Security Scheme by Using Steganography in Multi-Model Biometric System

Boby Kumar[1]; Deepak Sharma[2]; Dr. Navin Kr. Tyagi[3]
Department of Computer Science and
Engineering MIT Bulandshahr

Abstract:- **The process of automatically identifying a person based on their physiological and behavioural traits is known as biometric recognition. A unimodal or multimodal biometric system might be based on physiological or behavioural traits. Some shortcomings in the unimodal biometric system include spoofing, non-universality, intra-class differences, and noisy data. Using the face and palm images as templates, we are implementing a multimodal biometric system. A person's palm image can provide a wealth of detailed information about them. Palm image have three major lines, name as principle line, secondary line and wrinkles which are unique in nature. Face image have more feature than any other biometric traits. Face image is recognized easily in less time. Combining these two biometric template gives higher security. Message image kept secretly in the cover image called stego image. In this steganography technique we are using palm image as a Message and face image as a cover image. After getting stego image Identification process works. The important fe of identification process id De-Stego. This feature of identification will separate the message image (palm image) from cover image (face image). After separation of images the decision will take care, weather the image identified or not identified.**

Keywords:- Steganography Technique De-Stego, Face Image, Palm Image, Stego-Image Verification And Identification.

I. INTRODUCTION

Biometric Recognition is an act of recognizing the person quickly and automatically based on their physical and behavioural characteristic. The distinctiveness of these features makes biometric recognition systems increasingly common. Physiological or behavioural qualities cannot be lost or stolen because they are unique to everyone. The two different types of biometric systems are multimodal and unimodal biometric systems. Unimodal biometric systems only recognise single traits, such as only face recognition, fingerprint recognition, iris recognition, etc., whereas multimodal biometric systems recognise multiple traits, such as face and palm print recognition, iris and thumb recognition, and there can be multiple possible outcomes in this biometric system. Multimodal biometric systems are growing in popularity due to their capacity to inherit characteristics from unimodal biometric systems and rising demand. Almost all multimodal biometric systems share

three parameters: matching module, feature matching, and sensing.

In unimodal biometric system it is not possible because in this system having multiple things and attached with single modalities.

II. LITERATURE REVIEW

S.B. Verma et al. [8] proposed ''Comparative Study of FAST, MSER, and Harris for Palmprint Verification System''. In this paper they have compared the study of feature extraction of palm print using three different method name as FAST, MSER and HARRIS. In this comparative study they have taken two images of palm names as A and B. After that they have applied these three methods, then the FAST feature extraction detects 74 points, MSER detects 128 points, and HARRIS detects 289 points in the hand A image.

Qi Xiong et al. [12] proposed ''A Modified Chaotic Binary Particle Swarm Optimization Scheme and Its Application in Face-Iris Multimodal Biometric Identification'' After extracting the feature of both templates the complexity is much higher of extracted feature. To solve this problem, they have used modified chaotic binary particle swarm optimization (MCBPSO) algorithm for selecting the accurate feature. They have used The Institute of Automation, Chinese Academy of Science (CASIA) database for experiments.

S.B. Verma et al. [9] proposed ''Performance Analysis of Various fusion method in multimodal biometric'' They have analyzed various fusion in different- different process of an image. They have used four levels of fusion methods name as sensor level fusion, feature level fusion, score level fusion, decision level fusion. to process the image. Firstly, they have applied sensor level fusion in image acquisition. Then they have applied feature level fusion method in feature extraction. They have used score level fusion in score matching. And finally they have used decision level fusion for making the decision.

Mustafa Ahmed Shamil et al. [6] proposed "multimodal biometric system iris and fingerprint recognition based on fusion technique" was published. Basically they have researched on multimodal system and they used fingerprint and iris as a template. They said that multimodal recognition is more secure than single modal recognition system due to higher matching thing are present in multimodal system.

They used FUSION technique to processing the images. Two types of FUSION technique they used first one is Early fusion and Second one is Late Fusion

Joseph Teena et al. [3] proposed ''A multimodal biometric authentication scheme basedon feature fusion for improving security in cloud environment'' Once they have extracted the feature then they generated unique secret key by fusing the traits in two stages name as FAR (FalseAcceptance Rate) and FRR (False Rejection Rate). They have used these two features for measuring the robustness of the system. They have taken finger print, iris and palm print parallel from the database and extracted the feature.

