EFFECT OF FACE TAMPERING ON FACE RECOGNITION

Aruni Singh[1], Sanjay Kumar Singh[2]

[1]K.N.I.T., Sultanpur, India
arunisingh@rocketmail.com
aruniknit@gmail.com
[2]I.I.T., B.H.U., Varanasi, India
sks.cse@itbhu.ac.in

ABSTRACT

Modern face recognition systems are vulnerable to spoofing attack. Spoofing attack occurs when a person tries to cheat the system by presenting fake biometric data gaining unlawful access. A lot of researchers have originated novel techniques to fascinate these types of face tampering attack. It seems that no comparative studies of different face recognition algorithms on same protocols and fake data have been incorporated. The motivation behind this paper is to present the effect of face tampering on various categories of face recognition algorithms. For this purpose four categories of facial recognition algorithms have been selected to present the obtained results in the form of facial identification accuracy at various tampering and experimental protocols but obtained results are very fluctuating in nature. Finally, we come to the conclusion that it is totally unpredictable to select particular type of algorithm for tampered face recognition.

KEYWORDS

Spoofing, tampering, liveness, facial recognition technology, PCA, iSVM, LBP and SIFT.

1. INTRODUCTION

In the growing age of technology, biometrics is playing very crucial role in the area of security, surveillance, fraud detection and forensic science etc. Human effortlessly process the information obtained from various sensors, and draws the conclusions based upon their ability to recognize the person even with limited correlation, redundant information or when certain features appear partially, hidden, camouflaged, disguised or tampered. Based on technological aspects, certain algorithms are designed for Facial Recognition Technology (FRT). Performance evaluation in biometric systems is essential for any new development which is measured in terms of their accuracy, ease of use, speed, and other measurable criteria.

In biometric identification and authentication system, liveness detection is highly desirable. Liveness detection in face recognition is entirely based on classification of images of real face from the images of non-real or tampered face. Before inciting the classification of images of real face from images of tampered face, first of all it is needed to acknowledge the effect of tampering on face for various face recognition techniques. For the intended purpose of the performance evaluation of tampering on face in FRT, an efficient and benchmark database of images of tampered face as well as non tampered real face of same subject are highly desirable. The

DOI : 10.5121/sipij.2013.4407

available literature bears the witness that so many databases of face image are available but to the best of our knowledge, not even a single database of images of tampered face is available in public domain. For this purpose we have prepared a novel database having images of three categories of tampering effect on real face of same subjects at various protocols which is demonstrated in [1].

It is a very serious problem of society that the imposters and criminals always use different types of artificial mechanism to hide their facial identity at the time of offence and this poses a big challenge for the researchers.

From the state-of-the-art techniques discussed in section 2, it can be said that a lot of researchers have concentrated to detect spoofing attack depend on the characteristics of *motion*, *texture* and *liveness.* And they concentrated on particular constrained methods and applied their own specific techniques such as co-occurrence & deformation of facial organs, lambertance reflectance modals, optical flow evaluation, eyes blinking detection, least square sequence detection, eyes shape detection, high frequency component, facial thermo-gram, local shape analysis and multimodal approach for vitality detection in face image even others have also attempted to tackle the problem of disguised face and designed their own technique for discrimination of real face image from non-live or disguised face image but none have disclosed the effect of tampering on FRT.

That is why; the effect of face tampering on FRT is presented in this paper. For this purpose four categories of facial recognition algorithms have been selected and various face tampering effects are presented in the form of facial identification accuracy at various tampering and experimental protocols.

This paper is organized in seven sections where section 2 is a detailed literature survey of this area and section 3 includes evaluation algorithms. Section 4 explains the database description and section 5 demonstrate experimental evaluations. Section 6 is experimental analysis while section 7 contains conclusion and future directions.

