IMAGE QUALITY ASSESSMENT FOR FAKE BIOMETRIC DETECTION: APPLICATION TO FINGERPRINT AND FACE RECOGNITION

[1]SAKIL ANSARI, [2]V.KAMAKSHI PRASAD

Department Of CSE, College of Engineering, JNTUH, Kukatpally, Hyderabad, Telengana, India
E-mail: [1]sakilansari4@gmail.com, [2]kamakshiprasad@jntuh.ac.in

Abstract- The presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication and that requires the development of new and efficient protection measures. Here, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The proposed system aims to enhance the security of biometric recognition frameworks. The proposed system is tested on real time recognition from a web camera and on the publicly available dataset. The experimental results, which were obtained on publicly available data sets of fingerprint and 2D face, show that the proposed method is highly competitive compared with other state-of-the-art approaches and the analysis of the general image quality of real biometric samples reveals highly valuable information which may be very efficiently used to discriminate them from fake traits.

Index Terms- Attacks, biometrics, countermeasures, image quality assessment, security.

I. INTRODUCTION

The interest in the evaluation of biometric systems security has been increasing day by day that leads to the creation of numerous and very diverse initiatives that focused on this field of research[1] that includes the publication of many research works disclosing and evaluating different biometric vulnerabilities[2], [3], the proposal of new protection methods[4, 5, 6], related book chapters[7] the publication of several standards in the area, the dedication of specific track sessions and workshops in biometric-specific and general signal processing conferences[8, 19],and the organization of competitions that focused on vulnerability assessment, the acquisition of specific datasets, the creation of groups and the laboratories specialized in the evaluation of biometric security, or there may be the existence of several European Projects with the biometric security topic as main research interest.

The above all these initiatives clearly highlight the importance given by all parties that involved in the development of biometrics to the improvement of the systems security that brings rapidly emerging technology into practical use. The speed and very low complexity of the proposed technique is an added advantage that makes it very well suited to operate on real scenarios (one of the desired characteristics of this type of methods). As we know that it does not deploy any trait-specific property (e.g., minutiae points or face detection), the computation load needed for image processing purposes is very reduced and by using only general image quality measures fast to compute and combined with very simple classifiers. The system has been tested on publicly available attack databases of fingerprint and 2D face and also on real time. The proposed system has reached results fully comparable to those obtained on the same databases and here we follow the same experimental protocols by more complex trait-specific top-ranked approaches from the state-of-the-art.

II. LITERATURE SURVEY

In the entitled Paper Javier (Galbally Z.Wei, 2014), introduced a novel software-based multi-biometric and multi-attack protection method that targets to overcome part of limitations through the use of image quality assessment (IQA). It is not capable of operating with a very good performance under different biometric systems and also for diverse spoofing scenarios. In the paper (Poonam Dabas Z.Wei, 2013), introduced objective methods for measuring the quality of images. In this paper, the proposed method focused on the various quality measures and an algorithm to model HVS (Human Visual System). The properties of HVS are perceived brightness and frequency response and HVS is used to process input images.

The Approach of this paper [9] is based on the fact that hiding information in digital media requires alterations of the signal properties that introduce some form of degradation. The addition of a watermark or message leaves unique artifacts that can be detected using Image Quality Measures (IQM) is shown in this paper. The paper proves that image quality assessment can be used to discriminate between cover images and

stego-images. The paper also proves that the hypothesis that message-embedding scheme leave statistical evidence or structure in images that can be exploited for detection. In this paper [9], a new universal objective image quality index, which is easy to calculate and applicable to various image processing applications is proposed. The index is designed by modeling any image distortion as a combination of three factors:

A. Loss of Correlation

Here, the degree of linear correlation between x and y is measured. Its dynamic range [-1, 1].

B. Luminance Distortion

It will measure how close the mean luminance is between x and y. Here the dynamic range is [0, 1].

C. Contrast Distortion

It will measure how much similar are the contrasts are. Here the dynamic range is [0, 1]. The paper proves that the index outperforms the traditional method of error calculation of images for quality.

III. IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

In this paper, we have assumption that: "It is expected that a fake image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario for which the sensor was designed." Here, expected quality differences between real and fake samples may include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both type of images (entropy), structural distortions or natural appearance like face images captured from a mobile device will probably be over- or under-exposed; and fingerprint images captured from a gummy finger present local acquisition artifacts such as spots and patches. By following this "quality-difference" hypothesis, in the present research work we explore the potential of general image quality assessment as a protection method against different biometric attacks. Since the implemented features do not evaluate any specific property of a given biometric modality or of a specific attack so they may be computed on any image and the proposed method gives a new multi-biometric dimension. In the proposed state-of-the-art, the reasons behind the use of IQA features for liveness detection is supported by three factors:

1. The previous works for image manipulation detection [11, 12], and steg analysis [13, 14] in the forensic field has successfully used image quality. To an extent, various spoofing attacks like those which involve taking a picture of a facial image displayed in a 2D device (e.g., spoofing attacks with printed face images), may be regarded as a type of image manipulation which can be effectively detected, as shown in the proposed research work, by the use of different quality features.

2. The previous studies in the forensic area and different features measuring trait-specific quality properties have already been used for liveness detection purposes in fingerprint applications [5].This work gives a solid basis to the use of image quality as a protection method in biometric systems.

3. As human observers very often refer to the "different appearance" of real and fake samples to distinguish between them. So, different metrics and methods designed for IQA intend to estimate in an objective and reliable way the perceived appearance of images by humans. In the proposed system, we have used different quality measures to differentiate between real and fake images.

IV. PROPOSED METHOD

In this proposed method, we present a novel fake detection model which can be used in multiple biometric systems to detect different types of fraudulent access attempts. The goal of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, using image quality assessment. In the designed system, for real time recognition, we are interfacing camera to Raspberry pi and the camera will capture face image of a person and send to controller. Face and iris of the person from the image will be recognized by the controller and the finger print module will take the finger print from the person and send to controller. Then after controller will recognize the finger print of person from the data base and if they are matched then it will display the data on display unit.

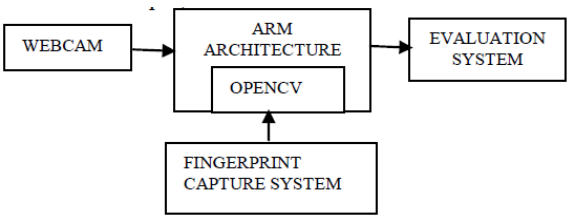

Fig.1 Architecture diagram for real time recognition from a web camera

A. Proposed algorithm for real time recognition

In real time recognition, at first we have collected at least 15 images from webcam and then after we have trained the collected images by using Linear Discriminant Analysis and finally we have tested the image of the same person (again image is taken from webcam).We have grabbed fingerprint of the person

from fingerprint scanner. Step wise description is given below.

1) Proposed Face Recognition

The process of putting a label to a known face is known as face recognition. The proposed algorithm includes the following four steps:

I. Face Detection
II. Face preprocessing
III. Training real time faces using Linear Discriminant Analysis (LDA)
IV. Face Recognition

Face Detection

The process of locating a face region in an image is face detection. In the proposed system, we have used Haar-based cascade classifier for face detection. This algorithm works for frontal faces, side-view faces, eyes, mouth, nose, etc.

Haar based cascade classifier:

It is an effective face detection method. At first, the algorithm needs a lot of positive images (images of faces) and negative images (images without faces) [15, 19] to train the classifier. After that, we need to extract features from it. Following are the Haar features:

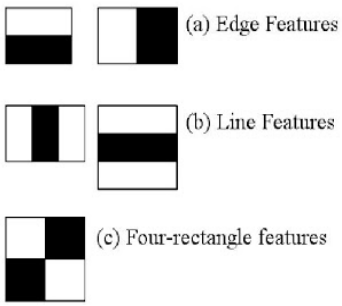

Fig.2.Haar features

The above features are just like our convolutional kernel and each feature is a single value obtained by subtracting sum of pixels under white rectangle from sum of pixels under black rectangle. Then all possible sizes and locations of each kernel is used to calculate plenty of features. We need to find sum of pixels under white and black rectangles for each feature calculation. Integral images are introduced to solve this and it simplifies the calculation and among all calculated features, most of them are irrelevant. So we will get over 160000 features and among them, we have to select the best feature and to obtain the best feature, we apply each and every feature on all the training images. It finds the best threshold which will classify the faces to positive and negative for each feature. The concept of this classifier is that instead of using all features on a window, group the features into different stages of classifiers and apply one-by-one.

Haar based cascade classifier using openCV:

In openCV, XML files [15] are stored and contains many pre-trained classifiers for face, eyes, smile etc. There are many cascade classifier in openCV like face detector, eye detector, mouth detector, etc.

