POB number system based Multi-image secret sharing

Ann Jisna James
Department of Computer Engineering
Pimpri Chinchwad College of Engineering,Pune
annjisna162@gmail.com

Prof.Reena Kharat
Department of Computer Engineering
Pimpri Chinchwad College of Engineering,Pune
reenakharat@gmail.com

***Abstract*—Secret sharing is the methodology in which secret is broken into multiple pieces called shares,therefore to recover back this secret ,all the n shares or a subset of the shares are required.The advantage of this form of encryption being that individual shares cannot reveal any useful information.First of such attempts where made by Adi Shamir and George Blakely, who individually ,were successfully able to implement this scheme.Since that period a consist advancement has been marked,the recent being executed upon multimedia data for secure storage and processing.A need for such encryption schemes are necessary in today's environment where majority of highly confidential and valuable data is stored online on cloud storage or other distributed environments. Also the need to secure the data, along with allowing it to be processed in the encrypted state is also necessary.Therefore in this paper an encryption scheme based on a POB Number System upon multiple images has been proposed. It splits the images into multiple shares and further increases its security by creating an inter-dependency among them.The final shares obtained are secure and reveal no information.**

***Index Terms*—Secret sharing,Permutation Ordered Binary (POB).**

I. Introduction

Secret sharing depicts the concept of breaking down and distributing a secret among a body of n partaking individuals, or parties, so that only pre-nominated set of entities are able to rebuild the secret by conjointly emulating their fragments of secret. Shamir was one of the pioneers who developed a threshold based secret sharing scheme in the year 1979.In his suggested scheme,a secret is diced into n set of shares,the recovery is only possible if k out of these n shares (k n) are brought together.Also any aggregation of (k-1) shares yields no result. Shamirs and Blakleys proposals were similar in nature,as both were based on (t, n) threshold secret sharing schemes, however Shamirs theme is more effective as it offers more privacy and accuracy,along with flexibility. Accuracy addresses that a secret s is precisely resolved by any k shares from the shares s1,...,sn, whereas privacy implicates with having connection to any k1 shares from s1,...,sn ,however it lacks in providing any insight into the mutual information or secret s:i.e.the liability of allotment of k1 shares is unrestricted of s.Extensive improvements were later added on to the existing Threshold schemes by Ito, Saito, and Nishizeki.An established secret sharing theme was put forth , where an authorized set of members had the right to reconstruct the shared secret by merging their shares.The key architecture of a secret sharing scheme usually dissociates all subsets of members into approved sections, who are unable to access the secret.Further if a collection can rebuild the secret so can a the super-set of the collection. In the case of an illegitimate group, if the collection cannot recover the secret a smaller subset of the same collection would also fail. Benaloh and Leichter demonstrate that if an access structure can be characterized by a minuscule monotone formula then it has an effluent secret-sharing scheme. Brickell introduced vector space schemes which provides secret sharing schemes for a wide system of access structures , being a very efficient algorithm but required further subsistence of function (φ) .B. Chor and E. Kushilevitz expanded secret sharing systems on constant domain with finite access structures.[9]Yet another note worth approach has been suggested by Sreekumar, build upon the POB mathematical notation.According to this scheme, a secret often divided into n shares each of which corresponds to the POB-values.For reverting back to the the original shares, 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

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[1]

$$\mathbf{b}j * (\overset{j}{\mathbf{p}}_j) \tag{1}$$

where

$$\mathbf{p}j = \sum_{i=0}^{j} \mathbf{b}_j \tag{2}$$

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.

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

978-1-5386-5257-2/18/$ 31.00

B. Multi-Secret Image Sharing

Visual cryptography can be split into major two sectors i.e (k,n)VCS and (n,n)VCS.In the first scheme to rebuild the secret a predefined subset of the shares may only be required,therefore the hidden information can be revealed even if some of the shares are lost or are not acquired.But this may lead to a degrade in the quality of the image reconstructed due to the use of OR operation which decreases the clarity and contrast. On the other hand in (n,n)VCS the regraded image has the same quality as that of the original images.The concept of (n,n)-MSIS scheme therefore implicates a schema in which multiple images are clubbed together but performing operations on them such that the shares obtained from them are related.To rebuild the information/image all the shares are required also since the shares are interlinked the all the images are reproduced are none are, in absence of any share. At present MSIS scheme have several type of utilization in different fields such as missile launching codes, e-auction ,e-voting etc

II. Review of Literature

Secret sharing can act as a solution to the ever increasing need of security for multi-media.The amount of multi-media especially images that circulate the internet is tremendous,hence allowing confidential images to pass through the network without being effected is necessary.With a number of proposed concept in secret sharing ,following the path of share formation through encryption and splitting of the image and later reconstruction once the entity has been safely obtained at the authentic end.despite this a number of shortcoming has been observed which ranges from security point of view to high space and computational requirements.Also the recovered image at the authentic end may face quality and clarity reduction.Also the number of images on which the security needs to be applied comes into light.hence taking all this into account a number of secret sharing schemes are present like Dynamic secret sharing that controls the ability to change access structures,Proactive secret sharing schemes follow a methodology in which the secret remains the same even when the sharers differ.Other schemes followed are based on polynomials or have a set of equation further distributing the shares formed into parts of image called Visual secret sharing schemes[8]. All the SS schemes solve one problem or the other but don't offer a complete solution like where some schemes might have excellent security it may have to compromise with high computational power or share size and vice verse.POB scheme comes as a rescuer in this arena.Introduced by A. Sreekumar and Dr. S. Babu Sundar the scheme doesn't only provide highly secure shares but also have low computational and space requirements.The scheme is applicable for (n,n) shares[2].

