Proposed Architecture for Enhancing the Efficiency of Security Systems by using Systematic Combination of Different Recognition Systems

Prateek Ranjan
Research Scholar,
NITRA Technical Campus
Ghaziabad, U.P., India

Keshav Jindal
Research Scholar,
NITRA Technical Campus
Ghaziabad, U.P., India

ABSTRACT
Envisaging a future where the interaction between human and a computer has become advanced enough so as to be able to understand the motion of an arm, blink of an eye or even the emotions of a human. With the interaction between humans and computers becoming decidedly easy for us, now is the right time to use such an advanced technology in order to secure our information in computers and private networks. We are well aware of the importance and the money spent in order to either collect information or to protect information. Therefore, in this paper we are proposing the architecture of a security system that uses the gesture and human body action recognition techniques in the efforts of creating a safe, secure and spoof free system for access to critically important information.

General Terms
Recognition System, Gesture Based Security System, Information Security

Keywords
Vein Recognition System, Hand Gesture Recognition, Action Recognition System, Information Security, Face Recognition System, Security System

1. INTRODUCTION
Today, with continuous advancements in technologies, the ability to secure information through unauthorized access is one of the major challenges faced by IT personnel. Major reasons for this increase in unauthorized access to sensitive information are the defects in the existing security systems or the weakness of the security system itself. Hence, effective and secure systems are required in order to make information and data safer from illegal access.

From times of the kings to today, when the most advanced technology exists, information and data are still the most important aspects of life. Along with the rapid increase in technology, the rate of cyber-crime has definitely risen exponentially. The most recent examples of cyber-crime are of the 2014 intrusions in SONY network and the iCloud, both now determined to be the most serious of all time. For the security of our information we are generally relying on the existing Passwords or Individual recognition Numbers (PIN's). However, they are generally not as secure as made out to be and can be easily cracked with the help of simple permutations and combinations. This jeopardizes any individual's personal information, supposing that the right combination is struck at any point of time. Whenever the hacker gets to the right PIN, the entire information or the database becomes compromised and it can be used to any extent without the knowledge of the real person.

Therefore, in today's world the most efficient method to secure information would be with the help of Biometrics where the physiological or the behavioral appearance of an individual is used to identify and authorize them to their information. For the authorization process, biometrical features like irises of eyes, hand gestures, heartbeat recognition, finger prints, vein recognition, action recognition and facial recognition techniques are generally used. The need to design an architectural structure which gives a secured access to information to only those who have authorization to it, is quickly becoming the focus for the IT Industry. Here, we are working on the idea of making a person their own password rather than creating different passwords for different accounts, in turn making the access to information safer and more reliable.

In this paper, we propose architecture for the security of private networks and stand-alone systems with the help of various recognition systems like Action Recognition, Vein Recognition and the Hand Gesture Recognition.

2. EXISTING RECOGNITION SYSTEMS
With the passage of time the need of a good authentication system has been the only thing to have been able to maintain its importance. The need of good authentication is as important as the need of information because if the information is not present, it becomes too arduous to achieve success in any field, be it a business, banking or any science related field and assuming that the information is present, without a proper security system, then it can be used for any means, putting to risk the day-to-day life of people. Therefore, all kinds of authorization systems have to be carefully scrutinized in order to make the information access secure. The existing systems are:

- Personal Identification Number [PIN].
- Finger Print/Palm Recognition System.
- Iris Pattern Recognition System.
- Face Recognition System.
- Vein Recognition System.
- Heartbeat Recognition System.
- DNA Recognition System.

2.1 Personal Identification Number [PIN]

Personal Identification Number is the one of the oldest ways of giving authorization to any user for accessing any information on a network but with rapid and continuous advancement in Security System Technology, the PIN passwords are the easiest way to crack into any kind of computer or network and it is unable to provide any kind of after-login security of the information. This implies that on the occasion of any person obtaining access to the PIN by any means, they can prove very harmful. The biggest agony with the PIN is the task of memorizing the PIN number. Having more than one account essentially means more PIN's which makes information access an almost painful process.

