A RELIABLE \((k,n)\) THRESHOLD BASED IMAGE SECRET SHARING SCHEME

1 NIKITA R. GOLE, 2 MADHUMITA CHATTERJEE

1 Lecturer, Department of Computer Engineering, BVU COE, Mumbai University, Navi Mumbai-400615, Maharashtra, India.
2 Professor, Department of Computer Engineering, RAIT, Mumbai University, Navi Mumbai-400706, Maharashtra, India.

1nikitagole@gmail.com, 2madhuma@rait.ac.in

ABSTRACT:
This paper presents a reliable \((k,n)\) threshold based secret sharing scheme using BPCS based Steganography. The secret means the colored image is represented with a square matrix \(S\). The square matrix \(S\) is divided into \(n\) image shares which are further distribute to \(n\) participants such that i) \(k\) participants are necessary to reconstruct the secret. ii) any \((k-1)\) or fewer participants cannot get enough information to reveal the secret. To distribute or send the shares to the authorized participants, a color image is used as the information hiding vessel for image shares. This scheme gives strong protection of the secret images, reduces the size of image shares, and maintains anonymity by embedding the secret shares inside vessel images.

1. INTRODUCTION

The effective and secure protections of sensitive information are primary concerns in commercial, medical and military systems (communication systems or networked storage systems). It is also important to any information process to ensure data is not being tampered. Encryption methods are one of the popular approaches to ensure the integrity and secrecy of the protected information. However, one of the critical vulnerabilities of the encryption techniques is single-point-failure, for example, the secret information can not be recovered if the decryption key is lost or the encrypted contents are corrupted during the transmission. To address these reliability problems, for large information content items such as secret images (satellite images or medical images), an Image Secret Sharing Scheme (SSS) is a good alternative to remedy these types of vulnerabilities.

In cryptography, secret sharing [3] refers to any method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.

For example, suppose you and your friend accidentally discovered a map that you believe would lead you to an island full of treasure. You and your friend are very excited and would like to go home and get ready for the exciting journey to the great fortune. Now who is going to keep the map? Suppose you and your so-called friend do not really trust each other and are afraid that, if the other one has the map, he/she might just go alone and take everything. Now we need a scheme that could make sure that the map is shared in a way so that no one would be left out in this trip. What would you suggest? To split the map into two pieces and make sure that both pieces are needed in order to find the island. You can happily go home and be assured that your friend has to go with you in order to find the island. This illustrates the basic concept of secret sharing.

A. Shamir invented \((k,n)\) threshold-based secret sharing scheme in 1979. Shamir further extended the secret sharing concept into images and referred as Visual Cryptography [3]. The general idea is 1) For a set \(P\) of \(n\) participants a secret image \(S\) is encoded into \(n\) shadow images called shares such that each participant in \(P\) receives one share and 2) certain qualified subset of participants can visually recover the secret image, but other, forbidden, set of participants have no information on \(S\). In Visual Cryptography [3], recovery for a set \(k\) of participants consist of copying the shares onto transparencies and then stacking them on a projector. The participants in a qualified set \(k\) will be able to see the secret image without any cryptographic computation. This method works only on black & white images.

To provide the security to image share while distribution of them to participants Bit-Plane...
Complexity Segmentation (BPCS) [6] based Steganography is good. It is a Steganography technique based on the property of human vision system, which effectively increases the information hiding capacity to as large as upto 50%. It uses a color images as the information hiding dummy data, i.e., the container, or carrier of the secret information.

BPCS relies on the fact that the human visual system is sensitive to patterns, but unable to identify random white noise. Therefore, to implement a BPCS algorithm, divide the image into regions and calculate the complexity of these regions. Any region with complexity above a certain threshold can be replaced with embedded data. This technique works on 24-bit true-color or 8-bit grayscale images.

The rest of the paper is organized as follows: Section 2 described a classification of Secret Sharing Schemes including Shamir's SSS, Section 3 described BPCS based Steganography. Section 4 described proposed work. The Result and Conclusion is given in section 5.

