ISSN:0975-9646

An Automated System for Signature Recognition and Authentication from Multishare Based Image Database

Sharayu S. Sangekar[1] , D.C.Dhanwani[2]

[1]*Student ME 2nd CSE P.R.Pote(Patil) College of Engineering & Management ,Amravati.*

[2] *Assistant Professor P.R.Pote(Patil) College of Engineering & Management ,Amravati*

***Abstract*- This paper emphasize on, how to improve security of biometric systems with the help of signatures using multilayer multishare approach of hierarchical visual cryptography. Hierarchical visual cryptography is defined on the basis of visual cryptography. Here we propose model, which highlights a novel approach of An Automated System for Signature Recognition and Authentication from Multishare Based Image Database. It creates shares of a signature image and achieve its encryption/decryption after going through visual cryptography. The overall effort of the proposed scheme is the achievement of creating multiple shares at multiple level. Our objective is to improve security, accuracy reliability and efficiency of signature image using hierarchical visual cryptography.**

Keywords- Visual Cryptography, Handwritten Signature, Multi-layer Multi-Shares, Hierachical Visual Cryptography, Signature Recognition.

1.INTRODUCTION

Hierarchical Visual Cryptography (HVC) is defined on the basis of Visual Cryptography(VC). Visual Cryptography is a technique which encrypts the image and converts it into unreadable format and by decrypting the image, original secret image is obtained. Encryption is the process of transforming the image into some other image using an algorithm so that any unauthorized person cannot recognize it [1].Visual cryptography is extended up to secret sharing, Visual secret sharing encrypt a secret image into transparent shares such that stacking a sufficient number of shares reveals the secret image without any computation [2].

Visual cryptography Scheme(VCS) algorithm's efficiency is very critical factor and reliability and level of security are some more metric which we need to consider while designing a VCS algorithm .The VCS system should be reliable enough such a way that intruders are not able to read the original image. One of the important functional requirement of any VCS system is size of shares which should be same as that of original image to prevent doubt for unauthorized user [3].

Secret Sharing permits sharing secret info among a bunch of participants such secret writing is potential providing all the participants unit gift with their shares. Secret ar divided into any choice shares. a vicinity of secret info is termed a share. whereas secret writing the information, it's needed to need all the shares on transparency then manufacture them in correct order. There unit varied secret sharing schemes.

Nowadays, human identifications are necessary for our routine activities such as entering any secure locations besides the many other applications. To that end, higher security levels need with easier user interaction which can be achieved using biometric verification. Biometric verification helps us to identify people based on their extracted physical or behavioral features. These features should have certain properties such as uniqueness, permanence, acceptability, collectability, and the cost to employ any biometric. Major analysis issue with biometric systems is change of state of biometric information over time as per the physical conditions or emotional situations of human beings. Signature is found to be the foremost authentic parameter within the field of authentication. Signature is that special pattern provided by human to authenticate himself/herself at secured and private zones.

Signature is the most common authentic entity from the user aspect that has been used earlier in numerous confidential purposes. For improving security of authentication system, the signature should be enrolled and verified. The Proposed authentication system is the replacement for password based authentication[4].

Signatures acts as a strong authentication feature of the signer. But, the manual verification of signatures by humans is tedious job. Therefore, an automated Signature verification system is required which will improve the authentication process and hence provide some secure means for authorization of legal documents. The main objective of signature verification system is to discriminate between two classes i.e. original and forgery.

A growing need for personal verification in many daily applications, signature recognition is being considered with renewed interest. Handwritten signature is the first few biometrics used even before computers. Signatures are widely accepted bio-metric for authentication and

identification of a person because every person has a distinct signature with its specific behavioural feature. This is an alternative approach for fingerprint based authentication mechanism. Fingerprint based authentication mechanism have two major problems: repetitiveness during authentication and non acceptability for some users. Hierarchical visual cryptography encrypts the secret in the form of levels. In this paper, the signature of a person is taken as input which is encrypted using hierarchical visual cryptography. HVC divides input signature image into four resultant shares. The shares appear in scrambled format but upon superimposition, the secret gets revealed.

