I J C T A, 10(9), 2017, pp. 957-965
© International Science Press

ISSN: 0974-5572

Secure and Privacy Protected Bank Locker System Using RFID and Biometrics

Sonali Patil* and Kapil Tajane*

ABSTRACT

Biometric data refers to metrics related to unique human characteristics like fingerprint, iris, face recognition, voice, palm print etc. Various security threats are raised while handling esoteric data. The current Bank Locker System uses manual methods like signature verification and keys to access the locker. In the current system, signature can be easily copied which poses as a threat to the security of the locker. Thus, a more secured locker system is the need of the hour. In this paper we propose a system which uses biometric feature recognition and authentication of the user using Secret Sharing Schemes. In the proposed system, the biometric feature of the user is considered as the secret for which shares are generated. Both the user and the bank will possess a unique share and only the combination of both the shares would generate the original secret.

Keywords: Security, Privacy, biometrics, secret sharing, RFID

1. INTRODUCTION

In the present bank locker system, the identity of the locker owner is not efficient due to manual methods followed. First identification of the customer is done through means of ID proof and signature. Then, to access the locker two keys are required, one being with the bank official and other with the locker owner. But they are prone to security threats as signature can be easily copied or Id proofs can be replicated by unfair means. Also in *some* locker systems password protection is used. But it is difficult to remember the password. Thus, arises a need to provide a more secure bank locker system. Digital lockers are also used to protect confidential documents or private accessories. These lockers use GSM technology as well as passwords for protection of the same. GSM technology sends a One Time Password (OTP) to the registered mobile number of the user for authentication purpose. There is a possibility that the mobile can be stolen or hacked by an intruder. So, to make the system more secure we propose a system that uses biometric features and RFID technology for identification and authentication of the user. The benefits of this system is that biometric features are unique and immutable. Thus, the proposed system increases the level of security and ease of access[1][2][3][4].

1.1. Biometric System

There are two levels for implementing a biometric system which consists of Enrolment and Authentication. The first step i.e Enrolment comprises of extracting biometric features (Palm print, iris, fingerprint, facial features). These features are stored in a template which can be used for future reference. The second step is authentication which involves creation of a template from a new capture of the required feature. The previously stored reference template is compared with the newly generated template [5][6][7].

* Pimpri Chinchwad College of Engineering, Pune, *Emails: sonalimpatil@gmail.com, kapiltajane@gmail.com*

	Univer-sality	Uni-queness	Perma-nence	Measur-ability	Perfor-mance	Accept-ability	Circum-venction
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Retina	H	H	M	L	H	L	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Ear	M	M	H	M	M	H	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Figure 1: Biometric Traits comparison

1.2. Fingerprint

In fingerprint based authentication impression left by the ridges of a human finger is used. Each individual has a unique fingerprint. Thus it can be used for individuals identification and authentication. As they are difficult to alter fingerprint authentication system is more secure and reliable.

Types of fingerprint patterns are arches, loops and whorls. In arches ridges run from one side to other of the pattern making no backward turn. In loops, one or more ridges enters in either side of the impression re curves, forms a loop and ends on the same side. In whorls, some of the ridges make a turn through at least one circuit [8][9].

1.3. RFID

Radio Frequency Identification uses radio waves for automatically tracking and identifying tags attached to objects. These tags contain electronically stored information which is read by a RFID Reader. The reader sends a signal to the tag and reads its response.

RFID tags can be active or passive. Active tags periodically transmit its ID signal and uses an on-board battery. Whereas, a passive tag uses radio energy transmitted by the reader. Thus, passive tags are widely used over active tags [3].

1.4. Secret Sharing

Even though multi modal biometric systems provide a certain degree of security over uni modal systems, it does not solve all the security concerns. So to add an additional layer of security, we use secret sharing mechanisms. A technique to distribute a secret among group of participants, where each participant is allocated with a unique share of the secret is called a secret sharing. The original secret data can be generated back only when enough (threshold) number of shares are combined together [10][11].

A new system is proposed based on two factor authentication using RFID and biometrics to increase the security of the existing bank locker system.

2. LITERATURE SURVEY

2.1. Shamir’s Secret Sharing

Shamir’s secret is an algorithm is based on polynomial equation where secret is a constant term.

$$f\left(x\right)=a_0+a_1x+a_2x^2+.....+a_{k-1^{k-1}}$$

In the above equation highest degree is, k-1 which is decided as threshold-1.

