Face and Thumb Based Multimodal Bio-Metric Authentication using Harris Feature Extraction and Stenography

Pallavi S Biradar, Anand Jatti

Abstract*: In the past recent, identification of a person in an effective manner is a foremost concern for any security authentication in numerous applications such as, banking, e-commerce, communications etc. One of the best identification technology for person identification and authentication compared with the existing password based authentication is the multimodal biometric technology. Multimodal can be defined as, a system which uses two or more biometrics for identification of person. In the paper we propose a multimodal bio-metric system with a unique methodology and features extraction method incorporated in system for a secure authentication. The two modalities used in the system are face and thumb. We use Harris based image feature extraction for both and choose the best unique features from both and fused using concatenation. The extracted unique features are embedded in a cover image using modulo operator based steganography technique. This encrypted data is shared as an image file to the receiver for authentication. At the receiver end the hidden features are decrypted and separated into face and thumb features. These decrypted features are compared with the pre-trained authorized person feature, based on the multi-svm classifier result the person is decided as authorized or unauthorized. The accuracy of the system is been calculated and was resulted in a good accuracy. The system can be made much more secure by adding an additional secret key for encryption and decryption.

Keywords: Bio-metric, Harris, modulo operator, multi-modal, multi-svm. Stenography.

I. INTRODUCTION

Safe keeping is maximum significant part nowadays. Personal documentation remains chief chunk of security schemes. Currently recognition over conservative mode like keyword, card, key etc., remain not dependable any longer. So in its place of these conservative methods, biometric expertise is castoff in numerous solicitations. Biometric machinery is castoff for Verification or Confirmation and Empathy, which is founded on biometric modality. The biometric schemes are untrustworthy, if a solitary modality is castoff then may be replicated but once we custom two or additional amount of modalities can dodge such replication glitches we go on for multimodal biometric individualities. In any marketable and protected organization brands use of a exclusive username besides its conforming watchword for authentication of a individual which can be chopped by prisoners and can disagreement the entrances of security. Interruption is insufferable in great secured zones like protection schemes, bank dealings on online interchange/ and administration bureaucrats. Biometrics postulates practice of a quantifiable physical features and interactive trait in contradiction of individuality theft. Interactive method customs acknowledgement of sign, voice etc. although physiological method comprise impression, retina, iris, DNA, palm print etc. For every distinct topographies of outlines and counterplot are exclusive and be determined throughout his/her complete life. The arrangement would not necessitate a perfect antagonism since bid section and registered template most probable determination not be undistinguishable. For example, in situation of a thumbprint, examples will differ founded on sensitive part that any specific scan shelters and grade of solidity of edges outcomes from variable pressure through examination. As an alternative, whether an antagonism is announced be dependent upon Hamming coldness, grade of transformation, among proposal instance and registered pattern. The knowledge's producer sets degree of parity obligatory to describe a counterpart founded on widespread investigation with knowledge in common and skimming device in precise. The explanation of match is continuously a probabilistic perception as it is through humanoid assessment of thumb print. Organization would not necessitate a faultless match as bid illustration and registered pattern utmost probable will not be matching. For instance, in circumstance of a thumb print, the examples will fluctuate founded on fingertip part that any specific scan refuges besides degree of firmness of edges that outcomes from changing pressure through the test. As an alternative, whether a match is proclaimed be contingent upon Pretense space, degree of variance, amongst bid section and registered pattern. The knowledge's constructer cliques the grade of equivalence mandatory to describe a match founded on widespread investigation with knowledge in common and perusing method in specific. The description of match is continually a probabilistic thought as it is through human assessment of thumb print.

II. EXISTING METHODOLOGIES

The verification arrangement by biometric topographies are characterized as single and double modality founded authentication scheme. In singular method substantiation biometric method topographies as of one method of input cast-off for acknowledgement or empathy. There remain definite difficulties through single method authentication schemes like deteriorating. For example shortage of biometric pattern.

Revised Manuscript Received on September 25, 2020.