2. NOMENCLATURES

SSS Secret Sharing Scheme
BPCS Bit-Plane Complexity Segmentation
PSS Perfect Secret Sharing
RSS Ramp secret Sharing
\( k \) Threshold
\( n \) Number of participants
\( p \) Player i
\( q \) Prime Number
\( d \) Pixel of Secret
\( G \) Projection Matrix
\( R \) Remainder Matrix
\( S \) Secret matrix
\( \text{tr}() \) Trace of Matrix
\( \text{bpp} \) Bit Per Pixel
\( \alpha \) Image Complexity
\( a_0 \) Typical value of \( \alpha = 0.3 \)

3. CLASSIFICATION OF SECRET SHARING SCHEME

Depending on the number of participants required to reconstruct the secret, Secret Sharing Schemes can be broadly classified as,

3.1 \( k = n \) Image Secret Sharing Scheme

In these SSS [4], all the shares are necessary to reconstruct the secret. When space efficiency is not a concern, these schemes can be used to reveal a secret to any desired subsets of the players simply by applying the scheme for each subset. This approach quickly becomes impractical as the number of subsets increases.

\[ a \in [0,1] \]

\[ a_0 = 0.3 \]

\[ n \in [1,256] \]

\[ k \in [1,n] \]

\[ p \in [1,256] \]

\[ q \in [1,256] \]

\[ d \in [0,255] \]

\[ G \in [0,255] \]

\[ R \in [0,255] \]

\[ S \in [0,255] \]

\[ \text{tr}(G) \in [0,255] \]

\[ \text{bpp} \in [0,255] \]

\[ \alpha \in [0,1] \]

\[ a \in [0,1] \]

\[ a_0 = 0.3 \]

\[ n \in [1,256] \]

\[ k \in [1,n] \]

\[ p \in [1,256] \]

\[ q \in [1,256] \]

\[ d \in [0,255] \]

\[ G \in [0,255] \]

\[ R \in [0,255] \]

\[ S \in [0,255] \]

\[ \text{tr}(G) \in [0,255] \]

\[ \text{bpp} \in [0,255] \]

\[ \alpha \in [0,1] \]

\[ a \in [0,1] \]

\[ a_0 = 0.3 \]

ISSN: 0974-3596 | October '09 – March '10 | Volume 2 : Issue 1 | Page: 206
On computer and television screens, the smallest division of color data is a pixel. In computer memory, each pixel is represented by a binary value. The more bits that are used to represent each value, the wider the range of colors are for each pixel. Typical amounts of bits per pixel (bpp) are 8, 24, and 32. With these binary pixel values, and knowledge of which part of the picture each one represents, bit planes are constructed.

4.1 Bit Plane

A bit plane is a data structure made from all the bits of a certain significant position from each binary digit, with the spatial location preserved. BPCS addresses the embedding limit by working to disguise the visual artifacts that are produced by the steganographic process. The human visual system is very good at spotting anomalies in areas of homogenous color, but less adept at seeing them in visually complex areas. When an image is deconstructed into bit-planes, the complexity of each region can be measured. Each bit-plane can be segmented into "shape-informative" and "noise-looking" regions [7]. A shape-informative region consists of simple patterns, while a noise-looking region consists of complex patterns. Areas of low complexity such as homogenous color or simple shapes appear as uniform areas with very few changes between one and zero.

4.2 Bit-Plane Decomposition

A multi-valued image (P) consisting of n-bit pixels can be decomposed into a set of n binary pictures. For example, if the image is an n-bit gray image, it is shown as,

\[ P = (P_1, P_2, ..., P_n) \]

in case the image is a Red, Green, Blue color picture, it is shown by

\[ P = (P_{R1}, P_{R2}, ..., P_{Rn}, P_{G1}, P_{G2}, ..., P_{Gn}, P_{B1}, P_{B2}, ..., P_{Bn}) \]

Where P_{R1}, P_{G1}, P_{B1} are the most significant bit-planes (MSB), while P_{Rn}, P_{Gn}, P_{Bn} are the least significant planes (LSB).

4. BIT-PLANE COMPLEXITY SEGMENTATION BASED STEGANOGRAPHY

Bit Plane Complexity Segmentation steganography is a modern method of data hiding [8]. Earlier methods of image steganography simply replaced the least significant bits of each pixel with hidden data. This practice had very low embedding rates because visual defects rapidly develop as more significant bits are used. These defects are most noticeable in areas of homogenous color, where they usually appear as noise-like static. As more data is added, the noise becomes more pronounced, until the image fades to unintelligible static. The degradation can become obvious and severe with only 10 to 15 percent of the image replaced with secret data.

On computer and television screens, the smallest division of color data is a pixel. In computer memory, each pixel is represented by a binary value. The more bits that are used to represent each value, the wider the range of colors are for each pixel. Typical amounts of bits per pixel (bpp) are 8, 24, and 32. With these binary pixel values, and knowledge of which part of the picture each one represents, bit planes are constructed.

