An Optimal Secret Message based Image Sharing Method to Avoid Cheater in Message Reconstruction

Preeti Rahangdale
Research Scholar
Computer Science and Engineering Department
Samrat Ashok Technological Institute Vidisha
(M.P.)

Yogendra Kumar Jain
Head of Department
Computer Science and Engineering Department
Samrat Ashok Technological Institute Vidisha
(M.P.)

ABSTRACT
Multimedia confidential data uses internet communication channel for transmission. It is not very safe to transmit data via internet communication channel. So it is desired to secure the data before transmitting. Recently various algorithms have been proposed in this context. But there is problem of wrong reconstruction due to fake player participation. To overcome this problem, the proposed method presents an optimal approach for secret sharing. Proposed approach totally depends upon threshold. A secret image can be split into N small sub-files and combination of any T sub-files the original file can be recovered without errors.

Keywords
Secret image, Secret sharing, Share building, Share distribution, Secret share reconstruction

1. INTRODUCTION
With rapid growth of computers and computer networks, enormous amount of digital data can easily be transmitted or stored over network. However, the intruders can easily sense or manipulate the confidential data transmitted over the networks, by some cryptographic tools. So recently numerous of research has been carried in the field of information security.

In information security field, secret sharing is a process of distributing confidential message among a set of participants. Every participant has been allocated with a share of the secret .Then confidential message can only be retrieved when the entire participant combined together; individual shares are of no use on their own.

In secret sharing scheme, due to security concern of confidential message, it is required to divide secret message (SM) into N subpart and share each part with N different host and retrieve the confidential message by combining all N different part when required. Blackly [1] and Shamir [2] introduce secret sharing scheme first time in 1979. Moreover blackly secret sharing scheme cannot stop fake player to make participation during secret recovery and which lead to generate wrong message.

Recently researcher had presented numerous methods to make a control over such fake attempts [3], which broadly divided into two categories cheating detection and cheater identification. In cheating detection method, authorized members have to detect whether there exists a cheater in revealing the secret data or not [4].The second can be used to identify the cheater [3].

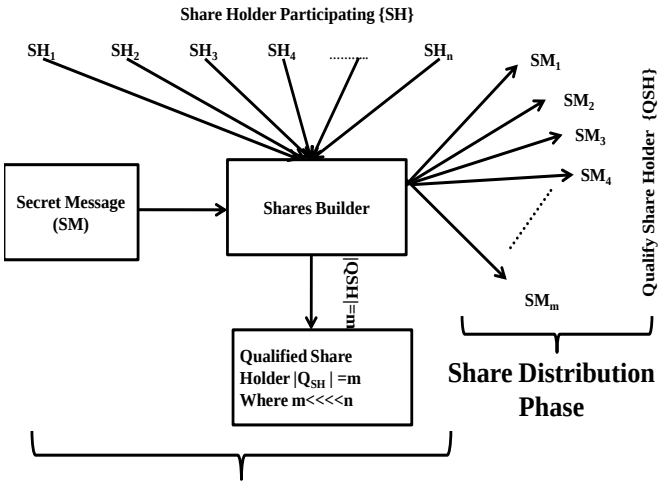

Figure 1:- Share Building and Distribution Phase

The basic idea of secret sharing is to divide information into several pieces such that certain subsets of these pieces (shares) can be used to recover the information. Fake players want to retrieve several shared information, in order to make participate in reconstruction of secret information and try to destroy the information.

Secret sharing scheme having three different phases namely share building phase, share distribution phase and secret reconstruction phase. Share building phase used to select share holder as QSH (Qualify Share Holder) from participant set of share holder SH. Where cardinality of |QSH|= m and |SH|=n and m<<<n, as shown in share building phase of figure 1.

Share distribution phase used to distribute each sub message to each and every qualify share holder QSH as show in share distribution phase of figure 1.

Share building phase distribute all N different shadow image, then share recovery phase combine any random T phase to reconstruct original message image.

