RESEARCH PAPER | Engineering | Volume : 3 | Issue : 5 | May 2013 | ISSN - 2249-555X

Implementation of Image Secret Sharing Scheme

KEYWORDS: Image Processing, Secret Sharing

Miss. Aarti G. Ghule
Computer Science & Engineering, Sipna C.O.E.T
Amravati, India

Dr. Prashant R. Deshmukh
Computer Science & Engineering, Sipna C.O.E.T
Amravati, India

ABSTRACT *Secret sharing (also called secret splitting) refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use on their own. In an Effective Implementation of Image Secret Sharing Scheme, image secret sharing method which incorporates two k-out-of-n secret sharing schemes: Shamir's secret sharing scheme . The technique allows a colored secret to be divided as n image shares so that: i) any k image shares ($k \leq n$) are sufficient to reconstruct the secret image in the lossless manner and ii) any ($k - 1$) or fewer image shares cannot get enough information to reveal the secret image. It is an effective, and secure method to prevent the secret image from being lost, stolen or corrupted. In comparison with other image secret sharing methods, this approach's advantages are its large compression rate of the image shares, its strong protection of the secret image and its ability for the real time processing.*

I. Introdauction

Secret sharing is one type of key establishment protocols. The Trusted Authority (TA) divides the secret into pieces and distributes the pieces to different users. These pieces are called shares. Shares contain partial information about the secret. However, shares are constructed in such a way that although the secret can be reconstructed by combining a number of shares, simply examining individual user's share will not reveal the secret information at all.

The effective and secure protections of sensitive information are primary concerns in commercial, medical and military systems (e.g. communication systems or network storage systems). Needless to say, it is also important for any information process to ensure data is not being tampered. Encryption methods are one of the popular approaches to ensure the integrity and secrecy of the protected information. However, one of the critical vulnerabilities of encryption techniques is the single-point-failure. For example, the secret information cannot be recovered if the decryption key is lost or the encrypted content is corrupted during the transmission. To address these reliability problems, in particular for large information content items such as secret images (say satellite photos or medical images), an image secret sharing scheme (SSS) is a good alternative to remedy these types of vulnerabilities. Blakley and Shamir invented two (k, n) threshold-based SSS independently in 1979. The general idea behind "secret sharing" is to distribute a secret (e.g., encryption/decryption key) to n different participants so that any k participants can reconstruct the secret, and any ($k - 1$) or fewer participants cannot reveal anything about the secret. Karnin suggested the concept of perfect secret sharing (PSS) where zero information of the secret is revealed for an unqualified group of ($k - 1$) or fewer members. Apparently, there is a subtle difference between the unqualified group cannot obtain any information about the secret and the unqualified group cannot reconstruct the secret with some information. For example, an unqualified group may know information about the secret as an even number, but the group still cannot discover the exact value of the secret. Specifically, Karnin used a term referred as information entropy (a measurement of the uncertainty of the secret), denoted as H(s) where s is a secret shared among n participants. The claim of PSS schemes must satisfy the following:

1. a qualified coalition of k or more participants, C can reconstruct the secret(s) s:

$H(s|C) = 0 \ \forall C| \geq k,$

2. an unqualified coalition of ($k - 1$) or few participants, C has no information about the secret(s), s:

$H(s|C) = H(s) \ \forall C| < k.$

For these requirements in PSS schemes, a secret has zero uncertainty if the secret can be discovered by k or more participants. On the contrary, the secret, in PSS schemes, remain the same uncertainty for ($k - 1$) or fewer members. Therefore, there is no information exposed to the ($k-1$) or fewer members. When exposed information is proportional to the size of the unqualified coalition, these types of SSS are referred as a ramp secret sharing (RSS). Various research papers are devoted on the topics of PSS schemes and RSS schemes.

Naor and Shamir extended the secret sharing concept into image research, and referred it as visual cryptography. Visual cryptography is a PSS scheme, and requires stacking any k image shares (or shadow images) to show the original image without any cryptographic computation. They are not applicable for lossless image recovery due to:

i) image shares have larger image size compared to the size of the original secret image and
ii) the contrast ratio in the reconstructed image is quite poor.

A better image secret sharing approach was presented by Thien and Lin. With some cryptographic computation, they cleverly used Shamir's SSS to share a secret image. The method significantly reduces the size of the image shares to become 1/k of the size of the secret image, and the secret image can be reconstructed with good quality. A drawback, in terms of security, requires that the image is permutated by a key before the image share can be computed.

II. LITERATURE REVIEW

We describe several (k, n) threshold-based SSSs and describe how a secret and an image is shared among n participants. These schemes are briefly described in this section with their interesting features.

1.1Shamir's Secret Sharing Scheme:

Shamir developed the idea of a (k, n) threshold based secret sharing technique ($k \leq n$). The technique allows a polynomial

Volume : 3 | Issue : 5 | May 2013 | ISSN - 2249-555X

function of order (k −1) constructed as,

$f(x) = d0 + d1x + d2x2 + \ldots + dk-1xk-1 \pmod p$,

where ,the value d0 is the secret and p is a prime number. The secret shares are the pairs of values

(xi, yi) where $yi = f(xi)$, $1 \le i \le n$ and $0 < x1 < x2 \ldots < xn \le p - 1$.