Further hybridization of POB was introduced by the authors Deepika M P and A. Sreekumar,the proposed a system that uses CRT (Chinese Remainder Theorem) in combination with POB.The The proposed scheme further shows pixel expansion during share generation due to which the space tradeoff ha to considered during the storage of the shares.The recovered image is lossless and hence retains the information in the image without any loss.Due to use of permutation the chances of guessing a particular share becomes equal to $(1/p(^n_r))^m$,which is quite negligible (m is the no of shares)[4].

Cloud storage is a prominent method of storage for large multimedia.But it may not be the most secure form of storage since there are chances that a third party may acquire the data or the information may be compromised on it.POB has been implemented as a solution along with shamir's encryption.Intially shares are generted from the images using shamir's upon which pob is applied.This secures the images by forming shares of the image which can be stored at different location to ensure privacy.only authentic users can acquire all these shares to form the final image,rebuilding is done using Langrangesinterpolation.The shares can further be processed and the recovered image obtain is similar to implementing the processed on the original image itself,giving the ability for a user to spread the shares and get it processed individually without reveling the actual data[3].

Authors Priyanka Singh,Balasubramanian Raman,Nishant Agarwal,Pradeep K.Atrey have came forth with a unique manner of using pob in which they it is implemeted on individual pixels as well as neighboring pixel such that any tampering on the image is immediatley reflected onto the reconstructred image.In the proposed method the tampered area is removed from the image hence changes to shares can be marked.[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 framework points at tackling the issue of sharing multi-images at a time securely.The framework takes within the images and applies POB plot on which ,which gets connected at pixel level and each picture is changed over to the comparing POB value.Now the pictures obtained are encourage taken and each picture is XOR-ed with its predecessor (the primary image is taken as such due to the absence of predecessor).Again the reverse bits are taken before producing the ultimate output of the system.

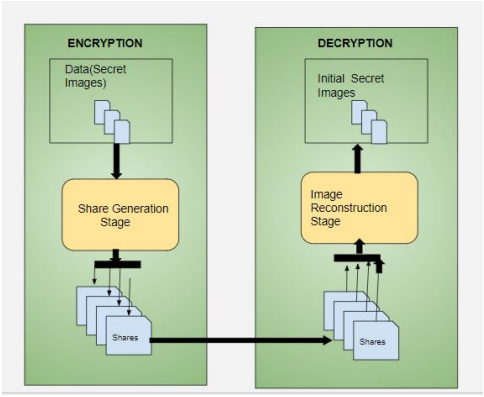

Fig. 1. Block Diagram of System Architecture

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.
  $Ti = pi \oplus Ti - 1$, 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 .

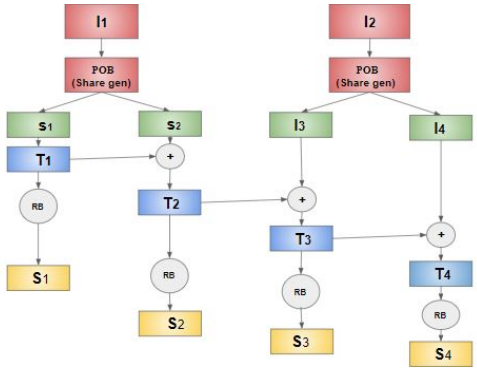

Fig. 2. Block Diagram for share generation

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.

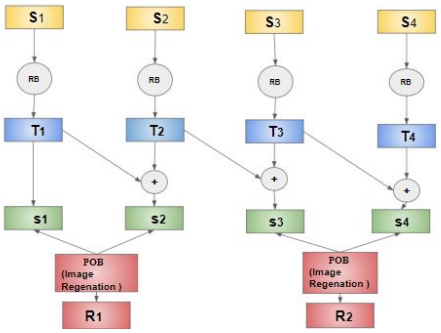

Fig. 3. Block Diagram for share regeneration

V. Mathematical Model

- Let two bytes be considered for sharing then: Q = 11011110 10100001
- Take random numbers as two bytes be 4, and 3
- T= 110011110 101100001
- X= 10**1010* 1*01****0. (taking value at Xi position)
- X= 101010100 100110100
- Y=011001010 001010101 (Y=T $\oplus$ X) The indices of these sections generated are 98, 88 and 59, 20.
- The pob shares are 1100010 1011000 and 0111011 0010100.
- S1= 0100011 [reverse (s1)]
- S2= 0101110 [reverse (s1 $\oplus$s2)]
- S3=1000000 [reverse (s2 $\oplus$s3)]
- S4=1010100 [reverse (s3 $\oplus$s4)]
  Recovery of shares
- s1= 1100010 [reverse (S1)]
- s2= 1011000[reverse (S1 $\oplus$S2)]
- s3= 0111011 [reverse (S2 $\oplus$S3)]
- s4= 0010100 [reverse (S3 $\oplus$ S4)]
- The original value from pob indices are taken to obtain X= 101010100 100110100 Y=011001010 001010101
- T= 110011110 101100001 (T=X $\oplus$ Y)
- Removing the 4th and 3rd bits original share value is obtained Q = 11011110 10100001