Pallavi S Biradar, M.Tech Scholar, Dept. Of Electronics and Instrumentation Engineering, RV College of Engineering, Bangalore

Dr. Anand Jatti, Associate Professor, Dept. Of Electronics and Instrumentation Engineering, RV College of Engineering, Bangalore

For such situations dual modality are castoff and additional topographies like outlines and countered from finger print and iris are castoff for verification. We precast few existing methods of the multimodal biometric techniques and proposed a better multi biometric technique to overcome the existing method limitations.

A. Android Built Multimodal Biometric Validation

Xinma Zhang, et.al [1] plan and cultivate an effective Android founded multimodal biometric validation method through face and voice. In view of hardware presentation restraint of smooth incurable, containing RAM, GPU, and CPU etc., that cannot capably undertake the responsibilities of loading and speedily handling great quantity of information, a face recognition technique is presented to professionally abandon redundant circumstantial of images and diminish the redundant information. Additionally, an enriched indigenous binary design coding technique is obtainable to progress sturdiness of mined face features. They likewise increase the conservative endpoint finding knowledge, called as voice action discovery method, that can competently upsurge recognition accurateness of voiceless and changeover information and increase voice identical efficiency. To increase verification accurateness and efficiency, they existent an adaptive fusion approach which progressively assimilates qualities of face and voice biometrics instantaneously. The cross authentication trials with public folders establish encouraging verification presentations associated with certain modern approaches.

B. Multimodal Biometric using Iris and Finger Knuckles

Abderrahmane et.al [2] multi-biometric method to validate consumers founded on their foremost knuckle finger arrays by four limbs besides iris is projected. An indigenous grain descriptor specifically binaries numerical image topographies takes remained working to excerpt the topographies for every of biometric qualities deliberated in order to progress biometric founded personal confirmation. The evaluation outcomes on PolyU contact less hand dorsal imageries databank and iris databank specify that projected multi-biometric verification with consortium function founded score fusion outstrips prevailing renovation founded union methods.

C. Face-Iris founded Biometric Verification

Basma et.al [3] proposes a face and iris multimodal bio-metric arrangement founded on hybrid glassy fusion. Its standard is acknowledgment of individual by combining numerous interactive and bodily personalities or fusing numerous uni-modal biometric schemes by dissimilar stages of fusion. The projected structures are chief extracted from face and iris modalities and remain founded on 2D Gabor filter. SRKDA is formerly smeared on mined structures set in instruction to choice the appropriate and differentiate ones. The projected scheme is appraised on CASIA Iris databank and investigate fallouts achieved have revealed its enactment in authentication mode associated to prevailing modern systems.

D. Sparse Representation Based Multimodal Biometric

Ke Meng, et.al [4] propose a multimodal authentication scheme assimilating ear and face founded on sparse illustration founded classification. Ear and face enquiry examples are major prearranged correspondingly to originate Sparsity founded match grooves, and that are formerly collective through sum instruction for confirmation. Our influence is twofold: first, custom two Sparsity founded metrics and dual biometric qualities to establish the greater enactment of SRC founded confirmation to well-known multimodal fusion approaches by cosine relationship LLR, SVM and the Second one empirically examine softness and possibility of SRC founded confirmation and authenticate association amongst its presentation and inter class reparability of examples in dictionary. The SRC founded one too several assessment is not desirable to biometrics or situations where mediocre interclass severability is accessible.

E. Finger Knuckle Biometric Authentication

Jayapriya et.al [5] proposes Finger Knuckle Print (FKP) based biometrics one of novel emergent modality castoff for gratitude of a discrete. Finger Prominence is rich in feel, a contactless biometric mannerism with extremely unique features. In this exertion, Gabor filter quality founded arithmetical methodology is castoff to excerpt feature vector as of respectively segmented FKP. In adding, KNN procedure is castoff to train scheme for removing feature vector. PolyU databank and IIT Delhi databanks are castoff to check the projected FKP biometric verification. Projected FKP biometric verification method is employed and tentative outcomes display that average proficiency of procedure.