A signature recognition(SR) system authenticates the identity of any person, based on an analysis of his/her signature through a set of processing steps. The major steps are as follows:

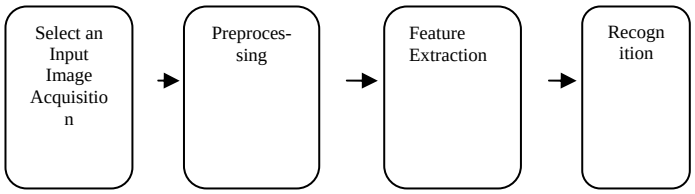

Fig 1.1 Basic Stages of Signature Recognition System

1. **Image acquisition** :- The signatures to be processed by the system should be in the digital image format. The data for the offline signature verification system acquire from various ways like by optical pad, scanner etc. The signature samples are scanned and then scanned images are stored digitally for further processing.
2. **Preprocessing**:- The purpose of Signature pre-processing step is to make signatures standard and ready for feature extraction. Preprocessing is an essential step to improve the accuracy of Feature extraction and Verification.
3. **Feature Extraction**:- The efficiency of a signature verification system mainly depends on Feature extraction stage. Feature extraction techniques should be fast and easy to compute so that system has low computational power. Selected features should discriminate between genuine and forgery signature. Features extracted for static signature verification can be divided as Global, Local and Geometric features.
4. **Recognition**:- Recognition step compares test signature features with genuine signature features based on various clustering techniques and makes a final decision for recognition as authenticate or non-authenticate users[5].

2.LITERATURE SURVEY

Moni Naor and Adi Shamir [2], invented and pioneered visual cryptography] in 1994 at the Eurocrypt conference. The (k, n) Visual Cryptography Scheme can decode the concealed images without any cryptographic computations. It contains black and white pixel only and it was for sharing single secret. The secret image is divided into exactly two random shares i.e. Share1 and Share2. To reveal the original image, both shares are required to be stacked. They use complementary matrices to share a black pixel and identical matrices to share a white pixel. When two shares are superimposed, if two white pixels overlaps with eachother, the resultant pixel will be white and if a black pixel in one share overlaps with either a white or black pixel in another share, the resultant pixel will be black. This implies that the superimposition of the shares represents the Boolean OR function.

Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson [7] stated that, in visual cryptography scheme(VCS), all n shares have equal importance.They had given a general access structure in 1996, in which given set of n shares is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Any k shares from qualified subset of shares can reveal the secret information, but less than k shares from qualified subset of shares can not reveal any secret information. Even k or more shares from forbidden set can't reveal secret information. It is also for sharing the single secret having black and white pixel only. They analyze the structure of visual cryptography schemes and prove bounds on the size of the shares distributed to the participants in the scheme. They provide a novel technique to realize k out of n threshold visual cryptography schemes. Construction for k out of n visual cryptography schemes is better with respect to pixel expansion than the one proposed in and for the case of 2 out of n is the best possible. The construction for 2 out of n schemes has log n pixel expansion.

Ravi Bhushan Tiwari, Sanjay Sharma and Sidhu [8], developed Biometric authentication System using fingerprint. Fingerprint identification is one of the most important approaches for identification. Fingerprint identification has been publicized because of its consistency and uniqueness over the period of time. Biometric identification process has gained popularity with the recent advancement of computing capability. The uniqueness of the fingerprint and the processing power has gained popularity in various walks of our life for the purpose of authentication and verification.

Eun suk Cho and Yvette Gelogo [9], stated that human iris biometric based identification has attracted the attention of research and development community. Iris recognition is the somewhat accurate form of identification known to man. It is also capable of making a match from a database of over 1 million records in less than a second.

Bansal, Gard, and Gupta [5], proposed a contour matching algorithm; which is used to track the basic pattern in a sample signature and verify it. A contour can be best described as the outline of the signature. They used vector quantization method to extract critical point and then apply the matching algorithm.