2.2 Finger Print/Palm Recognition System

The Finger Print Recognition is one of the most basic starters of the Biometrics Recognition Systems. With Finger Prints, it is believed that all people have unique finger prints. Earlier, with this type of identification, it was thought to be an exhaustively secure authorization system. Nonetheless, today, with the advancement of Security System Technology, the flaws in finger print recognition system have become more evident. Further, it is not reliable in case the fingers are dry or dirty as it can make mistakes in recognition and besides, with passage of time the accuracy of the machine decreases.

2.3 Iris Pattern Recognition System

The difference between each and every person's Iris patterns has been medically proven, and these prints remain stable for a long duration of time. But, the major problem with this type of identification would be the inability of the machine to identify the pattern correctly for people who wear contact lenses [19]. The cost of an Iris Recognition machine proves to be counter-productive and the scanning is highly time-consuming.

2.4 Facial Recognition System

The Facial Recognition System can be easily implemented with the help of a simple camera and some simple programming skills. Despite this, the major defect with this kind of recognition becomes the effects of changes in light, person's hair, age and other kind of facial expressions on two-dimensional recognition. Certainly, if a person cannot be identified because of a simple change in facial expression, then the whole system will have to be overridden since it would be a lot of trouble for the person to keep the same expression all the time.

2.5 Vein Recognition System

The vein recognition system uses the vein patterns in the fingers and the palms in order to recognize the pattern of the vein. The vein recognition is one of the most advance methods of identification. This method of authentication offers a precisely accurate method of identification, having a false rejection rate (FRR) of 0.01%, and a false acceptance rate (FAR) of 0.00008% or lower [4]. Moreover, it has the contactless identification system contributing to the long life of the hardware which is a tricky business when it comes to the Fingerprint/ Palm print technologies.

2.6 Heartbeat Recognition System

The heartbeat recognition system works on the base of converting the heartbeats into an encryption key using mathematical equations and the electrocardiograph machine (ECG) reading the person's palm vein. This was proved through research done by the Chinese researcher, Chun-Liang Lin at National Chung Hsing University in Taichung, Taiwan. They used two ECG machines and found uniquely different patterns of heartbeats for different people and even the patterns of heartbeats of a single person didn't remain same [18]. This makes Heartbeats more secure and trustworthy for the safety of the system.

Table 1: Comparison of Different Systems

Biometric System's	Accuracy	Cost	Security	Stability
Fingerprint	Medium	Low	Low	High
Facial Recognition	Low	High	Low	Low
Iris Scan	High	High	High	High
Hand Gesture	High	Low	High	Medium
PIN	High	Low	Low	High
DNA Recognition	High	High	High	High
Heartbeat	Low	Medium	Low	Low
Vein Recognition	High	Low	High	High

3. WORKING OF THE TECHNOLOGIES USED IN PROPOSED ARCHITECTURE

Firstly, to understand the working of any of the Biometric System, the need is to come to terms with the general working of the most of the basic Biometric System Architecture.

In Figure 1, the basic working for any of the recognition techniques is shown where firstly the image input is taken from the user and in the second step the image is processed in a computer. All the recognition systems have predefined data sets, also known as Trained Sets, which are matched with the input given by the users of the system. The system responds accordingly to the user's authorization.

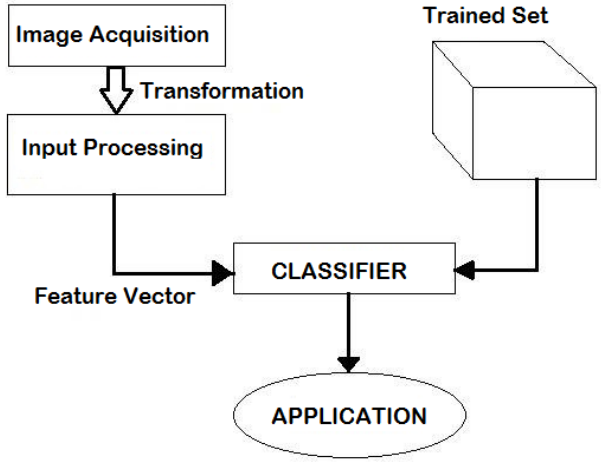

Figure 1: Basic Recognition Model

After getting to know the basic recognition model of any recognition technique, it is very important to understand what are the technologies used in this paper and their working. This paper is all about increasing the efficiency of the security systems with keeping the cost of the whole system in mind. So the used technologies in the paper to propose the architecture are:

- Action recognition.
- Facial Recognition System.
- Vein Pattern Recognition.
- Hand Gesture Recognition.

