A Novel Linearly Bounded Secret Sharing Scheme that Supports Prioritization of Shares

Subhajyoti Barman
Department of Computer Science
Techno India University
Kolkata, India
barman.subhajyoti@gmail.com

Hiran Nandy
Department of Computer Science
Techno India University
Kolkata, India
hiran.tiucse@gmail.com

Subashis Biswas
Department of Computer Science
Netaji Subhash Engineering College
Kolkata, India
subashiscse@gmail.com

***Abstract*— Secret Sharing is a technique of decomposing a secret into number of shares in such a manner that reconstruction of the secret is only possible by a subset of shares that has at least a specific minimum size. Adi Shamir and George Blackley individually proposed the idea of Secret Sharing for the first time, but high computational complexity and noise like shares are the main issues of these schemes. However, using current state of the art schemes it is possible to perform this task in linear time without producing noise like shares.**

Providing special privilege to a subset of shares is not supported by the existing schemes. It would be a novel concept if it is possible to assign special priority to a set of shares during decomposition of secrets. Hence a linear time bounded scheme is being proposed which decomposes any secret into N number of shares among which M (M≤N) of them are specially privileged. During reconstruction of the actual secret, a subset of shares with a minimum size K (M≤K≤N) which essentially contains all the specially privileged shares or mandatory shares is required.

Keywords*— *Secret Sharing; Prioritized Shares; Linearly Time Bounded

I. INTRODUCTION

Cryptography is the process of converting secret information encrypted in such format that only the recipient would be able to understand the content of the message. The problem of this method lies in the fact that this kind of encrypted information always attracts the attackers to decode this hidden information. To resolve this problem steganography is used with cryptography, where the encrypted message gets hidden under the cover of a digital image, video, audio, etc. So these apparently innocent covers do not attract the attackers anymore and the number of attacks become less. The only problem of this method is that the total encrypted information remains embedded under a single cover. So if somehow the cover gets lost, or gets corrupted then the encrypted information also gets lost, which is not desirable. This problem can be overcome by using Secret Sharing (SS) Scheme. In this approach the actual secret gets decomposed among number of shares and each of those shares contains partial information of the secret. During reconstruction process a predefined number of shares are needed, where each individual share has the same importance. Let's consider a situation where a country wants to decompose the key of a weapon triggering system into a number of shares using SS Scheme to distribute them among supreme authorities and top level army heads of the country. Now, while triggering the weapon if the permission of all the supreme authorities of the country is mandatory along with an additional support of a specific number of army heads, then it is difficult to address this scenario using the currently available SS schemes. To address this situation a special SS scheme is required, which can associate some special privilege to a specific number of shares. This paper is focused to address this kind of privilege association constraint with the existing SS scheme. In this scheme secret are decomposed among N numbers of shares and among them it associates special privilege to M numbers of shares to make them mandatory shares. During reconstruction a predefined number (K) of shares is required that essentially contains all the mandatory shares. The relation between M, N and K can be considered as $M \leq N \leq K$. To achieve this functionality here the secret and shares are considered as a binary string and each share partially matches with the secret string. Actually these shares get generated from the secret message string by masking few bit information. Masking is done in such a way that all the missing bit information on individual shares can be recollected only when K numbers of shares get available essentially having M mandatory ones in them. All mandatory shares are indispensable because mandatory shares contain some special bit information in some specific position uniquely present in them and this is the consideration which makes them mandatory. This share generation and reconstruction is done only using simple logical ANDing and ORing operations and as all string traversal is done constant number of times so the time complexity of this proposed algorithm is asymptotically bounded by a linear polynomial.

This paper has been organized as follows. Sections II, highlights existing schemes for Secrete Sharing. Section III illustrates the proposed scheme. Section IV is for performance analysis of the proposed scheme and Finally, Section V concludes the paper with some further remarks.