F. Multimode verification founded Electronic voting Kiosk

Gurubasavanna et.al [6] deliberates about stages to alleviate the sanctuary concerns and how chance out in voting can remain augmented by familiarizing voter to partake the capability to vote as of any electorate level if he fits to some additional electorate from selected sanctioned voting interiors. The polling procedure can be prepared additional protected by connecting finger print or bio metric founded verification in project laterally through iris and face gratitude topographies. Paper also deliberates how raspberry-pi can be employed to construct the original.

G. ARM7 Based Biometric Security

Ramesh et.al [7] we are competent to gather the client limb patterns and mobile number at similar time as commencement cabinet currency payable then customer most operative get correct of entrance to locker device. By insertion of finger at the component though it become correct of entrance to mechanically produces each time detailed four number code as a communication to cell of accredited customer through GSM modem associated to microcontroller. The code gotten by method of customer have to be arrived by resources of crucial keys at keypad. Subsequently pending hooked on it payments whether or not it is heaps a lawful one or currently not and leases in client for additional get correct of entrance to.

H. Dual Biometric Authentication

Tripty et.al [8] proposed a method using the preprocessed iris imageries of any individual and thumb print, the outlines and countourlets are attained. Localization trailed by a stabilization of an iris images is agreed for feature abstraction by Gabor convolution, although minutia abstraction of an improved fingerprint images is prepared by Crossing Number technique. These topographies of countourlets and contours gotten as of a tested tributary and in instruction to acquire the similar notches, they are projected with examples in database. Evaluation methods castoff are Euclidean and hamming distance correspondingly for fingerprint and iris. Design of resemblance and transformation of notches are attained after transient of corresponding to grouping section. The score gotten lastly is castoff to apprise whether individual is authentic or bluffer. For a serious condition together scores necessity to be accorded means for high sanctuary connected submissions together the notches necessity to be coordinated independently so the mixture will stretch recovered outcomes.

III. PROPOSED METHODOLOGY

We propose a better multimodal biometric system with face and thumb as basic biometric inputs. The figure below shows the encryption and decryption of the complete module.