3.1 Action Recognition

The Action recognition system works with a camera, where it is used to provide the input to the computer and with the help of MATLAB IMAGE PROCESSING, the camera inputs are processed and analyzed from the given trained set. This ultimately helps the system to arrive at a particular result and identify the poses given by the user.

In the proposed system the Action Recognition System is used to monitor the poses of the user and identify his/her actions whether they are safe or not. As shown in the Figure the user's body part are divided into 14 segments [6] and matched with the pre-stored trained sets. Granted that the person's input is matched with the trained set and his/her activities are suspicious then the admin can be alerted for performing a check on the user for his activities.

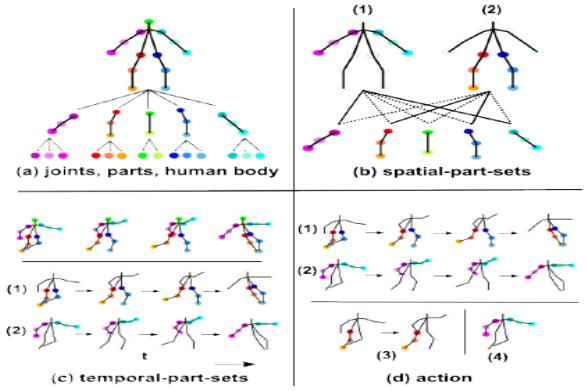

Figure 2: Action Recognition System [6]

Just taking a situation as an example if computer gets input of a person holding the gun then system will generate an automatic alert message for the Administrator of the system for proper action (i.e. to call police or ambulance) to be taken against the impostor.

3.2 Facial Recognition System

Although, Facial Recognition System has been in the list of hot research topics for a long time, yet, at the same time, it cannot guarantee 100% spoof proof authentication to the rightful user of the information. The basic types of face recognition system are Principal Components Analysis (PCA), Linear Discriminant Analysis (LDA), and Elastic Bunch Graph Matching (EBGM) [8].

Here, Facial Recognition system is taken to be working on the technique of Principle Component Analysis (PCA), commonly referred to as the *Eigen Faces*. The PCA works by first investigating the Principle components of the faces provided the gallery images are same and normalized in order to line up the eyes and mouth of the user in the image system. After the investigation, the PCA system is used to reduce the data of the image by a method of compressing and deleting the unnecessary parts of the faces, removing the inessential data from the image, making it of a lower dimension and uncomplicated enough for analysis for matching purposes[8].

3.3 Vein Pattern Recognition

The Vein Recognition System is one of the most accurate and latest methods for the recognition work to be done. This method is based on the technique of tracking the finger and palm veins with the help of Infra-Red Light.

According to the basic working of the proposed architecture of the vein pattern recognition system, it consists of four steps i.e. Image Acquisition, Image Segmentation and Alignment, Image Enhancement and Feature Extraction [3].

In the process of image acquisition, near-infrared (NIR) exposure obtains the high quality image. This special device is developed to acquire the images of finger vein without being affected by ambient temperature. The source of the light is taken to be the LED light. Being a monochromatic light source, the rays of light irradiates from the back of the skin and the image is taken. The major portion of the shadow is finger vein image of light which has irradiated through the human hand [3].

After the image acquisition the step of Image Segmentation and Alignment comes in which the normalization of the image is performed. Because of the portion of the veins in the fingers usually varies across the different parts of the fingers, therefore it becomes necessary to normalize the image before extraction and matching.

Next comes the process of Image Enhancement and Feature Extraction. For the enhancement procedure, the *Bicubic Interpolation* method is taken for enhancing and resizing of the image and in the enhancement process at the final stage, the histogram equation is used in order to enhance the grey level contrast of the image. In the last step of the feature extraction, the main features of the image are extracted from the enhanced image by help of fractal model developed by Mandelbrot, providing a good method to represent the ruggedness of natural surfaces, furthermore, giving us a good tool in order to successfully analyze the image and compress it [10]. After all the four steps the last step is to match the image with the trained set and the input image obtained from the user, to provide the authorization to the user.