Original image = $SM^{X}_{1,T} + SM^{X}_{2,T} + SM^{X}_{3,T} +,,,,,,,,+ SM^{X}_{T,T}$

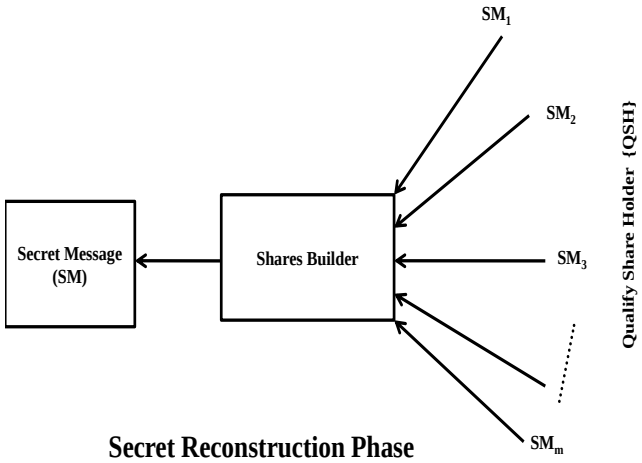

Figure 2:- Share Secret Reconstruction Phase

The method used so far requires all shared images for recovery. In real application, if recovery is possible using some shared images then it can save the time and also stop fake player participation. In this paper, a Secret sharing method is proposed which is based on threshold value. A secret image is divided into N sub-images and by combining any T sub-images, the original image is recovered without error. Here T<<<N.

The rest of the paper is organized as follows. Section II briefly introduces some related techniques. In Section III, the proposed methodology is described in detail. The experimental results are shown in Section IV. Finally the conclusion is drawn in Section V.

2. RELATED WORK

Parakh and Kak have presented a technique for multi-secret sharing [5]. They have used recursive computational approach. They worked on multi-secret sharing approach in order to hide (k – 2) secrets. These secrets are of size b. This can be applying as a steganography. Here the steganography is used to convey the hidden information in order to perform the authentication and verification as well. Authentication and verification has applied on both contents which is shareable and secret also. In Further, the author worked on information of web, sensor networks and information dispersal schemes.

With the rapid growth of mobile communication [6], there is a need to make new mobile phones having attractive features. With this aim, the mobile phone gives the facility of photo sharing which is very popular among users. In context of photo sharing, Ra and Ortega have proposed an efficient algorithm with preserving privacy of the user. It works on the small photos efficiently. The model provided by the authors has worked with respect to facebook also. These P3 features have not required any changes in the software of the mobile phone, but impose some overhead in the work.

