# Encryption-Decryption based on secure multimedia transmission using AWS

**Chandan K S[1], Ravikumar M N[2], Divyashree S[3]**

*[1]PG student, Dept. of EC&E, MCE, Hassan, Karnataka, India*
*[2]Associate Professor, Dept. of EC&E, MCE, Hassan, Karnataka, India*
*[3]Assistant Professor, Dept. of IS&E, YDIT, Bangalore, Karnataka, India*

---***---

**Abstract -** *Biometric systems square measure associate integral a part of physical access management systems. Biometric systems make sure that associate opportunity to use a system or service is completed by a sound user. These systems square measure employed in varied applications like ATMs, voting system, aadhar card, group action management system etc. The biometric systems square measure operating for a quite while and their use is increasing. there's a necessity for low value, climbable systems with high availableness. During this paper a cloud primarily based biometric system design is planned, to form the system economical and economical for remote enrollment. Authentication node is implemented on a Raspberry Pi that may be a low value pruning on UNIX. The system is capable of capturing multimodal biometric traits like face and fingerprints and sends them to cloud service by end-to–end coding method. The planned design is investing the ability of cloud to make the system climbable and pluggable. so the employment of Raspberry Pi makes the biometric system low value and transportable.*

***Key Words*: Biometric System, Cloud Service, Encryption, Microsoft Azure, Raspberry Pi, Remote Transmission.**

## 1. INTRODUCTION

Security of pc knowledge, info and pc networks has become vital in today's world. A great amount of resources square measure being endowed to make secure systems. Biometric systems square measure a secure thanks to certify a person and to grant access to services or a system solely to legitimate users. [1] during this computer-driven era, fraud and the loss or revealing of knowledge and connected intellectual property square measure having upward trend. Users have several accounts and use multiple passwords on associate ever-increasing range of computers and websites. protective and managing access while protective the user's identity, the info and pc systems has become a troublesome task.

At the guts of all security systems is that the conception of authentication- verificatory that the user is WHO he claims to be. [2] Traditional ways for authentication rely upon external things like tokens, passwords, keys which might be simply lost or forgotten. This issue may be solved through bioscience as every person has distinctive biometric options. Biometric systems square measure used to secure facilities, counter fraud and shield access to computer networks. Biometric traits square measure actual characteristics or entities that square measure accustomed determine a personality's. Physiological biometric traits embody fingerprint, palm print, hand vein, iris, retina, ear or the DNA info of a personal.

The biometric systems are getting present because of the availability of low value implementations however still the gap is there because the client area unit hard higher and cheaper solutions. Within the typical approach the systems area unit engineered upon a standard shopper server design, this limits the scalability, accessibility, plug ability moreover because the value of implementation is high. In recent years, optimum resource utilization has become a keyword to make the systems and this has given a drive to develop cloud primarily based systems. The cloud primarily based systems provide low cost, ascendable and versatile solutions for next generation computing wants. The Raspberry Pi acts as a far off enrollment and authentication node. This technique will be used for remote authentication and enrollment of a multimodal biometric system. The multimodal biometric system overcomes the restrictions of the unimodal biometric system, reduces dishonorable access, and additionally has more accuracy [1], the cloud implementation provides the plug ability and quantify ability needed by real time application of biometric identification systems.

### 1.1 Objective

**1.1.1 Background/Objectives:** Cloud computing has been emerging technology in recent years. But security is the main concern for the user not to accepting the cloud computing systems. Among them lack of trust and multi tenancy are the major issues, altogether comes under authentication problem

**1.1.2 Methods/Statistical Analysis:** These problems are mainly in third party management model and self managed models as well. In order to overcome such tribulations Biometric is the major concern. Even in biometric research group is very much concentrating on security of biometric templates. For the security of biometric template, the two encryption algorithms such as AES, RSA have been imposed on templates.

**1.1.3 Findings:** The biometric template will be safe in transit and storage as well in both cloud consumer and cloud provider side to improve the reliability of cloud.

**1.1.4 Applications/Improvements:** If such approach has been adopted then confidence regarding the usage of cloud will be greater than before.

