SECRET SHARING SCHEMES FOR SECURE BIOMETRIC AUTHENTICATION

Sonali Patil, Kapil Tajane, Janhavi Sirdeshpande

Abstract— There are some application areas where increasing concerns over personal information in computer system has increased interest in computer security. Increasing access to the internet and information resources has a great impact in our everyday life and in making people more dependent on computer systems and networks. This dependency has brought many threats to information security. Thus authenticity of the user becomes major issue in today's internet applications. As a result, secure mechanisms are required to protect computers and important information against vulnerabilities like ID spoofing and unauthorized access to computer resources. To solve this problem, this paper proposes a fingerprint based authentication system using visual cryptography methods. In the analysed system the fingerprint template gets divided into two shares with the help of the basic visual cryptography techniques, keeping one with the participant in the form of ID card and saving the other one in the database. This share kept in the database will be the same for all participants. This kind of approach solves two major problems related to fingerprint based system such as falsification and costly maintenance of large fingerprint database.

Index Terms— Authentication, Biometric, Cryptography, Data Security, Secret sharing, Steganography, Visual cryptography.

1 INTRODUCTION

SECURITY is an important issue in information technology. It is an important issue which is ruling the internet world today. Study of mathematical techniques and its various aspects are main criteria in cryptography. Confidentiality, security, authentication are main issues in security. Visual cryptography and visual secret sharing are used to share a secret. Sensitive and important data can be shared secretly using visual secret sharing method. The secrets are encrypted and are shared to different participants. The participant's shares are decrypted to reconstruct the secret. In (k, n) scheme t shares are needed to reconstruct the original secret. Single participant share is not valid, only when t shares are combined the original secret is reconstructed.

Shamir [1] developed (k, n) threshold scheme, where a dealer encrypts and divide the secret into n number of shadows. This scheme is proposed in the year 1979. The dealer then distributes the shadows to the authorized participants. Any t out of n, authorized participants can cooperate to reveal the secret data with their corresponding shadows.

Visual secret sharing developed by shamir[1] from the (k, n) – threshold concept. Secret image is encoded into random images named as shadows, during transmission the shadows are transmitted instead of secret.

- *Sonali Patil is pursuing Ph. D. from AmravatiUniversity and currently working as Assistant professor at PCCOE, Pune, India, PH-9226094990. E-mail: sonalimpatil@gmail.com*
- *Kapil Tajane is currently pursuing masters degree program in Computer Engineering from PuneUniversity, India, PH-9823400036. E-mail: kapiltajane@gmail.com*
- *Janhavi Sirdeshpande is currently pursuing masters degree program in Computer Engineering from PuneUniversity, India, PH-8888843856. E-mail: janhavi26.sirdeshpande@gmail.com*

1.1 Secret Sharing

Due to fast growth of Internet applications, digitized data becomes more and more popular. Because of the ease of digital duplication and tampering, data security becomes an important issue nowadays. In certain application cases, 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) proposed first the concept of (k, n) threshold secret sharing to solve this problem. The scheme is designed to encode a secret data set into n shares and distribute them to n participants, where any k or more of the shares can be collected to recover the secret data, but any k -1 or fewer of them will gain no information about it.

Secret sharing 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 one type of secret sharing scheme there is one dealer and n players. The dealer gives a share of the secret to the players, but only when specific conditions are fulfilled will the players be able to reconstruct the secret from their shares. The dealer accomplishes 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 (sometimes it is written as an (n, t)-threshold scheme).

1.2 Biometrics [2]

Biometrics is the detailed measurements of the human body. Biometrics deals with automated methods of identifying a person or verifying the identity of a person based on physiological or behavioral characteristics. A comparison of some biometric techniques made by A. Jain et al. in 1997 is provided in following figure [2].

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Low	Medium	Low	High	Low
F. Thermo-grams	High	High	Low	High	Medium	High	High

Table 1: Comparison of Biometric Technologies.