Steps for Face Detection:

Loading Haar detector:

Here, pre trained XML file is loaded to perform face detection.

a. Accessing the webcam

Here, we access the webcam from the computer to grab the image.

b. Detecting a face using the Haar Classifier

Before detecting face in camera frame, we should perform the following steps:

i. Grayscale color conversion

As face detection only works on grayscale images. Therefore, we should convert the color camera frame to grayscale.

ii. Shrinking the camera image

The size of the input image determines the speed of face detection i.e. it is very slow for large images but it is very fast for small images and detection is fairly even for low resolution. Thus, we should shrink the camera image to a more reasonable size.

iii. Histogram equalization

We should perform histogram equalization to improve the contrast and brightness because face detection is not as reliable in low-light conditions.

After performing these above preprocessing steps, we can now detect the face.

iv) Face pre-processing

As face recognition is extremely vulnerable to changes in lighting conditions, face orientation, face expression, thus, it is very important to reduce these differences as much as possible. In the proposed system, we have used histogram equalization for face preprocessing. For our convenience, the proposed system only uses eye detection and we ignore other facial features like mouth, nose etc.

v) Eye detection

It is a very useful for face preprocessing, because for frontal faces we can always assume a person's eyes should be horizontal and on opposite locations of the face and should have a fairly standard position and size within a face, although there are changes in facial

expressions, lighting conditions, camera properties, distance to camera, and so on. We have used pre-trained XML files for eye detection.

vi) Eye search regions

The proposed system shows both left and right eyes region with small rectangle when the system captures the image. After this step, we perform the following steps:

a) Geometrical transformation and cropping: It includes scaling, rotating, and translating the images so that the eyes are aligned and then followed by the removal of the forehead, chin, ears, and background from the face image.

b) Separate histogram equalization for left and right sides: This step standardizes the brightness and contrast on both the left- and right-hand sides of the face independently.

c) Smoothing: Here, the image noise using a bilateral filter is reduced.

d) Elliptical mask: Here, the elliptical mask removes some remaining hair and background from the face image.

vii) Training real time faces using LDA

We can easily collect the face from the camera. This step includes training phase and testing phase.

Training phase:

Distinguishing between the faces from different people is training phase and collecting the faces from the camera is training set. After collecting faces from the camera, we should train the faces.

The proposed system is trained by using LDA.

Linear Discriminant Analysis:

LDA is a powerful statistical face recognition technique that overcomes the limitation of Principle component analysis technique by applying the linear discriminant criterion [16].The criterion tries to maximize the ratio of the determinant of the between-class scatter matrix of the projected samples to the determinant of the within class scatter matrix of the projected samples. It helps to group images of the same class and separates images of different classes of the images. It is based on 1D eigenvector matrices that appear somewhat like faces when viewed as 2D images [12]. Its basic principle is that it calculates one special eigenvector and eigenvalue for each person. In the proposed system, we have used openCV function to access internal data structures of LDA. These data structures are used for mathematical calculations. These data structures are usually stored as floating-point numbers typically ranging between 0.0 and 1.0.They are often either a 1D row or column matrix.

viii) Face Recognition

In this step, we find that who a person is just from a facial image. Here we have used Fisher face algorithm for face recognition. In the proposed system, we have used openCV function to recognize the faces. In openCV, there are many FaceRecognizer algorithms. In our system, we have used Fisher face algorithm. Face verification can be done to confirm if the result of the prediction is reliable or whether it should be taken as an unknown person.

The facial verification can be done by reconstruction of facial images followed by calculating similarity between reconstructed images and input images. We use openCv functions to perform above steps. Thus, we have used fisher faces algorithm, it needs higher threshold so here we have used threshold, say 0.7.

2) Proposed Fingerprint recognition method

Fingerprint is another biometric check to the system. In the proposed system, we have used openCV for fingerprint. Here, we grab the fingerprint [18] of the person at registration time and then we verify the fingerprint at verification time in real time verification.

Binarization:

It is the process of converting a pixel image into binary image. At first, we grab the image from the fingerprint scanner and apply binarization. It enables us to remove any desired noise from the image and help us to make the contrast better between the kin and the wrinkled surface of the finger. In the proposed system, we have two phases: Register phase and another is verify phase.