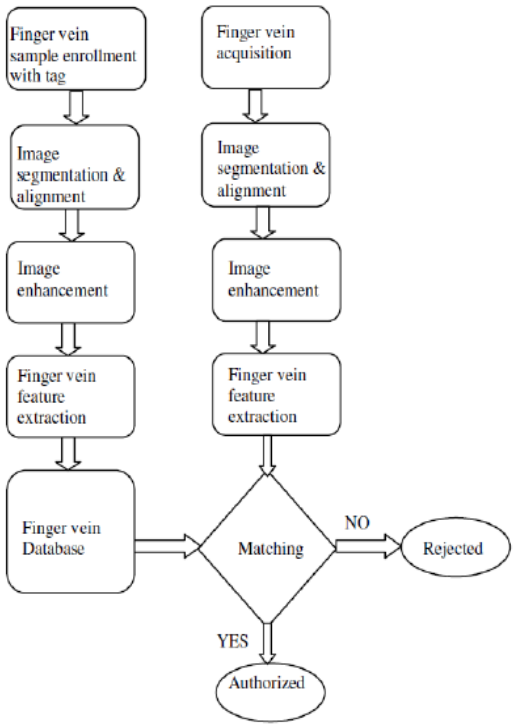

Figure 3: Finger Vein Recognition System [4].

3.4 Hand Gesture Recognition

Using the Hand Gesture Recognition in place of conventional PIN passwords is the idea because usually it hard to spoof as the gesture movements which are stored in the data set will be dynamic i.e. not restricting the user with predefined sets of gesture or actions. The Hand Gesture will be known only to the user and even the admins would not know the passwords. Citing the structure of memory known, the computers saves everything in the form of binary codes, moreover in an encrypted format, it will be greatly troublesome for the unauthorized person to gain access to it as well as to decode it. This makes the hand gesture recognition system more complex to crack in respect of the PIN code cracking. The hand gesture recognition works on these basic four steps [9][11][14].

3.4.1. Image Acquisition

An input image frame is captured from the camera.

3.4.2. Segmentation and Detection of the Image

The input image is segmented into two parts. Both of them are manipulated by the algorithms fed in the system by the designers. The skin pixels and the moving hand pattern manipulation is done simultaneously till the time of analyzing the resultant data,. After the analyzing part, a new image is created containing the location of the center of the hand (Moving / Static).

3.4.3. Hand Motion Tracking

Around 10 frames are collected through the same mechanism and the movement of center of the hand is detected.

3.4.4. Pattern Recognition

By tracking the user's hand motion, the features of the motions are compared with the pre-stored data sets (Trained Sets) and the maximum matching feature is selected and executed by the application.

4. THE PROPOSED ARCHITECTURE

As explained above, using the pre-existing technologies, we will be working to present the architecture of a security system that can't be bypassed effortlessly and will help in reducing the threats to the information in any private network or stand-alone computers. This system can be taken as an effort to decrease the human interaction to avoid the intentional false entry in the parameters and the information system.

The entire verification process is shown in the figure where the recognition steps are divided into a *3-level check*. The levels are divided into 3 stages and an OTP mechanism will work simultaneously, which will be invoked only if the admin has given override to the user at any level. The levels of the system are as following:

1. Action Recognition and Facial Recognition.
2. Vein Recognition.
3. One Time Password Mechanism.
4. Hand Gesture Recognition.