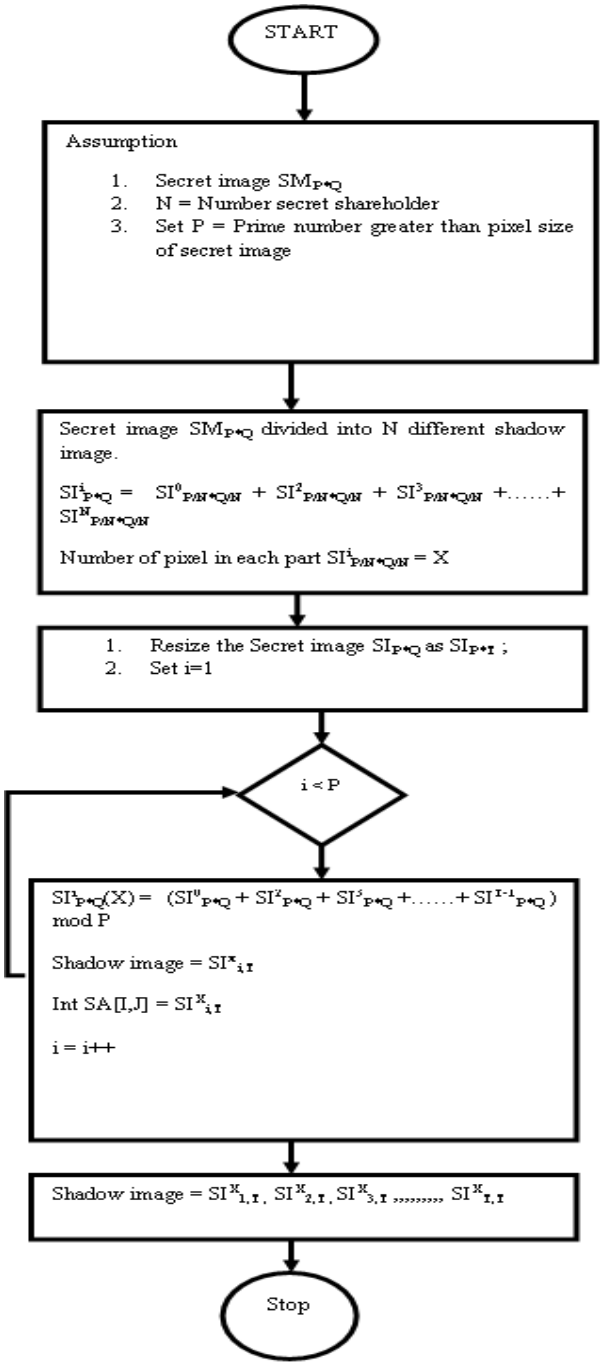

Figure 3: Proposed Methodology for Secret Sharing.

Anbarasi and Kannan proposed a lossless secret sharing approach in order to spread the secret to collection of participants, each of whom is allocated with a share of the secret [7]. The actions of the participant are used to reconstruct the secret. Individual participant's action is useless. Sharing system's reversible images and threshold approach is used to achieve novel sharing secret color images. Secret image pixel colors will be converted to rating system of order m. Quantization process has been applied by the authors in order to enhance the quality of the image. Peak signal to noise ratio has been calculated in order to examine the quality of the output images, and the result is lossless.

Chien and Hwang proposed a method to embed a secret image and the cover image to reduce image distortion shade [8]. The most important aspect of recovery is, to reconstructs the lost secret image. Many existing schemes work well for the first task, but most failed to recover the secret image successfully. To solve this problem, the method based on a field power of two Galois instead of prime numbers is proposed. The experimental result shows that the system provides shadow image of satisfactory quality, and properly reconstructs the secret image and cover with lossless image.

Chen proposed a lossless image sharing method for gray level images [9]. Hill cipher method has been used to divide the image. Then the concept of random grid has applied to the sub-images. The pixel expansion rate has decreased and image recovery has been lossless. The experimental result was far better than the previous approach

3. PROPOSED METHODOLOGY

The proposed methodology is used to split the secret message image SMI into N different shadow images like SMI1, SMI2, SMI3 ……. SMIn at sending end. Whereas at receiving end, original image can be recovered by combining T (T<<<N) different shadow images. In order to achieve this goal proposed work is divided into two phases secret sharing phase and secret recovery phase.

3.1 Secret Sharing Phase

In secret sharing phase, initially secret image $SM_{P,Q}$ can be divided into N different sub images. Then on the basis of pixel value of that sub part threshold value is evaluated. The threshold value is depends upon random prime number, which is just greater than pixel value of original image as shown in figure 3.

Secret sharing phase is responsible for share building and share distribution. Share building phase takes $SM_{P,Q}$ as input. Then chooses a prime number P_{num}, just greater than highest pixel value of secret image message $SM_{P,Q}$ i.e. P or Q (P if P>Q or Q if Q>P).

Secret sharing phase divides secret image message $SM_{P,Q}$ into N subpart such as $SM^0_{P/N*Q/N}$, $SM^1_{P/N*Q/N}$, $SM^2_{P/N*Q/}$,,,,,,,,,, $SM^{N-1}_{P/N*Q/N}$. Then for each part calculate N different coefficients by using equation 1.

$$SM(X) = (SM + s^1_X + s^2_X + \ldots\ldots + s^{T-1}_X) \bmod P \quad \ldots\ldots\ldots 1$$