VI. Result

Above figure shows the input images given to the system, on these input images following operations are performed i.e. in first step POb values are obtained then XORing is performed, in last step we are reverse bit function is applied to generate final shares i.e. S1, S2, S3, S4, S5. Intel(R)core(TM) i3, 250GHz, 64-bit processor with 8GB RAM.Java was used as an implementation platform. The secret sharing scheme based on the POB Number System for multiple images was tested on gray-scale (png format) of size 256*256 standard images.The

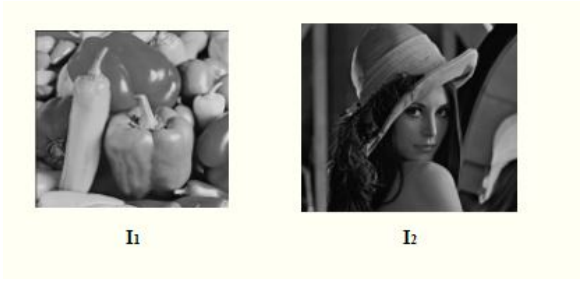

Fig. 4. Input Images

size of the shares after applying the algorithm is same as the size of the original test images.The obtained shares reveal no secrets.

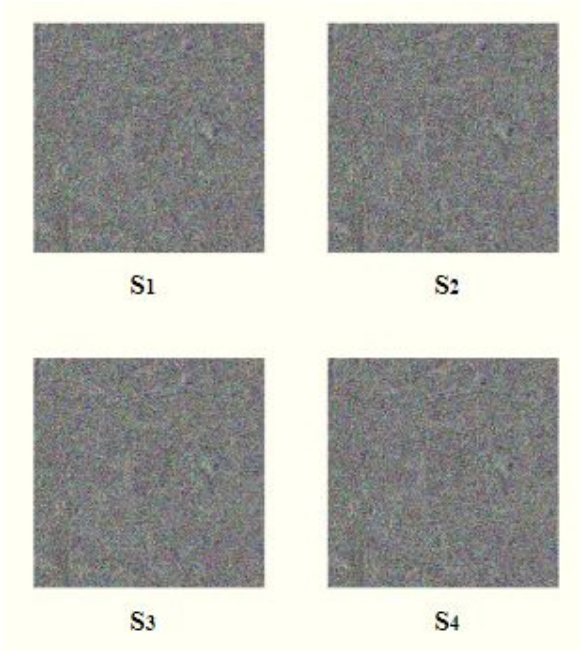

Fig. 5. Output Images

VII. Conclusion

To further secure the storage and exchange of media,an attempt has been made in which secret share scheme based upon POB has been proposed.The security of the images are reinforced by creating depemdency among the image shares.The proposed scheme is effectient, as POB representation is unique the dependency among the images ensure that all the shares are required for any information retrival.

VIII. 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. 2012.
[2] . Sreekumar and Dr. S. Babu Sundar An Efcient Secret Sharing Scheme for n out of n scheme using POB-number system.
[3] Priyanka Singh,Balasubramanian Raman,Manoj Misra "Just process me, without knowing me: a secure encrypted domain processing based on Shamir secret sharing and POB number system,Springer june 2017 .
[4] Deepika.M.P , A. SreekumarA Novel Secret Sharing Scheme Using POB Number System and CRTInternational Journal of Applied Engineering Research 2016 .
[5] Priyanka Singh,Balasubramanian Raman,Nishant Agarwal,Pradeep K. AtreySecure Cloud-Based Image Tampering Detection and Localization Using POB Number SystemACM Transactions on Multimedia Computing, Communications, and Applications,2017.
[6] Priyanka Singh,Balasubramanian Raman,Nishant Agarwal,Pradeep K. AtreyTowards Encrypted Video Tampering Detection and Localization Based on POB Number System Over CloudIEEE 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] Noura Al Ebri, Joonsang Baek and Chan Yeob Yeun, Study on Secret Sharing Schemes (SSS) and their applications.",IEEE(2011)
[9] K.N. Sandhya Sarma, Hemraj S. Lamkuche and S. Umamaheswari, A Review of Secret Sharing Schemes ScienceAlert open access jornal."
[10] Amos Beimel, Secret-Sharing Schemes: A Survey, Springer 2011
[11] Adi Shamir, "How to Share a Secret, Communications of the ACM", Nov. 1979.
[12] Moni Naor and Adi Shamir, "Visual Cryptography, Advances in cryptology"- EUROCRYPT94, Lecture Notes in Computer Science, vol. 950, pp. 1-12, 1995