### 1.2 Problem Statement

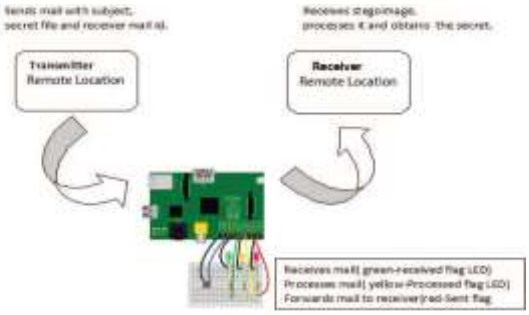

Sends mail with subject, secret file and receiver mail id.
Receives stegoimage, processes it and obtains the secret.
Transmitter Remote Location
Receiver Remote Location
Receives mail( green-received flag LED)
Processes mail( yellow-Processed flag LED)
Forwards mail to receiver(red-Sent flag

**Fig -1:** Illumination of End to End Description

The sender sends the appropriate predetermined subject in the email along with the file path of the cover, secret files and the receiver's email id. The reception is done by the Raspberry Pi which checks for a new email every 15 seconds. Once the appropriate email is received from the sender, the mechanisms delineated in Fig. 2 are done, with TAS when the secret is text and IAS when an image is to be sent covertly. The final stego-image is then automatically transmitted via an insecure channel, such as the internet, to the recipient.

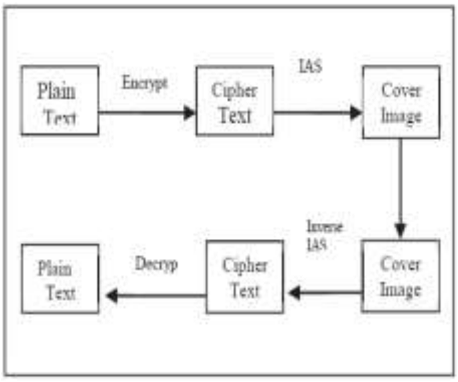


**Fig -2:** Proposed Security Model

In case of IAS, comparisons have been made between the existing 1 bit , 2 bit LSB and the proposed 3 bits per 2 pixels LSB steganography on the basis of PSNR, MSE [7]. The error metric values from the Table 1 show that the proposed 3 bits per 2 pixels embedding technique has yielded is almost the average of the results yielded by the 1 bit and 2 bit LSB techniques. The proposed embedding technique is facilitated by a higher embedding capacity than the 1 bit LSB, and a higher PSNR than the 2 bit LSB as can be inferred from Table 1. In case of IAS, the process is illustrated with various attacks.

## 2. LITERATURE SURVEY

RPi has been used for numerous applications, in [3], the authors have projected a system that focuses on value saving and enhancing the standard of service within the field of technology aided teaching. Raspberry Pi and its net interface stores files that are sent from remote computers and consider these power point files or transportable Document Files (PDF) on the multimedia projector. It targets to substitute laptops with Raspberry Pi, which can not solely significantly scale back the value involved, however additionally can facilitate achieving quality of service because the system can consume a smaller quantity of power. In another implementation [4] authors planned a picture capturing technique in associate degree embedded system supported Raspberry Pi boards. Most of the popularity systems square measure supported a computer, the portability of that is restricted by its weight, size and therefore the high power consumption.
In [5], group action of the scholars is taken mechanically based biometric traits like fingerprint. Here the photographs square measure captured by the fingerprint sensors. The hardware parts used square measure Arduino UNO board, Wi-Fi defend, GSM Shield, Keypad, LCD show, Adafruit Fingerprint sensing element and Raspberry Pi. This implementation may be a shopper server based mostly implementation. Besides this there square measure several real time applications of RPi [7] [8] [9].

The security is additionally a part of biometric systems. Kaul and Sheikh [7] have planned knowledge security for end-to-end transmission that is achieved by many alternative trigonal and uneven techniques for message confidentiality, message authentication and key exchange victimization transport layer security. They planned combination of 2 trigonal algorithms AES and Blowfish to reinforce security. AES is enhanced by modifying the S-boxes, columns, and then combination of increased AES and blowfish is employed for knowledge confidentiality. Message digest five is employed for authentication. Key exchange is completed victimization ECDHA, Elliptic Curve Diffe- Hellman rule. Security into planned design is achieved by group action this approach for end–to-end encryption of biometric traits captured by enrollment node.