Where SM is secret image message, T is threshold coefficient i.e. number of useful pixel in an subpart of image, coefficients s^1, s^2, s^3, ,,,,,, s^{T-1} are randomly selected from integers. The threshold value is responsible to generate shadow image of a subpart. Coefficient values are less than selected $P_{num..}$ A matrix M [P,Q] is used to store these coefficients. Dimension of matrix M is as same as original image dimension. Now coefficient values for a particular part stores in corresponding row of matrix M [P,Q] as shown in equation 1a.

$$\begin{pmatrix} x_1^1 x_1^2 x_1^3 \ldots\ldots x_1^{t-1} \\ x_2^1 x_2^2 x_2^3 \ldots\ldots x_2^{t-1} \\ \vdots \\ x_t^1 x_t^2 x_t^3 \ldots\ldots x_t^{t-1} \end{pmatrix} \begin{pmatrix} SM_1 \\ SM_2 \\ \vdots \\ SM_t \end{pmatrix} = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_T \end{pmatrix} \boldsymbol{mod\ T} \quad \ldots.1$$

Then on the basis of N different pixel value X, corresponding coefficient value SM(X) is used to evaluate shadow image SM^i. Proposed Secret sharing scheme generates N different shadow images. Each part SM^i contains (X_i, Yj) pixel and their precede part SM^{i-1} contains (Wi, Xi), whereas follower part SM^{i+1}contains (Yi, Zi) in such a manner that last part precede first part and first part follow last part.

Now Share distribution phase is used to distribute N different shadow images, obtained from share building phase to their respective recipient. This phase is also responsible for proper shuffling of confidential message among the entire N participant. And original message is recovered by combining secret of only T participant.

3.2 Image Recovery Based On Shadow Images

Share distribution phase distributes all N different shadow images, then share recovery phase combine any random T shadow images to reconstruct original message image.

Original image = $SM^X_{1,T} + SM^X_{2,T} + SM^X_{3,T}$ +,,,,,,,,,+ $SM^X_{T,T}$ …….2

N different pieces of secret image message are assigning to N different participants. A set of T different participant coordinate their share and recover original secret image message. The proposed scheme maintains an array SM(X) = {$SM(X_1)$, $SM(X_2)$, $SM(X_3)$,,,,,$SM(X_T)$}, to contain the value of coefficient of T different shadow images. The reconstruction of secret image is presented as follow

1. Restructure set of all the T shadow image by using matrix M [P, Q] which contain coefficient value of pixel of respective shadow image.
2. Retrieve the i^{th} element of each row which is below to the respective T^{th} shadow image as SMi (Xi) .
3. Then evaluate the value of T_i such as $SMi(X_0)$, $SMi(X_1)$, $SMi(X_1)$……. $SMi(X_{t-1})$.
4. By using T, calculate pixel coefficient value of each Si(Xi) as

$SMi(X_0) = (SM + s1X + s2X + \ldots\ldots + sT\text{-}1X) \bmod P$

$SMi(X_1) = (SM + s1X + s2X + \ldots\ldots + sT\text{-}1X) \bmod P$

$SMi(X_2) = (SM + s1X + s2X + \ldots\ldots + sT\text{-}1X) \bmod P$

...

$SMi(X_{T-1}) = (SM + s1X + s2X + \ldots\ldots + sT\text{-}1X) \bmod P$ ……3

5. All the above equation gives the value of pixel coefficients of each SMi (Xi) as s1X, s2X… sT-1X.
6. Repeat the step 3 & 4 for each and every T shadow image.
7. Reconstruct the original secret image message by:

$$SM \equiv \sum_{i=1}^{t} SX_i \left[\prod_{j=1,\, j\neq i}^{t} \frac{-s_j}{s_i - s_j} \right] \bmod p$$

4. ENVIRONMENT SETUP AND RESULT ANALYSIS

The image with dimension P*Q is sub divided into N parts. All parts are of equal size having dimension M/T* M/T. To recover the original image, only T shadow images are required. After collecting any T shadow images the original image is recovered without any loss. Table 1 shows the comparative study of proposed technique with the existing work. It is found that the proposed approach is lossless and

require only T shadow image to recover original image whereas existing method requires the entire N shadow images.

