IJCTA, 10(8), 2017, pp. 733-738 ISSN: 0974-5572
© International Science Press

Multi Secret Image Sharing Scheme using Boolean Arithmetic

Shilpa B. Ovhal* and Reena Kharat**

ABSTRACT

Sharing of personal information and private data through the medium of internet has grown exponentially in recent years. Therefore,it becomes very important to secure our data from unauthorized access in this digitized world. There are many cryptographic techniques which were used for providing security to the data, but these methods need encryption and decryption techniques, which involves high computation cost. Many secret sharing techniques were proposed for providing security to shared information. A High computational complexity was encountered in most of the previous schemes making it difficult to use for information sharing.In this paper, methods of cryptographic techniques are discussed for encrypting and decrypting secrets which provide security to the images over the network.In recent work, n secret images are shared among n or n+ 1 shared image, which has a problem as one can recover partial secret information from n-1 or fewer shared images. In this paper, the proposed method uses Boolean arithmetic operation to recover from this problem.

Keywords: Secret Sharing, Image Sharing, Partial Secret, Cryptography, Computational Complexity.

1. INTRODUCTION

Use of internet is increasing widely, therfore it becomes difficult & unsafe to transfer information over internet in this digitized world. Information is always begging for the security and reliable transmission. Many methods were proposed to secure this digitized data which includes data hiding, cryptography andsecret sharing.

Image secret sharing is the technique of distribution of secret image among the participants or group members within agroup, each of the participants holding only a share of the secretand individual shares are of no use in order to reconstruct the original secret. When a definite number of shares are combined togetherthen and only then the original secret can be reconstructed and individual shares do not indicate the original secret.This process of secret sharing scheme includes the security of data storage and computational cost. Computations are arithmetic and logical which are used for encryption and decryption. Risk of data corruption and data loss can be minimized by splitting data into number of pieces and keeping the pieces across different locations.

Transferring data has become an essential part of digital communication. To communicate securely there areso many internet applications are used. Hence, the information security against unauthorized access has become a mainobjective. This objective has led to advances in various techniques for data hiding. Well known techniques are Steganography, Watermarking and Cryptography which are widely used to hide the original message. To embed message within another object, steganography is used to reconstruct original secret known as a cover work by tweaking its properties. Another well known technique for inserting information into an imageknown as digital watermarking. Cryptography sender converts plaintext to cipher text by using encryption key and other side receiver decrypts cipher text to plaintext.

* Department of Computer Engineering Pimpri Chinchwad College of Engineering Pune-44, *Email: shilpa.ovhal@gmail.com*

** Department of Computer Engineering Pimpri Chinchwad College of Engineering Pune-44, *.Email: reenakharat@yahoo.com*

2. LITERATURE SURVEY

The paper [1] proposes threshold access structure for multi-secret sharing. It uses a two-level encoding for sharegeneration from multiple secret images. In the first level ofencoding secure Boolean based operations are used. The secondlevel of encoding uses Chinese remainder theorem and LagrangeInterpolation. It is mainly useful for secure encryption of multiplesecret images with two levels of encoding. It has the ability torecover secret images without any distortion. Another advantageis to share n secret images among k shares.

In the paper [2], Christian L. F. Corniaux, Hossein Ghodosi proposed that In a *k*-threshold secret sharing scheme, a dealer whoholds a secret *s* distributes parts of this secret (the *shares*) to*n* players; If *k* or more of these players pool their shares, theyare able to determine *s*, but if less than *k* of them pool theirshares, they cannot infer any information on *s*. In 1979, Shamirintroduced such a scheme, based on polynomial interpolation ina finite field. This scheme is widely used in other cryptographicprotocols, because it is simple, elegant and above all informationtheoreticallysecure. There are a few proofs of the scheme'ssecurity, but to our knowledge, none of them is entirely basedon the information-theoretical entropy function introduced byShannon in 1948. We propose such a demonstration.

In the paper [3], Maroti Deshmukh, Neeta Nain and Mushtaq Ahmed proposed method which focuses on Xor operations and modular arithmetic for generating shares and revealing secrets. They overcome the inaccuracy in Chen et al. [9] scheme and propose an (*n*, *n*)-MSIS scheme.Proposed schemes do not disclose partial secret informationfrom (*n*"1) or fewer shared images.

