# Amended Biometric Authentication using Secret Sharing

Janhavi Sirdeshpande
ME Student
Pimpri Chinchwad College Of Engineering, Pune, India

Sonali Patil
Asst. Professor
Pimpri Chinchwad College Of Engineering, Pune, India

## ABSTRACT
Visual cryptography is a secret sharing scheme where a secret image gets divided into number of pieces called shares and not a single share disclose any information about secret image. There are some automated methods to identify and verify the user based on the physiological characteristics. To deal with such methods, there is a technology called biometrics which measures and statistically analyze the biological data. The biometric samples which are stored in the database as a secret are unique for each user so that no one can predict those samples. The addition in number of users increases the size of the database which affects space and time complexity. The intent of this paper is to overcome these issues by applying (2, 2) visual cryptography for amend biometric authentication. The experimental results show great reduction in space and time complexity.

## General Terms
Authentication, Biometrics, Secret sharing.

## Keywords
Minutiae extraction, PIN, SSIM, Visual cryptography.

## 1. INTRODUCTION
Security is an important concern in the field of information technology. It is an important thing as per as concern to the ruling of internet over people today. Also, the rapid growth of authentication systems has changed the view of people toward the way these systems deal with. In such systems, the Personal Identification Number (PIN) or password is a prime thing. PIN or password is generally used to protect any system, financial information of person against unauthorized access. Now a days attacks at authentication systems have become a worldwide issue. Traditional system is authenticated by using a PIN or password which is not reliable in point of view of security. Thus in such a case it becomes mandatory to provide protection and security to such a system against any attack. Using fingerprint biometric identifier may solve this problem as biometric sample of each person is unique. This paper introduces a merging of biometrics [12] with secret sharing. The idea behind proposed scheme is, the fingerprint image gets divided into two shares out of which one share will be given to the user in ID card and remaining share will be stored in the database. The share which is stored in the ID card can be embedded in the user's photograph. This share can be embedded by using steganography [13]. The idea of embedding share with the help of steganography has been taken from one of the reference papers where all the possible methods for embedding a share are explained [11]. By superimposing these two shares, the reconstructed image will be formed. The reconstructed image will be matched with fresh image given by user. Pattern matching of reconstructed image and fresh image will be carried out by using minutiae extraction algorithm. This concept will definitely resolve the problem of falsification and maintenance of large databases.

### 1.1 Secret Sharing [1]
Due to fast growth of Internet applications, the digitized data becomes popular. Because of the ease of digital duplication, there exists an issue like data security. In some application areas, it is a risk if a set of secret data is held by only one person without extra copies because the secret data set may be lost incidentally or modified intentionally. In some other cases, it might be necessary for a group of persons to share a certain set of secret data. Shamir (1979) [1] proposed the concept of (k, n) threshold secret sharing to solve the problem. The Shamir's scheme divides a secret data set into n shares and distributes them to n participants, where any k shares or more than k shares can be collected to recover the secret data, but any k -1 or fewer of them will gain no information about it.

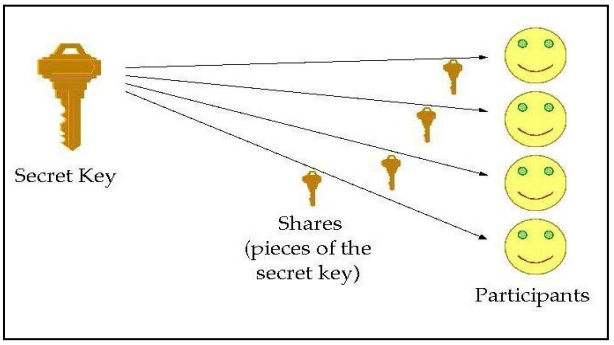


**Fig 1: Concept of Secret Sharing**

In one type of secret sharing scheme there is one dealer and n participants. The dealer gives a share of the secret to the participants. These participants are able to reveal the secret from their shares. The dealer reveals this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of fewer than t players can. Such a system is called a (t, n)-threshold scheme [10] (some-times it is written as an (n, t)-threshold scheme).This paper proposes a merging of secret sharing with biometrics to enhance security and privacy in biometrics based authentication systems. This paper introduces a biometric system which includes a (2, 2) secret sharing scheme for enrollment of fingerprint in the system and the minutiae extraction algorithm for pattern matching purpose. If we compare existing biometric systems with the biometric systems including secret sharing, then we come to know that the biometric system with secret sharing is much better than existing systems. Following table shows the comparison.

