FAKE FACE DATABASE AND PRE-PROCESSING

Aruni Singh, Sanjay Kumar Singh and Shrikant Tiwari

Department of Computer Engineering
IIT(BHU), Varanasi, India
arunisingh@rocketmail.com
sks.cse@itbhu.ac.in
shrikant.rs.cse@itbhu.ac.in

ABSTRACT

Face plays an ethical role in human interaction compared to other biometrics. It is most popular non-intrusive and non-invasive biometrics whose image can easily be snapped without user co-operation. That is why; criminals and imposters always try to tamper their facial identity. Therefore, face tampering detection is one of the most important bottlenecks for security, commercial and industrial orbit. Face tampering detection is one of the most important bottlenecks for security, commercial and industrial orbit. In particular, few researchers have addressed the challenges for the disguise detection but inadequacy is benchmark database in public domain. This paper addresses these problems by preparing of three category of tampered face database within the framework of FRT (Facial Recognition Technology) and evaluates the performance of this database on face recognition algorithms. These categories of database are dummy, colour imposed and masked face.

KEYWORDS

Dummy Face, colour imposed face, masked face, Facial Recognition Technology, tampering.

1. INTRODUCTION

Due to wide application of biometric technology in information security, law enforcement, surveillance, and others, it plays a crucial role and attracts intensive interest from researchers for personal authentication. Among all biometrics, face plays an ethical role in human interaction. It is most popular non-intrusive and non-invasive whose image can easily be snapped without user co-operation [2]. That is why; criminals and imposters always try to hide their face by means of tampering. The sample image of cheating is shown in Fig.1. Therefore, face tampering detection is highly desirable in security, commercial and industrial orbit.

Techniques by which the imposters cheat the authentication system by presenting the fake biometric are known as spoofing. For security concern, research must be focus in the direction of accurate classification of image of real face from the image of tampered face because criminals or imposters always use different types of tampering mechanism for the concealment of their facial identity. If captured image from scene is image of real face then it needs to go to FRT otherwise switch towards other forensic techniques for imposter's and criminal's identification. It can be said that without spoofing measurement the advancement in FRT is defenceless to attack.

Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA - 2013
pp. 13–24, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3602

To develop any new methodologies or techniques, efficient and benchmark database is required. Although so many databases are available in public domain for FRT, but to the best of our knowledge, not even a single database of tampered face is available in public domain to test the performance of face recognition algorithms and to discriminate the real face from tampered face. For verification and validation of tampering detection methodologies, benchmark standard database is essential. For this purpose we have prepared real and tampered both type of face images of same subject.

Several research groups have built face databases with a lot of variations in poses, illuminations, snapshot time, follow-up time etc. for evaluating and comparing the performance of the face recognition algorithms. FERET database [12][13] contains 14051 eight-bit gray scale human face with frontal, left and right profile views, and quarter left and right views of images including variations in illumination and expression. It was created by FERET program, which ran from 1993 to 1997[14]. XM2VTS database [15][16] contains multimodal database of 295 subjects with follow-up after four months including speaking head shots and rotating head shots [14]. It is a huge video database containing wide range of pose angle variations. But it does not include any information about the time acquisition parameters, such as illumination angles, illumination colour or pose angle [14]. Yale B [17] contains gray face image of 15 subjects having 64 different lighting angles and 9 different poses, variation in light and expression. The lighting variations are as centred-light, left-light and right-light [14]. AR face database [18] contains colour image of 126 (70 males and 56 females) subjects having variation in illumination, expression, occlusion under strictly controlled environment and total 4000 colour frontal view images. The images were taken during two sessions. PIE Database [19][20] contains images if 68 subjects which were captured with 13 different poses, 43 different illumination conditions and 4 different facial expressions, for total 41,368 colour images with resolution of 640x486. MIT face database contains face images of 16 people having variations in pose, light, scale(zoom) including 6 levels of Gaussian pyramid [14]. ORL database contains face images of 40 people along with the variation of poses, expression snapshot time, background, occlusion, open eyes, close eyes and glass etc. [14]. PF01 database contains the true color face image of 103 people (53 males and 50 females) representing 17 variations (1 normal face, 4 illumination variation, 8 pose variation, 4 expression variations) per person [3].