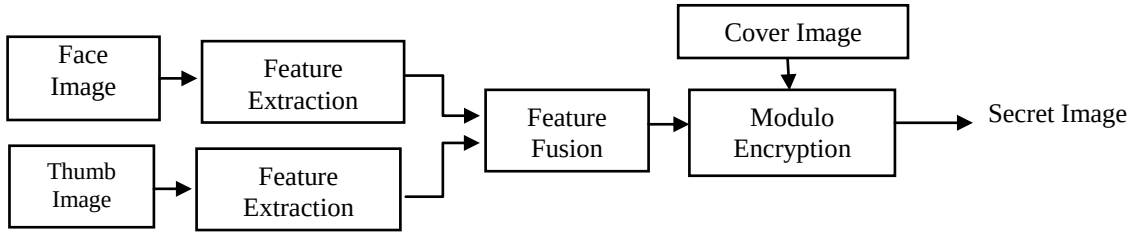

Figure 1. Encryption Block

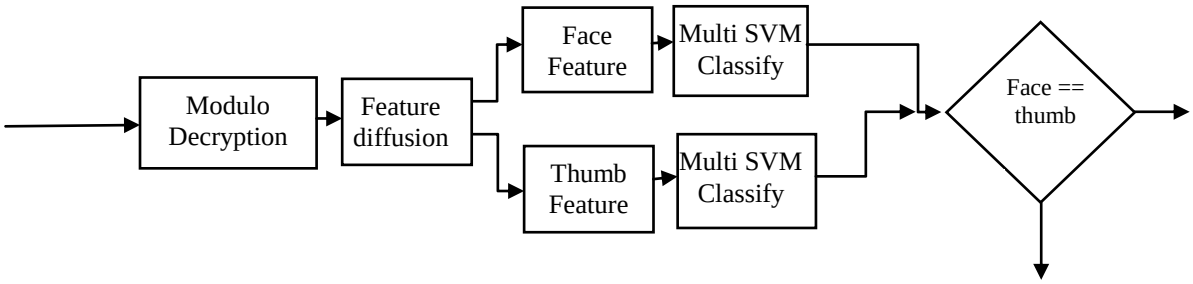

Figure 2. Decryption and authentication block

As an initial step the user is required to select the cover image which is used to encrypt the features and sent to the receiver. In the next step the user selects the text images for face and thumb, for which the Harris features are been extracted. Out of the complete extracted features, we choose only the maximum effective features from both face and thumb are fused by concatenation. The features are hidden using modulo operator with the prefixed bit of the image pixels and saved in local which is later transmitted to authenticator. The detailed flow of the same is shown in figure 1 above. At the receiver end the secret image is loaded and features are decrypted using modulo operator with same bit decryption given during encryption. The decoded features are diffused into face and thumb features, which are compared with the database authorized features using multi-SVM. The individual result of multi-SVM are cross checked for matching as a secondary authentication. If both the face and thumb choose are of a same person then the authentication is done successfully. Figure 2 shows the flow of decryption in detail.

A. Importance of face in biometric:

Biometric authentication in smart phones was familiarized approximately five years ago once iPhone flung its thumbprint scanner in 2013. It remained one of things about iPhone that was insignificantly examined. Currently, five years far along, it looks like an essential safety feature for smart phones. Fast onward few years and iPhone X blows everybody to thump on Facial Acknowledgement. The Face ID option in iPhone eradicated necessity for a fingerprint scanner, permitting customers to unravel their phone deprived of exploit whatever. Now closely every novel smartphone in marketplace has face recognition feature. Facial acknowledgment proposals a speedy, involuntary, and unified authentication experience. Seamless incorporation since there's no necessity of explicit hardware, modest mobile or webcam is sufficient. Facial acknowledgment is quite suitable, as modest as captivating a photo.

B. Importance of face in biometric:

Francis Galton composed a book named fingerprint in 1892. Thumb print was the first volume that put nimble on prominence of thumb print documentation in human lifecycle. It expressions how thumb print can be castoff as unique uniqueness tools. In 2018 we practiced the changeover of upcoming creation. Where we practiced self-driving car, AI, uprising of robots and drone, and digitalization of each aspect of our lifespan. At the similar period till day, we still challenged subjects like uniqueness theft, keyword breach, bank operation rupture and many more. These problems are unceasingly knocking prominence to such arrangement that is exclusive, remain unaffected and incredible to break.

Not only that such exclusive structures were employing prominence to streamline more methodology for government and business agencies that might make their process easy, safe and effective than forever before. Yes, we texture the prominence of thumb print documentation scheme in 2018 and will discover it's indispensable in 2020 too in many phases of our lifecycle.

A thumbprint in its narrow wisdom is an imprint left by the friction edges of human limb. Biometrics denotes to quantity and examine human body features such as thumb print gratitude. Fingerprint gratitude is potential by the fingerprint scanner.

C. Harris Features

Harris Corner Finder is a corner recognition operative that is usually castoff in computer vision processes to excerpt corners and gather structures of an imageries. It was first familiarized by Stephens and Harris in 1989 upon the development of Morava's corner finder.[1] Associated to the preceding one, Harris' corner finder proceeds variance of curve score hooked on explanation with orientation to course straight, as an alternative of consuming shifting blotches for each 45 degree viewpoints, and partakes been shown to be extra precise in distinctive amongst corners and edges.[2] Subsequently then, it partakes remained enhanced and accepted in numerous procedures to preprocess imageries for succeeding submissions.

D. Modulo operator based encryption and decryption

Embedding using modulo operator:

The unspecified integer features are embedded hooked on cover image by correcting pixel standards of objective models. Pixel standards of cover auditory are distributed by 16. Remainders are matched with target hexadecimal numbers and pixel of cover images are attuned in such a way that the residue is equivalent with objective hexadecimal numbers.