**Table 1. Comparison of Existing Biometric System and Biometric System with Secret Sharing**

| Parameters | Existing Biometric System | Biometric System with Secret Sharing |
|---|---|---|
| Accuracy | Low | High |
| Overhead | Low | Moderate |
| Irreversibility | Computationally hard to reconstruct the original biometric template from the stored reference data, i.e., the protected template | Easy to generate the protected Biometric template. |
| Unlink ability | easy to generate the protected Biometric template. | Protected templates should not allow cross-matching |

## 1.2 Visual Cryptography [2]

Visual cryptography (VC) is a secret-sharing scheme which uses the human visual system for performing operations. Naor and Shamir introduced Visual Cryptography (VC) in 1994 [2]. Naor and Shamir derived the scheme that specifies how to encode a single pixel. This scheme is described in the figure 2 given below.

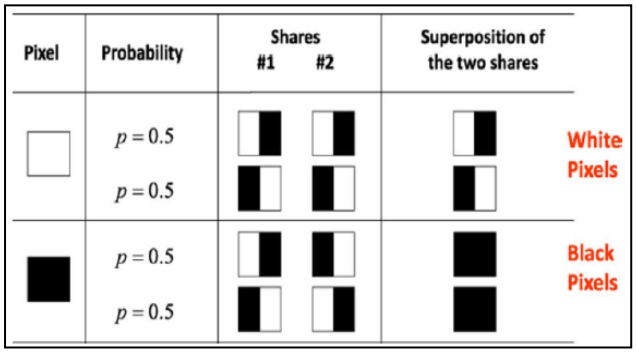


**Fig 2:Visual Cryptography**

The above figure illustrates that a pixel P gets divided into two shares according to the black and white pattern. For creating the shares, vertical shares are used. The created shares define the possible combinations of black and white rows. By superimposing these shares we can get the original secret image. All this can be done with human visual system.
There are number of visual cryptographic schemes which are described below.
1: (2, 2) – In this scheme, a secret image is divided into two shares and by stacking those shares one can reveal the secret. Here, both the shares are important to reveal the secret.

2:( 2, n) – In this scheme, a secret image gets divided into n shares and out of those n shares, any two random shares can reveal the secret.

3 :(n, n) – This scheme illustrates that a secret image is divided into n shares and the secret can be revealed if and only if, all the n shares are taken into consideration.

4:(k, n) – In this scheme, a secret gets divided into n shares and out of those n shares any randomly chosen k shares or group of k shares can reveal the secret.

# 2. RESEARCH METHODOLOGY

This paper proposes a method to enhance security and privacy in fingerprint based biometric system using secret sharing. The method includes merging of biometrics[12] feature like fingerprint and secret sharing. The idea behind this method is – the input for the proposed method will be a fingerprint image taken from user. This image will be a secret image. The secret image then divided into two shares, share 1 and share 2. Out of these, first share will be provided to the user in user's ID card and the second share will be stored in the database. By superimposing the two shares, secret image can be revealed. Creation of share is for getting the sample of fingerprint from user so that the fingerprint taken from user will be stored in the database. Next time when user will give a fingerprint, the fresh image given by user will be matched with the image stored in the database. The minutiae extraction algorithm is used for pattern matching of fresh image and the database image. Minimum 90 points will be taken into consideration for minutiae matching. If these 90 points will get matched, then the user will be a valid user. Two algorithms are used in the proposed work – (2,2) secret sharing algorithm[12] and minutiae extraction algorithm. Use of these two algorithms will sort out two problems such as falsification and costly maintenance of large databases.

## 2.1 (2,2) Secret Sharing

In 2 out of 2 secret sharing method[12] , a secret image gets divided into two shares. For revealing the secret image, two shares should be superimposed. The X-OR method is used for superimposing the shares. The X-OR algorithm is given below-

```
S=size (Input image)
For i=1 to S
If (pixel==1)
If (randomNumber==1)
Share1=[1  0]
Share2=[1  0]
Else
Share1=[0  1]
Share2=[0  1]
Else
If (randomNumber==1)
Share1=[1  0]
Share2=[0  1]
Else
Share1=[0  1]
Share2=[1  0]
End
End of Loop
```

(2,2) secret sharing is used in this paper to have more security and privacy of the data. This method is more advantageous than any other traditional authentication system. The working of (2,2) secret sharing is represented by the following figure 3.