In the paper [4],Ali A.Yassin, Abdullah A. Hussain, Keyan Abdul-Aziz Mutlaqproposed a scheme which focuses on two-factor authentication that used image partial encryption to overcome above aforementioned issues and drawbacks of authentication schemes. Additionally, we use a fast partial image encryption scheme using Canny's edge detection with symmetric encryption is done as a second factor. In this scheme, the edge pixels of image are encrypted using the stream cipher as it holds most of the image's data and then applied this way to authenticate valid users.

In the paper [5], Kajal Chachapara, Sunny Bhadlawala proposed that framework allow generating a key for particular users with particular permissions. Cloud user can generate keys for different users with different permissions to access their files. This framework uses cryptography algorithms like AES and RSA. AES is most secure algorithm in cryptography. Once key is generated; user (user who have generated a key for their own files) can provide that key to decided user (user for whom key is generated). So when decided user will try to access files on cloud with that key, permission decided by owner will be given to that user. This is partial access to user and more secure then providing password to user. Cloud service providers can also add concept of defining files also like cloud user can generate key for particular file, particular user and particular permission. Those keys then can be provided to different users.

3. SHAMIR'S SECRET SHARING

Secret sharing is the technique of distribution of secrets among the participants or group members within a group, each of the participants holds only a share of the secret and individual shares are of no use in order to reconstruct the original secret. The original secret can be reconstructed only when a definite number of shares are combined together and individual shares do not indicate the original secret.

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret .Counting on all participants to combine the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

4. TZUNG-HER-CHEN’S METHOD

Chen and Wu et proposed an efficient (n, n + 1)-MSIS scheme based on m Boolean XOR operations. In this scheme n secret images areused to generate the n + 1 shares. For decryption all n + 1shared images are required to reveal the n secret images.In this scheme the capacity of sharing multiple secretimages are increased. It uses only XOR calculations for twomeaningful images so, it can not produce randomizedshared images. The encryption algorithm of the Tzung-Her-Chen’s (n, n)-MSIS scheme is given in Algorithm 1.

Algorithm 1: *Chen’s Method*. [3] Sharing Procedure.

```
Input: $n$ secret images $\{I_1, I_2,\ldots,, I_n\}$
Output: $n + 1$ shared images $\{S_1, S_2\ldots S_{n+1}\}$.
1. Generate random matrix T(Temp)
   $T = random(0, 255)$
2. Compute $n - 1$ random matrices $\{B_1, B_2\ldots 0B_{n-1}\}$
   using XOR operation
   $B_i = I_i \oplus T$ where $\{i = 1, 2, \ldots\ldots\ldots, n - 1\}$
3. Generate shared images
   $S_1 = T$
   $S_2 = B_1$
   $S_i = B_i \oplus B_{i-1}$, where $\{i = 3, 4, \ldots\ldots\ldots, n\}$
   $S_{n+1} = I_1 \oplus B_{n-1}$
```

The recovery procedure is reverse of the sharing procedure.

Input to the recovery procedure is n + 1 shares and

outputs are n recovered images. For decryption all n + 1

shared images are required to reveal the n secret images. Therecovery procedure of the Tzung-Her-Chen’s (n, n)-MSIS scheme is given in Algorithm 2.

Algorithm 2 ::*Chen’s Method*.[3] Recovery Procedure.

```
Input: $n + 1$ shared images $\{S1, S2 \ldots Sn+1\}$.
Output: $n$ Recovered images $\{R_1, R_2\ldots R_n\}$.
1. Compute first recovered image using XOR operation
   $R_1 = S_1 \oplus S_2 \oplus S_3 \ldots \oplus S_n$
2. Compute $n - 1$ random matrices $\{B_1, B_2\ldots B_{n-1}\}$
   using XOR operation
   $B_1 = S_1$
   $B_k = S_k \oplus B_{k-1}$ where $\{k = 2, 3, \ldots\ldots\ldots, n - 1\}$
3. Recover remaining secret images $\{R_2, R_{3,}\ldots\ldots\ldots, R_n\}$
   $R_k = B_k \oplus S_1$, where $\{k = 2, 3, \ldots\ldots\ldots, n\}$.
```

5. PROPOSED METHOD

In proposed method we used Boolean Addition, subtraction and reverse bit function to encrypt and decrypt process.

