A Novel Secret Sharing Scheme Using POB Number System and CRT

Deepika M P
Research Scholar, Cochin University of science and technology, Kochi, Kerala, India.

Dr. A Sreekumar
Assistant Professor, Cochin University of Science and Technology, Kochi, Kerala, India.

Abstract
Secret sharing (also called secret splitting) refers to methods for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use on their own. Secret sharing schemes are ideal for storing information that is highly sensitive and highly important. Examples include: encryption keys, missile launch codes, and numbered bank accounts. Each of these pieces of information must be kept highly confidential, as their exposure could be disastrous; however, it is also critical that they should not be lost. Secret sharing schemes are important in cloud computing environments. Secret sharing has also been suggested for sensor networks where the links are liable to be tapped by sending the data in shares which makes the task of the eavesdropper harder. The security in such environments can be made greater by continuous changing of the way the shares are constructed. In this paper we introduce a scheme to share a secret among n participants, i.e. a n out of n secret sharing scheme, based on a new number system called Permutation Ordered Binary Number System (POB number system) and Chinese Remainder Theorem (CRT). This scheme is an efficient one with respect to security and performance. Even though the size of the shares is more than the size of the secret, the reconstructed original secret will have the same size as the original secret. So the scheme is a loss less scheme.

Keywords: VC schemes, POB number system, Secret Sharing, CRT.

Generalization
Let’s generalize the idea. Given a secret s, and there are n parties to share the secret, then the secret sharing scheme must follow the following properties:
1. All n parties can get together and recover s.
2. Less than n parties cannot recover s.

This kind of secret sharing may not suffice in certain cases. In some situations; some k shares will be enough to reveal the secret information, where k is less than n; (k < n)

(k, n) Secret Sharing
To generalize the properties, we get (k, n) secret sharing. Given a secret s, to be shared among n parties, that sharing should satisfy the following properties:
1. Availability: greater than or equal to k parties can recover s.
2. Confidentiality: less than k parties have no information about s.

In (2, 2) Visual Cryptography proposed by Moni Naor and Adi Shamir in 1994[2], the original image is divided into 2 shares. Both shares are required to reveal the secret image. If a white pixel is encountered in original image the first row in Fig 1 is selected with probability 0.5 and the shares are assigned as shown in the figure. Similarly if a black pixel is encountered, the last row is selected with probability 0.5 and assigned to each share. And in the reconstruction phase, the superimposition of both the shares reveals the original image.

![Figure 1: (2, 2) Visual Cryptographic Scheme](image)

In (k, n) visual cryptography scheme, n shares are generated from original image and distributed. Original image is
recognizable only if k or more shares stacked together, where value of k is between 2 to n. If fewer than k shares stacked together, original image cannot be recognized. It gives flexibility to user. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained. Blundo et. al [3] proposed an optimal contrast k-out-of-n scheme to alleviate the contrast loss problem in the reconstructed images.

Ateniese [4] proposed a more general method for VC scheme based upon general access structure. The access structure is a specification of qualified and forbidden subsets of shares. The participants in a qualified subset can recover the secret image while the participants in a forbidden subset cannot.

The VC scheme concept has been extended to grayscale images rather than binary images. Blundo et al [5] proposed VC schemes with general access structures for grayscale images. Hou[6] transformed a gray-level image into halftone images and then applied binary VC schemes to generate shares. Although the secret image is grayscale, shares are still constructed by random binary patterns carrying visual information which may lead to suspicion of secret encryption.

Myodo [6] proposed a method to generate meaningful halftone images using threshold arrays. Wang et. al.[7] produced halftone shares showing meaningful images by using error diffusion techniques. This scheme generates more pleasing halftone shares owing to errors diffused to neighbor pixels. Visual secret sharing for color images was introduced by Naor and Shamir based upon cover semi groups. Hou [8] devised schemes for color shares by applying halftone methods and color decomposition. Hou decomposed the secret color image into three (yellow, magenta and cyan) halftone images. He then devised three colored 2-out-of-2 VC schemes which follow the subtractive model for color mixture by exploiting some of the existing binary VC schemes.

Visual cryptography schemes were applied to only black and white images till year 1997. Verheul and Van Tilborg [9] proposed first color visual cryptography scheme. In this visual cryptography scheme one pixel is distributed into m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel, there is exactly one color region colored, and all the other color regions are black F.Liu, C.K.Wu, X.J. Lin [10]proposed a new approach for colored visual cryptography scheme They proposed three different approaches for color image representation: In first approach, colors in the secret image can be printed on the shares directly. It works similar to basic visual cryptography model. In second approach separate three color channels are used. Red, green, blue for additive model and cyan, magenta, yellow for subtractive model. In third approach, binary representation of color of a pixel is used and secret image is encrypted at bit-level. This results in better quality of image

All the previous researches in visual cryptography were focusing on securing only one image at a time. Wu and Chen [11] were first researchers, who developed a visual cryptography scheme to share two secret images in two shares.