The available literatures bear the witness that a large number of researchers have expended very much attention, efforts and time to develop the face image database for FRT. These efforts have led to the construction of large database with the wide variety of different faces. It is not out of place to mention here that to sweep out the deficiency of tampered face database, we have spent our contribution and prepared the database of both real and tampered face images of same subject.

This contribution is divided in six sections. Section 2 explains the database description with acquisition protocols and database profile and section 3 demonstrates issues and challenges for database acquisition. Section 4 demonstrates the database pre-processing for evaluation while section 5 contains performance of face recognition algorithms on tampered face images. Last section 6 includes conclusion and future scope.

2. DATABASE DESCRIPTIONS

The collection of a large number of heterogeneous objects in any domain is very challenging in all respect. Unlike face recognition, no standard benchmark database is available in public domain for tampering detection. Therefore, we have made our own protocol and prepared the database for vitality detection.

Fig. 1: The sample of cheating image (Adopted from [26])

2.1. Database Acquisition Protocol

For the effectiveness of database we have prepared four types of heterogeneous database using coloured 12.2 megapixels, 5x optical stabilized camera. The images have been taken at a distance of nearly 24 cm. to 30 cm. in an uncontrolled environment. The captured images are natural images without imposing any constraints neither on the targeted subject nor their surrounding such as background and illumination etc. More than 12 months of time have been spent for the database preparation. Samples of obtained face images are shown in fig. 2.

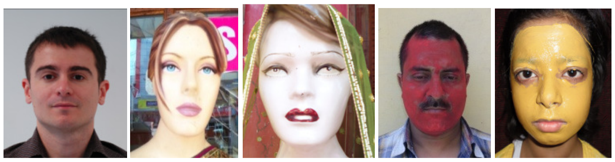


Fig. 2: Sample face images

For efficient and reliable database acquisition we have set our protocol and acquired the said database. We have taken the photographs of 10 pose (3 right pose, 4 left pose, 1 frontal pose, 1 pose 10^0 upward from front and 1 pose 10^0 downward from front) of each subjects. The camera position is set at the approximated angles shown in the Fig.3 and obtained sample images are shown in Fig.4. Angles between the poses are maintained by $\theta = {}^{x}/_{r}$ radians, where x is the 'arc' size and r is approximated distance of camera from the targeted subject [25]. We have taken the images in natural outdoor environment where neither camera nor targeted subjects are set at accurately fixed position. For database acquisition we have set a protocol to take the tampered face image on the same background and lighting effect as on real face imaging of same subjects.

2.2 Database Profile

For our assertion, we have prepared two types of database: Real face image database and tampered face image database.

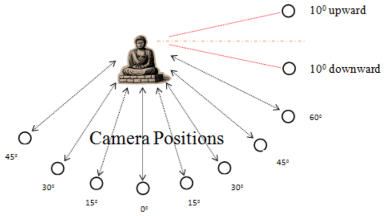


Fig. 3: Camera positions for the pose variation (adopted from [25])

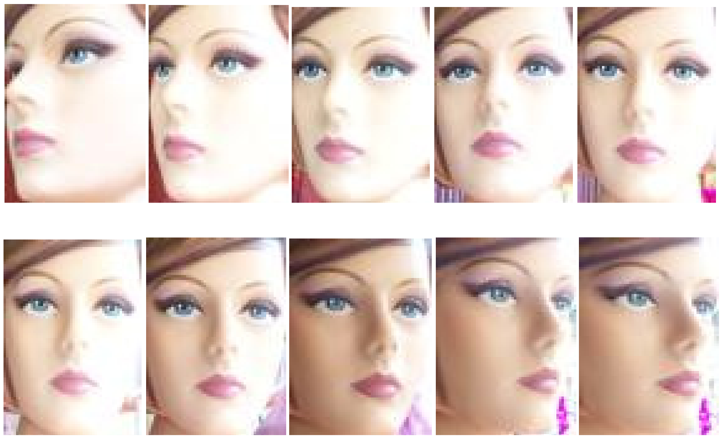


Fig. 4: Pose variation of captured face images (adopted from [25])

2.2.1 Real Face Image Database - For real face image database we have acquired two databases.

i) From Standard organizations – We have collected 100 face images from standard publically available database organizations.

