Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

MULTI-IMAGE SECRET SHARING BASED ON POB BASED SECRET SHARING SCHEME

Ann Jisna James[1] Prof.Reena Kharat [2]

Department of Computer Engineering P.C.C.O.E,Pune
Department of Computer Engineering P.C.C.O.E,Pune

Abstract- *Secret sharing refers to the process of splitting a secret such that n number of shares are formed out of it ,this ensures that the recovery of secret is only possible if qualified subset is present.Such encryption make the data secure with minimal amount of attacks as a single share can not reveal any information. The earliest successful attempt in this arena was made by Adi Shamir and George Blakely who implemented this method successfully for threshold scheme ,since then a steady advancement has been observed ,the latest schemes are implementable on multimedia frameworks for generating shares and ensuring privacy of the data.This paper attempts a survey on different schemes and their advancement.It focuses on the POB number system based secret sharing scheme introduced by A. Sreekumar and Sundar,which follows an n out of n scheme in which n number of shares are generated from a secret and the values in these shares are converted to respective POB values.*

Keywords- *Secret sharing,Permutation Ordered Binary (POB);*

I. INTRODUCTION

Secret sharing relates with the idea of dividing and sharing a secret among a group of n participating individuals, or parties,so that only pre-designated set of individuals are able to reconstruct the secret by collectively cumulating their portions of secret. Shamir was the first to develop a threshold based secret sharing scheme around the year 1979. In proposed scheme, a secret is partitioned into n set of shares such that any k out of n shares (k n) are needed to remodel the original secret , but any combination of (k 1) shares do display the original secret or a part of it . Both Shamir's and Blakely's proposals are (t, n) threshold secret sharing schemes, however Shamir's theme is more practical as it offers excellent privacy and correctness,along with flexible. Correctness implicates that a secret s is unambiguously determined by any k shares from the shares s1,...,sn, whereas privacy cares with having access to any k1 shares from s1,...,sn however it fails to deliver any insight into the shared info or secret. s ;i.e.,the likelihood distribution of k1 shares is free of s.Extended capabilities were later enclosed in to the present threshold theme by Ito,Saito, and Nishizeki . A generalized secret sharing theme was place forth , wherever any approved set of participants had the aptitude to recover the shared secret by pooling their shares. The access structure of a secret sharing theme usually segregates the set of all subsets of participants into sanctioned sets, who are unable to instaurate the secret.Further most of the schemes consider the monotone property. This means that if a cluster can recover the secret so can a the superset of the cluster. In the case of an unauthorized group, if the cluster cannot recover the secret a smaller subset of the cluster would also fail to recover the secret.Benaloh and Leichter proved that if an access structure can be described by a minuscule monotone formula then it has an efficient perfect secret-sharing scheme.Vector space schemes introduced by Brickell which provides secret sharing schemes for a wide family of access structures , being a very efficient algorithm but required further subsistence of function (φ) .B. Chor and E. Kushilevitz put forth secret sharing systems on illimitable domain with finite access structures.[9]Now of recent secret sharing theme has been projected by Sreekumar predicated on the POB mathematical notation.According to this theme, a secret often divided into n shares specified the values in these quotas correspond to the POB-values.For initiation of the key, the POB-values within the parts are reverted back to the decimal number system and so these values are cumulated to reconstruct the pristine secret.

A. Permutation Ordered Binary (POB) Number System

Permutation Ordered Binary (POB) Number System with two non-negative integral parameters, n and r, where n r. The system is denoted by POB(n,r). In this number system, all .integers are presented in the range 0,....,rn-1, as a binary string, say B = bn-1,bn-2,....,b0, of length n, and having precisely r 1s.Each digit of this number, say, bj is associated with its position value, given by

$$\mathbf{b}j * (\mathbf{p}_j^j) \qquad (1)$$

where

$$\mathbf{p}j = \sum_{i=0}^{j} \mathbf{b}_j \qquad (2)$$

and the value represented by the POB-number B, denoted by V (B), will be the sum of position values of all of its digits.