Walia et al. [11] proposed ''Secure multimodal biometric system based on diffused graphsand optimal score fusion''. In this paper the author explained that most of the multimodal biometric system has an issue of lack of robustness and security. To overcome this problem,they have proposed multimodal biometric system based on face, iris and ear optimality scorelevel fusion. In this proposed model they combined unimodal feature with related key featureand to give feature transformation. In this model they have combined multiple modalities to achieved a robust and reliable multimodal biometric system.

III. METHOD USED

Firstly, in the biometric system we will verify the user with the help of multiple biometric traits such as palm print, face and some other credentials as Name, Address, mobile number, etc. We have acquired these images via simple camera (CMOS camera) and apply steganography technique. CMOS camera is efficient to acquire the images and takes very lesspower.

Steganography is a method or science of hiding secret information in cover image. The interface in which the secret information kept called Cover image.These cover image travel from sender to receiver. After applying the steganography, the images converted into Stego image. This stego image directly stored in the database for further identification. Apart from this, we can store some other information related to person such asName, mobile number, address, department number, etc.

Below these credentials we will add during registration

➢ *User Data*

- Name
- Address
- Department
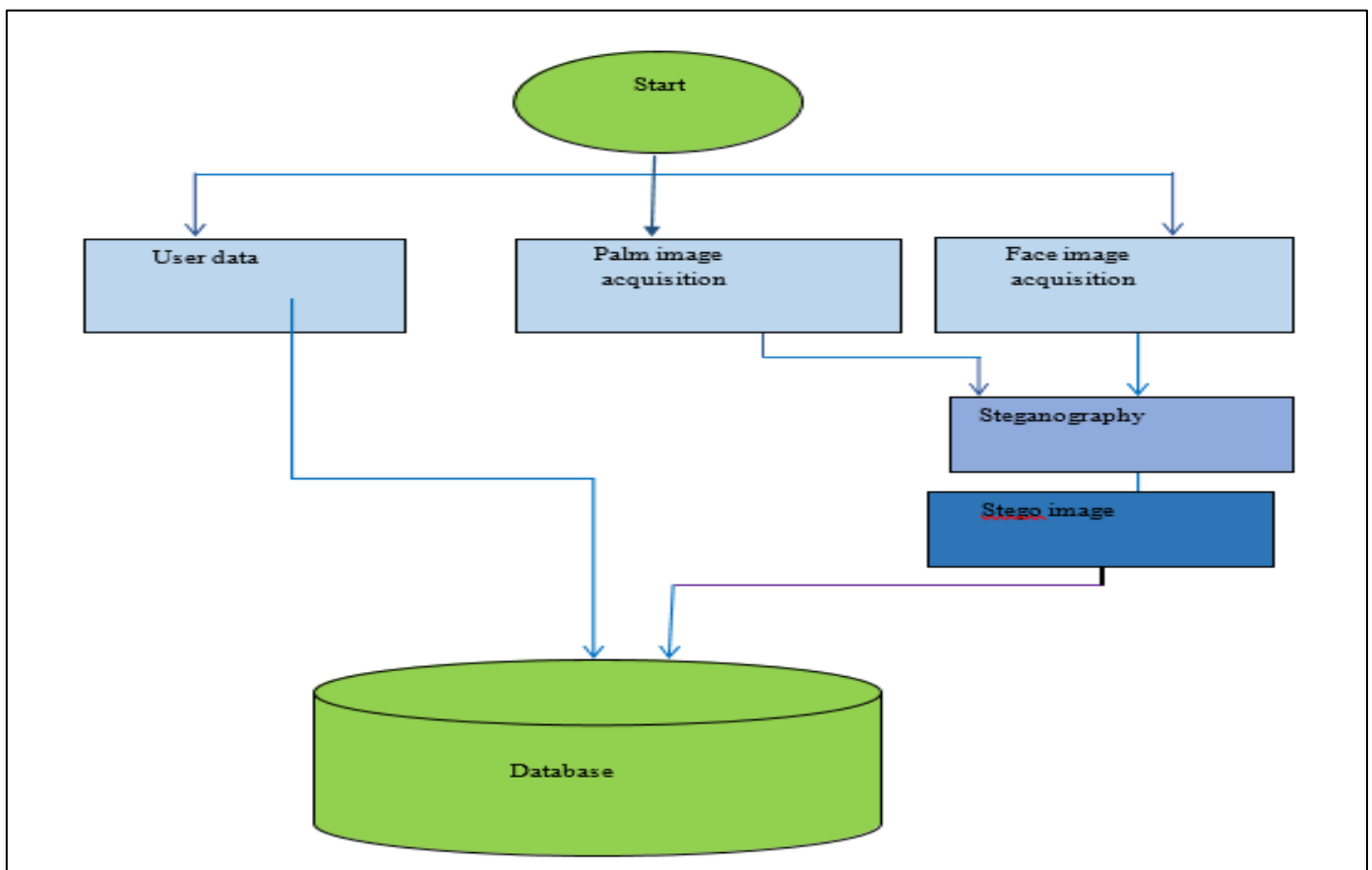- ID Card Number

