. 8

(b) One more requirement is the digit that select in the key should be less than or equal to 7.

Assume key K= 271. Here the number of digit in the key is less than the number of blocks in the message, so the digits in the key are repeated so that the total length is equal to that of the number of blocks (say 8) in the plaintext.

Now the key K= 27127127

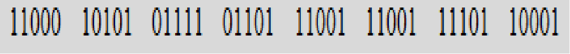
Now perform the step 3; the message will become



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Secret ,SI | 11111 | 11111 | 01010 | 01110 | 10101 | 10001 | 11011 |
| Key, K | 2 | 7 | 1 | 2 | 7 | 1 | 2 |
| Cipher, CI | 11000 | 10101 | 01111 | 01101 | 11001 | 11001 | 11101 |

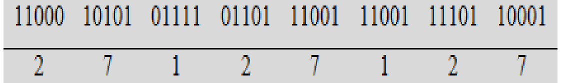
So the cipher text is;
11000101 01011110 11011100 11100111 10110001;
In decimal form **197 94 220 231 117**

DECRYPTION
Suppose the 5 pixels of Cipher Image is **197 94 220 231 117**
The binary equivalent is 11000101 01011110 11011100 11100111 10110001
Divide the cipher text into 5 bits block;



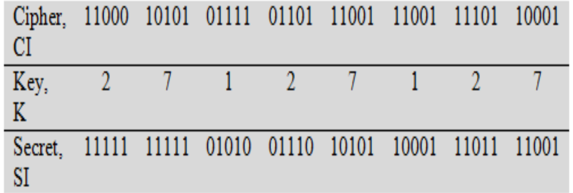
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 11000 | 10101 | 01111 | 01101 | 11001 | 11001 | 11101 | 10001 |

Here the key is K= 271.The number of digit in the key is less than the number of blocks in the cipher, so the digits in the key are repeated so that the total length is equal to that of the number of blocks (say 8) in the Cipher Image.
Now the key K= 27127127



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 11000 | 10101 | 01111 | 01101 | 11001 | 11001 | 11101 | 10001 |
| 2 | 7 | 1 | 2 | 7 | 1 | 2 | 7 |

Now perform the step 3; the cipher text will become



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Cipher, CI | 11000 | 10101 | 01111 | 01101 | 11001 | 11001 | 11101 | 10001 |
| Key, K | 2 | 7 | 1 | 2 | 7 | 1 | 2 | 7 |
| Secret, SI | 11111 | 11111 | 01010 | 01110 | 10101 | 10001 | 11011 | 11001 |

So the message is;
11111111 11010100 11101010 11000111 01111001;
In Decimal form **255 212 234 199 121**

## CONCLUSION

The paper mainly focuses on images. The proposed scheme can be used as an encryption scheme along with a key, in addition to the secret sharing purpose. Here we have considered the gray scale images. The proposed scheme can be extended to color images also. In the case of color images we have to perform the algorithm separately on three channels red, blue and green. The main advantage of the proposed scheme is, there is no information loses.

## REFERENCES

[1] M.Naor, A. Shamir, Visual cryptography, in: Proceedings of the Advances in Cryptology, Eurocrypt ’94, in: LNCS, vol.950, 1995, pp.1–12.

[2] M. Nakajima, Y. Yamaguchi, "Extended visual cryptography for natural images", J. WSCG, vol. 10, no. 2, pp. 303-310, 2002.

[3] G. Ateniese, C. Blundo, A. D. Santis, and D. Stinson.Visual cryptography for general access structures , Information and Computation, 129(2):86–106, 1996.

[4] Ito, Ryo, and Hidenori Kuwakdo. "Hatsukazu. Image size invariant visual cryptography." IEICE Trans. Fundamentals (1998): 2172-2177.

[5] Ching-Nung Yang. New visual secret sharing schemes using probabilistic method. Pattern Recognition Letters, 25(4):481-494,2004.

[6] Ching-Nung Yang and Tse-Shish Chen.New size-reduced visual secret sharing schemes with half reduction of shadow size. IEICE Transactions, 89-A(2):620-625,2006.