From PIE Database – Collected the face images of 30 subjects with 10 poses per subjects of equal lighting conditions.
From AR Database – Collected the face images of 30 subjects with 10 poses per subjects of equal lighting conditions.
From Yale B database – Collected the face images of 40 subjects with 10 poses per subject of equal lighting conditions. Sample face images of standard organizations are shown in Fig. 5.

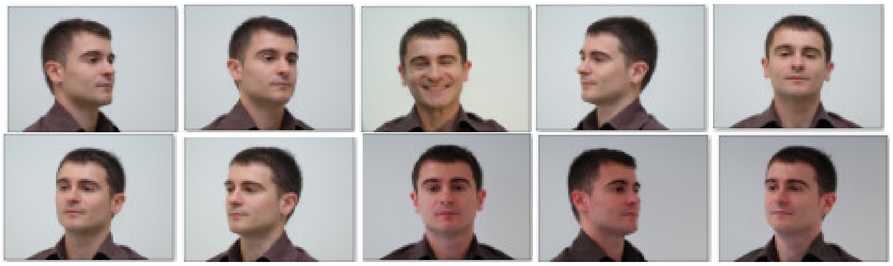


Fig. 5: Samples of benchmark face images of standard organization

ii) Own prepared real face image database – We have acquired the real face image database of 150 volunteers and captured 10 poses of each volunteers from the camera positions as said earlier. Sample real face images of own prepared database are shown in Fig. 6.

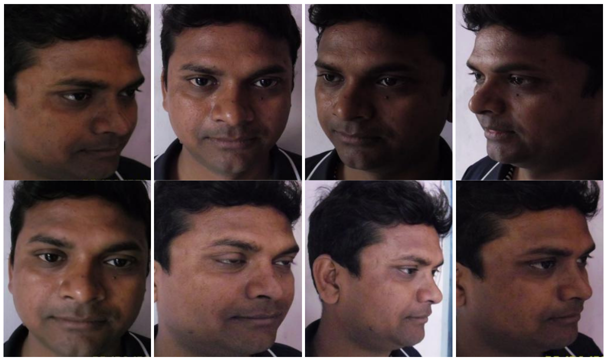


Fig. 6: Samples of own acquired face images

2.2.2 Tampered Face Image Database – In this section, we have categorized the database, imposed with three types of tampering and acquired the images.

i) Dummy Face Image - For 100% tampered face we have acquired 200 dummy face images which are bifurcated as 120 females and 80 males. Dummies are available at various public places in uncontrolled environment and in unconstrained condition. Acquired dummy face images are natural day light images shown in Fig. 7.

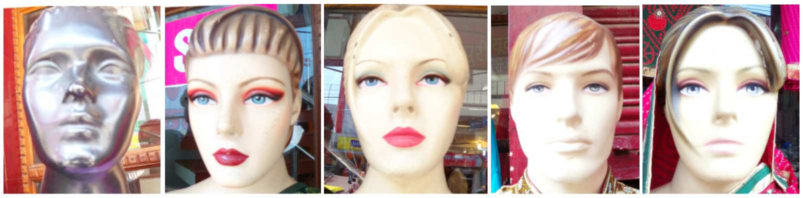
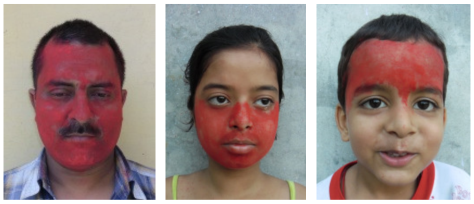