➢ *Face Image*
➢ *Palm Image*

Fig 1: Flow Chart Showing the Process of Steganography

IV. RECOMMENDATIONS FOR EFFECTIVE IMPLEMENTATION

A. Face Image:

Face recognition system plays very important role in biometric system. Basically facial recognition system categories into some steps to acquire and store in the database. Firstly, image acquis ion will be done with the help of simple camera. Later analysis of acquired image will be done. After analysis of captured image, image converted into binary (data form) form to store in the database. In the face, having many robust information of as compare to any other biometric recognition system.
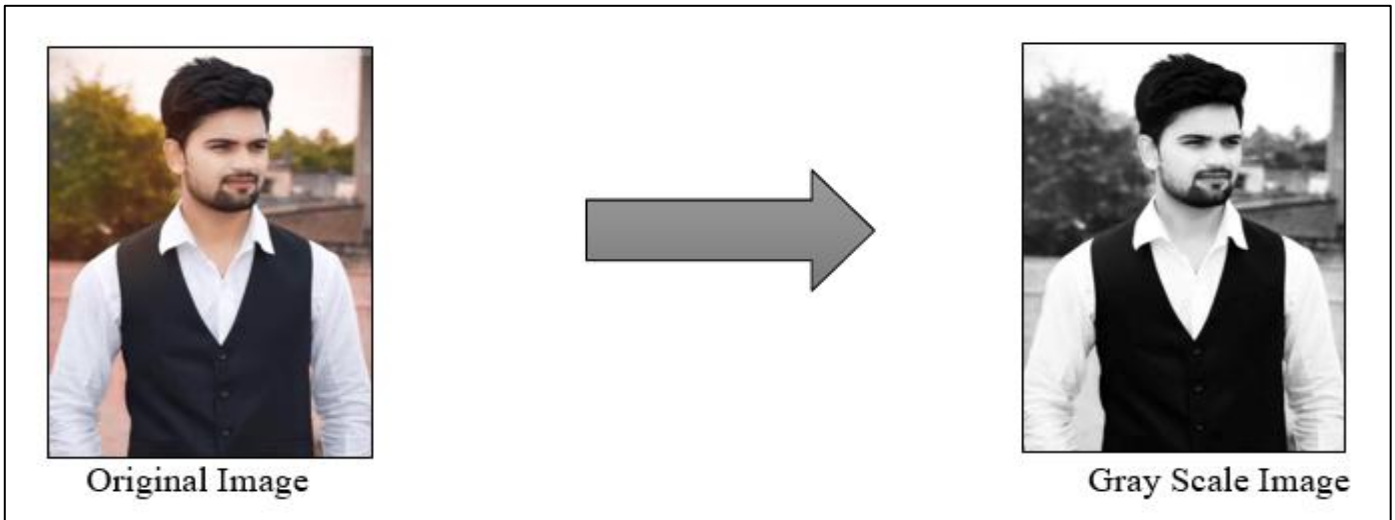

Fig 2: Process of Face Recognition

B. Palm Image:

Palm print biometric system is basically new recognition system as compare to some other biometric system like as fingerprint, face, ear recognition system. Palmprint has unique recognition system and having high usability. Palmprint having three basic line which is Principal Line, Secondary Line and Wrinkles. These line gives rich information of a person which can easily identify. Palmprint having more feature (ridges, delta point, minute feature, principal line) than the finger print, hence palm print biometric system is advisable for better security purpose.