As way because the cloud implementations square measure thought of R. Trade has mentioned [10] however piracy will be reduced by the combination of embedded system and therefore the cloud computing technology. This analysis additionally highlights on the benefits of using cloud computing technology, Linux software system, ARM processor and therefore the Raspberry Pi. In [11], the various challenges, opportunities and therefore the transactions in cloud computing square measure outlined. This paper provides a short introduction on SaaS, IaaS, PaaS and regarding the kinds of cloud. This paper also explains however with cloud computing resources will be shared in an efficient manner reducing the value. It shows what challenges square measure featured by the developers, engineers, administrators etc. Current paper is that specialize in however the portability and ease of Raspberry Pi will be combined with Cloud associate degreed secret writing technique to style an authentication system with high accessibility, quantify ability, security , movableness and low value.

## 3. PROPOSED SYSTEM

The Fig.describes the design of the projected system. The projected system primarily consists of 3 modules:

### 3.1 Raspberry Pi- For Image Capturing

RPi Model B is connected to a show via Associate in Nursing HDMI-to-HDMI or via a VGA-to-H DMI cable to the HDMI port on the RPi. It's connected to the FS88 fingerprint scanner at the USB port. The PiCamera is connected to the RPi via the CSI connecter. The face and fingerprint pictures area unit captured and keep within the RPi. To create the biometric service node moveable it's having the Wi-Fi adapter connected. This can be shown in fig.

### 3.2Encoding Module-For Security

These pictures keep on the RPi area unit sent to a foreign location. because the biometric trap its ought to be protected once transmittal over a channel end-to-end encoding is employed. AES-256 rule are going to be used enforced in C# language.

### 3.3 Cloud Service-For measurability and Performance

Cloud Computing may be a buzzword of the new world. The RPi isn't capable of performing dynasty the intensive calculations concerned in extracting the feature vector, storing and retrieval of biometric traits from massive databases etc. this can be achieved by a cloud service. The cloud fills this void and any augment security, device management and then on [17]. In this work, the encrypted pictures area unit sent to a cloud wherever the photographs area unit decrypted and therefore the original image is retrieved. The cloud service is enforced as a software-as-a-service (SaaS).Fig. five shows the diagram of the proposed cloud service service. This can create the implementation secure and system. an extra issue will be noted that just in case of high distributed. Security applications wherever the information is required to be unbroken in private premises solely, then the cloud service will be replaced by a far off procedure running on personal serveras an online.

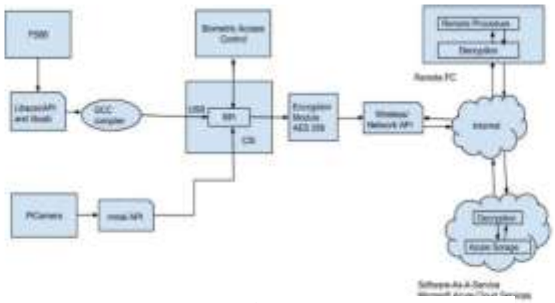


**Fig -3:** Design of the projected system

## 4. SYSTEM REQUIREMENTS AND SYSTEM SPECIFICATION

The system planned here may be a multimodal biometric system, face and fingerprint square measure the biometric traits beneath consideration. The hardware demand for the remote node is as follows.

### 4.1 Raspberry Pi

Raspberry Pi may be a credit-card sized minor laptop. It's a small computer that brings all the practicality that square measure delivered by a desktop computer. it's become a wide used device for learning programming since last one year. The Raspberry Pi has a Broadcom BCM 2835 a System on chip (SoC). SoC has ARM 1176JZF-S 700MHz processor, Video Core IV GPU and with 512 MB memory. It uses associate degree Coyote State card for booting and knowledge storage. The RPi has associate degree local area network port for network affiliation, USB port for connecting exterior USB devices, small USB slot for power provide, HDMI port to attach to show and General Purpose Input Output (GPIO) pins to attach to alternative hardware devices. [5] [12]