Gady Agam[10], proposed another scheme of offline signature recognition which is warping based. He present a new approach for reducing the variation in signature based on curve warping. The input signature image is pre-processed in first stage to convert the signature into curves. The resulting curves are then warped and are compared using a derived metric to determine their similarity. The conversion of signature into curve has done using curve normalization, structural graph representation.

Vahid and Hamid [4], proposed an offline signature verification using LRT and SVM. They used the LRT locally for line segments detection for feature extractions and SVM for classification. The proposed system consisted of the two models (a) Learning genuine signatures and (b) Verification model. Preprocessing phase was shared between learning and verification models. Feature extraction phase includes the line segment detection, line segment existences validation, feature vector extraction and summarization, and feature vector normalization. In the classification phase, they used SVM with Radial Basis Functions (RBF) kernel to achieve the best results.

Coetzer [11], stated that Hidden Markov Model (HMM) is one of the most widely used models for sequence analysis in signature verification. Handwritten signature is a sequence of vectors of values related to each point of signature in its route. He developed a system that automatically authenticates offline handwritten signatures using the Discrete Radon Transform (DRT) and a hidden Markov model (HMM).

Debnath Bhattacharyya and Samer Kumar Bandyopadhyay [12], elaborates that the statistical knowledge is used to perform some of the statistical concepts like the relation, deviation, etc between two or more data items to find out a specific relation between them. Generally, it follows the concept of Correlation Coefficients which refers to the departure of the two variables from independence. In signature verification system, average signature (template) is calculated from previously collected signatures, stored in knowledge base, when new input signature is read, correlation concept is followed to find the distance between the test signature and average signature, then to decide if it is accepted or rejected. .

Vu Nguyen [13], given that when a forged signature comes, its symbolic representation is compared with prototypes stored in database. In other words, Structural approach is based on the relational organization of the low-level features into higher-level structures, and then theses structures are matched with models stored in database. Structural features use Modified direction and transition Distance Feature (MDF) which extracts the transition locations and are based on the relational organization of low-level features into higher- level structures.

Kaewkongka T and his colleague [14], used Hough transform as a basic approach for the task of signature recognition. They applied Hough transform to detect stroke lines from the signature image. The Hough transform is mainly used to extract the parameterized Hough space from the thinning signature as unique feature of signature.They applied the straight line Hough transforms to signature image to map Cartesian coordinates into polar coordinates of radius and angle. The unique feature is extracted by finding the vote's value in the accumulator from the Hough space.

Bharadi and Kekre[15], proposed global as well as grouping based features, for determining information in pixel of the signature.They used Walsh transform to the horizontal pixel distribution and vertical pixel distribution, this transform is fast to calculate.

Zhang [16], have proposed a Kernel Principle Component Self- regression (KPCSR) model for off-line signature verification and recognition problems. Developed from the Kernel Principle Component Regression (KPCR), the self- regression model selected a subset of the principle components from the kernel space for the input variables to characterize accurately each person's signature, thus offering good verification and recognition performance. A modular scheme with subject-specific KPCSR structure proved to be efficient, from which each person was assigned an independent KPCSR model for coding the corresponding visual information.

Proposed Methodology

Proposed methodology consists of encryption and decryption of a signature image

Steps for Encryption and Decryption:-

Step 1- Select Input Image. Input image should be a signature image.

Step 2-Draw signature image or we can directly load signature image from database.

Step 3-Crop effective features adaptively or manually.

Step 4-Create shares at level 0,level 1,level 2 and level 3.

Step 5-Decrypt shares at level 3,level 2,level 1 and level 0.

Step 6-By combining all the shares , we will get an original plain image.

Step 7-Add that signature image to the database.

Step 8-Input another signature image for signature recognition.

Step 9-Original signature image will be accepted and will authenticate an user and forged signature will be rejected.

Step10-Stop.