During register phase, fingerprint is grabbed from fingerprint scanner and features points are stored in the buffer in hexadecimal form. Now during verify phase, again the fingerprint is taken from fingerprint scanner and here also the feature points are stored in buffer in hexadecimal form. If the previous feature point values match with the current feature point then authentication is success otherwise authentication is failed.

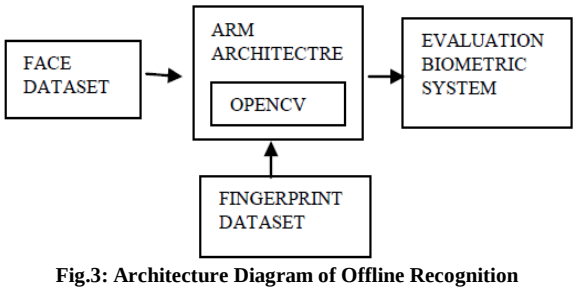

Fig.3: Architecture Diagram of Offline Recognition

B. PROPSED ALGORITHM FOR OFFLINE DATASET

In offline recognition, we have used publicly available dataset for both face and finger which is explained below.

1. Proposed Face Recognition:

The proposed system includes mainly following three steps in face recognition:

i)In first step, we have to find a good database of faces with multiple images for each individual.

ii) The second step is to detect faces in the database images and use them to train the face recognizer.

iii) The third step is to test the face recognizer to recognize faces it was trained for.

Dataset:

In the proposed system, we have used publicly available AT &T "The Database of faces" also known as "The ORL Database of faces". This database has ten different images of each of 40 distinct subjects. The images were taken at different times, varying the lighting, facial expressions (open or closed eyes, smiling or not smiling) and facial details such as glasses or without glasses for some subjects. The images were taken against the dark homogeneous background with subjects in an upright and frontal positions.

We have used all the files in PGM format. Here the size of each image is 92 ×112 pixels and having 256 grey levels per pixel. In the proposed system, the images are organized in 40 directories i.e. one for each subject and having names of the form SX, where X is the subject number from 1 to 40.In each of the above directories, there are ten different images of that subject that have the names of the form Y.pgm, where Y indicates the image number for the subject between 1 to 10.

Testing phase

We have used fisher faces algorithm in our proposed system. Here we form test dataset. So we take one image from each subject and we form test dataset .Here in the test dataset 40 images for 40 subjects and all the images are converted into bitmap (.bmp) image format.

Training phase:

Here we form training dataset from ORL database by extracting 40 images that are present in test dataset. Now for each person, we have 9 different images in all 40 directories. Now we have total 360 images in our training dataset. Here also, all the images are converted into bitmap (.bmp) image format.

2. Proposed Fingerprint recognition method:

Fingerprint of a person is the secondary biometric check to the system. We have used publicly available databases for the fingerprint. The following diagram shows the images of fingerprint taken from publicly available dataset:

Fig 4: Fig. Images of Fingerprint Dataset:

The system is built by publicly available dataset. The datasets are DB1, DB2, DB3 and DB4.In these databases, the prints of 10 individual is available with 8 different positions of prints of each individual. Out of 8 positions of prints, 4 are used for training purpose and 4 are used for evaluating the system.

Procedure:

i) First we grab the fingerprint from the system and then we have to apply Binarization. Binarization helps in removing noise and also it helps to make the contrast better between the kin and the wrinkled surface of the finger. The following figure 5 shows the comparison between grayscale and binarized fingerprint image:

ii) After obtaining binary image, we are ready to calculate our feature points and feature points descriptors. We skeletonize the image to improve the process a bit more. The skeletonization process creates more unique and stronger interest points. The skeletonization process is based on Zhang-Suen line thinning approach. The following figure 6 shows the Comparison between binarized and thinned fingerprint image using skeletonization techniques:

Fig.6 Comparison between binarized and thinned fingerprint image using skeletonization techniques.

iii) After getting skeleton image, we go for crossing points on the ridges of the fingerprint called minutiae points. We have used Harris Corner Detector for this purpose. The following figure 7 shows the Comparison between thinned fingerprint and Harris corner response, as well as the selected Harris corners.