As shown in figure 2.1, a secret image is divided into n=3 shares. Now, the reconstruction of the original image requires at least k=2 shares which is the threshold value. If there are less than ‘k’ number of shares, the secret cannot be reconstructed[10].

Thus in this case, using any 2 shares, we can reconstruct the original secret.

Suppose the secret is 5432, then we generate a polynomial of degree 1(k-1) as k=2. Hence we get,

f(x)=5432 + 23x

where,

a0=5432 (secret)

a1=23 (random number)

The reconstruction can be done by using Lagrange’s interpolation formula. We generate two polynomials.

$$l_0 = X - X_1 / X_0 - X_1 * X - X_2 / X_0 - X_2$$

$$l_1 = X - X_0 / X_1 - X_0 * X - X_2 / X_1 - X_2$$

Reconstruction formula:

$$f\left(x\right)=\sum_{j=0}^{2} y_j l_j\left(x\right)$$

Thus, the original image has been reconstructed.

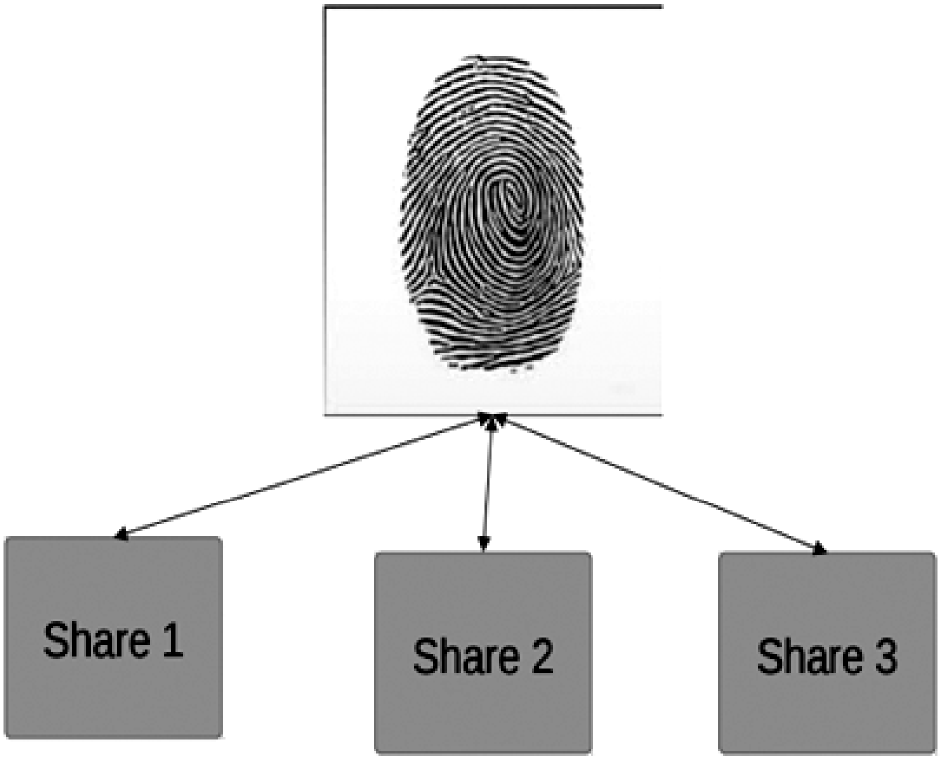

Figure 2: Construction of shares of Biometric Trait

2.2. Thein and Lin Scheme

Here, pixels values are used in polynomial instead of random numbers as in case of Shamir's Secret sharing[11].

The steps are explained below :

Step 1: Generate a random sequence with a secret key to calculate the value of O, the resultant vector is expressed as 'Q'.

Step 2: Group the vector values in groups of two each.

Step 3: Using the secret key, iterate through the groups, and compute the polynomial as follows:

$f(x) = ax + b$, x: secret key value, (a, b): feature value.

Step 4: Generate 3 values, and append them in 3 planes:

$fi(1)$, $fi(2)$, $fi(3)$

Step 5: Iterate through all the feature vectors and perform steps 3 and 4.

Step 6: The resultant 3 planes are the shared feature vectors.