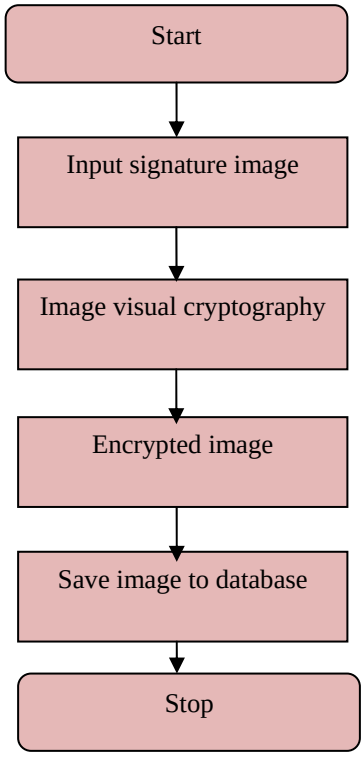

Fig.1.2.Flowchart for encryption of an image

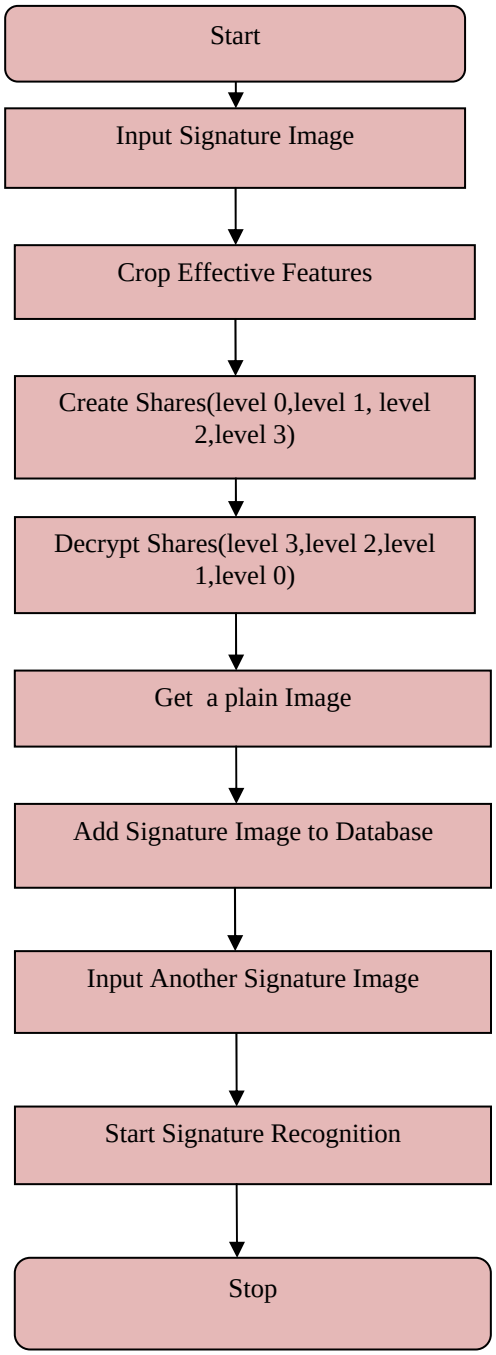

Fig.1.3.Flowchart for encryption and decryption of an image

1.Image Encryption:-

In this phase image is encrypted by using multiple-shared approach. Initially signature is given as an input image which we draw or can be laoded directly from database. Then we can crop the features such as entropy, mean intensity,pure height and pure width manually or adaptively. After that shares of input image will be created at level 0, level 1,level 2 and level 3.Hierarchical visual cryptography is used for creating shares.

2. Image Decryption :-

Proposed image decryption method works exactly opposite as that of the encryption phase. In first step select an encrypted image. Then the image will be decrypted at level 3,level 2,level 1 and level 0.Finally; all the decrypted images are fused together to get a plain image which is same as the given input image

The proposed methodology consists of image on which we have to perform multi-share cryptography. The selected image is encrypted. The encrypted image is to be stored in database. While during performing decryption operation the stored encrypted image from database is to be decrypt. After performing decryption we get the original plain image.

The image which we have given to the system will be stored in an encrypted form. Then the process of image recognition is applied; in this process the image stored in the database is recognised. First the encrypted image in the database is loaded and it is decoded so that it should be visible by naked eyes. then the image in the decoded form and image stored in the database is compared and finally we get the matched image in the form of output.