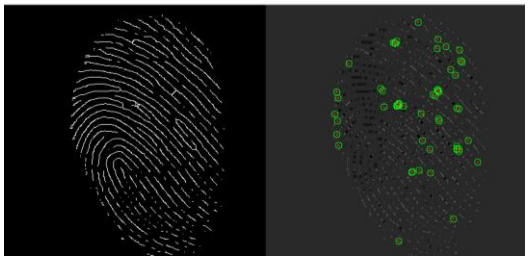

Fig.7 Comparison between thinned fingerprint and Harris corner response as well as the selected Harris corners.

iv) After getting key points, now we have to create some of formal descriptor of the local region around that key point to be able to uniquely identify it among other key points. In the designed system, we have used scale invariant feature transform (SIFT) descriptor. This helps to calculate the descriptors. Now we can retrieve a descriptor for each detected key point of any given fingerprint.

v) Now we have database containing a set of feature descriptors for the training persons in the database. Suppose we have a single new entry, consisting of multiple descriptors for the key points found at registration time and now we have to match these descriptors at registration time with the descriptors stored in the database to see which one has the best match. In the proposed system, we have used a brute force matching using the hamming distance criteria between descriptors of different key points.

vi) Now we have all the matches stored in the database i.e. we have each matching couple we will have the original key point, the matched key point and a floating point score between both matches, representing the distance between the matched points. We have performed Euclidean distance to perform matching process. We go for the biggest score in order to select the best match. The following figure 8 shows the matching process visualized.

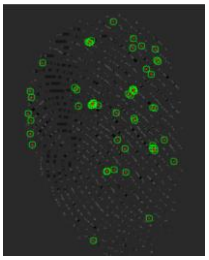

Fig.8 a. Original key points

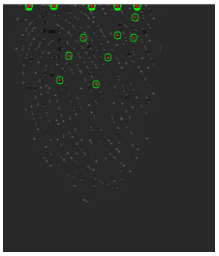

Fig.b. Matched key points

V. EXPERIMENTAL RESULTS

A. Real Time Recognition from Webcam

Images collected through web camera are shown in Fig [9]. For better performance, we should take at least 15 images from the camera. In the proposed system,face of the image captured by the camera has been recognized with similarity of 93% and fingerprint authentication has been successfully done.The experiment shows that image quality assessment plays a very important role in fake biometric detection. The result shows that facial expressions,lighting,position of the face while capturing image from the webcam helps in detecting fake images.For fingerprint biometric,the position of the finger at the time of taking fingerprint with the help of fingerprint scanner and the moisture present in the finger play a very important role in finger print authentication.The experiment shows that the position of the finger at the time of fingerprint registration and the posistion of the finger at the time of fingerprint verification must be identical.Figure 9 shows the image taken by the camera,figure 10 shows that image is taken at the time of testing from webcam,figure 11 shows the face recognition with similarity of 93% and figure 12 shows the fingerprint authentication has been done successfully.

Fig.9 Images captures from web camera

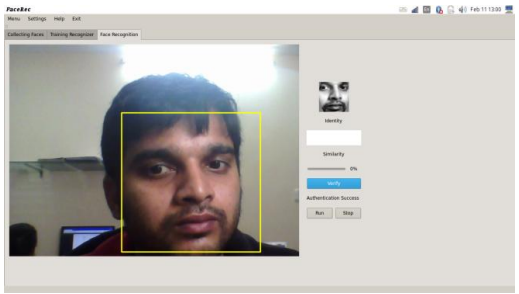

Fig 10: Image acquisition using web camera

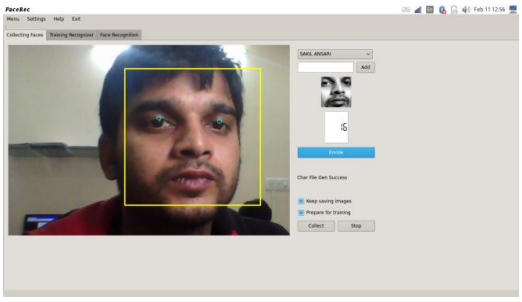

Fig 11: Fingerprint authentication

B. Recognition Performance of Dataset (offline Face Recognition)

In the proposed system, we have tested all our test images with image number 1 to 40 images. In the experiment, we get true result 37 times. This says that 37 images are correctly recognized by the face images of correct person. Here, we get false result 3 times i.e.3 images are recognized by face image of wrong person. The following table1 shows the true positive rate, true negative rate and performance of the system. True positive rate (TPR) is the ratio of the total number of recognized images to the total number of test images. True negative rate (TNR) is the ratio of the total number of unrecognized images to the total number of test images.