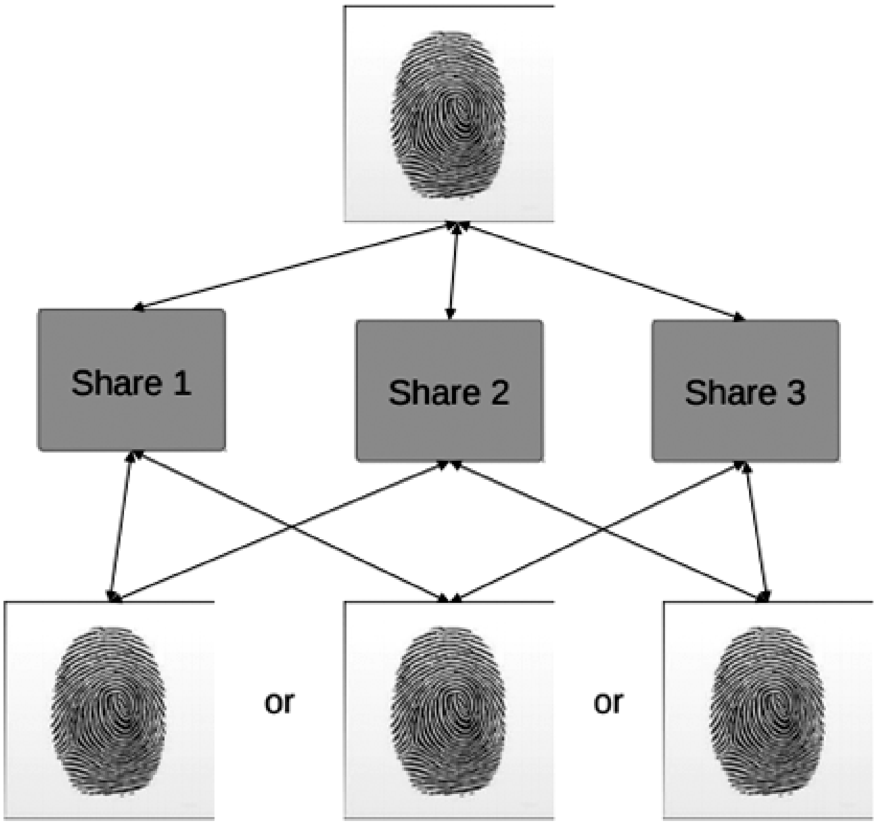

Figure 3: Reconstruction of Biometric Trait from Shares

2.3. (2, 2) XOR Secret Sharing Scheme:

[12] is a simple techniqie based on modulo 2 operation. In this technique a secret is divided into two shares. For gettibg the original secrte back in the reconstruction process both the shares are needed. It can be extended upto (n, n) secret sharing.

2.4. Comparative Analysis

Table 1
Comparative Analysis of existing schemes

Schemes Parameters	*Shamirs's Secret Sharing Scheme [10]*	*Thein and Linsecret Sharing Scheme [11]*	*Xor Secret Sharing Scheme [12]*
Threshold	(k, n)	(k, n)	(2, 2)
Computational Complexity	High	High	Very Low
Space Complexity	O(k)	O(k)	O(1)
Accuracy	High	High	Moderate
Entropy	Low	Low	High
Security	High	High	Low
Ideal	Yes	Yes	Yes

3. ARCHITECTURE OF PROPOSED SYSTEM

The system uses a Raspberry Pi which is interfaced with a fingerprint scanner through which fingerprint of the customer is taken during enrolment and authentication.

The Raspberry Pi is also interfaced with Arduino which is connected with the RFID reader/writer through which the data is written or read into the RFID card of the user during enrolment or authentication. If the user is authenticated then access is granted and the relay drive is activated which will open the bank locker and access will be granted to the customer.