Proposed technique uses (T, N) secret image sharing scheme, where T= threshold and N =8. For analyzing the proposed technique, 8 bit gray Lena image having dimension 256*256 is used to show the result. As pixel value of original image is lies between 0 – 255 hence 257 is chosen as Prime number which is just greater than 255. Then on the basis of this prime number, T is evaluated as 4, by using equation 3.

Now by using secret image sharing scheme described in section 3, eight shadow images are generated which are shown in Figure 4 -12. The proposed work is implemented using MATLAB platform which is easy to use and provide various tools in order to analyze the images.

N=8, calculated T=4 and the size of original Lena image is 256*256, so the size of each eight shadow image is 64*64. Since threshold value is 4, then any four combinations of shadow images can generate the original image as shown in figure 13. By comparing with the original image, it is found that there is no error between the original image and the recovered image.

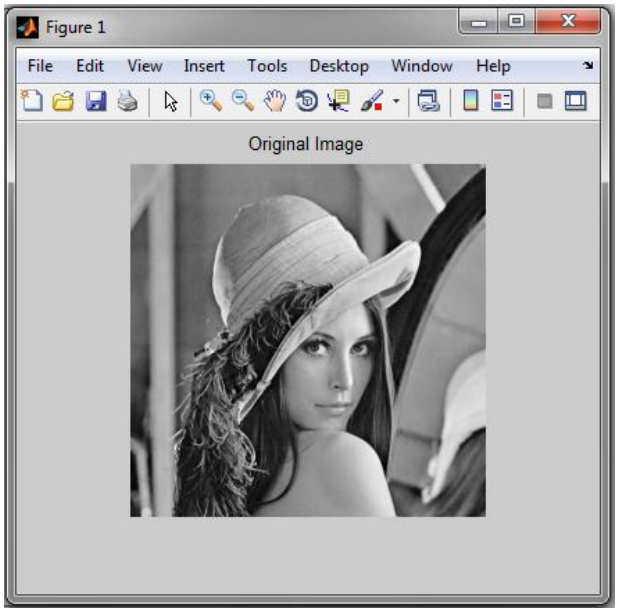

Figure 4: Original Image.

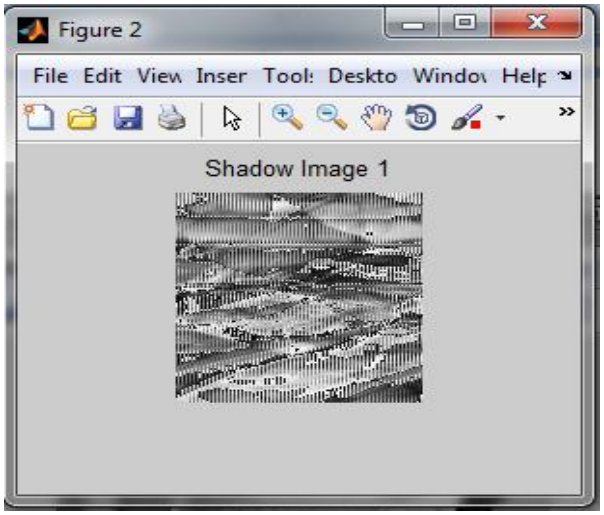

Figure 5: Image shadow 1.

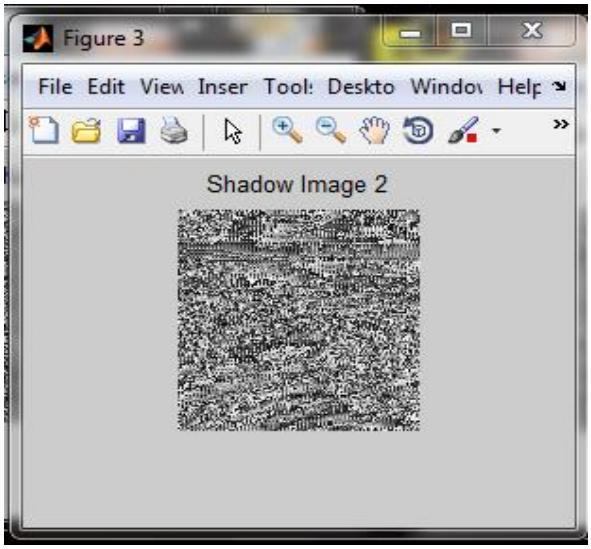

Figure 6: Image shadow 2.