II. RELATED WORK

Adi Shamir [1] and George Blackley [2] individually proposed threshold based SS schemes first time in the year 1979. Shamir's SS scheme was based on polynomial interpolation. High computational complexity ($O(n^3)$) and noisy share generation can be considered as the disadvantages of this scheme. On the other hand Blackley's proposed scheme is based on hyper plane geometry. Although this scheme performs better in terms of runtime complexity than Shamir's proposal, but still difficult computational approach and quadratic time complexity are the discouraging features of this scheme. Another SS scheme was proposed by Asmuth-Bloom [3] based on the Chinese remainder theorem. This work also

addresses the problem with quadratic time bound, but its easier computational approach provides a positive edge over Blackley's proposed scheme. Additionally, all the above mentioned schemes generate noise like shares which could attract attackers easily. To overcome this problem, Lin and Tsai [4] proposed an (N K) threshold SS scheme that uses Steganography to hide shares under meaningful cover images. Yang et. al.'s [5] work improved authentication ability of the previously mentioned scheme and prevented dishonest participants from cheating. Both these works used Shamir's polynomial interpolation approach for which the cubic time complexity issue remained unaddressed in these schemes. However, recent research works [6], [7], [8], [9] has proposed SS schemes that use simple logical operations for share generation and reconstruction in linear time. However, till now no research work has focused on providing special privileges to a specific set of shares which is addressed in this work.

III. PROPOSED WORK

A. CONCEPT

This scheme considers the secret as a binary string of bits as this proposed scheme is designed to work upon bit level. The main idea is to generate N (number of participants) numbers of shares, of which M (M≤N) numbers of shares should be mandatory in such a manner that the reconstruction of the secret is only possible when K (M≤K≤N) numbers of shares come together must having all M mandatory shares. Theoretically, M≤K≤N≥2, but for betterment of safety one should consider 2≤M≤K≥3≤N.

So the actual aim is to generate shares by removing bit information from the actual secret in such a manner that all the bit information can only be recovered by ORing K numbers of shares that poses all M mandatory shares. So for all shares, bit information of first ${}^{N}C_{K-1}$ bits of consecutive ${}^{N}C_{K-1}$+M bits is reset for exact K-1 numbers of shares and those are made present in exactly (N-K+1) numbers of shares and the missing bit pattern should remain unique for each bit position of the secret message. For next M bits each bit of the secret message should only be present in one of the M mandatory shares and is masked from all other mandatory and non-mandatory shares provided each mandatory copy should contain only one such bit information. The same thing is repeated for all the successive bit positions. To implement this idea it is required to form N separate binary strings of length ${}^{N}C_{K-1}$+M where in the first ${}^{N}C_{K-1}$ bit positions, each bit position of N different strings should contain a unique combination of 0s and 1s such that the total number of 0s for that position is K-1. Apart from this for the last M bits, for each bit position only one string should contain only a single 1 and rest of the strings should contain 0 for that bit position. Different shares can be generated by repeatedly ORing each of those strings with the actual binary secret message. These strings are used to strip information from the actual binary secret string, so they are termed as 'Masks'. Shares, which are generated by masks having a single 1 in any of the last M bit positions act as a mandatory share as that bit information of the secret is uniquely present in them. All the other shares are termed as non-mandatory shares.

