International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Performance Analysis of Various Secret Sharing Techniques

Surbhi Sharma[1], Pradeep Kumar[2]

[1]M-Tech Student, JSSATE, Noida, Dr A.P.J Abdul Kalam Technical University, India

[2]Assistant Professor, JSSATE, Noida, Dr A.P.J Abdul Kalam Technical University, India

Abstract: ***Various secret sharing schemes have been developed since Shamir [6] proposed secret sharing scheme in 1979 for the application of key distribution. A secret sharing scheme allows a dealer to protect a secret among a set of participants with each participant holding one share. A study is done on multiple secret sharing schemes based on matrix projection and secret sharing scheme for implicit data security. In secret sharing scheme based on matrix projection, secrets are organized in form of square matrix. Data pieces are said to be implicitly secure if no explicit encryption key is used and pieces in themselves do not reveal any information until at least certain number of them brought together. In this paper we analyze both types of secret sharing schemes and at last a secret scheme based on visual cryptography is also discussed.***

Keyword: Secret sharing schemes, Shamir's secret sharing scheme, Multiple secret sharing, Space efficient secret sharing

1. Introduction

A secret sharing scheme allows a dealer to protect a secret among a set of participants with each participant holding one share. The access structure of secret sharing scheme is the set of subsets of participants that are authorized to reconstruct the secret using their shares.

A secret sharing scheme is called perfect if any subset in the access structure can recover the secret while any unauthorized subset cannot gain information (in the information theoretic sense) about the secret. Shamir's threshold scheme is perfect secret sharing scheme based on Lagrange interpolating polynomial. Blakley's threshold scheme is not perfect because each participant knows the secret lies on hyper plane determined by his or her share.

(k,n) Threshold scheme – In (k,n) threshold scheme as discussed in [6], our goal is to divide data D into n pieces $D_1,D_2….D_n$ in such a way that:

1) Knowledge of any k or more D_i pieces makes D easily computable.
2) Knowledge of any k-1 or fewer D_i pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

Following are some properties of (k,n) threshold scheme:

1) The size of each piece does not exceed the size of the original data.
2) When k is kept fixed, D_i pieces can be dynamically added or deleted (e.g. when executives join or leave the company) without affecting the other D_i pieces.
3) It is easy to change the D_i pieces without changing the original data D-all we need is a new polynomial with same free term.

2. Properties of Secret Sharing Schemes

Secret sharing schemes can have many properties as discussed in [1]. There are various dynamics such as whether it is easy to change secret(s), whether it is easy to change access structure. We may need to change shares at different time rounds so that the shares from different time rounds cannot be pooled together to recover the secret(s). This is called proactive feature of secret sharing scheme and it can improve the overall security of secret sharing scheme. Another property is verifiable feature. We can verify whether the dealer or the participants have followed the sharing protocols honestly when the secret sharing scheme is verifiable.

Most of the schemes in which it is easy to add users are polynomial based since a new share is just a new point evaluated on the polynomial. So the dealer can easily compute a new share and securely give it to new user without affecting existing users.

3. Shamir's Secret Sharing Scheme

This scheme is based on polynomial interpolation. Following is the algorithm as discussed in [6]:

1) Choose a prime p, $p > \max(D,n)$,where D belongs to Z_p is the secret.
2) Choose k-1 random numbers $a_1,a_2…$, a_{k-1} ,uniformly and independently from the field Z_p.
3) Using a_i, $1 \le i \le (k-1)$ and secret D, generate polynomial f(x) of degree k-1 , $f(x) = D + a_1x + a_2x^2 +…+ a_{k-1}x^{k-1} (\text{mod } p)$.
4) Sample f(x) at n points $D_i = f(i)$,$1 \le i \le n$ such that the shares are given by(i,D_i).

Reconstruction of the secret is performed by interpolating any k points (shares) and evaluating D = f(0).

Note – By using tuples of polynomial values as D_i pieces, we can get a hierarchical scheme in which a number of pieces needed to determine D depends on their importance .For example ,if we give the company's president three values of f(x), each vice -president two values of f(x) and each executive one value of f(x), then a (3,n) threshold scheme enables checks to be signed either by any three executives ,

or by any two executives one of whom is vice – president ,or by the president alone.

4. Multiple Secret Sharing Schemes based on Matrix Projection

In multiple secret sharing schemes m secrets are shared among a group of participants on a single access structure.

4.1 Bai's Scheme

Suppose dealer wants to share a secret m×m matrix S. Then Bai's multiple secret sharing scheme (a (k,n) threshold scheme) based on matrix projection method [3], [4] can be constructed in following two phases:

Phase one: Construction of shares from Secret matrix S

1) Construct a random m×k matrix A of rank k where m > 2k-3.
2) Choose n random k×1 vectors x_i any k of which are linearly dependent.
3) Calculate n shares $v_i = Ax_i \bmod p$ for $1 \le i \le n$.
4) Compute a projection matrix $S' = (A(A'A)^{-1}A') \bmod p$.
5) Calculate a remainder matrix $R = (S-S') \bmod p$.
6) Destroy the matrix A, the vector x_is, the projection matrix S',the secret matrix S.
7) Distribute n shares v_i to n participants and make the remainder matrix R publicly known.