1.3 Visual Cryptography [1]

Visual cryptography (VC) is a secret-sharing scheme that uses the human visual system to perform the computations. Naor and Shamir introduced Visual Cryptography (VC) in 1994 [1] .Examination of one share should reveal no information about the image. Naor and Shamir devised the scheme that specifies how to encode a single pixel, and it would be applied for every pixel in the image to be shared. This scheme is illustrated in the figure given below.

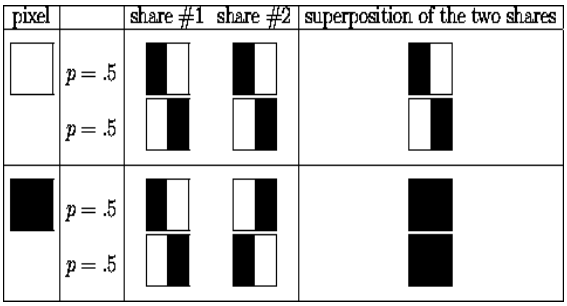


Fig.1.1 Visual Cryptography

A pixel P is split into two sub pixels in each of the two shares. If P is white, then a coin toss is used to randomly choose one of the first two rows in the figure above. If P is black, then a coin toss is used to randomly choose one of the last two rows in the figure above. Then the pixel P is encrypted as two sub pixels in each of the two shares, as determined by the chosen row in the figure. Every pixel is encrypted using a new coin toss.

Suppose we look at a pixel P in the first share. One of the two sub pixels in P is black and the other is white. Moreover, each of the two possibilities "black-white" and "white-black" is equally likely to occur, independent of whether the corresponding pixel in the secret image is black or white.

Thus the first share gives no clue as to whether the pixel is black or white. The same argument applies to the second share. Since all the pixels in the secret image were encrypted using independent random coin flips, there is no information to be gained by looking at any group of pixels on a share, either. This demonstrates the security of the scheme.

Visual cryptography is a cryptographic technique Which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). It involves breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. In this technique n-1 shares reveals no information about the original image. We can achieve this by using one of following access structure schemes [8].

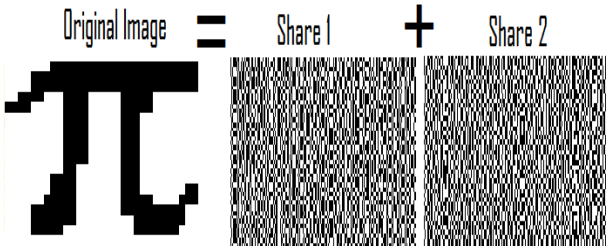
1:(2, 2) – Threshold VCS: This is a simplest threshold scheme that takes a secret image and encrypts it into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

2 :(2, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed.

3 :(n, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that only when all n of the shares are combined the secret image will be revealed.

4:(k, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

E.g. Encryption of the letter PI



1.4 Embedding the image

Digital communication has become an essential part of infra-

structure nowadays, a lot of applications are Internet-based and in some cases it is desired that the communication be made secret. Two techniques are available to achieve this goal: one is cryptography, where the sender uses an encryption key to scramble the message, this scrambled message is transmitted through the insecure public channel, and the reconstruction of the original, unencrypted message is possible only if the receiver has the appropriate decryption key. The second method is steganography, where the secret message is embedded in another message. Using this technology
even the fact that a secret is being transmitted has to be secret Steganography is the art and science of hiding information. There are two main directions in information hiding: protecting only against the detection of a secret message by a passive adversary, and hiding data so that even an active adversary cannot remove it. There are a lot of real applications of Steganography. For example during the 80s some confidential cabinet documents were passed to the English press so Margaret Thatcher had the word processors modified to encode the identity of the user into the word spacing of the documents so the identity of an information source could be found out. The Embedding Process is given as follows:

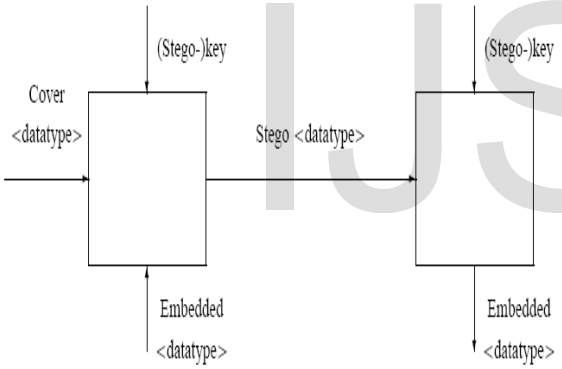


Fig. 1.2 Process of embedding the image

Steganography embeds a secret message in a cover message, this process is usually parameterized by a stego-key, and the detection or reading of an embedded information is possible only having this key. Likewise, Fingerprinting embeds separate mark in the copies of digital media, this embedded information serves as a serial number, it can be detected who supplied this media to third parties.

2 LITERATURE SURVEY

2.1 Fingerprint based authentication application using visual cryptography methods (Improved ID card) [8]

In this paper a (2, 2) secret sharing scheme has been implemented for authentication purpose. An alternative approach of using the fingerprints is presented in this paper, this paper solves two major problems related to fingerprint based automatic access control systems which are falsification and the costly maintenance of the large fingerprint database. In the proposed application an input fingerprint image is divided into two shares with the help of the basic VC techniques, keeping one with the participant in the form of ID card and saving the other one in the database. This share kept in the database will be the same for all of the participants. While accessing, stack the corresponding shares together and compare the obtained image with the provided fresh fingerprint using any modern minutia extraction algorithm. In our application the administrative database will store the integer seed which will be used to generate the set of the required random permutations. Thus the problem of storing large sequences of random numbers in database will be avoided. Moreover the shares of the participants will be stored in their ID cards and the administrator will have to maintain the database where only the dummy share and the integer seed will be stored. For entrance the participant will provide her share in the form of ID card, which will be met by the system. Using the reverse permutation, dummy share and applying the VC techniques system will generate the image of the fingerprint provided by the participant during the registration. This image will be compared with the newly provided fingerprint using any of the modern minutiae extraction algorithms. If the results of the comparison will match, entrance will be allowed,

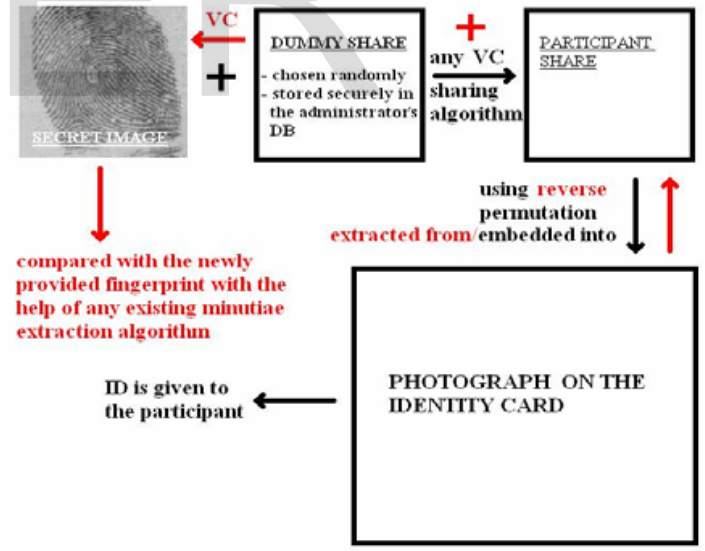


Fig. 2.1: Registration and authentication process.

2.2 Application of Visual Cryptography to Biometric Authentication [9]

In this paper, visual cryptography and some of its schemes are reviewed. This paper reviews and applies visual cryptography, a perfectly secure method of keeping images secret, for possible use in biometric identification and protection. The basic concept of visual cryptography is to divide secret images