Fig 3: Process of Palm Recogintion

C. Stego Image:

Stego image is an image in which secret information are kept. After the processing of steganography stego image generated. While processing of psalm image and face image, a single image generated name as stego image. Stego image is a type of encoded information in which it can be placed in anywhere. Stego image contain secret information in which no one can suspect that it having some useful information, because the stego image is almost similar to the cover image. The similarity of the stego image is based on the LSB concept. In the LSB concept the single or double digit changes and in that single or double digit the data (secret information) can be stored. Below the image showing before (cover image) and after (stego image) image.

Fig 4: Process of Stegonation

The above image showing that the efficiency of stego image. In the stego image there are not much changes as compare to cover image. This is why, because in the stego image there are only 2 bit changing of LSB bit. Hence secret message can be kept with the help of this technique.

V. CONCLUSION

We will get the secret information in De-stego technique which we had kept secretly during verification process. In the verification process of biometric, face image combined with palm image called stego image. This stego image stored in the database for further identification work. In the identification process firstly we need to acquire the face image and that face image has already stored in the database along with palm image.

After acquiring the face image preprocessing of the image will be done. Identification module will work on the next stage from the preprocessing. If face image is identified, then matched image (stego image) will be fetched out from the database to do remaining work. After fetching the face image (stego image) De-stego will be done. In this stage if De-stego technique applied then palm image separated from the face image. Once the palm image separated from the face image with the help of De-stego then acquired palm image will be matched to the separated image.

REFERENCES

[1]. Ammour, Basma, et al. "Face–iris multimodal biometric identification system." *Electronics* 9.1 (2020): 85.

[2]. Chandran, Saravanan, and Satya Bhushan Verma. "Touchless Palmprint Verification using Shock Filter, SIFT, I-RANSAC, and LPD." *IOSR Journal of Computer Engineering* 17.3 (2015): 01-08.

[3]. Joseph, Teena, et al. "A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment." Journal of Ambient Intelligence and Humanized Computing (2020): 1-9.

[4]. Karthika, P., R. Ganesh Babu, and K. Jayaram. "Biometric based on steganography image security in wireless sensor networks." *Procedia Computer Science* 167 (2020): 1291-1299.

[5]. Mishra, Ashish. "Multimodal biometrics it is: need for future systems." *International journal of computer applications* 3.4 (2010): 28-33.

[6]. Mustafa, Ahmed Shamil, Aymen Jalil Abdulelah, and Abdullah Khalid Ahmed. "Multimodal Biometric System Iris and Fingerprint Recognition Based on Fusion Technique." *International Journal of Advanced Science and Technology* 29 (2020): 7423-7432.

[7]. Singh, Arun Kumar, Juhi Singh, and Harsh Vikram Singh. "Steganography in images using lsb technique." *International Journal of Latest Trends in Engineering and Technology (IJLTET)* 5.1 (2015): 426-430.

[8]. Satya Bhushan verma and Saravanan Chandran. "Comparative Study of FAST MSER and Harris for Palmprint Verification System." *International Journal of Scientific & Engineering Research* 7.12 (2016): 855-858.

[9]. Satya Bhushan verma, and Chandran Saravanan. "Performance analysis of various fusion methods in multimodal biometric." *2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES).* IEEE, 2018.

[10]. Satya Bhushan verma, and Saravanan Chandran. "Touchless Region based Palmprint Verification System." *International Journal of Computer Science and Information Security(IJCSIS)* 15.4 (2017).

[11]. Walia, Gurjit Singh, et al. "Secure multimodal biometric system based on diffused graphs and optimal score fusion." IET Biometrics 8.4 (2019): 231-242.

[12]. Xiong, Qi, et al. "A modified chaotic binary particle swarm optimization scheme and its application in face-iris multimodal biometric identification." Electronics 10.2 (2021): 217