2. LITERATURE REVIEW

Face recognition has been uprosed as an active research topic in last decades and more than thousands research papers have been published in this area. In spite of fair amount of advancement in face recognition systems, face spoofing is still a serious threat to the targeted systems. It can be said that without spoofing measurement the advancement in FRT is defenseless to attack. Based on the clues for attack detection, anti-spoofing techniques for 2-D face recognition are classified as *motion*, *texture* and *liveness* [2].

2.1.1. Motion Analysis

Motion analysis extracted the features of movements of planner photographs and real 3D objects and ultimately declare that the movement of planner object is different from 3D real face movement. The interest point in motion analysis is to detect the generated clues when two dimensional counterfeits are presented to the system input to the camera in the form of images or frames extracted from video. In many cases deformation due to movement is used to detect the spoofing. Li J. *et al*. [3] have proposed first work towards the face spoofing counter-measure.

Tan X. *et al.*[4] demonstrated the Lambertain reflectance model to derive the difference between 2D image of re-print attack and live 3D face, in real access attempt. They have derived an equation to estimate latent reflectance information in both the scenarios using either retinex-based method or Gaussian-based approach [5][3]. The technique extracts the latent reflectance features and classifies the live 3D face image from 2D face photograph image. But in the case of tampered face this technique will not produce discriminating results because tampered face is also a 3D face. Hence the objective of face spoofing detection is defeated.

K. Kollreider *et al.* [6] detected the spoofing score by combining face part detection and optical flow estimation. In this technique, the trajectory of certain face part of live face is exploited against spoof face using optical flow analysis and Gabor feature extraction followed by heuristic classifier. The same authors again evaluated the fusion score from various expert systems that concurrently observes the 3D face part's motion which is the liveness property such as eyes blinking and mouth movements [7] and finally detected the liveness.

W. Bao *et.al* in [8] have extracted four basic types of optical flow fields named as translation, rotation, moving forward/backward and swing. They have demonstrated that real face is an irregular 3D objects, which means the optical flow field generated by head motion and facial expression are irregular. The first three optical flow fields generated by 2D and 3D objects are quite similar but the fourth field 'swing' of 2D and 3D objects have differences, which means, in the case of shaking and raising, head movement produce better differences in 'swing, optical flow field. This technique is not suitable in the case of tampered or disguised face because this will produce quite equal 'swing' value for both tampered and disguised face.

The work done by M.D. Marsico *et al.* [9], used user motion such as smiling, eyes blinking, and pronunciation of specific sentence which checks the user response and then declare the liveness of image. W.R.Schwartz *et al.* [10] describe the face spoofing techniques based on partial least square and low level descriptors. They explored the both spatial and temporal information to learn distinctive characteristics between 'live' and 'spoof' among the images and video frames.

Analysis of movement of facial components, especially eyes in sequence images for vitality detection is also demonstrated by H.K. Jee *et al.* [11]. They compare the shape of eyes in sequential images and detected vitality.

2.1.2. Texture Analysis

Texture analysis counter-measures take an advantage of texture patterns that may look unnatural when exploring the input image.

Li *et al.*[12] have explored the high frequency component using Fourier Spectra and found that high frequency component of photographs is less than that of live face image because recaptured photographs are smaller in size and produce less high frequency components than real live image. This technique is applicable only for less sampled or low resolution photographic images but may not produce expected results for high resolution (quality) image.

To detect the playback photo attack J. Bai *et al.*[39] exploited the fact that during playback attack, the observed face will have a flat geometry, then movements are associated as a flat surface movements. Then they modeled the captured image or frame extracted video by Bidirectional Reflectance Distribution Function (BRDF). When BRDF is decomposed into specular

components and diffuse components, then dichromatic model is created and classify the recaptured face image with live face image by using linear SVM. The work done by Gao X. *et al.* [14] also extracted same physics based technique for vitality detection. There is limitation of this technique that this technique requires reasonably sharp images.

Another method investigated by B. Peixoto *et al.*[15] based on Difference of Gaussian (DoG) filter. The brightness of DoG filtered image on LCD screen affects the recaptured image in a way that the high frequency regions (borders) become susceptible to a 'blurring' effect due to the pixels with higher value of brightening their neighborhood, whereas recaptured image show less borders than their real image.