Fig. 7: Sample Dummy Face Images

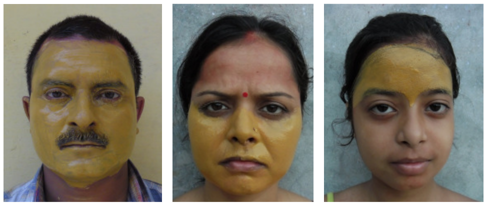
ii) Colour Imposed Face Image - Colour imposed face images of volunteers described above are acquired by applying synthetic colour on facial surface. 60 volunteers were not convinced to tamper their faces. Hence only 90 subject's colour imposed face images are acquired for database at said protocol. In this category, database of each subject with nearly 100%, 60% and 30% tampering of face surface are acquired. The sample of colour imposed face images are shown on Fig. 8.



(a) (b) (c)

Fig. 8: Colour Imposed Face Images
(a) Nearly 100%, (b) Nearly 60% and (c) Nearly 30% tampered

iii) Masked Face Image - Only 120 volunteers (out of 150) were convinced for masked face photo session. For masked face preparation, a cosmetic cream is used whose effect looks equivalent to the mask when imposed on the facial skin. In this category, database of each subject with nearly 100%, 60% and 30% tampering of face surface are acquired. The sample masked face images are shown on Fig.9.



(a) (b) (c)

(b)

Fig. 9: Masked Imposed Face Images
(a) Nearly 100% tampered, (b) Nearly 60% and (c) Nearly 30% tampered

3. ISSUES AND CHALLENGES IN DATABASE ACQUISITION

There are so many challenges to develop a comprehensive and adequate face image database. One of the most fundamental problems is ability to take consistent, high-quality, repeatable images. To produce repeatable results a lot of fundamental variables, such as image background, illumination, snapshot time etc. must be controlled. While the most obvious variables involved are the lighting either by camera equipment (*flash*) or by the environment (*day, night, cloud, fog etc.*). To take the stable and consistent images electromechanical equipments are required. A lot of issues and challenges are involved in our face image database acquisition and some of them are mentioned as follows-

- In real life scenario, it is not easy to acquire each and every type of desired photographs in laboratory. We have to go various places for required imaging. It is very time consuming to move from one place to another to take the photographs.
- The preparation of database of one volunteer takes nearly 50 minutes (*10 minutes for non tampered face imaging, 20 minutes for colour imposed face imaging, 20 minutes for masked face imaging*).
- Most of the time, the volunteers get monotonous and feel irritation from the photo session.
- For the acquisition of own database, the selection of volunteers depending upon their availability of time for the photo session is very problematic.
- Most of the time volunteers were not convinced to spend 50 minutes of time for image acquisition.
- 60 volunteers were not convinced to tamper their face from synthetic colours and 30 were not convinced to tamper their face for mask preparation.
- Dummy faces are not available at single places which are spread out at various public places. That's why; it is time consuming to move from one place to other place for photograph acquisition.
- It is very difficult to convince the owner of the dummies to capture the face image of dummies. Most of the time they require the advertisement of their business and showrooms.
- Unlike real faces we don't have any control over pose, expression, illumination and occlusion on dummy faces. So without any artificiality we have taken the photographs which are available in the public places or markets.
- For the adequate database, the face and camera both should be still but in our case camera stand could not be setup at the different-different public places.
- Since, the database contains outdoor face images situated at public places. Therefore, the background of images could not be controlled.
- Weather is always not in the favorable condition for the image acquisition.

4. Database Pre-Processing

The obtained images are coloured images with the variety of lighting and shadowing effects. Processing of any algorithm on the coloured image will take a lot of time. Therefore, for the testing of various algorithms we require pre-processing. We have done the pre-processing steps as shown in Fig.10.

4.1 Rotation

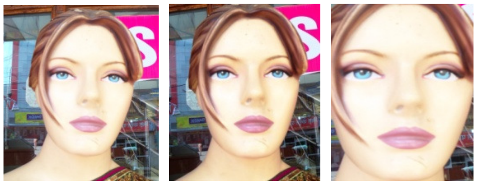
The photographs are taken in natural outdoor environment without any constraints and without any stable camera setting. Hence, some time eyes of the subjects are not in horizontal position. To setup the eyes in horizontal position, rotation (*in the same plane of image*) of image is required. The sample of rotation is shown in Fig.10.