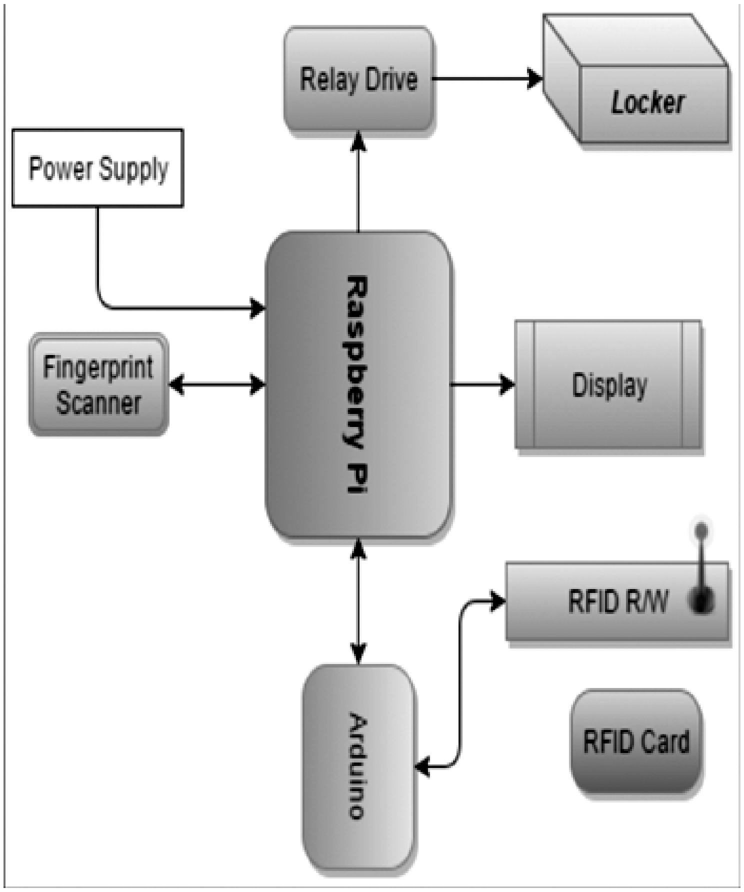

Figure 4: System Design

4. PROPOSED SYSTEM

Proposed system uses a two factor authentication using RFID and fingerprint data to provide more security to the existing bank locker system. The user has to undergo following procedure:

4.1. Enrolment

During enrolment, user has to give a live fingerprint from which shares are created using Thein and Lin secret sharing scheme. One share is stored in the bank database and the other is embedded in the RFID card which is given to the user.

4.2. Authentication

When user swipes the RFID card the embedded share is extracted. It is then combined with the share in the bank database and the original fingerprint is reconstructed using a secret sharing scheme. The user is also supposed to give a live fingerprint which is then compared with the reconstructed fingerprint. Only if both the fingerprints match then the user can access the bank locker or else access is denied.

This makes sure that only the owner of the locker can access it. It also eliminates the intervention of the bank official. It thus, provides a fast, easy and secure access.