J. Maata *et al.*[16] represents the face image spoofing detection using texture and local shape analysis to detect the playback photo attack from single face image. They derived the technique to detect the difference of texture and gradient structure in feature space. With the help of LBP based mocro-texture analysis, two complementary low level features, Gabor wavelets and HOG (*Histogram of Gradients*) are extracted to detect the face spoofing.

2.1.3. Liveness Detection

These techniques try to detect the vitality based on the capture of life symptoms from the test image by analyzing spontaneous movements of the facial organs that can't be detected from the photographs.

Eyes blinking is the natural physiological phenomena and this technique is used by G.Pan *et al.* [17] and demonstrated that eyes blink in a temporal image sequence after captured by camera. Eyes blinking based approach has been explored for live face detection. Rapid closing and opening of eyelids are measured with the help of comparison of two or more image sequence using Viola & Jones [18] cascade adaboost approach. L.Sun *et al.*[19] also detected the liveness with the help of eyes blinking using random fields. It is difficult to predict the blinking activity at a particular time span. Therefore, they divide the eyes blinking into two states, *close state* and *non close state* and applied a Conditional Random Fields (CRF), a probabilistic model for segmenting and labeling the sequence data. At last they succeeded to detect the liveness. The main limitation of this technique is that most of the people don't open their full eyelids at their normal vision and in this situation it is very difficult to discriminate open eyes from close eyes. In this approach high user co-operation is needed for data acquisition and the camera should be placed at same horizontal level to that of eyes which is not easy task. The practical application of this method is not feasible as there is variation in height of an individual.

The vein map of face image may also be used for liveness detection using ultra-violet camera because it is also a secure method but it requires a very special and costly camera. Facial thermo-gram is also applied by Socolindky D. A. *et al.* [20] for liveness detection using thermal infrared camera. In this technique very costly camera and highly user co-operation is needed. This technique is very efficient technique even to detect the facial spoofing after plastic surgery because after plastic surgery, the blood flow in the veins don't reflow as before the surgery, that's why facial thermo-gram change its thermal image.

2.2. Multimodal Spoofing Detection

Apart from single modal, multimodal approach against face spoofing are also described in [21],[22]. They have exploited the lips movement during speaking. Face together with voice is used for anti-spoofing. The limitation of this technique is that an additional hardware (voice recorder) and user co-operation are needed for data acquisition.

G.Chetty in [23] has used multimodal based audio-visual cross modal fusion for liveness detection. He demonstrated Bayesian fusion approach based on mutual dependency models for joint analysis of acoustic and visual speech features for liveness detection. Same author has also addressed the liveness checking scheme using multimodal fuzzy fusion in [24] by designing a mutual dependency modals which extract the spatio-temporal correlation between face and voice dynamics during speech generation.

R.Tronci *et al.* [24] performed both static and dynamic analysis in order to detect complementary information about *motion*, *texture* and *liveness*. They extracted the problem of 2D face spoofing attacks detection as combination of several clues. Static analysis allows detecting photo attack and reinforced with video analysis based on motion and liveness clues. Ultimately they have got satisfactory result after score level fusion using weighted sum rule. B. Biggio *et al.* [25] have also demonstrated the fusion at matching score level and focus on the system made up of a fingerprint and face matcher to detect the spoofing attack.

2.3. Face Tampering Detection

In spite of the detection of different types of spoofing attack in face images several researches have been contributed in the cases of disguised and sketched face identification. A lot of research have been discussed in [26] for artist identification after tampering their face by artificial means. D.B. Megherbi and Y. Mio in [27] have demonstrated the advantage of sub-image patch and patches pre-processing instead of whole image. Finally they applied correlation technique to identify the individuals under affine transformation on disguised and varying facial expressions. Further I.Pavlidis and P. Symosek [28] raised the issues and challenges for disguised face detection. They concluded that the upper band of near infrared is particularly advantageous for disguised detection. H. S. Bhatt *et al.* [29] presented very efficient technique for extracting features of sketched face of a digital face image based on granular computing followed by uniform circular local binary pattern, and for matching genetic optimization based approach is used to obtain better identification performance.