III. ANALYSIS OF PROBLEM

Thien and Lin proposed a (k, n) threshold-based image SSS by cleverly using Shamir's SSS to generate image shares. The essential idea is to use a polynomial function of order (k − 1) to construct n image shares. This method reduces the size of image shares to become 1/k of the size of the secret image. Any k image shares are able to reconstruct every pixel value in the secret image. Thien and Lin also provided some research insights for lossless image recovery using their technique.

Since Thien and Lin's method reduces the size of image shares to become 1/k of the size of the secret image, the scheme can not be qualified as a "perfect" image SSS . In fact, this method is a multiple-secret "ramp" SSS . In other words, the information about the secret exposed is proportional to the number of shares available until the number of shares becomes k or more. In addition, the pixel values in a natural image are not random because the neighboring pixels often have equal or close values. A secret image can be possibly recovered from less than k image shares because neighboring pixels are highly correlated. To address these security issues, Thien and Lin suggested an idea by permutation the order of pixels (with a permutation key) in the secret image before the image shares are computed. Conversely, the secret image can still be reconstructed from any k image shares by solving the permutated image and applying inverse-permutation using the permutation key. Nevertheless, the permutation key becomes the single-point-failure in the system because the key can get lost or corrupted.

IV. PROPOSED WORK

We will Implement the Algorithm related to schemes which summarized in following

objectives:

- Study the Secret Sharing Scheme.
- Implementation of an algorithm.
- Checking applicability with images.
- Comparing Efficiency of schemes proposed by our algorithm with the existing schemes.

Among several interesting properties of matrix projection SSS, an image application can be easily extended from this scheme's ability to share multiple secrets. The pixels in an image can be regarded as elements in a matrix. Although the technique is not a PSS scheme, it has strong protection on the secret, even if the remainder matrix R is made public. However, matrix R can become single-point-failure if it is corrupted or lost. To overcome this problem, we propose to use Thien and Lin's method (which is essentially a Shamir's SSS) to share the remainder matrix R without any permutation.

V. APPLICATION

- Medical applications such as telediagnosis require information exchange over insecure networks. Therefore, protection of the integrity and confidentiality of the medical images is an important issue.
- A secret sharing scheme can secure a secret over multiple servers and remain recoverable despite multiple server failures. The dealer may treat himself as several distinct participants, distributing the shares between himself. Each share may be stored on a different server, but the dealer can recover the secret even if several servers break down as long as he can recover at least t shares; however, crackers that break into one server would still not know the secret as long as fewer than t shares are stored on each server

VI. CONCULSION

We proposed an image SSS using essentially technique Shamir's SSS. A colored secret image can be successfully reconstructed from any k image shares, but cannot be revealed from any (k − 1) or fewer image shares. The size of image shares is smaller than the size of the secret image. Another advantage is the this scheme can be used in almost realtime by simultaneous processing smaller blocks partitioned from the secret image. For all these block images, we can parallel process the generation of image shares or the reconstruction of the secret image.

VII. Acknowledgment

I take this opportunity to express my profound gratitude and deep regards to my guide (Dr.P.R.Deshmukh) for his exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by him time to time shall carry me a long way in the journey of life on which I am about to embark.

REFERENCE [1] A. De Santis and B. Masucci, "Multiple ramp | schemes," vol. 45, no. 5, pp. 1720–1728, July 1999 | [2] A. Shamir, "How to share a secret," | Communications of the ACM, vol. 22, no. 11,pp | . 612–613, Nov. 1979. | [3] C.-C. Thien and J.-C. Lin, "Secret image sharing," | Computers & Graphics, vol. 26, no. 5, | pp. 765–770, 2002. | [4] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On | secret sharing systems," vol. IT-29, no. 1, | pp. 35–41, Jan. 1983. | [5] G. Blakley, "Safeguarding crypographic keys," | presented at the Proceedings of the FIPS 1979 | National Computer Conference, vol. 48, Arlington, | VA, June1997 pp. 313–317. | [6] G. R. Blakley and C. Meadows, "Security of ramp | schemes," presented at the Advances in Cryptology | – Crypto '84, G. R. Blakley and D. Chaum, Eds., | Aug. 1984. | [7] L. Bai, "A strong ramp secret sharing scheme using | matrix projection," presented at the Second | International Workshop on Trust, Security and | Privacy for Ubiquitous Computing, Niagara-Falls, | Buffalo, NY, 2006. | [8].M. Naor and A. Shamir, "Visual cryptography," | presented at the Proceedings of the Conference on | Advances in Cryptology – Eurocrypt '94, A. De | Santis, Ed., Berlin, Germany, 1994, pp. 1–12. | [9] Y.-S. Wu, C.-C. Thien, and J.-C. Lin, "Sharing and | hiding secret images with size constraint," | Pattern Recognition, vol. 37, no. 7, pp. 1277–1385, | 2004 |