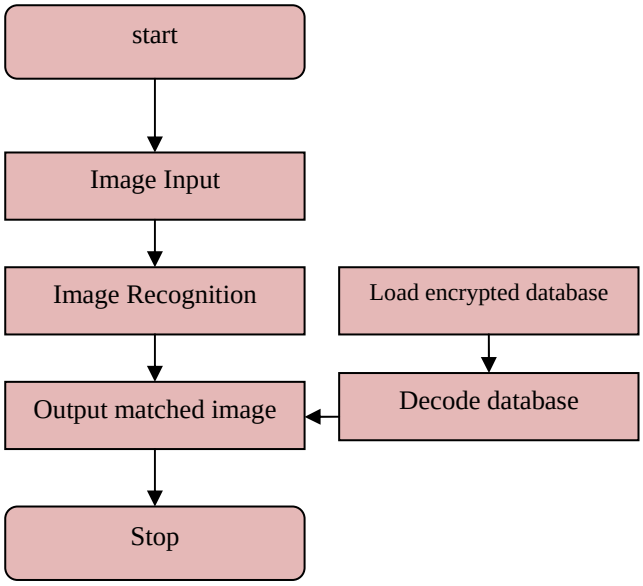

Fig.1.4.Flowchart for signature recognition

Hierarchical Encryption algorithm:-

Level 0 Encryption:-

Step 1: Start
Step 2: Input image
Step 3: Extract RGB channel of an input Image.
Step 4: for i=1 to all pixels
Swap(R(8), G(8), B(8))
from MSB=LSB
LSB=MSB
End.
Step 5: Create share 1 from Red and Green channel
Create share 2 from Blue channel.
Step 6: Save.

Level 1 Encryption:-

Step 1: Start
Step 2: Input images from level 0
Step 3: Extract Red, Green and Blue channels from input images.

Step 4: Extract share 1 from Red, Green channel
Create share 2 from Blue channel
Step 5: Save Share
Step 6: Stop.

Level 2 Encryption:-

Step 1: Input image
Step 2: Input images from level 1
Step 3: Extract Red and Green channels from share 1 of level 1.
Step 4: Extract Blue channel from share 2 of level 1
Step 5: Create share 1 from Red, Green and Blue channels.
Step 6: Save result
Step 7: Stop.

Level 3 Encryption:-

Step 1: Input images from level 2.
Step 2: Extract Red, Green from share 1 and Blue from share 1.
Step 3: Create Red, Green, Blue shares from level 2 shares.
Step 4: Save result.
Step 5: Stop.

- Pixel Swapping Algorithm

Step 1-Start
Step 2-Input Image
Step 3- For i=0 to length(Image)
Step 4- Read Pi
Step 5- $Pi=Pi_{MSB}+Pi_{LSB}$
Step 6- $Pi'=Pi_{LSB}+Pi_{MSB}$
Step 7- Set Pi' to I_E
Step 8- End

Where Pi- pixel value, Pi_{MSB}- MSB of pixel, Pi_{LSB}- LSB of pixel, Pi'-pixel variable for storing swapped result, I_E-new encrypted image.