4.2 Cropping

A lot of background effects are available in the obtained images. To remove the huge background effect, we have cropped the face from huge background scenes. The sample of cropping is shown in Fig. 10.

4.3 Illumination Compensation

Finally, all tampered face images have normalized to set all the subjects at normal gray level illumination and of same size [21].



Original Rotated Cropped

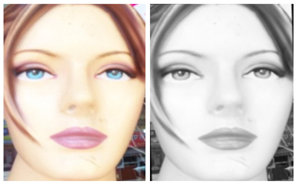


Fig. 11: Color to Gray scale

Fig. 10: Pre-processed Images

Illumination covariate together with pose is a real challenge in face recognition. Gross *et. al.* [28] describes that illumination, together with pose variation, is the most significant factor that alters the appearance of faces. The images of our database are captured during day time in outdoor environment, but are affected by change in weather conditions. Moreover, extreme lighting produce shadow and too bright images, which may diminishes certain facial features and affect the automatic recognition process [22].

In last decade Face Modeling, Normalization and Preprocessing, and Invariant Features Extraction approaches have been addressed to resolve the illumination problem up to the certain level [23]. In our case, we have used normalization and preprocessing approach for illumination compensation because the algorithm, of this category doesn’t require any training and modeling steps [25] and found satisfactory normalised images as an example shown in Fig. 11.

When illumination in gray scale image is high, normalization process reduces the illumination and when illumination in gray scale image is low, normalization process improves the illumination.

5. PERFORMANCES OF FACE RECOGNITION ALGORITHMS ON TAMPERED FACES

5.1 Evaluation Algorithms

To evaluate the performance of our developed tampered face database on face recognition algorithms we have selected four well-known holistic feature based classical algorithms : PCA, ICA, LDA and SVM.

5.1.1 Principal Component Analysis (PCA) - PCA commonly uses the eigenfaces in which the probe and gallery images must be the same size as well as normalized to line up the eyes and mouth of the subjects whining the images [4],[6]. Approach is then used to reduce the dimension of data by the means of image compression basics [7] and provides most effective low dimensional structure of facial pattern. This reduction drops the unuseful information and decomposes the face structure into orthogonal (uncorrelated) components known as eigenfaces. Each face image is represented as weighted sum feature vector of eigenfaces which are stored in 1-D array. A probe image is compared against the gallery image by measuring the distance between their respective feature vectors then matching result has been disclosed. The main advantage of this technique is that it can reduce the data needed to identify the individual to $1/1000^{th}$ of the data presented [8].

In Eigenspace terminology, each face image is projected by the top significant eigenvectors to obtain weights which are the best linearly weight the eigenfaces into a representation of the original image. Knowing the weights of the training images and a new test face image, a nearest neighbour approach determines the identity of the face.

5.1.2 Independent Component Analysis (ICA) - Independent Component Analysis [9] can be viewed as a generalization of PCA [5]. While PCA de-correlates the input data using second-order statistics and thereby generates compressed data with minimum mean-squared re-projection error, ICA minimizes both second-order and higher-order dependencies in the input. It is intimately related to the *blind source separation* (BSS) problem, where the goal is to decompose an observed component into a linear combination of unknown independent components [20, 22]. And then recognition is performed.

5.1.3 Linear Discriminant Analysis (LDA) - Linear Discriminant Analysis is a statistical approach for classifying samples of unknown classes based on training samples with known classes. This technique aims to maximum between-class (across users) variance and minimum within class (within user) variance. In these techniques a block represents a class, and there are a large variations between blocks but little variations within classes.

5.1.4 Support Vector Machine (SVM) - Support Vector Machine (SVM) is very popular binary classifier as methods for learning from examples in science and engineering. The performance of SVM is based on the structure of the Riemannian geometry induced by the kernel function. Although, SVM is binary classifier but now-a-days it received much attention for their applicability in solving pattern recognition problems. It computes the support vectors by the determination of hyper-plane that maximises the margin between the hyper-plane or closest points [27].