Steps for Shamir’s SSS:

1. Dealer selects \( n \) different non-zero elements \( x_i \), \( 1 \leq i \leq n \) from GF(q) randomly, where q is prime number larger than \( n \). Then \( x_i \) is sent to player \( i \) named \( p_i \), publicly.
2. Secret Share Distribution Phase
   a. Dealer select \( k-1 \) elements \( d_j \), \( 1 \leq j \leq k-1 \) from GF(q) randomly to construct \( k-1 \) degree polynomial denoted as: \( F(x) = d_0 + d_1 x + d_2 x^2 + ... + d_{k-1} x^{k-1} \) (mod q) where, \( d_0 \) is secret and q is prime number.
   b. The secret share \( y_i \) is computed as, \( y_i = f(x_i) \), \( 1 \leq i \leq n \) and delivered to \( p_i \) secretly.
3. Sharing Resuming Phase
   a. Any \( k \) members among total \( n \) players can resume the secret. Suppose \( k \) players are \( p_1, p_2, ..., p_k \), who provide secret shares \( (x_i, y_i) \), \( 1 \leq i \leq k \). Polynomial \( f(x) \) can be determined by secret \( (x_i, y_i) \), by using following polynomial:
   \[
   f(x) = \Sigma_{j=1}^{k} y_j \prod_{i=1, i \neq j}^{k} (x-x_i) (mod q)
   \]
   b. The value of secret \( d_0 \) can be computed by set \( x \) to zero in formula 1, \( f(0) = d_0 \). So set \( x \) to zero in formula 2 we can get the secret \( d_0 \) denoted by following formula,
   \[
   d_0 = f(0) \quad (mod q)
   \]
   \[
   k = \Sigma_{j=1}^{k} y_j \prod_{i=1, i \neq j}^{k} (x-x_i) (mod q)
   \]

**Figure 4: Bit Planes**
In Figure 4, the plane PR3 is mostly shape-informative, but PR6 is mostly noise-looking. PR4 is mixed with both shape-informative and noise-looking regions. It is reported that two regions can be segmented by using a “black-and-white border length” based complexity measure.

4.3 Complexity Measure

BPCS uses image segmentation based on the measure called complexity. Image Complexity [6] is defined as the length of the black-and-white border in a binary image. If the boarder is long, the image is complex, otherwise it is simple. The total length of the black-and-white border equals to the summation of the number of color-changes along the rows and columns in an image. For example, a single black pixel surrounded by white background pixels has the boarder length of 4.

Image Complexity α [6] is given by,

\[ \alpha = k / \text{the max. Possible B-W change in the image} \]

Where, \( k \) is the total length of black-and-white border in the image. So, the value ranges over \( 0 \leq \alpha \leq 1 \).

4.4 Conjugation operation to the embedding data

The embedding data can be arranged in a sequence of “bit-squares” (such as 8 x 8 squares). If a square is more complex than the complexity threshold value, embed it just as it is. Otherwise, apply the conjugation operation to the square to make it more complex than the threshold. This conjugation operation does not change any pattern information about the square. This guarantees that one can embed any computer data. However, there must be an entry in the “conjugation map” to recover the original data.

5. PROPOSEDMETHOD

For an \( I \times I \) secret image with intensity level as \( I \) (i.e., \( 1 \leq i, j \leq I \)) partition the secret image \( I \) as non-overlapped \( m \times m \) blocks for each RGB color. It procedures roughly \( I^2 \) blocks. To share each block I am using following scheme:-

Construction of Secret Shares from secret matrix S:

1. Construct an \( m \times k \) random matrix \( A \) of rank \( k \)
2. Determine its projection matrix \( \mathbb{F} \) and remainder matrix \( R = S - \mathbb{F} \)
3. If any element in matrices \( \mathbb{F} \) and \( R \) is greater than 251, go back to step 1 to reconstruct a new random matrix \( A \). Otherwise proceed to next step.
4. Choose \( n \) linearly independent \( k \times 1 \) random vectors \( x \), and \( n \) distinct values \( r \)
5. Calculate share \( v_i = (A \times x_i) \mod p \) for \( 1 \leq i \leq n \)
6. Use Thien and Lin’s image secret sharing scheme [2] to secretly share the matrix \( R \) as \( G_i = \left[ g_i^{0}, g_i^{1}, \ldots, g_i^{m-1} \right] \)

for \( g_i^{j}(k) = 1 \leq j \leq I \), and \( 1 \leq j \leq m \)

and \( r_i = i \) where \( i = 1 \) to \( m \)