into random shares. Decryption is performed by superimposing the shares. Hence the process does not require any special software or hardware device for cryptographic computations. This paper also introduces techniques of secret sharing i.e.
(2, 2) secret sharing scheme, threshold secret sharing scheme and multiple secret sharing scheme. This paper also concludes that which technique will be better for secret sharing purpose. The fingerprint is the most common human biometric characteristic that has been used for personal identification. Results obtained from comparing different biometric traits show that: the fingerprint has a high value in factors like permanence, distinctiveness and performance, and medium value in universality, collectability and acceptability, while the handwritten signature has the lowest value in universality, distinctiveness, permanence and performance. For improving security, reducing fraud and enhancing user convenience, biometric systems require the process of enrolment, verification and identification. In enrollment, the biometric template will be collected and stored in a database for eligible users. Verification is the process of confirming the authenticity of a biometric sample. Finally, identification is the process in which the identity of a biometric sample in a database is determined. Protecting and securing biometric templates in the database are of great importance to prevent systems from being vulnerable to some attacks. Data hiding techniques, such as visual cryptography can enhance the security by embedding additional information in biometric images. Using the basic scheme of visual cryptography for securing fingerprint authentication is suggested in [8], [9], [11].

2.3 Fingerprint Based Authentication System Using Threshold Visual Cryptographic Technique [11]

In the proposed paper the fingerprint template is divided into two or more shares using visual cryptographic technique followed by compression. One of these shares is stored into the server and the remaining shares are given to the users. Only these two participants who possess these transparencies can reconstruct the secret (biometric template) by superimposition of shares. This kind of approach solves two major problems related to fingerprint based automatic access control systems such as falsification and costly maintenance of the large fingerprint database.
The function of the existing fingerprint authentication usingvisual cryptography, when one share of the image from ID card is received, it searches the Database in the Data Server and retrieves the other share of the image and reconstructs the image by superimposition of these two shares. From the retrieved image above, minutiae are extracted.

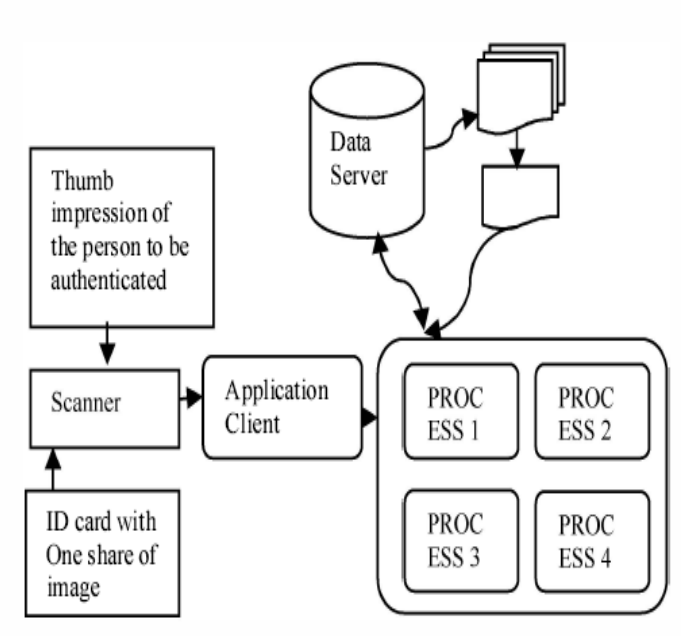


Figure 2.2 : Fingerprint Based TVC authentication System

During authentication the fingerprint received through online scanner is also processed and minutiae extracted. The output of the above two processes are compared. If found matching, person is authenticated. The disadvantage of the existing method is that since only two shares are available it will be easy for any intruder to reconstruct the image with one share that is available on the card.
The general block diagram for the proposed system is given in the figurel. There are four major processes to be done during authentication . They are :

Process 1 When one share of the image from ID card is received, it searches the Database in the Server and retrieves t-l shares of the image and reconstructs the image using Threshold Visual Cryptography (TVC) Techniques.

Process 2 From the retrieved image above, minutiae extracted.

Process 3 Thumb impression received through online scanner is processed and minutiae extracted.

Process 4 Minutiae output of Process 2 and Process 3 are compared. If found matching, person is authenticated.

In the proposed approach the secret image is divided into n-shares, which are printed into transparencies (shares) and can be stored into N back end servers. Only these participants who possess the transparencies can reconstruct the secret image by superimposition of shares.