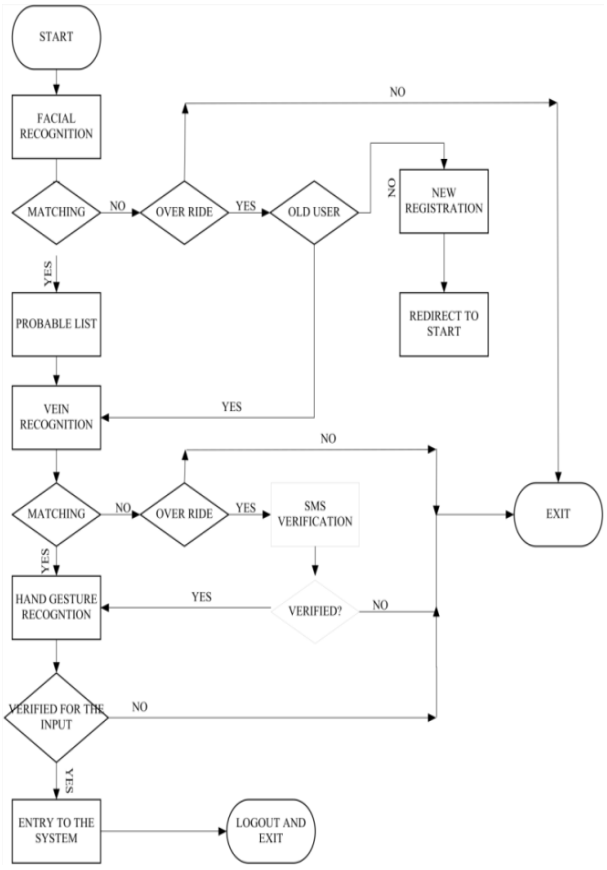

Figure 4: The Proposed Architecture

In **FIRST STAGE,** the camera will help the system to start the identification and authorization process through the processes of facial recognition and action recognition. The Action Recognition will help the system to identify the human body parts movements [6] and alert the admin of the system supposing something evasive is found. For example: The user is holding a gun and trying to jeopardize parameter, in this situation an alert message will go to admin and the proper action or the S.O.S. call can be made.

After the elementary Action Recognition, the process of facial recognition is carried out. Facial recognition being not 100% accurate [7] and correct, only helps in generation of a probable list, later on used in further steps to identify the person and give access to him/her.

The probable list is used whenever searching for the records of the person who has entered the system and it conjointly helps to identify the person faster at the Vein Recognition system.

After the first step of facial recognition, the main problem which came into consider is a case where the accuracy of the facial system plays its part and the person is left unidentified. In such a case the request of the entry is left with admin whether he wants the person to get access to the system or not. In the event the person is given the override, the admin will check for the user from the existing database himself/herself and will give entry only on the occasion that the person's database exists otherwise either the person will be forced to quit the system or will be asked to make a new registration.

The next step is of the Vein Recognition system with an immensely high recognition rate and is used in the system

[1],[2],[3],[4],[13]. According to the practical implementation and experimentation of the vein pattern system, the False Acceptance Ratio (FAR) is 0.008 and False Rejection Ratio (FRR) is 0.000[13]. Keeping this reading and the advantages of the system in mind, the user can trust the system to be very tough for the person to crack. In case the person is not matched at the vein pattern recognition step, the next step becomes the Hand Gesture Recognition. Suppose anyone is given an override in Vein Recognition system, the system will automatically have to generate a SMS on the user's mobile number (OTP) and in the later stages the system will ask the user to enter that password in order to get to the next step of the system.

Here the Hand Gesture Recognition System is used as a replacement of PIN system to access the information. Hand gestures trained sets are stored in the dynamic gesture form where the gestures registered are according to the need of the user, as an effort to not restrict the user from a password of few set patterns, making the system more secure. Including all of this, the system has a 'no-override' to this step. Consequently, in the event the password is wrong, the user is left with only two options:

FIRST: Exit the system.

SECOND: To reset the password in case the password is forgotten by the user.

These four steps stated above make a good spoof proof security system through the use of the gestures and various other recognition techniques. This system in this modern world can provide high level of security at a considerably lower cost than the other security system. Here, the hand gesture is used as the part of the system in an effort to replace the PIN authentication system. To make the information more secure, the information accessibility can be limited according to the ranks of the user. For example, in Armed Forces, the General and Major are not allowed to access same information, they access different amount of information on the same topic because of their level of work.

5. CONCLUSION

Effectively understanding the complexities of information economics and the needs of information security, throughout this paper, architecture of a security system with great efficiency has been proposed which can handle the safety of private networks and standalone computers. In conclusion, to provide a watertight security solution, here the architecture have combined different recognition systems after studying the pros and cons of all systems, thus eliminating the threats posing harm to our networks and systems. The cost and the effective accuracy of the systems have been kept in mind before combining the technologies. While designing the architecture it was kept in mind to ensure the elimination of the human interaction with the core system and delete the possibility of a forged entry through the override method, so as to remove the corruption at the admin level ensuring the solid foundation of the system.

After seeing the recent developments in the world of technology and the interaction between the humans and computers, we can change the human body to its own password rather than depending on the exacting task of remembering the long list of passwords for accessing the data which, most probably, are not even safe.