7. Each image share \( S_i \) is the combination of \( v_i \) and \( G_i \).

Embedding of secret shares into the vessel image:

1. A carrier image is a “vessel” or “dummy” image which is a color image in BMP file format, which hides (or, embeds) the secret information (i.e. image shares in BMP format).
2. Segment each secret image share \( S_i \) to be embedded into a series of blocks having 8 bytes of data each. These secret blocks are regarded as 8 x 8 image patterns.
3. If a 8 x 8 secret block \( B \) of image share is less than the threshold \( \theta \), then conjugate it to make it a more complex block \( B^* \). The conjugated block must be more complex than \( \theta \). (A typical value of \( \theta = 0.3 \) if the block is conjugated. Then record this fact in a “conjugation map.”
4. Segment each bit-plane of the vessel image into informative and noise-like regions by using a threshold value \( \theta \).
5. Embed each secret block \( B^* \) into the noise-like regions of the bit-planes or replace 8 x 8 block \( V \) of each bit-plane of vessel image (if it is complex than \( \theta \)) with 8 x 8 block \( B^* \).
6. If the block \( V \) is not complex, then keep the block \( V \) as it is in the vessel image.

Decoding of secret shares from the vessel image:

1. Search for complex blocks in the vessel image. If the block \( V \) is not complex than \( \theta \), then ignore the block \( V \). If it is complex than \( \theta \) then it is an embedded block \( B^* \).
2. Check the “conjugation map” of embedded block \( B^* \). The first bit indicate the image is color image or back & white image. (1-color image, 0-black & white image)
3. The remaining bits of conjugation map indicate the blocks of secret share that are conjugated. The value 1 of bit in conjugation map shows the corresponding block(B*) of image share is conjugated while embedding into vessel image. To get the original block (B) of image share conjugate the block(B). If the value of bit in conjugation map is 0 shows put the block as it is from image share.  

4. Similarly, decode all shares from vessel image to get the image shares $S_h$.

**Secret Reconstruction**

1. Collect $k$ shares from any $k$ participants, say the shares are $v_1, v_2, \ldots, v_k$ and construct a matrix $B = [v_1, v_2, \ldots, v_k]$.  

2. Calculate the projection matrix $\mathcal{E} = \left( B \cdot (B' \cdot B)^{-1} \cdot B' \right) \pmod{p}$

3. Verify that $\text{tr} (\mathcal{E}) = k$ and

4. Use Thien's and Lin's Secret Reconstruction formula
   
   $$G_i = p - g_i \cdot (j)$$
   
   Where $1 \leq i \leq \frac{m}{k}$ and $1 \leq j \leq m$

5. Construct a polynomial function of order $(k - 1)$ for $G_i$ where $i = 1$ to $m$
   
   $$g_i^{(j)}(x) = a_0x^{k-1} + a_1x^{k-2} + \ldots + a_2x^1 + a_1x^0 \pmod{251}$$
   
   Where $1 \leq i \leq \frac{m}{k}$ and $1 \leq j \leq m$  
   By solving the equation find the values for $a_0, a_1, \ldots, a_i$, which are the pixel values of Remainder Matrix $R$.

6. Compute the Secret $S = (\mathcal{E} + R) \pmod{p}$

---

**Figure 5: Secret Image, User**

**Figure 6: Image Shares for User Image**

**Figure 7: Reconstruction of User Image**

**Figure 8: Image Share 1**
Advantages

1. The image shares require $\frac{1}{k+1} / m$ size of the secret image due to this the size of image shares is significantly less than the size of the secret image.

2. If any image share is corrupted, the secret image will be obtained by remaining image shares.

6. CONCLUSION

In this paper, we present a $(k,n)$ image SSS which is effective, reliable and secure method to prevent the secret image from being lost, stolen or corrupted. A colored secret image can be successfully reconstructed from any $k$ image shares, but cannot be revealed from any $(k-1)$ or fewer image shares. The size of image shares is smaller than the size of the secret image. In comparison with other image secret sharing methods, this approach's advantages are its large compression rate on the size of the image shares, its strong protection of the secret image. Additional security is provided by using BPCS technique to further mask the image shares and embed them in the vessel image. Due to this any third party or unintended user can not identify that the vessel image is having any secret embedded in it.

7. REFERENCES


[8] Eric Cole "Hiding in Plain Sight: Steganography and the Art of Covert Communication".