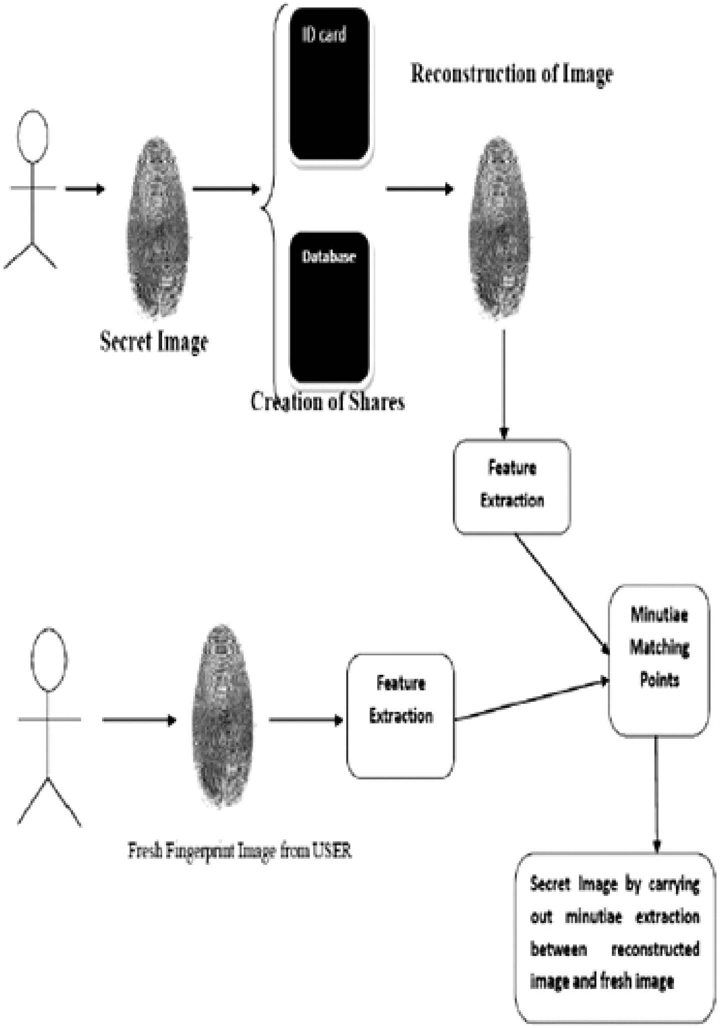

Figure 5: Proposed System

4.3. Comparative Study

The proposed system is compared with existing manual method for operating bank lockers. In proposed system two approaches are considered: Individual Account and Joint Account. In joint account two different shares are provided in RFID card to different holders.

Table 2
Comparative Analysis with existing and proposed system

Parameters	*Existing bank locker System*	*Proposed system with Individual Account Holder*	*Proposed system with Joint Account Holders*
Factors used	Signature	Fingerprint and RFID	Fingerprint and RFID
Database Size	High as individual data of each customers is needed	Low as only one share data need to be stored	Low as for two customers only one share data need to be stored
Privacy	Very Low	High	High
Protection of Biometric Data	–	Yes	Yes
Security	Low	High	High

The above table shows that the proposed system is better than the existing system on the parameters like factors used for the identification of the customer for bank locker, space complexity, privacy and security.

The proposed system can be effectively used for Individual Account holder as well as for Joint Account. Huge database size reduction is observed in proposed system with the existing system.

The protection of Biometric data used as a identification factor for the customer is the major outcome of implemented system.

The next section gives the details about size reduction result and security results.

5. RESULTS

The proposed system is implemented using python and Raspberry Pi. The biometric factor (fingerprint) is experimented on various sizes. The below table shows the reduction in size.

Table 3
Share Size Reduction with respect to original biometric trait

Image Size	*Vector Size*	*Share Size*
512×512	1×16	1×8
256×256	1×16	1×8
512×512	1×16	1×8
1024×1024	1×16	1×8

Highly reduced size database is observed from above table.

The below table shows the SSIM between original image and share image. SSIM stands for Structural Similarity Index between two images. In this paper SSIM is calculated to check similarity between original image and share image is shown in Table 2.

Table 4
SSIM of Original image and share image

Image Id	*SSIM for Original Image*	*SSIM for Share Image*
101_4.tif	0.9930	0.0087
101_3.tif	0.9556	0.0078
102_2.tif	0.9638	0.0065
103_1.tif	0.9765	0.0083
103_5.tif	0.9630	0.0067

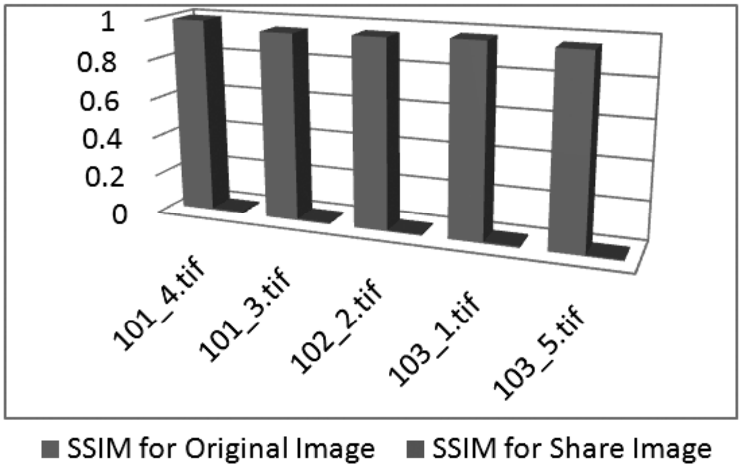

Figure 6: SSIM of Original image and share image

The SSIM is calculated to check similarity between original image and reconstructed image is shown in Table 3.