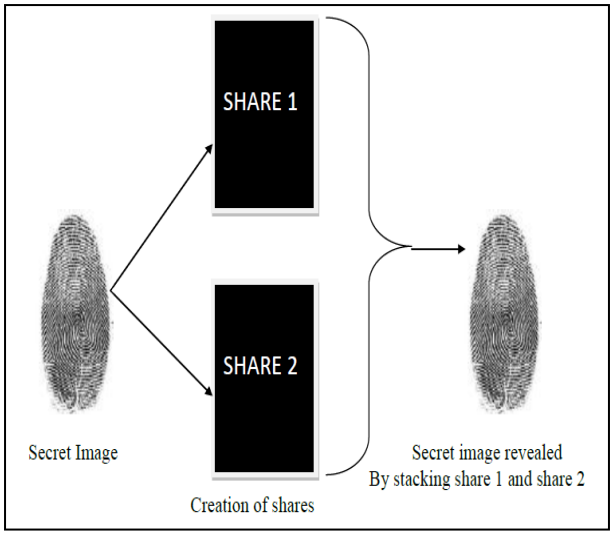


**Fig 3 : (2, 2) secret sharing**

Following figures figure 4 and figure 5 show how construction and reconstruction of shares is done by (2, 2) secret sharing method.

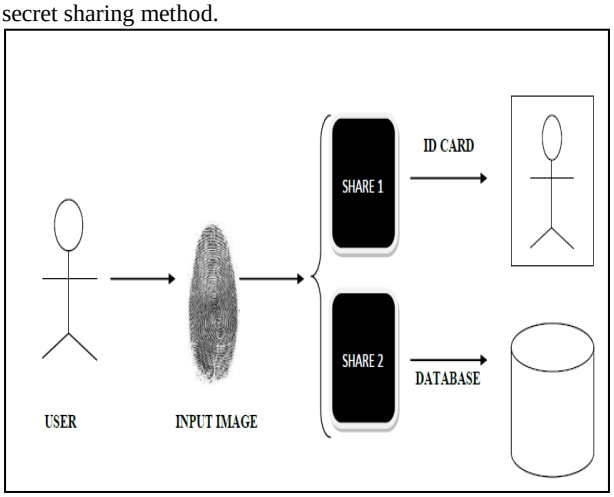


**Fig 4 : Construction of shares**

In the above figure, an input image gets divided into two shares where one share will be provided to the user and remaining share will be stored in the database.

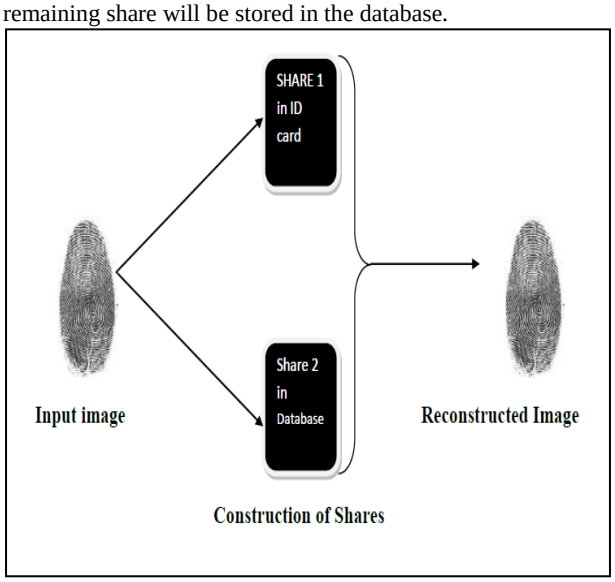


**Fig 5 : Reconstruction of shares**

In the above figure, the input image which is considered as a secret image, can be revealed by superimposing the two shares, that is – By combining share 1 and share2 we get reconstructed image as 'share12' where,

share12=bitor(share1, share2);

share12 = ~share12;