The above literatures holds the testimony that very less stimulation has been contributed to detect the face spoofing effect from single face image. Hence this research has been done to get the solution towards these technical and social problems.

3. EVALUATION ALGORITHMS

To evaluate the effect of face tampering on FRT four different categories of face recognition algorithms have been selected which are holistic, intelligence, texture and feature based algorithms.

3.1. Principal Component Analysis (PCA)

It is a holistic information based face recognition algorithm which uses the eigenfaces [30],[31] where the probe and gallery images which must be of the same size and normalized to line up the eyes and mouth of the subjects within the images. This approach is used to reduce the dimension of data by the means of image compression basics [32] and provides most effective low dimensional structure of facial pattern. The main advantage of this technique is that it can reduce the data needed to identify the individual to 1/1000th of the data presented [31]. 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. A probe image is compared against the gallery image by measuring the distance between their respective feature vectors then matching result is disclosed [13].

3.2 . Improved Support Vector Machine (iSVM)

Support Vector Machine (SVM) is a popular intelligent binary classifier based on the structure of the Riemannian Geometry induced by the kernel function. Amari *et al.* in 1999 [33] proposed a method of modifying a Gaussian kernel to improve the performance of a SVM. The idea is to enlarge the spatial resolution around the margin by a conformal mapping, such that the separability between classes is increased [34]. Due to the very prompt results with modifying kernel, this study proposes a novel facial expression recognition approach based on *improved SVM* (iSVM) by modifying kernels. We have tested this algorithm on our novel database and encouraging result is demonstrated in the figures mentioned below.

A nonlinear SVM maps each sample of input space R into a feature space F through a nonlinear mapping φ. The mapping φ defines an embedding of S into F as a curved sub manifold. We denote $\varphi\ (dx)$ the mapped samples of x in the feature space, a small vector dx is mapped to:

$$\varphi(dx) = \nabla\varphi.dx = \sum_i \frac{\partial}{\partial x^i}\varphi(x)dx(i) \tag{1}$$

The squared length of φ(dx) is written as: $ds^2 = |\varphi(dx)|^2 = \sum_{i.j} g_{ij}(x)dx^{(i)}dx^{(j)}$ (2)

Where $g_{ij}(x) = \left(\frac{\partial}{\partial x^{(i)}}\varphi(x)\right).\left(\frac{\partial}{\partial x^{(j)}}\varphi(x)\right) = \frac{\partial}{\partial x^{(i)}}.\frac{\partial}{\partial x^{(j)}}.K(x,x')|_{x'=x}$ (3)

In the feature space F, we can increase the margin (or the distances ds) between classes to improve the performance of the SVM. Taking equation (2) into account, this leads us to increase the Riemannian metric tensor $g_{ij}(x)$ around the boundary and to reduce it around other samples. In view of (1), we can modify the kernel K such that $g_{ij}(x)$ is enlarged around the boundary [34][13].

3.3 . Local Binary Pattern (LBP)

The LBP operator is a powerful texture descriptor [35]. The square matrix of pixels is considered to generate the labels. In this techniques binary number sequence after thresholding is considered as resultant labels and the histogram of labels is used as texture descriptor. Figure 1 illustrate the preparation of LBP operator.