Phase two: Secret reconstruction

1) Collect k shares $v_{i1},v_{i2},\ldots v_{ik}$ from participants.
2) Construct a m×k matrix $B = [v_{i1},v_{i2}\ldots v_{ik}]$.
3) Calculate the projection matrix $S' = (B(B'B)^{-1}B') \bmod p$.
4) Compute the secret $S = S'+R \bmod p$.

Drawback – The secrets are organized in square matrix and hence the number of secrets must be square. So there is necessity to stuff dummy secrets into square matrix if number of secrets is not square.

4.2 Wang's Scheme

In [1] Kai Wang et al. have proposed a scheme in which there is no need to stuff dummy entries into secret matrix. In this scheme secret matrix construction uses following method:

1) Suppose m ($m \ge 2$) is an integer and we have m secret numbers to share $s_1,s_2\ldots s_m$. Each number has binary representation of N .
   That is, $0 \le s_i < 2^N$,for i=1,…,m.
2) Now choose the smallest prime p such that $p^m \ge 2^N$. since $0 \le s_i \le p^m$, we can represent s_i based on radix p with m digits. That is, for each i =1,…m we have
   $s_i = s_{i,m-1}p^{m-1}+s_{i,m-2}p^{m-2}+\ldots+s_{i,1}p+s_i,0$,
   $0 \le s_{i,j} \le p-1$, j=0,…,m-1
3) So m×m matrix S can be constructed using representations of s_i's based on radix P as follows:

$$S = \begin{pmatrix} s_{1,0} & s_{1,1} & \cdots & s_{1,m-1} \\ s_{2,0} & s_{2,1} & \cdots & s_{2,m-1} \\ . & . & & . \\ : & : & & : \\ s_{m,0} & s_{m,1} & \cdots & s_{m,m-1} \end{pmatrix}$$

Note that we have chosen each row of S to be p-radix representation of an original secret. It is equally reasonable to choose the columns of S. No matter what value m takes we are always sharing a square secret matrix of which each element is utilized. So there is no need to stuff dummy secrets in matrix.

Table1: Comparison of Bai's Scheme and Wang's Scheme

Name of scheme	Search space of each entry	Bits occupied by each share	Stuffing of dummy secrets
Bai's Scheme	2^N	$\Omega(Nm^{1/2})$	YES
Wang's Scheme	$2^{N/m}$	$\Omega(N)$	NO

In addition to above comparison, threshold value (k) in Bai's scheme is limited at scales of square root of number of secrets (m) while in Wang's scheme, k is limited at scales of number of secrets.

5. Secret Sharing for Implicit Data Security

Data pieces are said to be implicitly secure if no explicit encryption key is used and pieces in themselves do not reveal any information until a certain number of them are brought together.

5.1 Recursive Hiding of Secrets

A scheme for recursive hiding is discussed in [2]. The implementation use exclusive-OR transformation to divide the secret into shares.

The scheme is based on recursion, in which a secret (S) is divided into pieces (say s1,s2 and s3). The concatenation of pieces s1, s2 and s3 is equal to S. Shares of s1 are created using exclusive-OR. Shares of s2 are created using partial shares of s1 and shares of s3 are created using partial shares of s2. Only the final shares , that is of s3 ,are shared between parties and exclusive-OR has been used in intermediate steps. It is not a threshold scheme. Secrets that are encoded using the above method may only be of size 2^t-1 for some positive integer t ; this is due to binary structure of scheme.

5.2 Space Efficient Secret Sharing

Scheme as discussed in [2] generates shares of size $|S|/k$-1 for secret S and threshold value k. Formally a space optimal (k,n) secret sharing scheme is a secret sharing scheme that ,for secret S produces shares of size $|S|/k$. And a space efficient secret sharing scheme is a secret sharing scheme that approaches the optimal factor of $|S|/k$ in terms of share size.