Actual working of the biometric system is illustrated below-

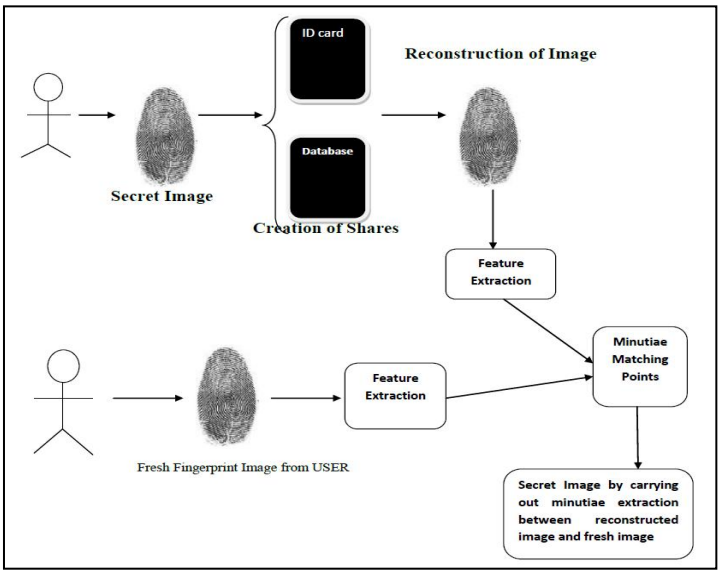


**Fig 6 : Working of biometric system**

## 2.2 Minutiae Extraction

Minutiae extraction algorithm is used in this paper for pattern matching of the secret image and fresh image taken by user. The minutiae extraction algorithm is given as below –

Step 1: Scan the image from top to bottom, left to right order by following only ridges

Step 2: Find the 0-1 transition, calculate the width of the ridge by noting the 1-0 transition

Step 3: Move to the next row and follow the same ridge. Note the width.

Step 4:If the width >=width in previous row there may be a top to bottom valley bifurcation .Call the bifurcation function to check if it is a minutiae point

else

If the width =< width in previous row there may be a bottom to top ridge bifurcation. Call the bifurcation function to check if it is a minutiae point

Step 5: Continue with the next row and repeat this for all the ridges in the given image or until maximum number of minutiae points have been obtained.

# 3. EXPERIMENTAL RESULTS

## 3.1 Construction of shares

In this phase, the input image gets divided into two shares, share 1 and share 2 respectively. The shares created are double the size of original image as pixel expansion is done. All the results shown in this paper are implemented by using MATLAB 2012 software.

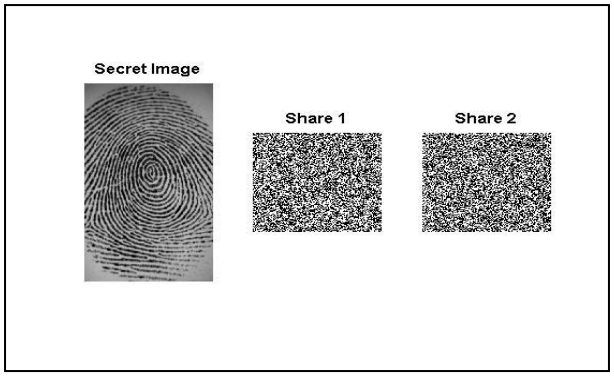


**Fig 7: Construction of shares**

## 3.2 Minutiae extraction and Minutiae matching

In this phase, the minutiae extraction will be done on both, the original image and the reconstructed image. The red points indicate ridge bifurcation and blue points indicate valley bifurcation.

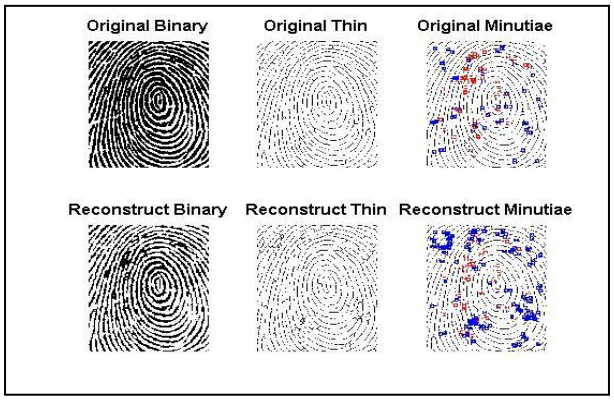


**Fig 8: Minutiae extraction on original image and reconstructed image**

After Minutiae Extraction, Minutiae matching will be done so that the reconstructed image and fresh image should get match with each other.