A histogram of labelled face image $face_l(x,y)$ is defined as

$$H_i = \sum_{x,y} I\{face_l(x,y) = i\}, i = 1,2, \dots \dots \dots . (n-1) \tag{4}$$

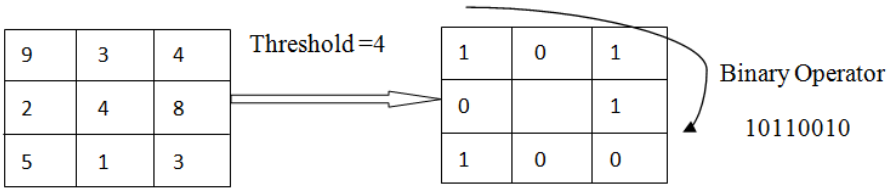

Figure 1. Preparation of LBP operator

In this LBP operator produces n different labels and

$$\text{If } face_l(x,y) = i \text{ then } I\{face_l(x,y) = i\} = 1$$
$$face_l(x,y) \neq i \text{ then } I\{face_l(x,y) = i\} = 0$$

The spatial information about whole face image is obtained by dividing into regions as in figure 2. Where R is the regions described as follows –

$$R_0, R_1, R_2, \dots \dots \dots \dots \dots . . R_{k-1} \text{ where } k \text{ is number of regions}$$

Spatially enhanced histogram is

$$H_{x,y} = \sum_{x,y} I\{face_l = i\} I\{(x,y) \in R_j\}, i = 0,1, \dots \dots \dots, n-1 \text{ and } j = 0,1, \dots \dots \dots, m-1 \tag{5}$$

After this process, obtained histogram $H_{x,y}$ contains complete information of whole face image of about local face macula, spots, surface flat areas, edges, and all about textures. This technique is novel in class information almost containing one training sample per class. Due to this reason here nearest neighbour classifier is used for classification.

For the measurement of dissimilarity among the images histogram intersection, log-likelihood and Chi-square distance are evaluated. And when image is divided into several regions then it is very much crucial to judge that some regions containing important cues such as eyes, lips and chin etc. We evaluate those regions with applying weighted chi-square statics.

$$\chi^2_\omega(S,M) = \sum_{i,j} \omega_j \frac{(S_{i,j} - M_{i,j})^2}{S_{i,j} + M_{i,j}} \tag{6}$$

in this ω_j is the weight for the image regions j.

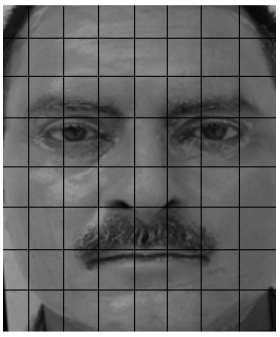

Figure 2. Face image divided into 8x8 window regions

3.4. Scale Invariant Feature Transformation (SIFT) -

In SIFT, features are extracted from images for matching between different pose of same subject [36]. These features are invariant to scale and orientation. Steps to find out these features [37] are as follows –

Step I- Scale Space Extrema Detection: Computation of locations for our potential interests by selecting maxima and minima of a set of Difference of Gaussian (DOG) filters applied at different scales all over the image. The scale space of face image is defined as function $L(x, y, \sigma)$ is obtained by convolving by Gaussian $G(x, y, \sigma)$ with input face image $face(x, y, \sigma)$:

$$L(x, y, \sigma) = G(x, y, \sigma) * face(x, y, \sigma) \tag{7}$$

Where $$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \tag{8}$$

σ is standard deviation of Gaussian $G(x, y, \sigma)$. The difference of Gaussian function $G(x, y, \sigma)$ is computed as the difference of Gaussian of two scale that are separated by two scale by a factor k:

$$D(x, y, \sigma) = \big(G(x, y, k\sigma) - G(x, y, \sigma)\big) * face(x, y) = L(x, y, k\sigma) - L(x, y, \sigma) \tag{9}$$

Local maxima and minima of $D(x, y, \sigma)$ are computed on comparison of sample point and its eight neighbors in current face image as well as nine neighbors in scale above and below. These selected points are local maxima and minima or candidate points.

Step II-Removal of unlike points: In this calculation the low contrast points and poorly localized points are removed by evaluating the value of $|D(x, y, \sigma)|$ at each candidate points. These candidate points are below the threshold value, points are discarded else selected.