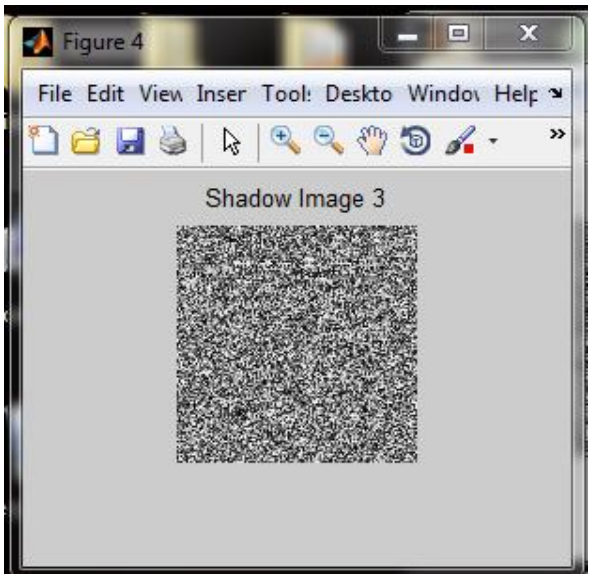

Figure 7: Image shadow 3.

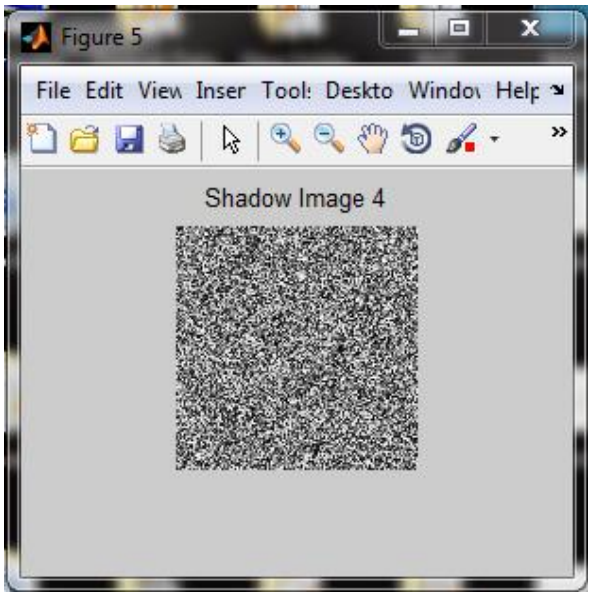

Figure 8: Image shadow 4.

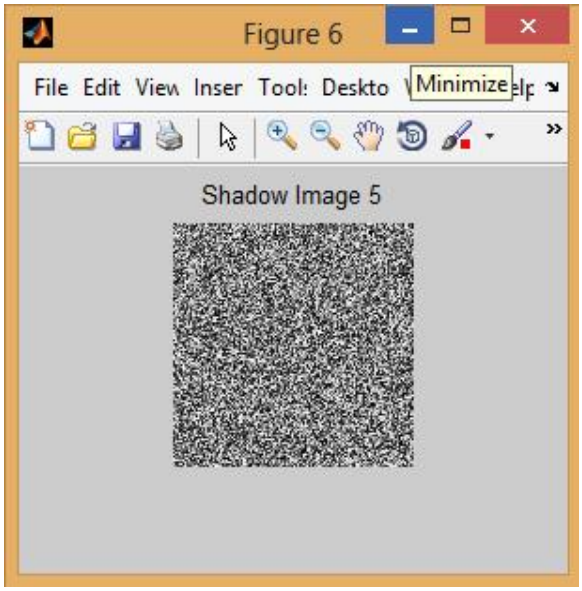

Figure 9: Image shadow 5.