Table 1 Shows TPR, TNR and performance of the system

Test images	TPR	TNR	Accuracy (%)
40	0.925	0.075	92.5

The proposed experiment shows that in fake biometric detection: facial expression, illumination and pose variation play a significant role. The experiment also shows that face details i.e. images with glasses or images without glasses help in identifying fake face images. So we can say that image quality is very important for biometrics checks.

C. Recognition Performance of Dataset (Offline Fingerprint Recognition)

Table 2: Performance of Fingerprint on different databases

Databases(DB)	Current match score (%)
DB1	92.6
DB2	86.50
DB3	84.63
DB4	91.30

The above table shows the performance of the fingerprint in current match score. The above table shows the biggest match score. The prints having biggest current match score is the best match. We have recorded the best current match score in the above table 2.The experiment shows that the position and the condition of the fingers play important role in fingerprint biometric check. The current match score for different database are different as mentioned in table 2 and we know that these databases are taken from different types of sensors. The experiment shows that if the feature points of the fingerprint at the time of registration match with the feature points of the fingerprint at the time of verification then the authentication is successful otherwise the authentication is failed. This proves that the position of the finger plays a very important role in fake biometric detection.

CONCLUSION

We can say that the study of the vulnerabilities of biometric systems against different types of attacks has been a very active field of research in recent years [1] and this leads to big advances in the field of security-enhancing technologies for biometric-based applications. The human eye finds difficult to make a distinction between real image and fake image after a short inspection when both real and fake images are very similar. Some differences between the real and fake images may become evident once the images are translated into a proper feature space. These disparities come from the fact that biometric traits have their own optical qualities (absorption, reflection, scattering, refraction), which other materials (paper, gelatin, electronic display) or synthetically produced samples do not possess. To provide good quality samples, sensors are designed. The proposed system has been evaluated on biometric modalities such as the fingerprint and face, using publicly available databases and as well as the face image captured by web camera and fingerprint scanner with well-defined associated protocols. The proposed system has been successfully designed and tested on both real time recognition and offline recognition. We successfully evaluated the performance of the designed system. The system uses publicly available dataset. The system uses different algorithms for recognizing different biometrics. The proposed work opens new possibilities for future work like use of video quality measures for video attacks, further evaluation on other image-based modalities like palm print.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.
[2] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in Proc. AWB, 2004.
[3] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," Pattern Recognit., vol. 43, no. 3, pp. 1027–1038, 2010.
[4] A.K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.
[5] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," Future Generat. Comput.Syst., vol. 28, no. 1, pp. 311–321, 2012.
[6] S. Venkatramaphanikumar and V. K. Prasad, "Nonlinear Face Classification with Modified 2DDTW," 2014 International Conference on Computational Intelligence and Communication Networks, Bhopal, 2014, pp. 223-227.
[7] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," Handbook of Biometrics. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.
[8] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.
[9] "Steganalysis Using Image Quality Metrics" Ismail Avcibas,, Member, IEEE, Nasir Memon, Member,IEEE, and Bulent

Sankur,Member IEEE,:IEEE TRANSACTIONS ON IMAGE PROCESSING,VOL. 12, NO.2, FEBRUARY 2003

[10] "Universal Image Quality Index", Zhou Wang, Student Member, IEEE, and Alan C. Bovik, Fellow, IEEE, IEEE Signal Processing Letters, march.2004

[11] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," J. Electron. Imag., vol. 15, no. 4, pp. 041102-1–041102-17, 2006.

[12] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 492–496, Sep. 2010.

[13] Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," IEEE Trans. Image Process., vol. 12, no. 2, pp. 221–229,Feb. 2003.

[14] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 111–119,Mar. 2006.

[15] http://docs.opencv.org/trunk/d7/d8b/tutorial_py_face_detection.html

[16] Chapter 8 of the book "Mastering OpenCV with Practical Computer Vision Projects", Packt Publishing, 2012

[17] Suman Kumar Bhattacharyya, Kumar Rahul, International Journal of Communication Network Security, ISSN: 2231 – 1882, Volume-2, Issue-2, 2013.

[18] Venkatramaphanikumar S, V Kamakshi Prasad, "Multi Feature Based Fingerprint Recognition With Score Fusion", International Journal of Applied Engineering Research, Vol. 10, No. 8, pp. 20393-20402, 2015.

[19] M. Sadanandam ,Dr. V. Kamakshi Prasad, "Robust features for GMM Based Language Identification System", International Journal of Speech Technology, Vol No.17, Issue No.2, pp.99-105, 2014.

★★★