5.2 Experimental Evaluation

For our evaluation process we have selected 6 pre-processed non-tampered face images of each subject as training dataset and 4 (2 colour imposed and 2 masked) pre-processed tampered face as test dataset. In the case of dummy face images, training and testing both images are dummy face images and considered in the category of non-tampered face images because real face image of those dummies are not available. The size of original images are 250x300 pixels denoted by L_0. All images are compressed with the help of Gaussian kernel [24] to obtain higher level of compressed images as L_1, L_2 and L_3. Where L_1 are of size 125x150, L_2 are of size 63x75 and L_3 are of size 32x38 pixels.

5.2.1 Experimental Results - We have done our experiments on above four algorithms and obtained results are shown in Table 1.

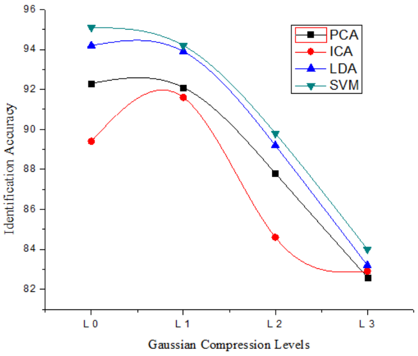


Fig. 12: Graph of Identification Accuracy of Real non-tampered Faces

Table 1: Identification Accuracy for various area of surface of face tampering

Training/Testing 60/40 %	Gaussian Compression Levels	PCA	ICA	LDA	SVM
Non-tampered / Non-Tampered	L_0	92.3	89.4	94.2	95.1
	L_1	92.1	91.6	93.9	94.2
	L_2	87.8	84.6	89.2	89.8
	L_3	82.6	82.9	83.2	84.0
Non-tampered / 30 % tampered	L_0	89.1	87.2	88.3	94.0
	L_1	88.7	86.8	88.1	93.6
	L_2	85.5	82.6	83.8	89.1
	L_3	82.5	80.6	79.8	82.9
Non-tampered / 60 % tampered	L_0	83.9	83.3	85.7	89.4
	L_1	83.6	80.2	85.2	88.8
	L_2	80.8	79.1	81.4	84.1
	L_3	78.5	78.8	78.7	80.3
Non-tampered / ~ 100 % tampered	L_0	81.4	82.8	83.5	86.2
	L_1	81.0	79.7	82.9	85.9
	L_2	76.7	75.1	76.9	81.8
	L_3	75.8	72.6	76.0	79.5

5.2.2 Experimental Analysis –The results show that the identification accuracy varies significantly depending upon the size of image, tampering area of the facial surface, environmental constraints and algorithms. The reason behind these variations are described as –

- Fig. 12, 13, 14, and 15 demonstrate that identification accuracy of all mentioned algorithms decrease as we increase the Gaussian level of compression.
- From Fig. 12 shows that highest identification accuracy at every level of Gaussian compression, it demonstrate that when face surfaces are not tampered the accuracy will be higher than tampered face.