$$V(B) = \sum_{j=0}^{n-1} \mathbf{b}j(\overset{j}{\mathbf{p}}_j) \qquad (3)$$

B Multi-Secret Image Sharing

A large variety of Visual cryptography schemes are present,on a higher level they can be partitioned into :(k,n) VCS and(n,n) VCS. In (k,n) secret sharing scheme.In case of the first type of scheme, secret image is split into n shares and at least k shares are required to construct the original image,less than k shares are deficient to decrypt the secret image.In (n,n) secret-sharing scheme, the secret image is encoded into n shares and the shares will not reveal the secret until all the n shares are present. However VCS has the a drawback of poor visual quality of rebuild image due to utilizing OR operation which reduces the contrasting and clarity . In visual cryptography, the concept of sharing of multiple secrets at a time is a novel and useful application. Therefore, the concept of (n,n)-MSIS scheme is present in which n secret images are encrypted into n number of shares which individually has disclose no legitimate/useful information about the n secret images. For recuperation of secret images,all n shares are required of all the images initially present are required.Currently, MSIS scheme have several type of applications in different arenas such as missile launching codes, access control, opening safety deposit boxes, e-voting or e-auction etc.[7]

II. Review of Literature

Most secret sharing schemes are based on cryptography which involves the encryption and decryption processes hence leading to high computation costs. Secret sharing schemes hide the secret image into several share images and distribute these share images . Till now many schemes have been proposed but most of the schemes face a shortcoming in the size of the shares obtained and further in case of the decreased quality of reconstructed image in this case POB offers a prominent solution. The novice method of POB scheme for secret sharing has been introduced by author A. Sreekumar and Dr. S. Babu Sundar.The introduced algorithm for the secret sharing scheme is applicable for (2,2) as well as (n,n).The image is split into shares and secret is then converted into a value corresponding to the POB number system.[2] The authors Deepika M P and A. Sreekumar has proposed a methodology in which secret sharing scheme using POB number system and CRT. . 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. along with Chinese Remainder theorem.[3]

The author proposes a scheme for a secure method for processing the encrypted images without any compromise to its privacy. The scheme follows an approach in which media is distributed into number of shares predicated on both Shamir's secret sharing and permutation ordered binary system. The scheme impeccably reconstructs back the pristine image at the end processing the confidential keys. These shares can be further processed over the cloud data centers and rebuilt using the Langrange's interpolation to compose the end result.Various image operations such edge sharpening, contrast improvement,etc has been applied on these shares. The processed image can be obtained from these processed shares only by the authentic entity possessing the secret keys.Also after processing the images obtained are equivalent to the images that would be obtained if the were performed on the original images .[4]

Image encryption scheme based on a POB Number System has been proposed.It splits the image details in thoroughly random shares, which is then stored at the cloud data centers. Further,the proposed theme confirms the shares at the pixel level. If any meddling is sensed at the cloud servers,the scheme can correctly identify the altered pixels via authentication bits and delimits the particular affected area. The tampered portion is additionally showcased back in the reassembled image that is obtained by the authentic end.[5]

An extension to the image encryption system has been proposed in which video context is taken and tamper detection based on POB number system has been implemented. In the system, a secret is divided into multiple POB shares. The concept works on secret sharing scheme for encryption of video frames and then, validation bits are fused in these shares for detection of interference. Each frame in the secret shares is verified at the pixel level via location, neighborhood and temporal values that are attached to each pixel in the shares.The content is then stored on cloud data centers where an invader may fiddle with one or more shares. In case of disturbance or change in shares, the proposed scheme detects them.These forged shares are displayed in the end result i.e the rebuilt video[6]

III. System Architecture/System Overview

The proposed system aims at solving the problem of sharing multi-images at a time securely.The system takes in the images and applies POB scheme on which ,which gets applied at pixel level and each image is converted to the corresponding POB value.Now the images obtained are further taken and each image is XOR-ed with its predecessor (the first image is taken as such due to the absence of predecessor).Again the reverse bits are taken before producing the final output of the system.

IV. SYSTEM ANALYSIS

A. Share Generation

POB share are generated and its value is extracted from the table and again xoring between image with its predecessor is followed. The proposed system follows the following algorithm:

- Take image from the user
- Split it into POB shares
- Extract value from the POB table as per the permutation obtained.S1(i, j)=POBv(A)
- Again take all the shares of the multiple images,xor each share with its predecessor except the first share which lacks a predecessor.Ti =Si ⊕Ti − 1, where i= 2,3,...,n
- Once the xored result is obtained take reverse bit of each to obtain final result. Si = Reverse Bits(Ti), where i= 1,2, .., n
- Obtain the final shares .