3 ANALYTICAL STUDY

3.1 2-out-of-2 Secret Image Sharing Scheme [11]

The basic idea of visual cryptography can be illustrated with the 2-out-of-2 scheme. In the 2-out-of-2 scheme, every secret pixel of the image is converted into two shares and recovered by simply stacking two shares together. This is equivalent to using the OR operation between the shares. In the (2, 2) secret sharing scheme, 4 subpixels are generated from a pixel of the secret image in a way that 2 subpixels are white and 2 pixels are black. The pixel selection is a random selection from each pattern.

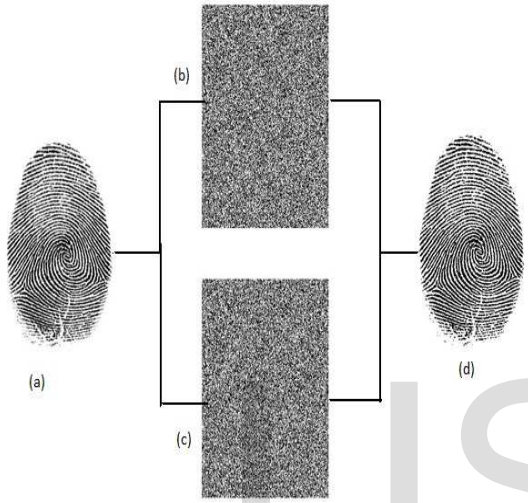


Fig. 3.1. Example of a (2,2) secret sharing scheme: (a) Secret fingerprint image (b) First share (c) Second share (d) Reconstructed fingerprint image

Drawbacks of (2, 2) scheme:

The drawback of (2, 2) secret sharing method is the limitation in the number of biometric samples. The ID card requests one secret share for each biometric template. However, increasing a user's biometric samples or using different types of biometric samples in a template can lead to increasing the accurancy and security in an authentication system. Moreover, it makes biometric systems spoofing more difficult. Further, fingerprint authentication systems may have thousands of users and it is therefore desirable to minimize the cost and capacity of storing biometric templates in a database.

3.2 Multiple secret sharing scheme

In this paper, the multiple secret sharing scheme is analysed for biometric authentication as it is more secured than (2, 2) secret sharing scheme. The following figure shows how exactly multiple secret sharing works.

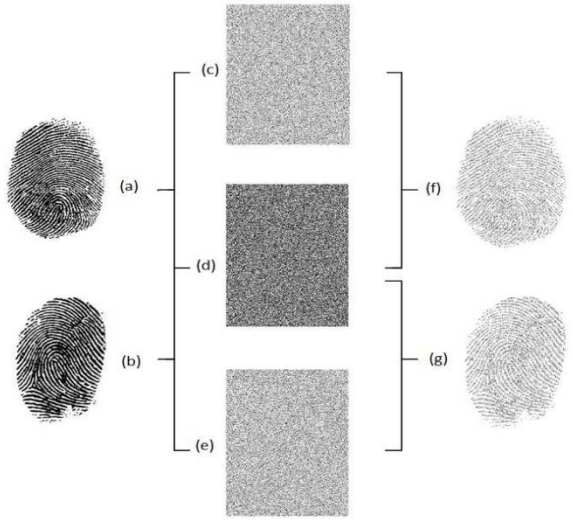


Fig. 3.2. Example of a multiple secret sharing scheme: (a) First secret fingerprint image (b) Second secret fingerprint image (c) Share A (d) Share B (e) Share C (f) Reconstructed secret 1 (g) Reconstructed secret 2.

How drawbacks of (2, 2) scheme will be overcome by multiple secret sharing schemes:

Using the multiple secret image sharing algorithm is one way to improve the system. In this process, two fingerprint images are given to the multiple secret sharing algorithm as secret images. After generating the shares, one of the shares could be embedded in an ID card, and the second share will be kept in the database with the third share being derived by rotation of the share which is stored in the database. So there is no need to store the third share in an ID card or in a database. In authentication, inserting the valid card into the system results in the stacking of corresponding shares and ultimately revealing the two fingerprint images. Entrance will be allowed if the comparision and matching of the newly provided fingerprints stored as the secret images with the physically obtained fingerprints are close together. In this scenario, an unauthorized user does not have access to the system. In addition, if the card is lost or stolen, it cannot be used because of the biometric detection technique.