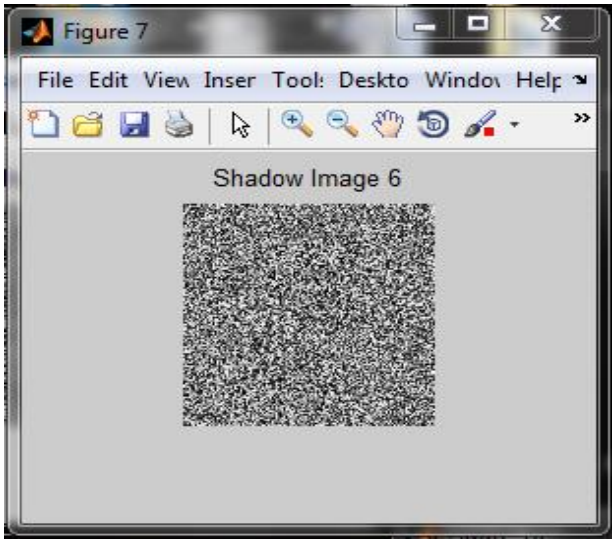

Figure 10: Image shadow 6

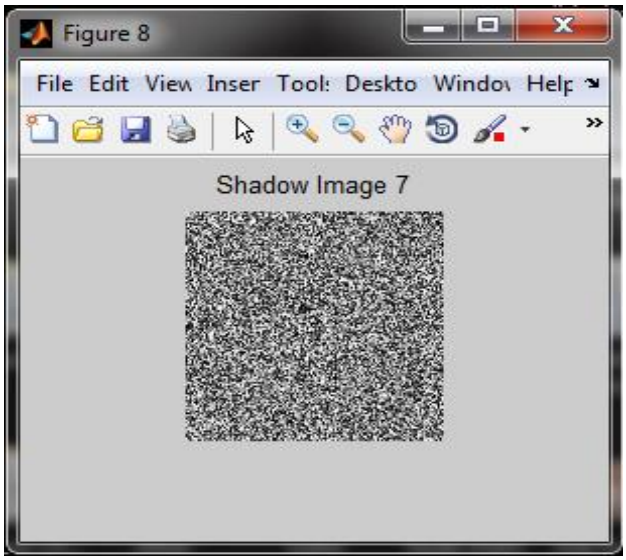

Figure 11: Image shadow 7

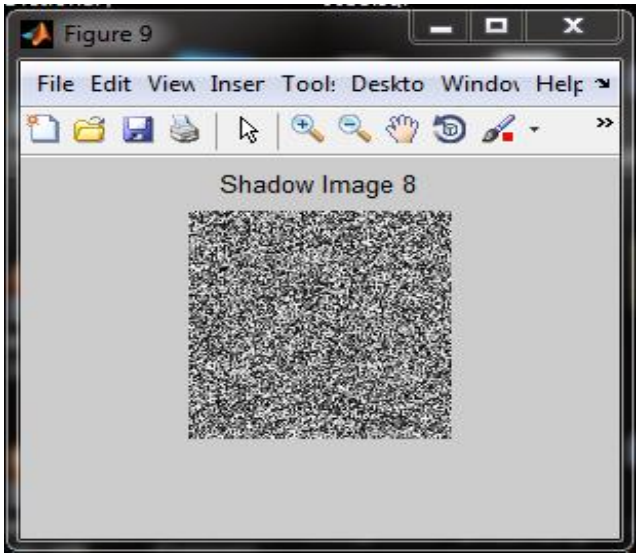

Figure 12: Image shadow 8

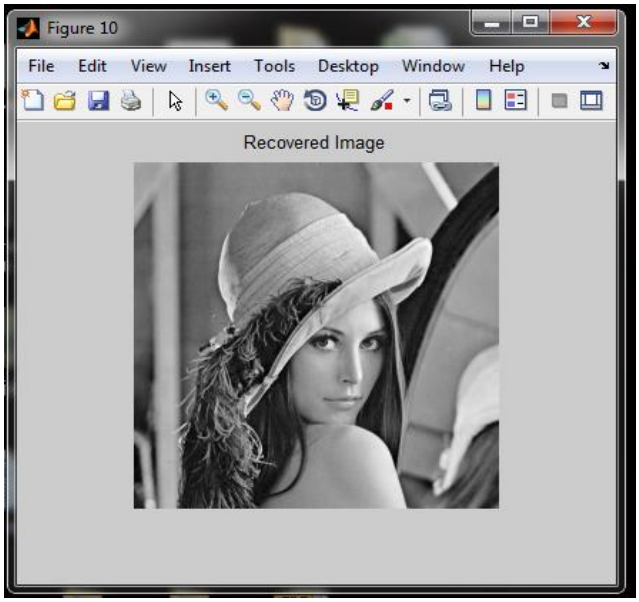

Figure 13: Final Recovered Image

The above experimental result shows that the proposed method has the following advantages. (1) Instead of all N shadow images, only T shadow images are required to recover the original image. (2) No one can obtain the information of the secret image from any one of the shadow image. (3) Time required to recover the original image is less, since it requires only T parts. Hence, the proposed method can progressively recover the original secret image without any loss.

Table 1:- Result Comparison.

Approach	Secret image	Sharing image	Recovered image
Yang's method (2004)	Binary	(m × n) (m × n)	Lossy
Shyu's method (2009)	Binary, gray-level, color	(m ×n) (m × n)	Lossy

Chen method (2011)	Binary	(m × n) (m × n)	Lossy
Thieh method (2003)	Binary	(m × n) (m × n/2)	Lossy
Wei-Kuei Chen Method (2013)	Gray-level	(m × n) (m × n/2)	Lossless
The proposed method	Binary	(TxT)	Lossless

5. CONCLUSION

This paper develops a secret sharing scheme and introduces an optimal threshold scheme which is based on prime number just greater than pixel value of original image. Proposed methodology use any random T subparts to reconstruct original image message in place of N subpart. This way proposed methodology avoids using fake player to make participate in image reconstruction. Along with that proposed methodology is quit faster than existing one as it requires only T subpart to combine which is very less than N.