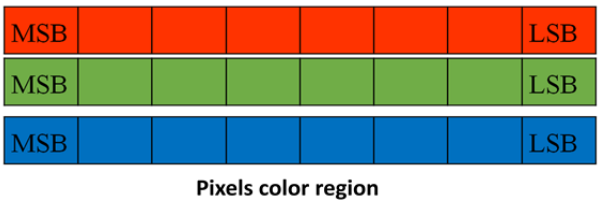

Fig.1.5.MSB and LSB representation of a pixel

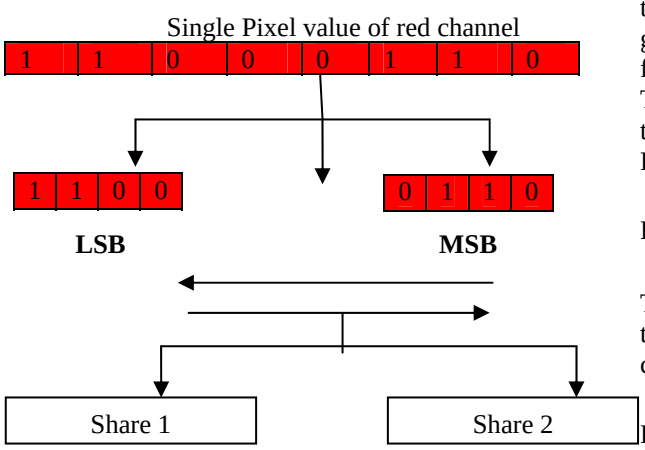

Fig.1.6.Procedure of shares creation

3.EXPERIMENTAL RESULTS

Table 1 -Comparison of Mean intensity of an Input image and Mean intensity of a decrypted Image

Name of Input Image	Mean Intensity	
	Original Image	Decrypted Image
Img1.bmp	0.76863	0.58431
Img2.bmp	0.74510	0.58431
Img3.bmp	0.75294	0.58431
Img4.bmp	0.74902	0.58431
Img5.bmp	0.76863	0.58431

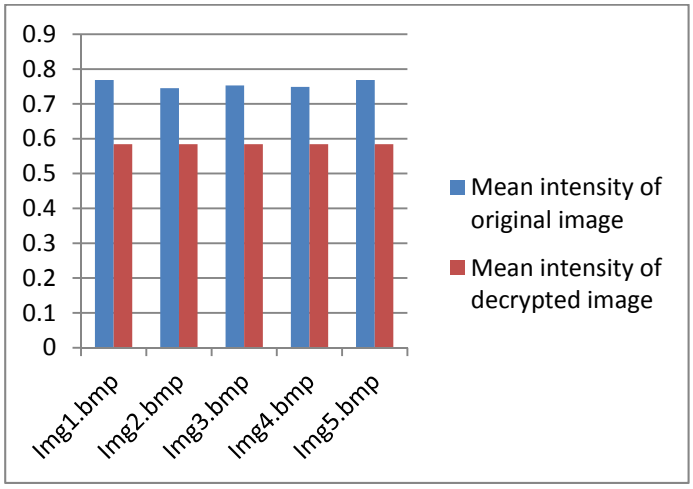

Fig.1.7. Graph shows relation between Mean intensity of an Input Image and Mean intensity of a decrypted Image

Quality Performance Measures In evaluating the performance of a signature recognition system, there are two important factors: the false rejection rate (FRR) of genuine signatures and the false acceptance rate (FAR) of forgery signatures and these two are inversely related.
The FRR is the ratio of genuine test signatures rejected to the total number of genuine test signatures submitted. The FRR called the type I error and is defined as,

$$FRR=\frac{\text{Total number of genuine test signature rejected}}{\text{Total number of genuine test signature submitted}}*100\%$$

The FAR is the ratio of the number of forgeries accepted to the total number of forgeries submitted. The FAR is also called the type II error and is defined as,

$$FAR=\frac{\text{Total number of forgeries accepted}}{\text{Total number of forgeries submitted}}*100\%$$

Table 2- Performance comparison of various signature recognition system

S.No.	Method	FAR(%)	FRR(%)
1.	Our Multishare Approach	0	2
2.	Support Vector Machine	2	4
3.	Enhanced Modified Direction	1.71	2.88
4.	Based on Fuzzy Modeling	12.7	12.7
5.	Virtual Support Vector Machine	16.00	13.00
6.	Modified Dynamic Time Wrapping	20.0	25.0
7.	Hierarchical Random Graph Model	11.6	21.6
8.	Euclidean Distance Model	43.6	38.1
9.	Weighting Factor Based Approach	16.85	3.30
10.	Hybrid Stastical Modelling	22.00	10.00
11.	Two Stage Neural Network classifier	09.81	03.00
12.	Network and Positional Cuttings	0	2.2

4.CONCLUSION

The paper gives a novel idea of signature based authentication using hierarchical visual cryptography. HVC encrypts the secret in three different levels. Shares generated out of HVC are used for authentication mechanism. All shares are high contrast in nature. Signature is considered as an authentication entity in this project. Signature based authentication is found to be powerful than biometric authentication as biometric patterns changes over time. Shares generated with this scheme are random in nature giving no information by visual inspection.