Step III-Orientation assignment: We build a histogram of gradient orientation $\theta(x, y)$ weighted by gradient magnitude –

$$m(x, y) = \sqrt{((L(x+1, y) - L(x-1, y))^2 + \big(L(x, y+1) - L(x, y-1)\big)^2} \tag{10}$$

$$\theta(x, y) = \tanh\left(L(x, y+1) - L(x, y-1)/(L(x+1, y) - L(x-1, y)\right) \tag{11}$$

Step IV-Key point descriptor evaluation: Finally, a local feature descriptor is computed at each key point. This descriptor is based on the local image gradient, transformed according to the orientation of the key point to provide orientation invariance. Every feature is a vector of 128 dimensions distinctively identifying the neighborhood around the key point.

Each key-point descriptor is extracted from probe face image and matched independently with stored key-point descriptor of gallery face image and best match is evaluated by nearest neighbor technique.

4. DATABASE DESCRIPTION

To validate our proposed effect of tampered face on FRT we have prepared two types of database: Real face image database and tampered face image database [1]. We have made our own protocol and prepared the database.

4.1. Real Face Image Database

For real face image database we have prepared two databases.

4.1.1. 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 some images are shown in figure 3.

Figure 3. Samples of benchmark face images of standard organization

4.1.2. Own 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 figure 4.

Figure 4. Samples of face images of own prepared database

4.2. Tampered Face Image Database

In this section, we have categorized the database, imposed with three types of tampering and acquired the images.

4.2.1. 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 with variation in illumination due to weather conditions. The targeted subjects are always affected by the illumination of weather conditions. The sample dummy face images are shown in figure 5.

Figure 5. Samples of Face images of Dummies

4.2.2. Colour Imposed Face Image

Colour imposed face images of 90 volunteers (*out of 150*) described above are acquired by applying synthetic colour on facial surface at our protocol. 60 volunteers were not convinced to tamper their faces. In this category, database of each subject with nearly 100%, 60% and 30% tampering of face surface are acquired to evaluate the performance of proposed methodology. The sample of colour imposed face images are shown on figure 6.

Figure 6. Samples of Colour imposed face images

4.2.3. 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 figure 7.

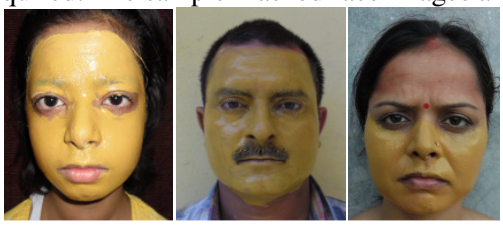

Figure 7. Samples of Masked face images

4.3. Database Pre-processing

The obtained images are colored images with the diverse lighting and shadowing effects. Processing of any algorithm on the colored image is a complex task. Therefore, for the testing of various algorithms, preprocessing is required. Rotation for lineup the eyes, cropping for background removal and illumination compensation [64] for removal of dazzling and dull effect of light are incorporated. Samples of the images after normalization are shown in figure 8.

Figure 8. Samples of Normalized Face images

5. EXPERIMENTAL EVALUATION

To evaluate the effect of face tampering on the face recognition algorithms stated earlier, for the evaluation of 90 subjects are considered whose colour imposed and masked face images are available. We have done our experiments in three folds:

i) We have taken preprocessed images of each subject and compressed those images using Gaussian Pyramid [38]. After compression we have found the images in the form of Gaussian levels. L_0 is original image of size 250x300, L_1 is first level of compressed image of size125x150, L_2 is second level of compressed image of size 63x75 and L_3 is third level of compressed image of size 32x38 pixels.

ii) In this experiment, only live face images are considered to evaluate the recognition accuracy. For this purpose we have set the 6 poses of each real face image as gallery images and 4 poses of each tampered face (*of corresponding non tampered real face*) are set as probe images. The experimental results are explained in the Table 1. Brief descriptions of abbreviations used in the table are mentioned below -

Real Face - Training and testing both are real face images.

Colour Imposed 30 % - Training face images are real non tampered face images while test images are the images whose 30 % facial surface is imposed with synthetic colours.