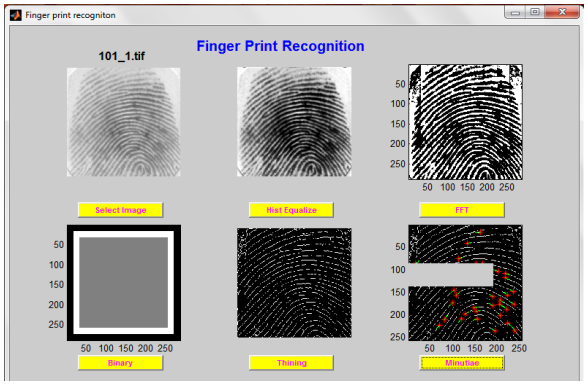


**Fig 9: Minutiae extraction process**

If the minutiae of reconstructed image and fresh image will get match with each other, then the result will tell us that the person is valid.

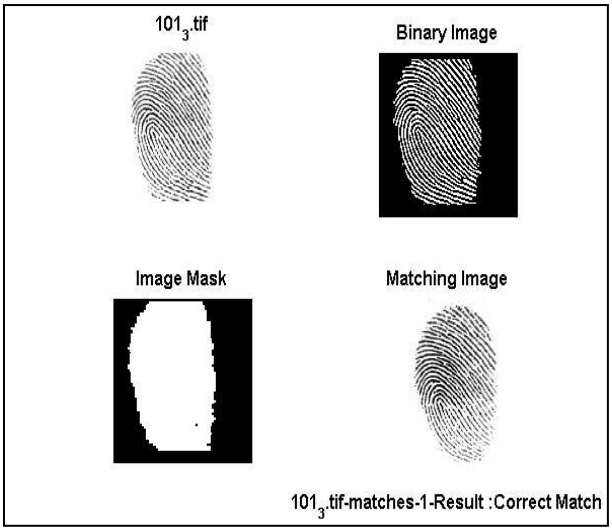


**Fig 10: Minutiae matching**

## 3.3 Comparative analysis of Traditional biometric system with proposed biometric system

Following table shows the comparison of traditional biometric system and biometric system with secret sharing on the basis of experimental results.

**Table 2. Comparison of traditional biometric system with proposed biometric system**

| Parameters | Traditional biometric system | Biometric system with secret sharing |
|---|---|---|
| Space Complexity | O(n) | O(1) |
| Time Complexity | O(n) | O(n) |
| Security | Less | More |
| Database Size | Dependent on number of users | Independent on number of users |

## 3.4 SSIM of (2, 2) secret sharing

The SSIM stands for Structural Similarity Index between two images. In this paper it is used to check similarity between original image and reconstructed image. Table 3 shows SSIM between original image, reconstructed image and share1, share2.

**Table 3. SSIM analysis : (2, 2) secret sharing**

| Secret Image | SSIM : Reconstructed image and secret image | SSIM for share1 | SSIM for share2 |
|---|---|---|---|
| 101_2.tif | 0.9040 | 0.0283 | 0.0283 |
| 102_2.tif | 0.8605 | 0.0281 | 0.0282 |
| 103_5.tif | 0.8805 | 0.0283 | 0.0284 |
| 104_2.tif | 0.8695 | 0.0281 | 0.0282 |
| 105_2.tif | 0.8597 | 0.0282 | 0.0283 |
| 106_6.tif | 0.8656 | 0.0282 | 0.0282 |
| 107_6.tif | 0.8229 | 0.0287 | 0.0287 |

Following graphs show the representation of SSIM of reconstructed image and SSIM for share1 and share2.