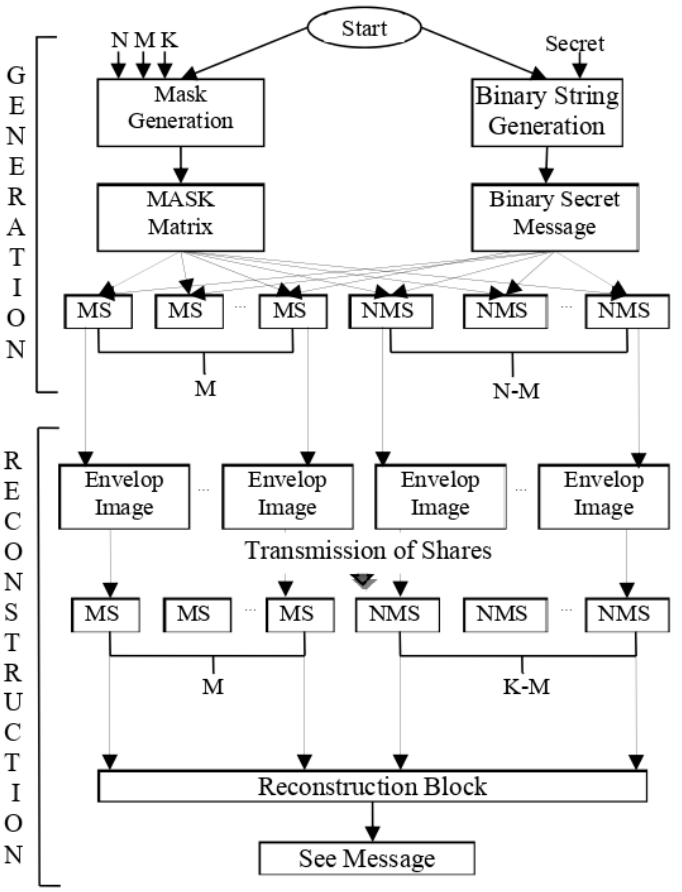


Figure 1: Block Diagram of the Proposed SS Scheme

B. ALGORITHM

The detailed implementation of the concept is being described here.

- Input : **N**=Number of total participants
  M=Number of mandatory shares
  K=Minimum number of shares essential for reconstruction of the secret.
  Sec=Character string of the secret

1) Generation Rule

- Step-1: First the secret , is converted into a binary string of bits, say the length of this string is L.
- Step-2 : To generate N numbers of different masks a matrix of dimension $({}^{N}C_{K-1}+M)\times N$ is formed of which first ${}^{N}C_{K-1}$ numbers of columns are filled up with all the different combinations of (K-1) numbers of 0s and (N-K+1) numbers of 1s. Now to add special privilege for the first M number of shares, last M numbers of columns are filled up according to the following rules:

  Mask[i][j]=1 if $j > {}^{N}C_{K-1}$ and $i=j - {}^{N}C_{K-1}$
  Mask[i][j]=0 if $j > {}^{N}C_{K-1}$ and $i!=j - {}^{N}C_{K-1}$

- Step-3: To make the length of each mask equal to the length of the binary secret, *i.e.* L, each mask is repeated (L/(${}^{N}C_{K-1}$ + M)) times and in case of the last repetition only (L mod (${}^{N}C_{K-1}$ + M)) bits are needed to be taken. These are the actual working masks.
- Step-4: Each mask is logically ANDed with the binary string of the secret and in this way shares are generated.
- Step-5: Each share gets hidden under a cover image by using simple logical operation and transmitted to one of the N participants. (Detailed procedure of this information hiding technique is discussed in the Information Hiding Protocol section.)

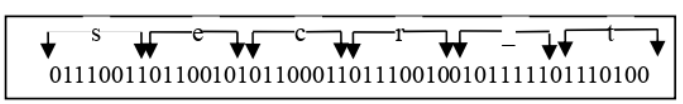
*2) **Reconstruction Rule***

- Step-6 : After receiving a cover image as a share the receiver restores the original share bits from the cover image by performing simple logical operation.(Detailed procedure is discussed in the Cover Image Transmitting Protocol section.)
- Step-7: When K numbers of extracted shares, must including all the mandatory shares come together, then just by logically ORing those shares the secret is reconstructed. (Detailed procedure is discussed in the Information extraction Protocol section.)

For better understanding of this algorithm a small example is taken which considers the string "secr_t" as the secret message and also considers N=7, M=3 and K=5.

*1) **Share Generation Phase***

- Step-1 : The binary string of the secret message is –



- Step-2 : The arrangement of first 35 columns of the mask matrix, each having 4 numbers of 0s and 3 numbers of 1s in the matrix form is as following

00000000000000000000011111111111111111
00000000001111111111000000000011111010
00001111110000001111000000111100001001
01110001110001110001000111000100010000
10110110010110010010011001001000100000
11011010101010100100101010010001000000
11101101001101001000110100100010000000

Now 3 additional column vectors are added for generating the mandatory masks. The final mask matrix looks like as follows:

00000000000000000000011111111111111100
00000000001111111111000000000011111010
00001111110000001111000000111100001001
01110001110001110001000111000100010000
10110110010110010010011001001000100000
11011010101010100100101010010001000000
11101101001101001000110100100010000000

- Step-3 : In this step each mask is repeated for (48/(35+3))=1 time and in the 2nd repetition bit information are kept till the 10th bit position. Thus all the masks are increased to length 48 bits. The working masks become as follows:

1st Mandatory Mask:
000000000000000000001111111111111111000000000000
2nd Mandatory Mask:
000000000011111111110000000000111110100000000000
3rd Mandatory Mask:
000011111100000011110000001111000010010000111111
1st Non-Mandatory Mask:
011100011100011100010001110001000100000111000111
2nd Non-Mandatory Mask:
101101100101100100100110010010000100000101101100 1
3rd Non-Mandatory Mask:
110110101010101001001010100100010000001101101010
4th Non-Mandatory Mask:
111011010011010010001101001000100000001110110100

- Step-4 : Shares are generated by logically ANDing the masks with the binary string of the original secret message as follows:

1st Mandatory Share:
000000000000000000000110111001001010000000000
2nd Mandatory Share:
000000000010010101100000000000100100100000000000
3rd Mandatory Share:
000000110100000001100000001100000000010000110100
1st Non-Mandatory Share:
011100010100010100000001010000000100000101000100
2nd Non-Mandatory Share:
001100100100000100100010010000000000001001010000
3rd Non-Mandatory Share:
010100100010000001000010000100000000001101100000
4th Non-Mandatory Share:
011000010010010000000010010001000000001100110100

that are only present in these mandatory shares.

- Step-5 : Now each share is hidden under an apparently innocent cover image and transmitted to one of the 7 participants.

2) Share Reconstruction Processes

- Step-6: After receiving a cover image the receiver extracts the share bit information from that image in the way mentioned previously.

- Step-7: It can easily be observed that ORing at least 5 shares that essentially includes all the mandatory shares makes it possible to reconstruct the binary string of the original secret message. Absence of even one mandatory share makes it impossible to losslessly reconstruct the secret information once again. Let us consider 3 mandatory shares along with 3rd and 4th non-mandatory shares for reconstruction. It is shown here that the result of their bitwise logical OR operation produces the actual secret once again.

```
00000000000000000000011011100100101000000000000
00000000001001010110000000000100100100000000000
00000011010000000110000000110000000001000011010 0
01010010001000000100001000010000000000011011000 00
01100001001001000000000100100010000000110011010 0
Result:
01110011011001010110001101110010010111101110100
        s       e       c       r       _       t
```

C. *COVER IMAGE MANIPULATION TECHNIQUE*

This part of the paper presents the information embedding/extraction techniques within a cover image using steganographic approach. This paragraph is comprised with two algorithms of two protocols, namely i) Information Hiding Protocol and ii) Information Extraction Protocol.

- Input: N shares and N cover images(32 bit bitmap).
- Output: N envelop images.
- Information Hiding Protocol: For each share, one envelop image is selected. Consecutive bytes of a share are embedded in consecutive pixels of the image. Each pixel is comprised of four bytes for ARGB values. 2 LSB bits from each of these ARGB components is then replaced by two bits of that share byte by using simple logical operation.

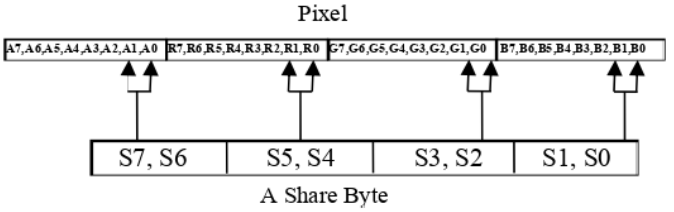
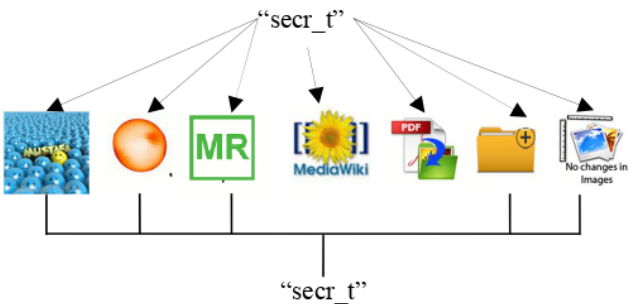


Figure 2: Information Embedding Technique in Pixel

This generates the first share image. This is repeated to generate N share images. As two bits are embedded in each colour component of a pixel, so maximum deviation in colour component is 3 which is unrecognizable to human eyes. So these shares would not catch the attention of the attackers.