Table 5
SSIM of Original image and reconstructed image

Image Id	*SSIM for Original Image*	*SSIM for Reconstructed Image*
101_4.tif	0.9930	0.9932
101_3.tif	0.9556	0.9569
102_2.tif	0.9638	0.9626
103_1.tif	0.9765	0.9780
103_5.tif	0.9630	0.9687

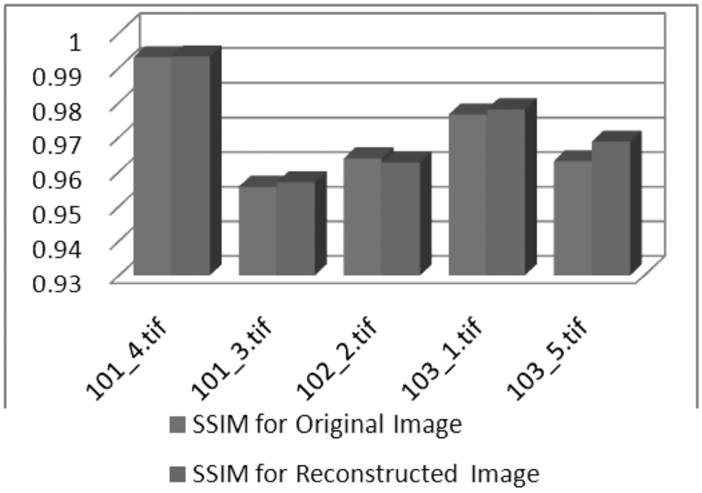

Figure 7: SSIM of Original image and reconstructed image

6. CONCLUSION

A secure and accurate Bank Locker System is proposed with protection of Biometric database by distribution of data in RFID card and Bank Database. It reduces the time complexity of searching to O(log n), as the user ID to be searched in the database is directly given in the RFID card. The space required is tremendously reduced of the original image because instead of storing the whole fingerprint image a very small share is stored in the database. Thus the proposed system provides more security and privacy compare to existing bank locker system.

REFERENCES

[1] Aruna Mane and Sirkazi Mohd. Arif, "Locker security system using RFID and GSM Technology", International Journal of Advances in Engineering and Technology, May 2013.

[2] Raghu Gangi, Subhramanya Gollapudi, "Locker Opening And Closing System Using RFID", fingerprint, Password And GSM, International Journal of Emerging Trends And Technology in Computer Science.

[3] Jyoti Jhawar, Amol G. Muley, "RFID based security system for Banks", International Journal on Recent and Innovation Trends in Computing and Communication.

[4] Kapil Tajane, Sonali Patil, "Enhancing Security of Banking Locker System Using Secret Sharing Scheme Based on Random Grids", International Conference by Springer ERCICA-2015,Banglore, August 2015.

[5] Pramila D. Kamble and Dr. Bharti W. Gawali "Fingerprint Verificationof ATM Security System by Using Biometric and Hybridization" International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012.

[6] Kapil Tajane, Sonali Patil, Janhavi Sirdeshpande, "Secret Sharing Schemes for Secure Biometric Authentication.", International Journal of Scientific and Engineering Research(IJSER) Vol 4, Issue 5,ISSN 2229 – 5518, June 2013.

[7] Kapil Tajane, Sonali Patil, Janhavi Sirdeshpande, "Enhancing Security and Privacy in Biometrics Based Authentication System Using Multiple Secret Sharing", IEEE Conference ICCUBEA-2015, PCCOE, Pune, Feb 2015.

[8] Anil K. Jain, Arun Ross and Salil Prabhakar "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004.

[9] D. Shekar and Goud and Ishaq Md. and P. J. Saritha "A Secured Approach for Authentication System using Fingerprint and Iris" Global Journal of Advanced Engineering Technologies, Volume 1, Issue 3-2012.

[10] Shamir, "How to share a secret, "Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[11] Chih-Ching Thien, Ja-Chen Lin, "Secret image sharing", Volume 26, Issue 5, October 2002, Pages 765–770.

[12] Kapil Tajane, Sonali Patil, Janhavi Sirdeshpande, "General Access Structure For Modulo-2 Secret Sharing Scheme", International Journal of Engineering Research and Technology(IJERT),Vol 1, Issue 2, ISSN : 2278 - 0181, October 2012.

[13] Kapil Tajane, Sonali Patil, Janhavi Sirdeshpande, "An Explication of Secret Sharing Schemes with General Access Structure" , International Journal of Advances in Engineering and Technology(IJAET) Vol 6, Issue 2, ISSN 2231 – 1963, April 2013.