**Fig -4:** Raspberry Pi Model

### 4.2 Futronic FS88 Fingerprint Scanner

This is the optical fingerprint device used for capturing live fingerprint at the remote enrollment/

authentication node running on RPi. FS88 could be a changed version of FS80 USB2.0 Optical Fingerprint Scanner from Futronic as shown in Figure 2. it had been certified by the federal Bureau of Investigation to be compliant with the PIV-071006 Image Quality Specification for Single Finger Reader. These facts recommend that, Futronic FS88 complies the U.S.A. Federal IP Standard 201 (FIPS 201) for private Identification Verification (PIV) of Federal staff and Contractors. [14] FS88 uses advanced CMOS device techn bailiwick and precise optical system to fulfill the rigorous requirement on fingerprint image quality. a novel ID is factory-programmed into the USB Device Register of every FS88 scanner. Therefore each FS88 scanner device is traceable and this can be extremely necessary for state identity administration comes.

**Fig -5:** USB Fingerprint Scanner –FS88 connected to Raspberry Pi.

## 4.3 SD card

The Coyote State card is put in with the O.S image and is additionally used as an enclosed storage for the RPi. During this analysis, Scandisk category ten 16GB Coyote State card is employed.

## 4.4 Power offer

Raspberry Pi Model B needs voltage of 5V and minimum 700mA current to figure. During this analysis Samsung USB charger with power offer 5V 2A is employed or an influence bank of 10000mah is employed to make it moveable. These elements area unit connected along to create the remote enrollment and authentication node for a face and fingerprint based mostly multimodal biometric system.

## 5. ADVANCED ENCRYPTION STANDARD (AES)

AES relies on a design principle referred to as a substitution-permutation network, combination of each substitution and permutation, and is quick in each software system and hardware. In contrast to its forerunner DES, AES doesn’t use a Feistel network. AES could be a variant of Rijndael that includes a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. Against this, the Rijndael specification as such is nominal with block and key sizes which will be any multiple of 32 bits, each with a minimum of 128 and a most of 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, though some versions of Rijndael have a bigger block size and have extra columns within the state. Most AES calculations are exhausted a special finite field. The key size used for an AES cipher specifies the amount of repetitions of transformation rounds that convert the input, referred to as the plaintext, into the ultimate output, known as the cipher text. The amount of cycles of repetition is as follows:

1. 10 rounds for 128-bit keys.
2. 12 rounds for 192-bit keys.
3. 14 rounds for 256-bit keys.

Each round consists of many process steps, each containing four similar however completely different stages, together with one that depends on the cryptography key itself. A collection of reverse rounds are applied to remodel cipher text back to the initial plaintext using identical encoding key.

## 6. SYSTEM IMPLEMENTATION

### 6.1Basic Hardware Setup

This can be achieved by desegregation small USB power cable, USB keyboard, USB mouse, 8GB S D card, coax and HDMI cable with the Raspberry Pi. For image capturing on the RPi the hardware affiliation is as shown in Fig.

### 6.2 Setting the Raspberry Pi for the primary time

To use Raspberry Pi, associate OS must be put in onto associate American state card. Within the current setup, the New out Of Box software system (NOOBS) is employed. Once the setup is copied onto the American state card, the Pi can currently boot into NOOBS and should show a listing of operative systems that one will choose to install. During this project Raspbian (Debian wheezy) Figure half-dozen. Basic Hardware setup of RPi O.S is used. [18]

### 6.3 Connecting Raspberry Pi to the LAN LAN/ USB

Wireless Wi-Fi Adapter First of all, it's needed that the Raspberry Pi ought to be connected to the LAN via LAN cables or Wireless local area network Adapter. Within the current work to create the

Biometric node portable it's interfaced with local area network Adapter. USB Wireless Wi-Fi Adapter RPi Ralink RT5370 is employed for LAN/internet connection. The RPi is sodden initial then once work into the Rpi desktop setting, the credentials for wireless network square measure provided. The plague window for net configuration is shown in Fig..The Node that's, RPi is now prepared for connecting to the cloud services.