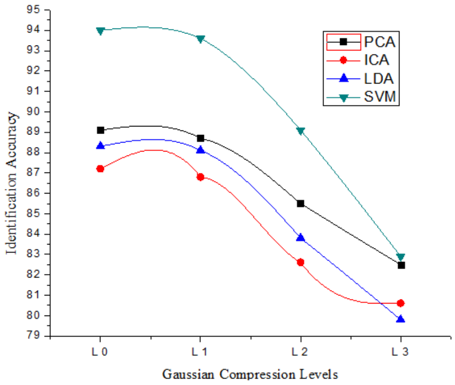


Fig. 13: Graph of Identification Accuracy of 30 % Tampered Faces

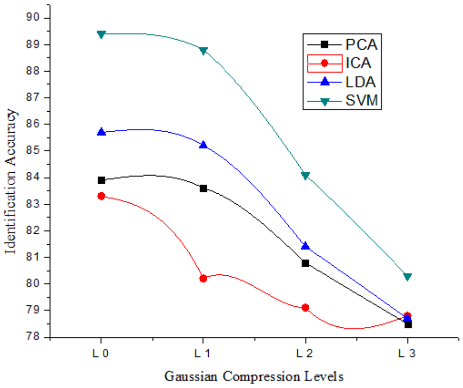


Fig. 14: Graph of Identification Accuracy of 60 % Tampered Faces

- It is clearly visible from Fig. 12, 13, 14, and 15 that the performance of all mentioned algorithms decreases on increasing the tampering area of facial surface.
- In the case of tampered face the graphs shown from Fig. 12, 13, 14, and 15 demonstrate that the identification accuracy of used algorithms is unpredictable at higher level of compression.
- From the above results it is unpredictable that which algorithm will be well suited for the tampered face recognition.
- The above results also demonstrate that on every level of compressed image it is not possible to select any particular algorithm.
- On compressing the images there is loss of some of their important features and therefore at higher level of compression, accuracy decreases in all case of algorithms and tampering.

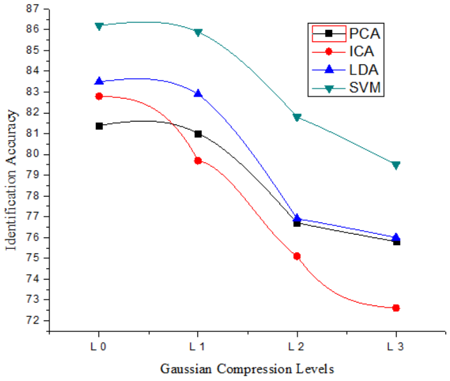


Fig. 15: Graph of Identification Accuracy of nearly 100 % Tampered Faces

- From each Fig. 12, 13, 14, and 15 it is clear that the performance of identification of SVM is high in every case.

6. Conclusion And Future Scope

Generally face recognition algorithms are developed based upon their facial properties. Therefore, in this paper we have selected holistic feature based algorithms to evaluate the identification accuracy and done number of experiments for tampered face. To select the category of algorithm for tampering but the results of our experimental are very fluctuating in all cases of compression. Therefore, it is totally unpredictable to select any particular type of algorithm for tampered face recognition. According to our hypothesis there should be separate module for the face tampering detection and integrated to the face recognition system.

We have evaluated the identification accuracy of tampered face concluded with possible research direction that i) Size of database should be increased to select the particular algorithm for tampering detection. ii) Some new algorithms are to be developed to detect the tampering in real world scenarios.

References

[1] A. Tefas, C. Kotropoulos and I. Pitas, “Using Support Vector Machines to Enhance the Performance of plastic Graph Matching for Frontal Face Authentication”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 23, No. 7, pp. 735-746, Jul. 2001.

[2] A. K. Jain, R. M. Bolle, and S. Pankanti, Eds., Biometrics: Personal Identification is a Networked Society. Norwell, MA: Kluwer, 1999.

[4] A.Singh, S.Tiwari, Sanjay Kumar Singh(2012): “Performance of Face Recognition Algorithms on Dummy Faces”, Advances in Computer Science, Engineering & Application, Advances in Intelligent and Soft Computing, Vol. 116/2012, 211-222.

[5] A.Antonelli, R.Cappelli, D.Maio, D.Maltoni, “Fake finger detection by skin distortion analysis", IEEE transaction on Information Forensics and Security 1(3), 360-373(2006).

[6] Y.Chen, A.Jain, S,Dass, "Fingerprint Deformation for Spoof detection”, Proceedings of Biometrics Symposium, Arlington, VA, pp. 27-28 (September).

[7] Yiyu Yao, “Perspective of Granular Computing”, IEEE International Conference on Granular Computing, Vol.1, pp. 85-90, 2005.

[8] S. A. Cole. “Suspect Identities A History of Fingerprinting and Criminal Identification”, Harvard University Press, Cambridge, Massachusetts, London, England, 2001.