J Shyu et al [12] proposed a scheme for multiple secrets sharing in visual cryptography, where more than two secret images can be secured at a time in two shares.

Ran-Zan Wang [13] developed a scheme “Region Incrementing Visual cryptography” for sharing visual secrets of multiple secrecy level in a single image In this scheme, different regions are made of a single image, based on secrecy level and different encoding rules are applied to these regions. 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 a new scheme which is not pixel-based but segment-based [14]. 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 recognize for the human eye and it may be easier for a non-expert human user of an encryption system to understand the working.

In (k, n) visual secret sharing scheme, it is not possible to recover the secret image though one less than k shares are available. This problem is solved in progressive visual cryptography scheme developed by D. Jin, W. Q. Yan, and M. S. Kankanhalli [15]. In progressive visual cryptography scheme, it is not necessary to have at least k shares out of n, as in (k, n) secret sharing scheme. If more than one share obtained, it starts recovering the secret image gradually. The quality of recovered image improves, as the number of shares received increases.

Permutation Ordered Binary Number System

POB number system called, Permutation ordered binary number system is a general number system with two nonnegative integral parameters, n and r, where n ≥ r developed by A. Sreekumar et. al [16] in the course of his research work. This number system is found to be very useful and more efficient than the conventional number system under use. In [6] they have used POB number system in a newly introduced secret sharing scheme.

The system is denoted by POB (n, r). In this number system, it is possible to represent all integers in the range 0, ..., \(2^n-1\) as binary string, say B = \(b_n b_{n-1} b_{n-2} \ldots b_0\) of length n, and having exactly r 1s. Each digit of this number, say, \(b_j\) is associated with its position value, given by \(b_j \times \left(\frac{\text{r}}{2}\right)^j\), where \(p_j = \sum_{i=0}^{\text{r}} b_i\) and the value represented by the POB number B, denoted by V (B), will be the sum of the position values of all of the digits.

i.e., \(V(B) = \sum_{j=1}^{\text{r}} b_j \left(\frac{\text{r}}{2}\right)^j\)

For example, 111001000 is a POB (9,4) number with value of 123.

In this example

\(p_1=1\)
\(p_2=2\)
\(p_3=3\)
\(p_4=4\)

\(V(111001000) = 1 \times \left(\frac{\text{4}}{2}\right)^1 + 1 \times \left(\frac{\text{4}}{2}\right)^2 + 1 \times \left(\frac{\text{4}}{2}\right)^3 + 1 \times \left(\frac{\text{4}}{2}\right)^4\)

\(= 1 \times 3 + 1 \times 15 + 1 \times 35 + 1 \times 70\)

\(= 123\)

2050
Algorithm for finding POB numbers
For a given pair of parameters n and r with r ≤ n, the algorithm takes three inputs: n, r and val with 0 ≤ val ≤ \(\binom{n}{r}\) - 1; or in a POB(n, r) number system, if a POB value, say val is given, then the below listed algorithm generates POB(n, r) number: B, such that V(B) = val.

**Algorithm I:** Generate POB-number corresponding to a given POB-value.

**Input:** three numbers n, r, and val with r ≤ n and 0 ≤ val ≤ \(\binom{n}{r}\) - 1.

**Output:** The POB number B = bn-1bn-2 ….. b0.

**Step 1.** Let j = n and temp = val

**Step 2.** For k = r down to 1 do:
1. Repeat {
2. \( j = j - 1 \)
3. \( p = \binom{j}{k} \)
4. if (temp ≥ p) temp = temp - p
5. bj = 1
6. else bj = 0
7. Until (bj = 1)

**Step 3.** if (j > 0)
For k = j - 1 down to 0 do:
\( b_k = 0 \)

**Remark:** B = bn-1bn-2 ….. b0 is the POB-number.

**Lemma 1:** Algorithm 1 generates the POB-number (n, r) corresponding to the given POB-value.

Consider POB (9, 4) number system:

<table>
<thead>
<tr>
<th>Sl.No</th>
<th>POB Number</th>
<th>Binary Equivalent</th>
<th>Sl.No</th>
<th>POB Number</th>
<th>Binary Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0 0 0 0 0 1</td>
<td>1 1 1 1 1 0 0 0 1</td>
<td>16</td>
<td>0 1 0 0 0 0 1</td>
<td>0 0 0 0 0 1 1 0 1</td>
</tr>
<tr>
<td>1</td>
<td>0 0 0 1 0 1</td>
<td>1 1 1 0 1 1 0 1 1</td>
<td>17</td>
<td>0 1 0 0 0 1 0</td>
<td>0 0 1 1 1 1 0 0 1</td>
</tr>
<tr>
<td>2</td>
<td>0 0 0 1 0 1</td>
<td>1 1 1 0 1 1 0 1 1</td>
<td>18</td>
<td>0 1 0 0 0 1 0</td>
<td>0 0 0 0 0 1 1 0 1</td>
</tr>
<tr>
<td>3</td>
<td>0 0 1 0 1 0</td>
<td>1 1 0 0 1 1 1 0 1</td>
<td>19</td>
<td>0 1 0 0 0 1 0</td>
<td>0 0 0 0 0 1 1 1 0</td>
</tr>
<tr>
<td>4</td>
<td>0 0 1 0 1 0</td>
<td>1 1 0 0 1 1 1 0 1</td>
<td>20</td>
<td>0 1 0 0 0 1 0</td>
<td>0 0 0 0 0 1 1 1 0</td>
</tr>
<tr>
<td>5</td>
<td>0 0 1 0 1 0</td>
<td>1 1 0 0 1 1 1 0 1</td>
<td>21</td>
<td>0 1 0 0 0 1 0</td>
<td>0 0 0 0 0 1 1 1 0</td>
</tr>
<tr>
<td>6</td>
<td>0 0 1 0 1 0</td>
<td>1 1 0 0 1 1 1 0 1</td>
<td>22</td>
<td>0 1 0 0 0 1 0</td>
<td>0 0 0 0 0 1 1 1 0</td>
</tr>
<tr>
<td>7</td>
<td>0 1 0 0 1 0</td>
<td>1 0 1 0 1 1 0 1 1</td>
<td>23</td>
<td>0 1 0 0 0 1 0</td>
<td>0 0 0 0 0 1 1 1 0</td>
</tr>
</tbody>
</table>

**Chinese Remainder Theorem**
In the following, some basic facts and conclusions of the CRT are summarized. This mathematical background knowledge is of elementary importance for the efficient realization of proposed secret sharing scheme.

**Theorem 1 (Chinese Remainder Theorem):**
Let the numbers \(n_1, n_2, \ldots, n_k\) be positive integers which are relatively prime in pair, i.e., gcd \((n_i, n_j) = 1\) when \(i \neq j\). Furthermore, let \(n = n_1n_2 \ldots n_k\) and let \(a_1, a_2, \ldots \) be integers.

Then the system of congruences
\[ x \equiv a_1 \mod n_1 \]
\[ x \equiv a_2 \mod n_2 \]
\[ \ldots \]
\[ x \equiv a_k \mod n_k \]
has a simultaneous solution \(x\) to all of the congruences, and any two solutions are congruent to one another modulo \(n\). Furthermore there exists exactly one solution \(x\) between 0 and \(n-1\).
A constructive proof of the Chinese Remainder Theorem is given in [5]. The unique solution \( x \) of the simultaneous congruences satisfying \( 0 \leq x < n \) can be calculated as

\[
x = \left( \sum_{i=1}^{k} x_i \eta_i s_i \right) \mod n
\]

Where \( \eta_i = \frac{n}{n_i} \) and \( s_i = \eta_i^{-1} \mod n_i \) for \( i = 1, 2, \ldots, k \)

**Solution for a system of linear congruence using CRT**

Use the Chinese Remainder Theorem to find solution for the following system of congruence;

\[
x \equiv 3 \mod 4
\]

\[
x \equiv 2 \mod 3
\]

\[
x \equiv 4 \mod 5
\]

First of all establish the basic notation. In this problem we have \( k = 3, a_1 = 3, a_2 = 2, a_3 = 4, n_1 = 4, n_2 = 3, n_3 = 5, \) and \( n = 4 \times 3 \times 5 = 60. \)

Calculate \( r_1 = \frac{n}{n_1} = \frac{60}{4} = 15 \)

\[
r_2 = \frac{n}{n_2} = \frac{60}{3} = 20
\]

\[
r_3 = \frac{n}{n_3} = \frac{60}{5} = 12
\]

Calculate \( s_1 = \eta_1^{-1} \mod n_1 \)

For that compute; \( s_1^2 \equiv 1 \mod n_1 \)