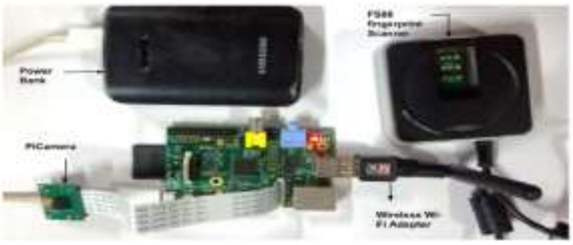


**Fig -6:** Basic Hardware setup of RPi

### 6.4 Putting in FS88 API and USB libraries in RPi to browse USB device

Futronic FS80 and FS88 are verified to figure well with the RPi model B. to create it wor k the Futronic libScanAPI must be put in on the Ras pberry Pi node. LibScanAPI is that the API library for applications to figure with Futronic's FS80 USB fingerprint Scanner. Kernel mode driver for FS80 scanner driver isn't out there, however the 'libScanAPI.so' works with a well-know n multiplatform library 'libusb'. libusb could be a library that permits user area applications access to USB devices. [19]. Th is can interface the FS88 fingerprint scanner with Raspberry Pi as shown in Fig and therefore the fingerprints is scanned. This half is enforced in C language.

### 6.5 Connecting the PiCamera to the Rpi board

The Raspberry Pi camera module will take full HD 1080p exposure and video, and may be controlled programmatically. The flex cable is in sorted into the connective set between the local area network associate d HDMI ports, with the silver connectors facing the HDMI port. There are primarily 2 utilities out there, 'raspistill' and 'raspivid'. 'Raspistill' is employed for capturing still pictures with the camera module and 'raspivid' is employed for capturing video stream with the camera module. These applications are statement operated, written to leverage the multimedia system Abstraction Layer (MMAL) API that runs over OpenMAX. The MMAL API simply uses the system than that bestowed by OpenMAX. MMAL could be a Broadcom specific API used solely by Video Core fourimplementations [20].After productive implementation of t hese steps; the Raspberry Pi is ready to capture the fingerprint and therefore the face pictures victimisation the FS88 fingerprint scanner and the PiCamera severally.

### 6.6 Cryptography of the captured pictures

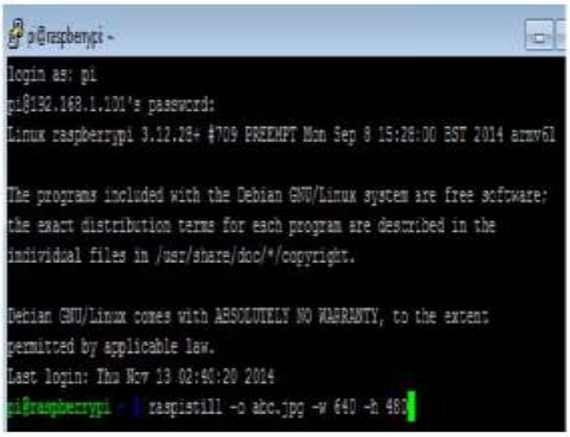
As during this analysis the biometric traits ar being transmitted over the channel to a cloud service, protective these traits is of nice concern on host computer itself before transmission. End-to-End encryption method is employed to defend the biometric traits. In this work, advanced cryptography Standard-256 algorithmic rule is employed. AES is predicated on a style principle called a substitution-permutation network, a mixture of each substitution and permutation, and is quick in each code and hardware. in contrast to its precursor DES, AES doesn't use a Feistel network. AES incorporates a fastened block size of 128 bits, and a key size of 128, 192, or 256 bits. For additional security, AES 256 is employed.

## 7. EXPERIMENTAL RESULT

The results can embrace the photographs captured by the Raspberry Pi, the encrypted pictures that area unit transmitted over the channel to urge uploaded on the Az ure storage and eventually the secret writing and cryptography of the encrypted pictures.