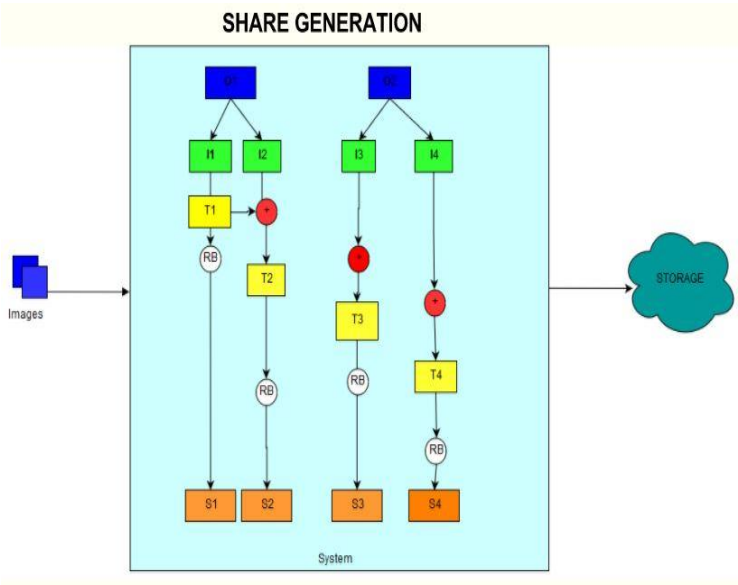

Fig. 1. Block Diagram for share generation

B. Image Re-Generation The above steps are followed in reverse order i.e from last to first to obtain the initial secret image.

- Take shares
- Ti = Reverse Bits(Si), where i= 1,2, ..., n.
- Once POB shares are obtained.Check it with the table to obtain the actual shares by using POB values.
- Obtain the two shares of all the images from above and combine them.
- Obtain original image.

V. MATHEMATICAL MODEL

The mathematical model for proposed architecture is as follows. Let S be a system. S=s,e,I,O,P Where,

s = Start of the program 1.

1. .Upload the image files.
2. Create 2 shares of each image using POB scheme.
3. Obtain the result of POB by extracting the value from the permutation table.
4. Take these outputs and xor each with its predecessor.
5. Take reverse bit for final output

e = End of the program

F(x) =F(I–> O|P)

F(x) is a function, mapping set of input images I to set of output sharesO, given a set of operations P.

The definitions of sets are as follows:

I= Input of the program (Image file)

O= Output of the program (Shares) S =s1, s2, ..., sn

Where s1 ...sn are the operations followed in a linear fashion.

VI. CONCLUSION

To facilitate secure exchange of images, an endeavor has been evoked in which the media information is distributed securely into multiple shares predicated on POB number system predicated secret sharing. The security is fortified for multiple images by further increasing the dependency of the images.The proposed scheme is effective, as POB representation is unique also the interdependence of images ensure that all the shares of the image set are required to recover even a single image.Intruder would further would not be able to recover the images even in the adverse case in which he may have all the shares since in POB the number of 1's need to be know to recover the value from the POB table.

VII. APPLICATION

The main thrust area of the project ranges from medical domain to financial and highly secure defence information.Use of this system would be also be helpful not only in-case of images but also can be utilized to provide security to video formats.

REFERENCES

[1] Chapter 8 "Permutation Ordered Binary Number System",shodhganga.
[2] A. Sreekumar and Dr. S. Babu Sundar "An Efficient Secret Sharing Scheme for n out of n scheme using POB-number system".
[3] Binu. V. P and A. Sreekumar"Generalized Secret Sharing using Permutation Ordered Binary System",Cornwell library 2014 .
[4] Deepika.M.P , A. Sreekumar"A Novel Secret Sharing Scheme Using POB Number System and CRT"International Journal of Applied Engineering Research 2016 .
[5] Priyanka Singh,Balasubramanian Raman,Nishant Agarwal,Pradeep K. Atrey"Secure Cloud-Based Image Tampering Detection and Localization Using POB Number System"ACM Transactions on Multimedia Computing, Communications, and Applications,2017.
[6] Priyanka Singh,Balasubramanian Raman,Nishant Agarwal,Pradeep K. Atrey"Towards Encrypted Video Tampering Detection and Localization Based on POB Number System Over Cloud"IEEE Transactions on Circuits and Systems for Video Technology, 2017
[7] Maroti Deshmukh,Neeta Nain Mushtaq Ahmed, An (n,n)-Multi Secret Image Sharing Scheme using Boolean XOR and Modular Arithmetic ,2016 IEEE .
[8] K.N. Sandhya Sarma, Hemraj S. Lamkuche and S. Umamaheswari, A Review of Secret Sharing Schemes ScienceAlert open access journal.
[9] Amos Beimel, Secret-Sharing Schemes: A Survey, Springer 2011.
[10] Adi Shamir, How to Share a Secret, Communications of the ACM, Nov 1979.
[11] Moni Naor and Adi Shamir, Visual Cryptography, Advances in cryptology- EUROCRYPT 94, Lecture Notes in Computer Science, vol.950, pp. 1-12, 1995.