In this problem we need to solve;

\[
15s_1 \equiv 1 \mod 4
\]

\[
20s_2 \equiv 1 \mod 3
\]

\[
12s_3 \equiv 1 \mod 5
\]

and we find that \( s_1 = 3 \) \( s_2 = 2, \) and \( s_3 = 3. \)

\[
x = a_1 s_1 s_2 + a_2 s_2 s_3 + a_3 s_3 s_1 \mod 60.
\]

Substituting, we obtain;

\[
3 \times 3 \times 15 + 2 \times 2 \times 20 + 4 \times 3 \times 12 = 359
\]

which reduces to \( x \equiv 59 \mod 60. \)

**Proposed System**

Secret sharing scheme using POB number system and CRT. In this section we describe the algorithm for the 2 out of 2 secret sharing scheme and in the next section, the algorithm for an n out of n scheme where n is greater than or equal to 3; \( n \geq 3 \). The proposed scheme is a block cipher; that is each byte is handles separately, for that the scheme assumes that the secret consists of a sequence of bytes.

POB number system is used to enhance the security level in the proposed secret sharing scheme. And it is found very useful and more efficient than the conventional number systems. We have also used Chinese Remainder theorem in our newly introduced secret sharing scheme.

2 out of 2 scheme

Let \( M = m_1 \ m_6 \ m_5 \ m_4 \ldots \ m_0 \) be one byte of the secret information from that we are constructing two shares. That means \( M \) is the byte of the secret information that is to be shared between two participants. We first find out the decimal equivalent of the secret information \( M \), say it is \( B \). Then we generate a POB \((11, 5)\) number corresponding to \( B \), say it is \( N \). that means \( M \) of having 8 bits are now converted into \( N \) of having 11 bits. Now randomly select two primary numbers less than 462 i.e., primary numbers less than \( \left( \frac{11}{2} \right) \), that say is \( p \) and \( q \) respectively. Then we find two quantities \( B \mod p \) and \( B \mod q \) as \( X \) and \( Y \). after that we generate two POB \((11, 5)\) numbers corresponding to \( X \) and \( Y \) say that are \( S_1 \) and \( S_2 \). The \( S_1 \) and \( S_2 \) represent the first 11 bits of two shares respectively.

**Algorithm III:** sharing byte into two shares.

Input: The secret information \( M = m_1 \ m_6 \ m_5 \ m_4 \ldots \ m_0 \) having 8 bits long

Output: Two blocks \( S_1 \) and \( S_2 \) of length 11 bits.

Global values: Two relative prime numbers \( p \) and \( q \)

Step 1: Let \( X, Y, S_1 \) and \( S_2 \) be 11 bit long integers. Set all the bits of \( X, Y, S_1 \) and \( S_2 \) to null.

Step 2: The input string \( M \) is converted into decimal equivalent value, say \( D \).

Step 3: Let \( N \) be the POB \((11, 5)\) number with value of \( D \). [use Algorithm I].

\[ N = n_1 \ n_0 \ n_1 \ n_2 \ n_3 \ldots \ n_0 \]

Step 4: Convert the POB number \( N \), into decimal equivalent, say \( B \)

Step 4: Let \( X = B \mod p \)

\[ Y = B \mod q \]

Step 5: Let \( S_1 \) is the POB \((11, 5)\) number with value of \( X \) and \( S_2 \) be the POB \((11, 5)\) number with value of \( Y \). [use Algorithm I].

**Algorithm IV:** Recover the secret information.

Input: Two shares \( S_1 \) and \( S_2 \) of length 11 bits each.

Output: The secret information \( M = m_1 \ m_6 \ m_5 \ m_4 \ldots \ m_0 \)

Global values: Two relative prime numbers \( p \) and \( q \)

Step 1: Let \( X \) and \( Y \) be the POB values corresponding to \( S_1 \) and \( S_2 \).

\[ X = V \ (S_2) \]

\[ Y = V \ (S_1) \]

Step 2: Generate the system of simultaneous congruence like following:

\[ Z \equiv X \mod p \]

\[ Z \equiv Y \mod q \]

Step 3: Solve the above system of simultaneous congruence using CRT method. [use Algorithm II]. And find the unique solution for the system, let it be \( Z \)

Step 4: Find the Binary equivalent of the \( N \), say \( M \). where \( M \) is the secret information.

\[ M = m_1 \ m_6 \ m_5 \ m_4 \ldots \ m_0 \]

**Lemma 1:** the above scheme is a 2 out of 2 secret sharing scheme.

In the algorithm III, the size of shares is 11 bits while the size of the secret information is 8 bits. That means two 11 bits are generated as shares with respect to a single byte in original secret information. There is pixel expansion during the sharing phase. But in the reconstruction time the secret image is 8 bit as such. So there is no loss of information in this scheme and it is efficient also.
Example 1:
Let us consider a secret, M=11001011.