- Information Extraction Protocol:
- Input: M mandatory envelops, K-M non-mandatory envelops.
- Output: The original secret message.

During extraction after receiving a cover image the receiver extracts the bit information from the ARGB colour components of the pixel by performing simple logical operations. When K numbers of extracted share bits come together, containing off course all the mandatory share copies, then by simply ORing those share bits the original secret is reconstructed.



IV. COMPLEXITY ANALYSIS

It is assumed here that the size of the secret is n. This is a bit oriented protocol as bits are the simplest unit to work upon. Now the conversion of a character string to the binary string is done following a pre specified format. So after this process of converting the length of the secret string gets multiplied by some constant factor(say,c,here c = 8).So,the final size of the string becomes cn. Constant number of mask strings of size cn are ANDed with the binary secret string. This bit wise AND operation requires a linear traversal of the whole string which costs linear time. Reconstruction of the share in this scheme is done by logical OR operation. Embedding bit information in a pixel of the cover image in the generation phase and extracting those bit information from that image in the reconstruction phase also need a linear traversal.

$$T(n)=\emptyset_1(n)+\emptyset_2(n)=O(n)$$

i.e. the total process of share generation, hiding of shares under number of cover images, extraction of shares from those cover images and reconstruction of shares in this scheme is linearly upper bounded.

V. CONCLUSION

This work has presented a (N, K, M) threshold Secret Sharing Scheme that associates the concept of specially privileged shares with the currently available SS schemes. While achieving this constrain it does not introduce additional computational complexity. Alike most efficient existing SS scheme, it can also perform share generation and reconstruction in linear time. To the best of our knowledge, this is the first work on prioritization of shares that has linear time complexity. In

future the work would focus on predicting the corruptness of the cover images of the mandatory shares to reduce the probability of losing the secret because of damage of the covers of the mandatory ones.

ACKNOWLEDGMENT

The authors of this paper acknowledge the constant support of the department of Computer Science and Technology, Techno India University, for providing them the platform for planning and developing the work in their department laboratories.

REFERENCES

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

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

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

[4] C.C. Lin and W.H. Tsai, "Secret image sharing with steganography and authentication", Journal of Systems and software, vol. 73, no. 3, pp. 405-414, 2004.

[5] C.N. Yang, T.S. Chen, K.H. Yu, and C.C. Wang, "Improvements of image sharing with steganography and authentication", Journal of Systems and Software, vol. 80, no. 7, pp. 1070-1076, 2007.

[6] S. Guha, S. Das, S. Sarkar and A.Chaudhuri "Visual Cryptography using pixel filtering technique for continuous tone 24-bit image" Proc of National Seminar on Role of ICT in improving Quality of life Page 61-72, 2010.

[7] Prabir Kr. Naskar, Ayan Chaudhuri, Ayan Chaudhuri, "Image Secret Sharing Scheme Using a Novel Secret Sharing Technique with Steganography" IEEE CASCOM Post Graduate Student Paper Conference 2010 Jadavpur University, Kolkata, India. Nov. 27, 2010; pp 62-65.

[8] P. K. Naskar, A. Chaudhuri, D. Basu and A. Chaudhuri, "A Novel Image Secret Sharing Scheme," Emerging Applications of Information Technology (EAIT), 2011 Second International Conference on, Kolkata, 2011, pp. 177-180.

[9] Y. x. Liu, Z. x. Wang and W. y. Yan, "Linear (k, n) Secret Sharing Scheme with Cheating Detection," Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, Liverpool, 2015, pp. 1942-1947.