[7] Ching-Nung Yang and Tse-Shish Chen. Visual secret sharing scheme: Improving the contrast of a recovered image via dierent pixel expansions. In Aurelio C.Campilho and Mohamed S.Kamel,editors, ICIAR(1) volume 4141 of Lecture Notes in Computer Science , pages 468-479. Springer, 2006.

[8]. Z. Zhou, G. R. Arce, G. Di Crescenzo, "Halftone visual cryptography", Proc. IEEE Int. Conf. Image Process., 2003-Sep.

[9] Z. Zhou, G. R. Arce, G. Di Crescenzo, "Halftone visual cryptography", IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441-2453, Aug. 2006.

[10]Parakh, A. and Kak, S. 2010. A Tree Based Recursive Information Hiding Scheme. To appear in proceedings of IEEE ICC 2010 – Communication and Information System Security Symposium („ICC‟10 CISS‟), May 23-27, Cape Town, South Africa.

[11]. Parakh, A. and Kak, S. 2009. Recursive Secret Sharing for Distributed Storage and Information Hiding, Advanced Networks and Telecommunication Systems (ANTS), IEEE 3rd International Symposium on, pages 1-3, 14-16.

[12]. Parakh, A. and Kak, S. 2009. Space Efficient Secret Sharing: A recursive approach. Cryptology ePrint Archive, Report 2009/365.

[13].T. H. Chen and K. H. Tsao. Visual secret sharing by random grids revisited. Pattern Recognition, 42(9):2203– 2217, 2009.

[14] T. H. Chen and K. H. Tsao. Threshold visual secret sharing by random grids. Journal of Systems and Software, 84(7):1197–1208, 2011.

[15].T. H. Chen and C. S. Wu. Efficient multi-secret image sharing based on boolean operations. Signal Processing, 91(1):90–97, 2011.

[16].O. Kafri and E. Keren. Encryption of pictures and shapes by random grids. Optics Letters, 12(6):377–379, 1987.

[17] Eric R Verheul and Henk C A , Van Tilborg. Constructions and properties of k out of n visual secret sharing schemes. Design codes Cryptography. 11(2):179-196, 1997.

[18] Ching-Nung and Chi –sung Laih. New colored visual secret sharing schemes. Design, codes and Cryptography, 20(3): 325-336, 2000.

[19] Chang-Chou Lin and Wn-Hsiang Tsai. Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24(1-3):349-358, 2003.

[20] Y. C. Hou, ―Visual cryptography for color images, Pattern Recognit., vol. 36, pp. 1619–1629, 2003.

[21].Alon, N. and Spencer, J. 1992. The Probabilistic Method, Wiley-Interscience, 2nd edition.

[22]. D. Jin, W.Q. Yan, and M.S. Kankanhalli. Progressive color visual cryptography. Journal of Electronic Imaging, 14:033019–1–033019–13, 2005.

[23] Bernd Borchert, WSI-2007-04,"Segment-based Visual Cryptography", WSI-2007-04.

[24]Shyong Jian Shyu and Hung-Wei Jiang," Efficient Construction for Region Incrementing Visual Cryptography", IEEE Transactions on Circuits and Systems For Video Technology, Vol. 22, No. 5, May 2012.

[25] C.C. Wu and L.H.Chen. S study on visual cryptography. Mater's thesis, Institute of Computer and information Science, National Chiao tung University, Taiwan,R.O.C, 1998.

[26].C. C. Thien and J. C. Lin, "An image-sharing method with user-friendly shadow images," IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 12, pp. 1161–1169, 2003.

[27].T. H. Chen and K. H. Tsao, "Threshold visual
secret sharing by random grids," Journal of Systems and Software, vol. 84, no. 7, pp. 1197-1208, 2011.

[28].Tuyls, P., Hollmann, H.D.L., Lint, J.H.V. et al. XOR based Visual Cryptography schemes Des Codes Crypt (2005) 37: 169. doi:10.1007/s10623-004-3816-4

[29]G.Horng,T.H. Chen,D.S.Tsai, Cheating in visual cryptography, Des Codes Cryptogr.38(2)(2006)219–236.