For liability this modification the frontward and backward alterations are designed by subsequent formula:

- Frontward Transformation f := diff-rem
- Retrograde Variance b:= rem+16–d if rem<=diff,
- while Forward Alteration f :=diff+16- rem and
- Regressive Alteration b: = rem-diff if rem > diff, where rem is outcome of modulo 16 processes and diff is objective hexadecimal characters.
- Founded on alterations cover pixel worth (p) is transformed to procedure the stego pixel worth.

Decryption Using Modulo Operator:

For mining target numbers as of stego image at receiver end major string dimension is take out from 16 amounts by typical LSB withdrawal method. At receiver side hidden data bounty standards are shared by 16 and residues of partition are hidden hexadecimal numbers. Now this is direct to the post handling method to get unique target topographies. Hexadecimal digits are transformed to their 4 bit binary equal. Each of the 4 bits is combined to form a binary text. Then each 7 bits are amended and transformed to their conforming decimal corresponding. The typescripts of ASCII standards are concatenated as per string dimension to develop original objective string.

E. Multi-SVM Classifier

Multiclass SVM targets to allocate tags to illustrations by using support vector machines, where the tags are strained from a limited set of numerous fundamentals. In ML, support vector machineries are overseen learning prototypes with supplementary knowledge procedures that examine data and identify designs, castoff for grouping and deterioration study.

The final authentication is done with a simple IF condition: if the face and thumb detected are of the same person the result is finally authenticated as successful.