[9] D.Willis and M.Lee, “Six biometric devices point the finger at security”, Network computing, June 1998.

[10] M.Sepasian, C. Mares and W. Balachadran. “Vitality detection in fingerprint Identification”, WSEAS Transaction Information Science and Applications, Issue 4, Volume 7, April 2010.

[11] C.Jin, H.Kim, S.Elliott, “Liveness Detection of Fingerprint Based on Band Selective Fourier Spectrum”, ICISC 2007, LNCS 4817, pp. 168-179, 2007.

[12] The FERET database (http://www.itl.nist.gov/iad/humanid/feret/)

[13] P.J. Phillips, H.Moon and R.Rizvi, (2000), “The FERET evaluation methodology for face recognition algorithms”, IEEE Transaction on PAMI, Vol. 22, No.10.

[14] J.A.Black, M. Gargesha, K.Kahol, P.Kuchi, S.Panchanathan," A framework for Performance evaluation of Face Recognition Algorithms ", http://cubic.asu.edu@VCCL.htm, PO Box 5406, Tempe, AZ 85287-5406, USA.

[15] The XM2VTS database (http://www.ee.surrey.ac.uk/Research/VSSP/xm2vtsdb/)

[16] J. Matas, M. Hamouz, K. Jonsson, J. Kittler, Y. Li, C. Kotropoulos, A. Tefas, I. Pitas, T. Tan, H. Yan, F. Smeraldi, J. Bigun, N. Capdevielle, W. Gerstner, S. Ben-Yacoub, Y. Abdeljaoued , E. Mayoraz, (2000), “Comparison of face verification results on the XM2VTS database,” Proceedings of the 15th International Conference on Pattern Recognition, Barcelona (Spain), vol 4, September, 858-863.

[17] The Yale B database (http://cvc.yale.edu/projects/yalefaceB/yalefaceB.html)

[18] The Purdue AR Face database (http://rv11.ecn.purdue.edu/~aleix/aleix_face_DB.html)

[19] T.Sim, S. Baker and M. Bsat, “The CMU Pose, Illumination and Expression (PIE) Database”, International Conference on Automatic Face and Gesture Recognition, 2002.

[20] The CMU PIE database (http://www.ri.cmu.edu/projects/project_418.html)

[21] R.C.Gonzalez, R.E.Woods, : Digital Image Processing, Pearson Education, (2009).

[22] Basri, R., Jacobs, D., 2004. “Illumination Modeling for Face Recognition”, Chapter 5, Handbook of Face Recognition, Stan Z. Li and Anil K. Jain (Eds.), Springer-Verlag.

[23] Javier Ruiz-del-Solar and Julio Quinteros, “Illumination Compensation and Normalization in Eigenspace-based Face Recognition: A comparative study of different pre-processing approaches”.

[24] P.J. Bert, E.H.Adelson, : “The Laplacian Pyramid as Compact Image Code”, IEEE Transaction on Communication, Vol. COM-31, No.4., (April 1983).

[25] Aruni Singh, Sanjay Kumar Singh and Shrikant Tiwari, "Comparison of face Recognition Algorithms on Dummy Faces", International Journal of Multimedia & Its Application (IJMA), Vol.4, No.4, pp. 121-135, DOI :10.5121/ijma.2012.4411, August 2012.

[26] Aruni Singh, Shrikant Tiwari and Sanjay Kumar Singh, "Dummy Face Database", International Journal of Computer Application, Issue 2, Volume 3, ISSN 2250-1797, pp. 193-201, 2012.

[27] B.Heisele, P.Ho and T. Poggio, “Face Recognition with Support Vector Machine: Global verses component based approach”, ICCV, Vol. 2, pp. 688-694, Vancouver, Canada, 2001.

[28] Gross, R., Baker, S., Matthews, I., Kanade, T., (2004). “Face Recognition Across Pose and Illumination”, Chapter 9, Handbook of Face Recognition, Stan Z. Li and Anil K. Jain (Eds.), Springer-Verlag.