By using a rotation technique in a way that binary images divide into two random, meaningless shares, according to their encoding process. The first secret image becomes visible by stacking the first and second shares and the second secret is revealed by rotating counter clockwise the pixel groups of the first share by θ (theta) and stacking it with the second share.

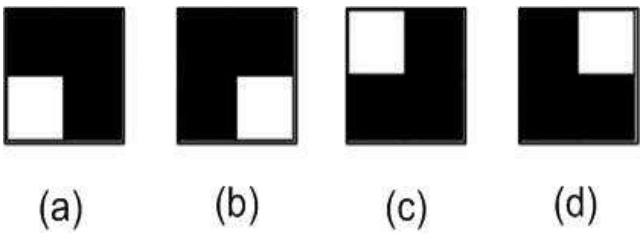


Fig. 3.3. Example of four possible patterns to be assigned in multiple secret sharing scheme for first share

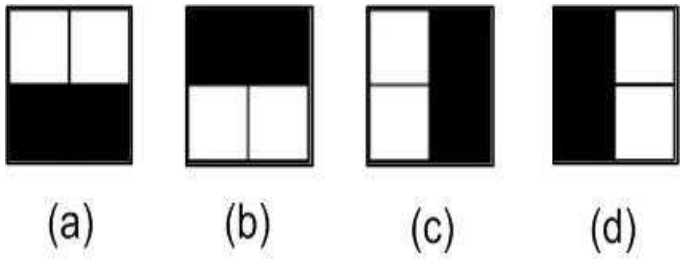


Fig. 3.4. Example of four possible patterns to be assigned in multiple secret sharing scheme for second share

Advantages of multiple secret sharing over (2, 2) scheme:

Applying multiple biometric templates for authentication can increase the security and is more efficient in terms of cost of storage, database capacity and bandwidth.

4 Comparative Analysis

SCHEMES / PARAMETERS	(2, 2)	(t, n)	(n, n)
Time Complexity	Low	High	High
Space Complexity	O(1)	O(t)	O(n)
Accuracy	High	Moderate	Moderate
Security	Low	High	Quite High
Cost Efficiency	High	Moderate	Low
Ideal	Yes	Yes	Yes

5 Conclusion

The biometric authentication system using secret sharing is secure against biometric template attack done at server side. The problem of falsification of the finger will be overcome because the entrance will succeed only if the participant will provide the ID card. There is no need for the administrator to maintain a large database of the finger- prints. The visual cryptography methods provide the security, accuracy and integrity of fingerprint templates in a system. The approach proposed in this report is efficient by utilizing the BIOMETRIC image from user and steganographing it with ID card. As the amount of data to be stored in the database increases, the risk associated with database misuse increases. As a result, the issue of database security and in-tegrity continues to cause several challenges and its necessary that further research be conducted in this direction. The approach proposed in this paper can be easily extended to other biometrics such as facial images, iris etc.

References

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

[2] 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.

[3] Stinson D.R., Tavares S.,. The Pseudo-Random Number.Selected Areas in Cryptography. 7th Annual International Workshop, Waterloo,Ontario, Canada. 2000,pp 100 - 101.

[4] Tsai e.S., Chang e.e., Chen T.S.,. Sharing multiple secrets in digital images. Department of Computer Science and InformationEngineering, 2001 Taiwan. ppl - 8.

[5] Bistarelli S., Boffi G., Rossi F., Computer Algebra for Fingerprint Matching. Universita"G. d'Annunzio", Dipartimento di Scienze, Pescara, Italy. 2003.,ppl- 10.

[6] Davide Maltoni . Handbook of Fingerprint Recognition. 2003,ppl- 366.

[7] Subba Rao Y.V.,. Presentation on Visual Cryptography and Its Applications. Department of Computer and Information Sciences, University of Hyderabad, India.2007,ppl- 42.

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

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

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

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