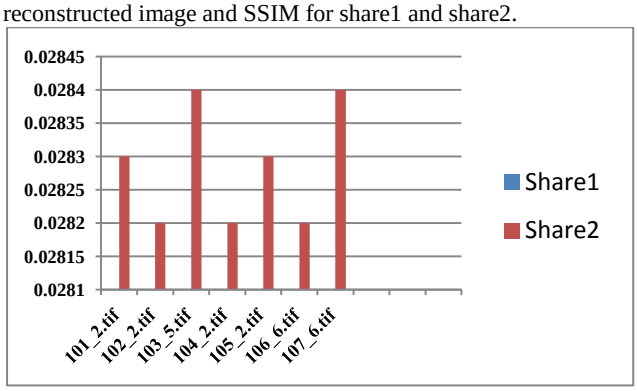


**Fig 11: Graph for SSIM of share1 and share2**

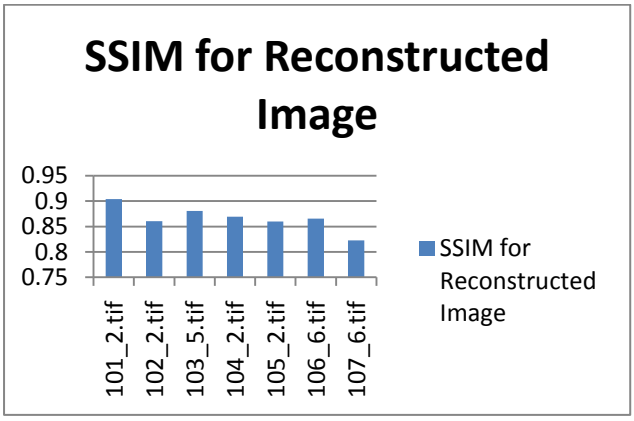


**Fig 12: Graph for SSIM of reconstructed image**

## 4. CONCLUSION AND FUTURE SCOPE

This paper implemented (2, 2) visual cryptography to overcome the issues like falsification and costly maintenance of large database. This implementation resulted in reduction of the time and space complexity of a system. The experimental results show that space complexity required for proposed biometric system is O(1) which is very less as compared to traditional biometric system. So, this paper concludes that applying (2,2) visual cryptography not only reduced the time and space complexity but also amended the biometric system.

## 5. ACKNOWLEDGMENTS

I have a great pleasure in presenting this paper. I have completed this paper under the guidance of Prof. Sonali Patil madam. I would like to express my sincere thanks and gratitude to my guide for her guidance and support. I would like to special thanks to entire ME (CE) Department for providing good infrastructure along with good facilities and support.

## 6. REFERENCES

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

[2] Noar M., Shamir A., 1995. Visual cryptography. Advances in Cryptography. Eurocrypt'94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag. 1 – 12.

[3] Jain A., Hong L., Pankanti S., Bolle R.,. An Identity Authentication System Using fingerprints. Department of Computer Science, Michigan State University, USA. 1997,pp 1- 66.

[4] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[5] Wu, HC and Chang, CC, "Sharing Visual Multisecrets Using Circle Shares," Computer Standards & Interfaces, Vol. 28, pp. 123-135. 373, 2005.

[6] Y.V. Subba Rao, Ms. Yulia Sukonkina "Fingerprint based authentication application using visual cryptography methods (Improved ID card),' , IEEE TENCON 2008, pp 1-5.

[7] N. Askari, C. Moloney, H. M. Heys "Application of Visual Cryptography to Biometric Authentication", Newfoundland Electrical and Computer Engineering conference, 2011

[8] Mrs. A. Vinodhini, M. Premchand, M. Natarajan "Visual Cryptography Using Two Factor Biometric system for Trust Worthy Authentication", IJSRP 2012, vol. 2, Issue 3.

[9] R. Mukesh, V. J. Subashini "Fingerprint based authentication System Using Threshold Visual Cryptographic Technique", IEEE ICAESM 2012

[10] Sonali Patil and Prashant deshmukh, "An Explication of Multifarious Secret Sharing Schemes", International Journal of Computer Applications (0975 – 8887), Volume 46– No.19, May 2012

[11] Sonali Patil, Janhavi Sirdeshpande and Kapil Tajane, "Analysing Secure Image Secret Sharing Schemes based on Steganography", International Journal of Computer Engineering and Technology, Volume 4, Issue 2, pp.172-178, March-April 2013

[12] Sonali Patil, Kapil Tajane and Janhavi Sirdeshpande, "Secret Sharing Schemes for Secure Biometric Authentication", International Journal of Scientific & Engineering Research, Volume 4, Issue 6, ISSN 2229-5518 June-2013

[13] Sonali Patil and Prashant Deshmukh, "Enhancing Security in Secret Sharing with Embedding of Shares in Cover Images", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 5, ISSN (Online) : 2278-1021, ISSN (Print) 2319-5940 May 2014