Share Generation

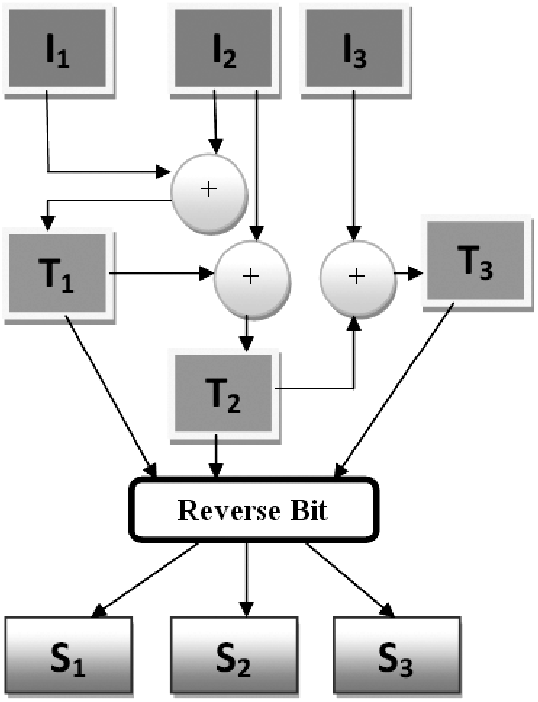

Figure 1: Share Generation by using Boolean addition and Reverse Bit function.

In the process of generating shares we have used simple Boolean addition and reverse bit function. There are n number of images i.e. {I_1, I_2,….., In}, Where first we generate temporary shares with the help of boolean addition. In the next level of encryption phase we have used reverse bit function to create shares.

Proposed algorithm for Share Generation

Input: *n* secret images {$I_1, I_2, \ldots, I_n$}

Output: *n* shared images {$S_1, S_2 \ldots S_n$}.

```
1. Generate Temporary share
   $T_1 = I_1 + I_2$
   $T_2 = I_2 + T_1$
   .
   .
   $T_n = I_n + T(_{n-1})$
2. Generate Shares using Reverse Bit Function.
   $S_1 = RB(T_1)$
   $S_2 = RB(T_2)$
   .
   .
   $S_n = RB(T_n)$
```

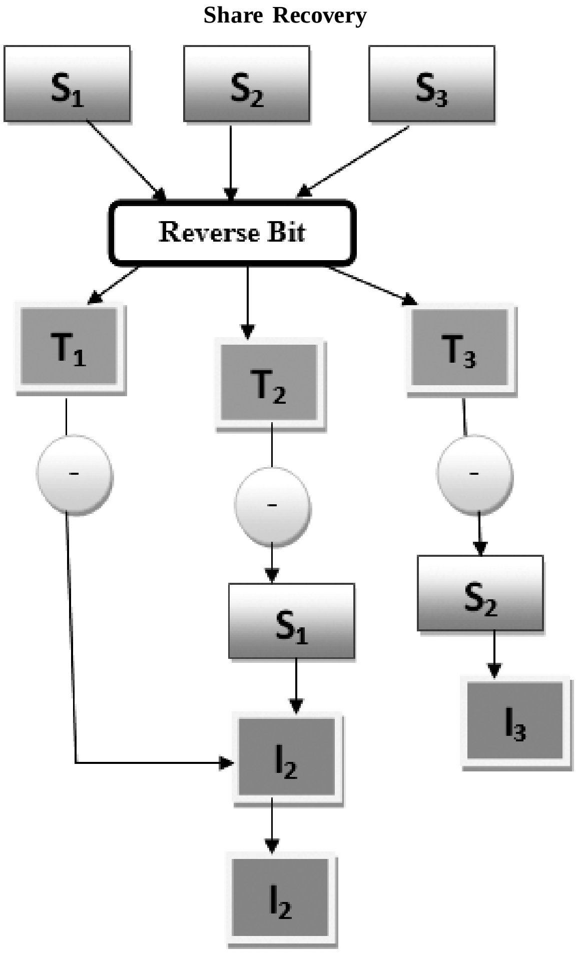

Figure 2: Share Recovery by using Boolean subtraction and Reverse Bit function.