### 7.1 Raspberry Pi

This section specifies the results made by the Raspberry Pi, which has the capturing of the biometric traits. To capture the image from the PiCa era we want to run a command on the LXTerminal of the RPi as shown within the Fig. Where rasp still is that the command, -o indicate the output and therefore the fundamentals. jpg is that the computer file name beside the format, -w and –h represents the breadth and therefore the height of the window. The next half is to capture the fingerprint biometric attribute by the FS88 fingerprint device interfaced with the Pi. The Fig shows the pic of the LXTerminal running the C code to capture the fingerprint image. Fig. shows the capturing of live fingerprint and therefore the captured fingerprint is shown in Fig.

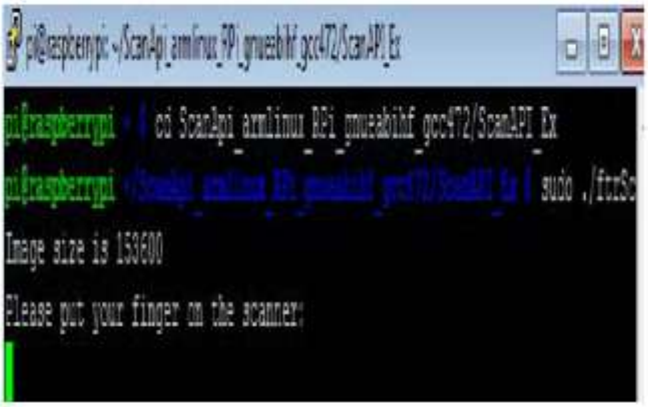


```
pi@raspberrypi ~
login as: pi
pi@192.168.1.101's password:
Linux raspberrypi 3.12.28+ #709 PREEMPT Mon Sep 8 15:28:00 BST 2014 armv6l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov 13 02:40:20 2014
pi@raspberrypi ~ $ raspistill -o abc.jpg -w 640 -h 480
```

**Fig -7:** pick of LXTerminal running command to capture pictures from the PiCamera



```
pi@raspberrypi: ~/ScanApi_armlinux_RPi_gnueabihf_gcc472/ScanAPI_Ex
pi@raspberrypi ~ $ cd ScanApi_armlinux_RPi_gnueabihf_gcc472/ScanAPI_Ex
pi@raspberrypi ~/ScanApi_armlinux_RPi_gnueabihf_gcc472/ScanAPI_Ex $ sudo ./ftrSc
Image size is 153600
Please put your finger on the scanner:
```

**Fig -8:** LXTerminal to capture the fingerprint image.

**Fig -9:** Enrollment of the user

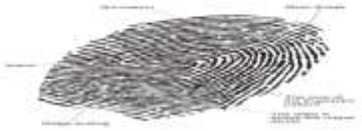


**Fig -10:** Fingerprint image captured on the RPi

### 7.2Encoding Module

After the capturing of the biometric traits, they'll be encrypted on the RPi victimization AES-256 so the ciphered pictures are transmitted over the channel to a distant location. The performance evaluation is finished on factors like encoding and secret writing time, the memory and processor usage and therefore the Avalanche couple electroconvulsive therapy. This may be enforced within the future. Figure the face image captured by the RPi.

### 7.3 Cloud Service

The ciphered pictures are sent to the Azure storage wherever the photographs are decrypted. Before decipherment hash code is made victimization SHA-2 to see the integrity of the biometric traits. If the hash code is same as made by the RPi consumer before the transmission, then decipherment method takes and also theoriginal pictures square measure retrieved. The uploading of captured biometric traits on the Microsoft Azure Server is completed so uploaded. Fig. fourteenshows the blob storage outline of the Microsoft Azure account. It is seen that the 2 pictures 'Frame_ex.jpg' (Face) and '20141103_165029.jpg' (Fingerprint) square measure uploaded to the cloud service with success.

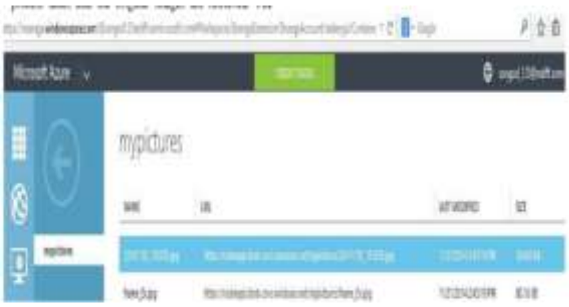


**Fig -11:** shot showing biometric traits that square measure uploaded on Azure Storage

## 8. CONCLUSION AND FUTURE WORK

### 8.1 Conclusion

In this paper an occasional price laptop Raspberry Pi is employed as a foreign enrollment and authentication node. The enrollment half is with success done and also the captured information is shipped to the cloud. The Fingerprint & face capturing sensors beside Wi-Fi adapter is with success interfaced to Raspberry Pi. The captured traits square measure sent to a Microsoft Azure primarily based biometric service, this service can extract the feature vectors and store it to the feature vector info.