In future work, the robustness of the proposed method against some famous steganalysis schemes can be improved.

6. REFERENCES

[1] Blakley, G.R., "Safeguarding cryptographic key", Proc. AFIPS National Computer Conf., vol. 48, pp. 313–317, 1979.

[2] Shamir, A., "How to share a secret", Commun. ACM, vol. 22, no. (11), pp. 612–613, 1979.

[3] Hu, C.M., Tzeng, W.G., "Cheating prevention in visual cryptography", IEEE Trans. Image Process, vol.16, no.(1), pp. 36–45, 2007.

[4] Zhao, R., Zhao, J.J., Dai, F., Zhao, F.Q., "A new image secret sharing scheme to identify cheaters", Comput. Stand. Interfaces, vol. 31, no.(1), pp. 252–257, 2009.

[5] Abhishek Parakh and Subhash Kak, "Recursive Secret Sharing for Distributed Storage and Information Hiding", ACM Proceedings of the 3rd international conference on Advanced networks and telecommunication systems, pp 88-90, 2009.

[6] Moo-Ryong Ra, Ramesh Govindan and Antonio Ortega, "P3: Toward Privacy-Preserving Photo Sharing" 10th USENIX Symposium on Networked Systems Design and Implementation, pp 515-528, 2013.

[7] Anbarasi, L.J. and Kannan, S., " Secured secret color image sharing with steganography", IEEE 2012, pp 44 – 48, 2012.

[8] Ming-Chun Chien and Hwang, J.G., "Secret image sharing using (t,n) threshold scheme with lossless recovery", IEEE, pp 1325 – 1329, 2012.

[9] Wei-Kuei Chen, "Image sharing method for gray-level images", The Journal of Systems and Software 86, Elsevier, pp 581–585, 2013.

[10] Ching -Nung Yang, Tse-Shih Chen, "Improvements of image sharing with steganography and authentication" Journal of Systems and Software Elsevier, vol. 80, pp 1070–1076, 2013.