IV. RESULT AND DISCUSSION

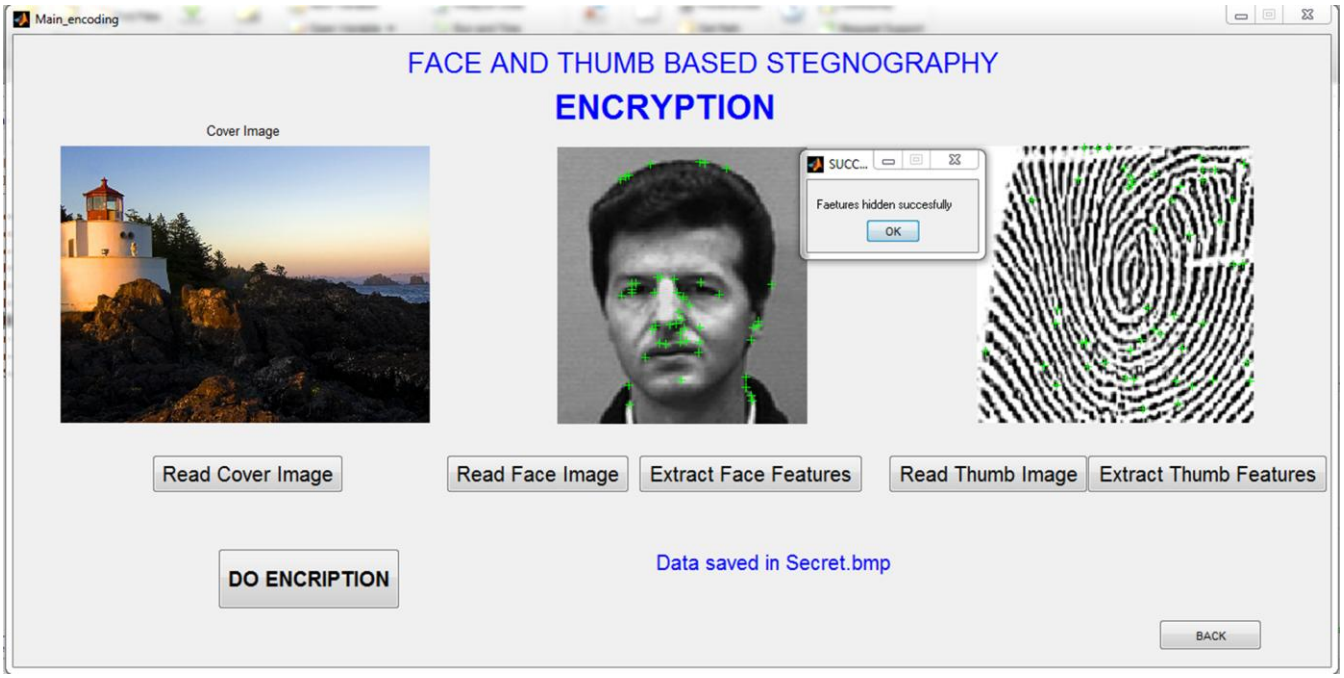

Figure 3. Resulted output of encryption

The above figure 3 shows the output screenshot of the complete encryption technique. We can observe the though there exist many corners for the thumb and face images we choose the best corners and hide the same in the cover image.

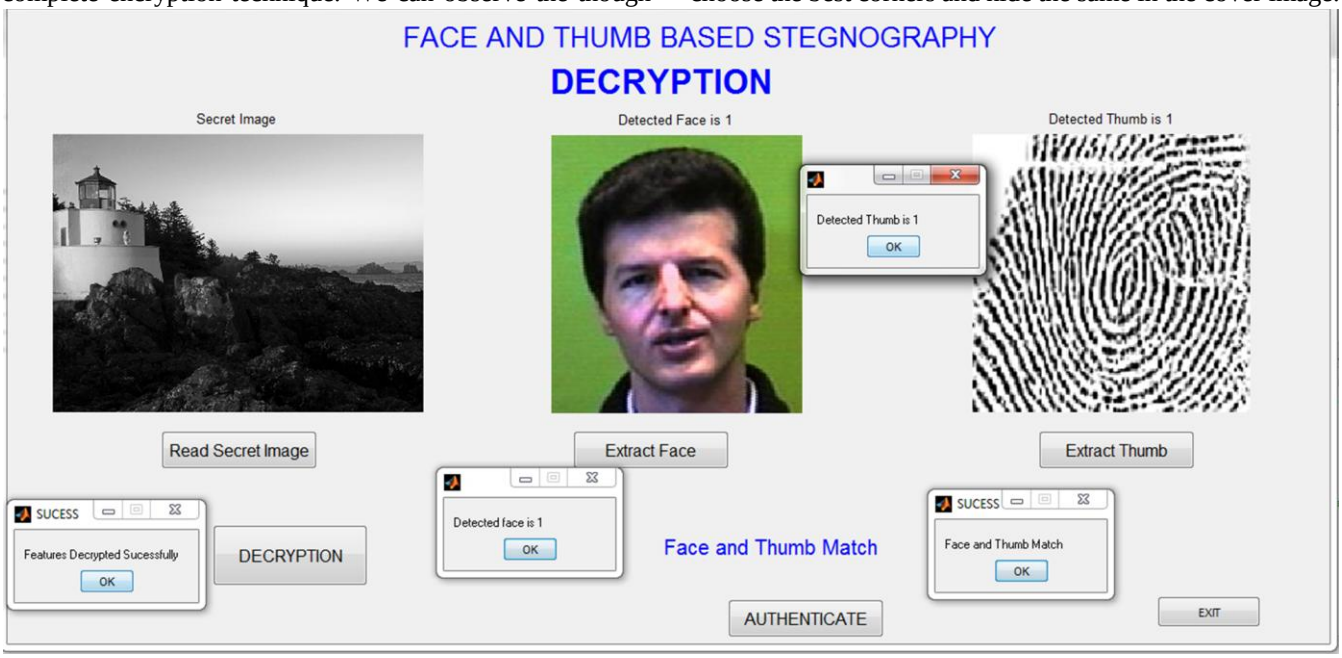

Figure 4. Resulted Decryption and Successful authentication

We can observe from the above figure 4, displaying face and the thumb chosen are of same person and hence the authentication was done successfully. We also verified by choosing images of face and thumb of different person during this the system was not authenticated.