5.FUTURE SCOPE

The concept of Signature recognition can be extended to other biometric identification system like handwriting, and when combined with other biometric aspects such as speech and face recognition can present a far better result than any individual system. On the other hand, we can increase the number and quality of extracted features, and combine between global and local features, because the system performance is mainly depending on the extracted features.

REFERENCES

[1] Adi Shamir,"How to share a secret," ACM N0014-76-C-0366, vol. 22, November 1979.

[2] Naor, M. and Shamir, A.,"Visual cryptography,"In Proc. Eurocrypt 94, Perugia, Italy, May 912, LNCS 950, pp. 112.,2010,Springer Verlag.

[3] Shubhra Dixit,Deepak Kumar Jain, and Ankita Saxena, "An Approach for Secret Sharing Using Randomised Visual Secret Sharing," 2014 Fourth International Conference on Communication Systems and Network Technologies 978-1-4799-3070-8/14 2014 IEEE.

[4] Vahid,Reza, Hamid Pourreza,"Offline Signature Verification Using Local Radon Transform and Support Vector Machines" International Journal of Image Processing (IJIP), Vol. 3, 2009. Ravi Bhushan Tiwari,Sanjay Sharma and Sidhu," Biometric authentication using fingerprint" ,Youth Education and Research(YERT), January 2013.

[5] Bansal, D. Garg, A. Gupta, "A pattern matching classifier for offline signature verification", IEEE 2008, pp.1160-1163.

[6] Mr.M.Venkatesh, Mr.S.Rajesh,"Security Analysis of Visual Secret Sharing Scheme," M.Venkatesh et al, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January-2014, pg. 127-134

[7] Giuseppe Ateniese ,Carlo Blundo and Alfredo De Santis, "Visual Cryptography for General Access Structures", information and computation 129, 86106 (1996), article no. 0076.

[8] Ravi Bhushan Tiwari,Sanjay Sharma and Sidhu," Biometric authentication using fingerprint" ,Youth Education and Research(YERT), January 2013.

[9] Eun suk Cho, Yvette Gelogo," Human Iris biometric Authentication using Statistical Correlation Coefficient", Journal of Security Engineering, March 2011.

[10] G.Agam, "Warping based offline signature recognition", Information forensic and security, Vol.2, issue 3 IEEE 2007, pp.430-437.

[11] Coetzer, Herbst, Preezp,"Offline Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model", EURASIP Journal on Applied Signal Processing, 2004.

[12] Debnath Bhattacharyya, Samir Kumar Bandyopadhyay and Deepsikha Chaudhury,"Handwritten signature authentication scheme using integrated statistical analysis of bi-color images", IEEE ICCSA 2007 Conference, Kuala Lumpur, Malaysia, August 26-29, pp. 72-77, 2007.

[13] Vu Nguyen; Blumenstein, M.; Muthukkumarasamy V.; Leedham G.,"Off-line Signature Verification Using Enhanced Modified Direction Features in Conjunction with Neural Classifiers and Support Vector Machines", in Proc. 9th Int Conf on document analysis and recognition, Vol. 02, pp. 734-738, Sep 2007.

[14] T. Kaewkongka, K. Chamnongthai, B. Thipakom, "Off- Line signature recognition using parameterized Hough Transform ", Proceedings of Fifth International Symposium on Signal Processing and its Applications, ISSPA '99, Brisbane, Australia, 22-25 August, 1999 Organized by the Signal Processing Research Centre, QUT, Brisbane, Australia.

[15] H. B. Kekre, V. A. Bharadi, "Off-line signature recognition Systems" International Journal of computer application, Vol 1, No.27, pp 48-56, 2010.

[16] Bai-ling Zhang, "Off-line signature recognition and verification by kernel principal component self- regression",Proceedings of the 5th International Conference on Machine Learning and Applications (ICMLA'06), 0-7695-2735- 3/06, 2006, 4 – 6.