### 8.2 Future Enhancement

Future work includes, the end-to-end encoding half, which is able to strengthen the safety just in case of business implementation. Planned system has application all told the biometric access management systems, that wants movableness, quantifiability and low implementation price.

## REFERENCES

[1] Omar Abdulwahabe Mohamad, Rasha Talal Hameed, NicolaeTapus, " Access Control Using Biometrics Features with Arduino Galileo", International Journal of Advanced Research in Computer Science and Software Engineering, vol 4, issue 8, Aug 2014.
[2] Biometric Authentication, Available: http://www.computer world.com/article/2556908/security0/ biometric-authentication.html.
[3] Dhaval Chheda, Divyesh Darde, Shraddha Chitalia: "Smart Projectors using Remote Controlled Raspberry Pi", International Journal of Computer Applications (0975 – 8887) vol. 82 – No 16, Nov 2013.
[4] G.Senthilkumar, K.Gopalakrishnan, V.Sathish Kumar, "Embedded Image Capturing System Using Raspberry Pi System", International Journal of Emerging Trends & Technology in Computer Science, vol 3, issue 2, March – April 2014.
[5] Karthik Vignesh, Shanmuganathan , A.Sumithra, S.Kishore and P.Karthikeyan, "A Foolproof Biometric Attendance Management System" International Journal of Information and Computation Technology, vol 3, Number 5 (2013), pp. 433-438.
[6] Camera Module. Available: http://www.raspberrypi.org/documentation/ usage/camera/README.md
[7] Shaikh Ammarah P. Vikas Kaul S K Narayankhedkar, "Security Enhancement Algorithm for Data Transmission using Elliptic Curve Diffie-Hellman Key Exchange", International Journal of Applied Information Systems – Foundation of Computer Science FCS, New York, USA and the International Conference & workshop on Advanced Computing 2014
[8] "Hiding Biometric Data" , IEEE transactions on Pattern Analysis and Machine Intelligence, vol. 25, No.11, November 2003
[9] Rajeeb Lochan Dash, Mrs. A. Ruhan Bevi, "Real-time Transmission of Voice over 802.11 Wireless Networks Using Raspberry Pi", International Journal of Engineering Development and Research, vol 2, issue 1 2014, ISSN: 2321- 9939.
[10] Md. Maminul Islam, Md. Sharif Uddin Azad, Md. Asfaqul Alam, Nazmul Hassn, "Raspberry Pi and image processing based Electronic Voting Machine" , International Journal of Scientific & Engineering Research, vol 5, issue 1, January-2014 1506 ISSN 2229-5518.
[11] Rushikesh Tade, "Embedded Cloud for Antipiracy" International Journal of Scientific & Technology Research, vol 2, issue 6, June 2013 Issn 2277-8616.
[12] Jianjiang Feng, Anil K. Jain,"Fingerprint Reconstruction: From Minutiae to Phase" IEEE Transactions On Pattern Analysis And Machine Intelligence, vol. 33, No. 2, Feb 2011
[13] About Raspberry Pi, Available: www.raspberrypi.org
[14]Available: https://encryptedtbn1.gstatic.com/images?q=tbn: ANd9GcT4bhmDSB ROA76ZfEXCBJ6FUKkEXHNmBhkRzBpZYfVs4EUfHUm
[15] FS88 FIPS201/PIV Compliant USB2.0 Fingerprint Scanner, Available: http://www. Futronictech.com/product_ fs88.html#
[16] Available: http://www.element14.com/community/servlet/ JiveServlet/showImage/2- 104955192660/DSC_2624_33%25 .JPG