V. CONCLUSION

Proposed methodology was given a best authentication. The study suggests a protected, biometric founded data hiding procedure by means of two stimulating work planetary: thumb and face features stenography seeing encryption. Henceforth, the project ambitions at conjoining encryption that can be beneficial for smart biometric authentication techniques.

FUTURE SCOPE

The method can be further updated by using an additional biometric like eye or nose to make the system little more complex. As an additional feature we can include OTP or pin based authentication which makes the system more secure. Different kind of features can also be included to which gather maximum information of face and thumb.

REFERENCES

1. X. Zhang, D. Cheng, P. Jia, Y. Dai and X. Xu, "An Efficient Android-Based Multimodal Biometric Authentication System With Face and Voice," in IEEE Access, vol. 8, pp. 102757-102772, 2020, doi: 10.1109/ACCESS.2020.2999115.
2. A. Herbadji, N. Guermat, L. Ziet and M. Cheniti, "Multimodal Biometric Verification using the Iris and Major Finger Knuckles," 2019 International Conference on Advanced Electrical Engineering (ICAEE), Algiers, Algeria, 2019, pp. 1-5, doi: 10.1109/ICAEE47123.2019.9014704.
3. B. Ammour, T. Bouden and L. Boubchir, "Face-Iris Multimodal Biometric System Based on Hybrid Level Fusion," 2018 41st International Conference on Telecommunications and Signal Processing (TSP), Athens, 2018, pp. 1-5, doi: 10.1109/TSP.2018.8441279.
4. K. Meng, Z. Huang, X. Wang and K. Wang, "Multimodal Biometric Verification Using Sparse Representation Based Classification," 2018 IEEE 3rd International Conference on Image, Vision and Computing (ICIVC), Chongqing, 2018, pp. 26-31, doi: 10.1109/ICIVC.2018.8492886.
5. P. Jayapriya and R. Manimegalai, "Finger Knuckle Biometric Authentication using Texture-Based Statistical Approach," 2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW), Erode, India, 2018, pp. 170-174, doi: 10.1109/I2C2SW45816.2018.8997143.
6. M. G. Gurubasavanna, S. Ulla Shariff, R. Mamatha and N. Sathisha, "Multimode authentication based Electronic voting Kiosk using Raspberry Pi," 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Palladam, India, 2018, pp. 528-535, doi: 10.1109/I-SMAC.2018.8653726.
7. K. Ramesh, M. V. Prasad and K. Hemachandran, "Design and implementation of advanced ARM7 based biometric security system using wireless communication," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2018, pp. 543-546, doi: 10.1109/ICISC.2018.8398859.
8. M. Hammad, Y. Liu, and K. Wang, "Multimodal Biometric Authentication Systems Using Convolution Neural Network based on Different Level Fusion of ECG and Fingerprint," IEEE Access, vol. 7, pp. 26527-26542, 2018.
9. S. Nakagawa, L. Wang, and S. Ohtsuka, "Speaker identification and verification by combining MFCC and phase information," IEEE Trans. Audio Spe., vol. 20, no. 4, pp.1085-1095, 2012.
10. W. Yang, Z. Wang, and B. Zhang, "Face recognition using adaptive local ternary patterns method," Neurocomputing, vol. 213, pp.183-190, 2016.

AUTHORS PROFILE

Ms. Pallavi S Biradar is pursuing her M-Tech from RV College Of Engineering Banglore in the department of Electronics and Instrumentation Engineering (Specialisation-Biomedical Signal processing and Instrumentation Engineering) since 2019. She has obtained her B-Tech (Electronics and Communication Engineering) from PES University Bangalore in the year 2018. Her area of interest will be in research in Image processing.

Dr. Anand Jatti is an Associate Professor in the Department of Electronics and Instrumentation Engineering for R V College of Engineering, Bengaluru, since 2002. He has pursed his Ph.D. in Digital Image in the field of Bio-medical image processing for VTU, Belgaum. He have published around 60 research presentations and publications in national and international journals. He was also been an as review committee member in around 10 journal publications as a review committee member. He is having 3 years of industrial and 19 years of academic experience, he also filed one patent in his name.