Secret sharing:
Let p and q (The global values, prime numbers) are 37 and 89 respectively.
The decimal equivalent of M is 203.
The POB (11, 5) number with the value 203 is 01100010110.
Say N=01100010110
Decimalequivalent of N, say B= 790.
Compute X and Y as follows;
X= 790 mod 37
Y= 790 mod 89
i.e. X=13 and Y=78
Let S1 is the POB (11, 5) number with value of 13 and S2 be the
POB (11, 5) number with value of 78
The two shares S1 and S2 are as follows;
S1=0001101101
S2=00101011001

Recovery:
Let p and q (The global values, prime numbers) are 37 and 89 respectively.
Find the POB values corresponding to S1 and S2.
V (S1) = V (0001101101) =13
V (S2) = V (00101011001) =78
The generated system of simultaneous congruence is;
Z ≡ 13 mod 37
Z ≡ 78 mod 89
Apply CRT, Algorithm II, and the unique solution obtained is
The POB (11, 5) number with the value 203 is 01100010110.
Say N=01100010110
The binary equivalent of 203 is;
(203) d =M= (11001011)2

Algorithm V: sharing byte into n shares.
Input: The secret information M = m1, m2, m3 ….. m0 having 8
bits long
Output: n blocks S1, S2……. Sn of length 11 bits.
Global values: n relative prime numbers P1, P2…. Pn
Step 1: Let X1, X2,…. Xn be the POB values corresponding to
S1, S2,….. Sn
X1 = V (S1)
X2 = V (S2)
.: 
Xn = V (Sn)
Step 2: Generate the system of simultaneous congruence like following;
Z ≡ X1 mod P1
Z ≡ X2 mod P2
.: 
Z ≡ Xn mod Pn
Step 3: Solve the above system of simultaneous congruence using CRT method. [Use Algorithm II]. And find the unique solution for the system, let it be Z
Step 4: Find the Binary equivalent of the N, say M. where M is
the secret information.
M = m1, m2, m3 ….. m0

Example 2: Let us consider 3 out of 3 schemes
Let us consider a secret, M=11001011

Secret sharing:
Let P1, P2, and P3 (The global values, prime numbers) are 37, 89 and 113 respectively.
The decimal equivalent of M is 203.
The POB (11, 5) number with the value 203 is 01100010110.
Say N=01100010110
Decimal equivalent of N, say B= 790.
Compute X1, X2 and X3 as follows;
X1= 790 mod 37
X2= 790 mod 89
X3= 790 mod 113
i.e. X1=13, X2=78 and X3=112
Let S1 is the POB (11, 5) number with value of 13, S2 be the
POB (11, 5) number with value of 78 and S3 be the POB (11, 5)
number with value of 112.
The two shares S1 and S2 are as follows;
S1=0001101101
S2=00101011001
S3=00111000101

Recovery:
Let P1, P2, and P3 (The global values, prime numbers) are 37, 89 and 113 respectively.
Find the POB values corresponding to S1 , S2 and S3
V (S1) = V (0001101101) =13
V (S2) = V (00101011001) =78
V (S3) = V (00111000101) =112
The generated system of simultaneous congruence is;
Z ≡ 13 mod 37
Z ≡ 78 mod 89
Z ≡ 112 mod 113
Apply CRT. Algorithm II, and the unique solution obtained is
203
The POB (11, 5) number with the value 203 is 01100010110
Say N = 01100010110
The binary equivalent of 203 is;
(203)₃ = M = (110010111)₂

Performance and security Analysis
The proposed scheme has pixel expansion in the secret sharing phase. So the space will be compromised in relation with the storage of shares. But in the reconstruction phase, have loss less reconstruction. We are construction one byte secret information (original information) from the 11 bit shares.
The proposed scheme is under POB (11, 5) number system. That means there is a total of 461 shares corresponding to one byte of secret. The probability of a correct guess of a share will be \(\left(\frac{1}{461}\right)^m\) per byte of secret. If there are m bytes in the secret, then this would mean that the probability of correct guess of a share will be as low as \(\left(\frac{1}{461}\right)^m\).

Conclusion
In the proposed system we have used both POB number system and CRT method. And both have great potential in secret sharing. The given scheme is effective in security wise and it is a loss less scheme also.

References