The scheme is based on recursion, in which a secret is divided into k-1 pieces and then pieces are encoded one by one in such a manner that shares of already encoded pieces

are reused to create new shares for next piece. Scheme deals with following two phases:

Phase one – Dealing phase

1. Choose a prime p ,p > max (s_{max},n),where s_{max} = max(si) , $1 \le i \le (k-1)$,and $s_1,s_2,\ldots,s_{k-1}$ are the pieces of secret S.
2. Randomly and uniformly choose a number a_1 belongs to Z_p and generate polynomial $f_1(x) = a_1x+s_1$.
3. Sample $f_1(x)$ at two points $D_{s_1 1} = f_1(1)$ and $D_{s_1 2} = f_1(2)$, which represents two shares of s_1.
4. Do for $2 \le i \le (k-1)$
   a) Generate polynomial, $f_i(x) = D_{s_{i-1}i}x^i + D_{s_{i-1}(i-1)}x^{i-1} + \ldots + D_{s_{i-1}1}x + s_i$.
   b) Sample $f_i(x)$ to create new shares
      i.If i < k-1,sample at i+1 points: $D_{s_i 1} = f_i(1)$
      $D_{s_i 2} = f_i(2)$
      :
      .
      $D_{s_i (i+1)} = f_i(i+1)$.
      ii.If i =k-1,sample at n points:
      $D_1 = f_i(1)$
      $D_2 = f_i(2)$
      :
      .
      $D_n = f_i(n)$.
   c) Delete old shares: $D_{s_{i-1}1}, D_{s_{i-1}2}\ldots, D_{s_{i-1}i}$.
5. the final n shares are given by(i,Di), $1 \le i \le n$.

Phase two: Reconstruction phase

1. Interpolate any k shares (i,D_i) to generate the polynomial of degree k-1,
   $f_{k-1}(x) = D_{s_{k-2}(k-1)}x^{k-1} + D_{s_{k-2}(k-2)}x^{k-2} + \ldots + D_{s_{k-2}1}x + s_{k-1}$
   And evaluate $s_{k-1} = f_{k-1}(0)$.
2. Do for all i = k-2 down to 1
   a) Interpolate i+1 shares given by $(m+1,D_{si(m+1)})$, $0 \le m \le i$ obtained from coefficients of $f_{i+1}(x)$ to generate polynomial of degree i,
   $f_i(x) = D_{s_{i-1}i}x^i + D_{s_{i-1}(i-1)}x^{i-1} + \ldots + D_{s_{i-1}1}x + s_i$.
   b) Evaluate $s_i = f_i(0)$.

6. Secret Sharing Scheme Based on Visual Cryptography

For above schemes huge amount of time is required for distribution and reconstruction of secret. This problem can be reduced to some extent by using secret sharing scheme based on visual cryptography. . In this scheme [7] no extra computation is required for reconstruction of secret. The scheme works on the principle that the message consists of a collection of black and white pixels and each pixel is handled separately. Each original pixel appears in n modified versions (shares), one for each transparency. Each share is a collection of m black and white subpixels, which are printed in close proximity to each other so that human visual system averages their black/ white contributions. This is also a threshold scheme, just like its counterparts which are text based, where out of n shares k are required for reconstruction.

The resulting structure can be described by n×m Boolean matrix S = $[s_{ij}]$ where s_{ij} =1 iff the j^{th} subpixel in i^{th} transparency is black. When transparencies $i_1,i_2\ldots i_r$ are stacked together in a way that properly aligns the subpixel,we see a combined share whose black subpixels are represented by Boolean "or" of rows $i_1,i_2..i_r$ in S. Following are important parameters:

- m – The number of pixels in a share. This represents loss in resolution from the original picture
- r – The size of collection of two matrices
- α – The relative difference in weight between combined shares that come from white pixel and black pixel in original picture.

7. Conclusion

We have analyzed some secret sharing techniques based on matrix projection method and implicit data security. Bai's scheme and Wang's scheme based on matrix projection have been compared. Wang's scheme overcomes the drawback of stuffing dummy secrets in Bai's scheme. Wang's scheme also reduces the share size as compared to Bai's scheme. A space efficient scheme based on recursion has been also discussed. It generates shares of size $\lceil |S| / (k-1) \rceil$ for a secret S. In secret sharing scheme based on visual cryptography no reconstruction method is required as human visual system can easily reconstruct the secret.

References

[1] Kai Wang et al., "A multiple secret sharing scheme based on matrix projection", Proceedings of 33rd annual IEEE international computer software and applications conference,U.S.A,pp.400-405,2009.
[2] Abhishek Parakh and Subhash Kak, "Space efficient secret sharing for implicit data security", Information Siences(2010)©ElsevierInc.doi:10.1016/j.ins.2010.09.013.
[3] Li Bai and Xukai Zou,"A proactive secret sharing scheme in matrix projection method",International Journal of Security and Networks,vol.4,pp.201-209,2009.
[4] Li Bai,"A strong ramp secret sharing scheme using matrix projection", Proceedings 0f 2006 international symposium on a world of wireless,pp.652-656,2006.
[5] Carlo Blundo et al., "Efficient sharing of many secrets",Lecture Notes in Computer Science,vol.-665,pp.692-703,1993.
[6] A.Shamir, "How to share a secret", Communication of ACM,vol.22,pp-612-613,1979.
[7] Moni Naor and Adi Shamir , "Visual Criptography", Eurocrypt 94 ,.1994.