6. REFERENCES

[1] M. Sravani and P. Praveen Kumar, "FVAS: An Embedded Finger-Vein Authentication System for Mobile Devices" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 11, pp: 2901-2904, November 2013.

[2] Muthuselvi M, Mr. Manikandan, "An Embedded Real-Time Biometric Recognition System for Defense system" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), Volume 5, Issue 4, PP 31-35, Mar. - Apr. 2013.

[3] DaryRam.T.R., "AN EMBEDDED FINGER VEIN RECOGNITION SYSTEM" IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308, Volume: 03 Special Issue: 01 | NC-WiCOMET-2014 | Mar-2014

[4] Masaki Watanabe, Toshio Endoh, MoritoShiohara, and Shigeru Sasaki,"Palm vein authentication technology and its applications"

[5] http://www.biometrics.org/bc2005/Presentations/Conference/1%2 Face Recognition Based on Principal Component0Monday%20 Face Recognition Based on Principal ComponentSeptember%2019/Poster%20Session/Watanabe_1568964435_BioSymposium_2005.pdf

[6] Chunyu Wang, Yizhou Wang, and Alan L. Yuille, Peking University, Beijing, 100871, China "An approach to pose-based action recognition" PP. 4321-4328

[7] Ali Javed,"Face Recognition Based on Principal Component Analysis" IJIGSP: International Journal of Image, Graphics and Signal Processing (IJIGSP)Vol.5, No.2,PP.38-44, February 2013.

[8] https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/face-recognition.pdf Nation Science and Technology Council (NSTC)

[9] Prateek Ranjan, Keshav Jindal, "Hand Gesture Recognition" IIMEDII-2015 Proceedings, ISBN- 978-16-31024-51-1, Vol. 1 21st March 2015, PP- 57-60.

[10] B. B. Mandelbrot, Fractals: Form, Chance and Dimension, San Francisco, CA: Freeman, 1977.

[11] Mohamed Alsheakhali, Ahmed Skaik, Mohammed Aldahdouh, Mahmoud Alhelou, "Hand Gesture Recognition System" Computer Engineering Department, The Islamic University of Gaza, Gaza Strip, Palestine, 2011

[12] Rafiqul Zaman Khan and Noor Adnan Ibraheem, "HAND GESTURE RECOGNITION: A LITERATURE REVIEW" International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3, No.4, pp: 161-174, July 2012

[13] A.Ushapriya, M.Subramani, "Highly Secure and Reliable User Identification Based on Finger Vein Patterns" Global Journal of Research in Engineering, Volume 11 Issue 3, Version 1.0 April 2011

[14] Swapnil Athavale, Mona Deshmukh, "Dynamic Hand Gesture Recognition for Human Computer interaction; A Comparative Study" International Journal of Engineering Research and General Science Volume 2, Issue 2,PP 38-55, Feb-Mar 2014, ISSN 2091-2730.

[15] Ross Anderson and Tyler Moore, "Information Security Economics – and Beyond" Computer Laboratory, University of Cambridge, 15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom.

[16] Ying Wu, Thomas S. Huang, "Vision Based Gesture Recognition: A Review" Beckman Institute, 405 N. Mathews University of Illinois.

[17] Kashmera Khedkkar Safaya, Prof. (Dr.) J. W. Bakal, "Real Time Based Bare Hand Gesture Recognition" IPASJ International Journal of Information Technology (IIJIT), Volume 1, Issue 2, PP. 1-9, July 2013 ISSN 2321-5976.

[18] Konstantinos N. Plataniotis, Dimitrios Hatzinakos, Jimmy K. M. Lee, "ECG BIOMETRIC RECOGNITION WITHOUT FIDUCIAL DETECTION" Edward S. Rogers Sr. Department of Electrical And Computer Engineering, 2006 Biometrics Symposium, University Of Toronto.

[19] Dr. S. Balaji, G. Gayathri, K. Lokesh, S. Sindhu, "A Novel Iris Recognition System Using Statistical Feature Analysis By Haar Wavelet" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, PP.- 2659-2662.

[20] Prakash Chandra Srivastava, Anupam Agrawal, Kamta Nath Mishra, P. K. Ojha, R. Garg, "Fingerprints, Iris and DNA Features based Multimodal Systems: A Review" I.J. Information Technology and Computer Science, 2013,Vol.- 02, 88-111.