In the process of recovering shares we have used simple Boolean subtraction and reverse bit function. There are n number of shares i.e. {S_1, S_2, ….., S_n}, Where first we recover temporary shares with the help of reverse bit function from given shares. In the next level of decryption phase we have used Boolean subtraction to reveal original images.

Proposed algorithm for Share Recovery

```
Input: n secret shares {$S_1, S_2,\ldots., S_n$}
Output: n recovered images {$I_1, I_2\ldots I_n$}.
1. Generate Temporary share
   $T_1 = RB(S_1)$
   $T_2 = \mathrm{RB}(S_2)$
   .
   .
   $T_n = RB(S_n)$
2. Generate Shares using Reverse Bit Function.
   $I_n = T_n\text{-}S(_{n-1})$
   $I_2 = T_2\text{-}S_1$
   .
   .
   $I_1 = T_1\text{-}I_2$
```

6. MATHEMATICAL ANALYSIS

I_1, I_2, I_3 these are original images having the values 00000100, 000000011, 00000111 sequentially.

Now by using Share generation algorithm shares are created. Temporary share $T_1 = I_1 + I_2 = 00000111$,

$$T_2 = I_2 + T_1 = 00001010,$$
$$T_3 = I_3 + T_2 = 00010001$$

Now, By using Reverse Bit function generated shares,

$$S_1 = RB(T_1) = 11100000$$
$$S_2 = RB(T_2) = 01010000$$

$S_3 = RB(T_3) = 10001000$ these 3 shares are created now, we have these 3 shares at the receiver's side.

Share recovery by using algorithm 2, exactly reverse procedure of share generaton.

$$T_1 = RB(S_1) = 00000111$$
$$T_2 = RB(s_2) = 00001010$$
$$T_3 = RB(S_3) = 00010001$$

From the shares we obtained temporary shares, by using Boolean subtraction we obtained recovered images from the given share.

$$I_3 = T_3\text{-}T_2 = 00000111$$
$$I_2 = T_2\text{-}T_1 = 00000011$$
$$I_1 = T_1\text{-}I_2 = 00000100$$

We obtained original images from the given shares at the receiver side.

7. CONCLUSION

In this paper, we have attempted to overcome the shortcomings in [3], and have proposed a (*n*, *n*)-Secret Sharing methodusing Boolean arithmetic. To increasethe randomness of shares we used reverse bit function. Theshared images of proposed schemes are random and havesame dimensions as those of secret images, which is more efficient.As compared to Xor operation,(*n*, *n*)-MSIS scheme is more easy and efficient for increasing randomness of shares.The use of only XORoperation on secret imagesis not agood idea because itreveals some amount of information.

REFERENCES

[1] L. Siva Reddy, Munaga V. N. K. Prasad "Multi-Secret Sharing Threshold Access Structure", 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI).

[2] Christian L.F. corniaux, hossein ghodosi, "An Entropy-based Deme onstration of the Security of Shamir's Secret Sharing Scheme", IEEE, PP. 46-48, 2014.

[3] Maroti Deshmukh, NEETA NAIN, Mushtaq Ahmed "An (*n, n*)-Multi Secret Image Sharing Scheme using Boolean XOR and Modular Arithmetic" 2016 IEEE 30th International Conference on Advanced Information Networking and Applications.

[4] Guo, Teng, Feng Liu, and ChuanKun Wu. "k out of k extended visual cryptography scheme by random grids." SignalProcessing 94 (2014): 90-101.

[5] Maroti Deshmukh, Munaga V.N.K. Prasad. "ComparativeStudy of Visual Secret Sharing Schemes to Protect IrisImage." International Conference on Image and Signal Processing (ICISP), (2014): 91-98.

[6] Chen, Tzung-Her, and Chang-Sian Wu. "Efficient multisecret image sharing based on Boolean operations." Signal Processing 91.1 (2011): 90-97.

[7] Chen, Chien-Chang, and Wei-Jie Wu. "A secure Booleanbasedmulti-secret image sharing scheme." Journal of Systemsand Software 92 (2014): 107-114.