Colour Imposed 60 % - Training face images are real non tampered face images while test images are the images whose 60 % facial surface is imposed with synthetic colours.

Colour Imposed ~100 % - Training face images are real non tampered face images while test images are the images whose nearly 100 % facial surface is imposed with synthetic colours.

Masked 30 % - Training face images are real non tampered face images while test images are the images whose 30 % facial surface is imposed with masking material.

Masked 60 % - Training face images are real non tampered face images while test images are the images whose 60 % facial surface is imposed with masking material.

Masked ~100 % - Training face images are real non tampered face images while test images are the images whose nearly 100 % facial surface is imposed with masking material.

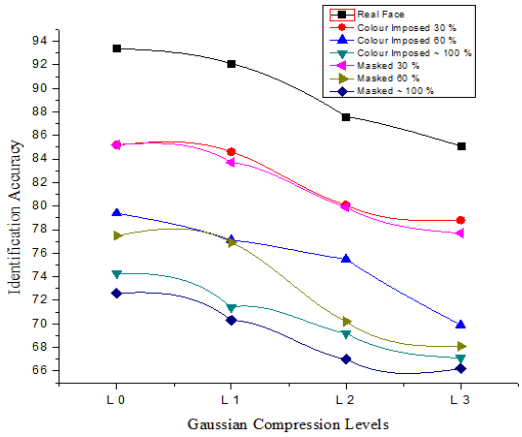

Figure 9. Graph of identification accuracy for PCA

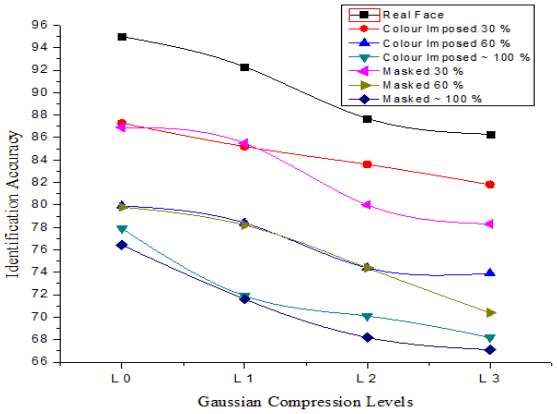

Figure 10. Graph of identification accuracy for iSVM

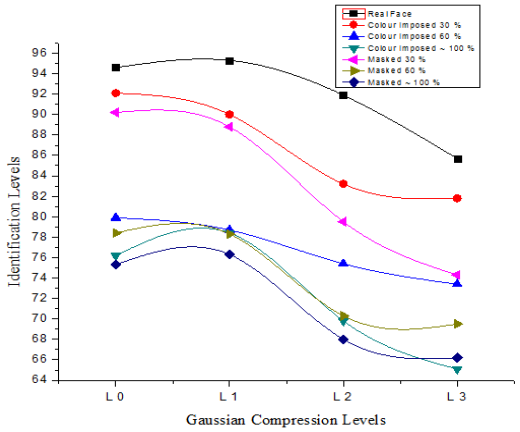

Figure 11. Graph of identification accuracy for LBP

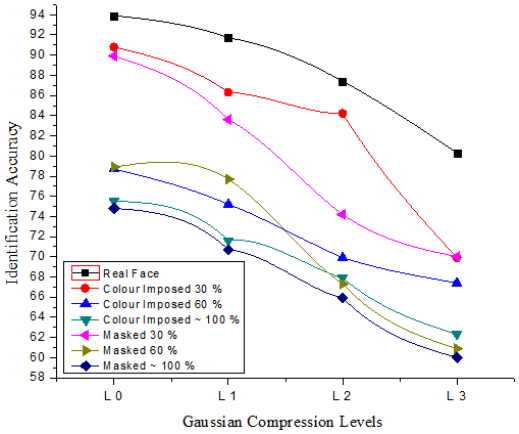

Figure 12. Graph of identification accuracy for SIFT

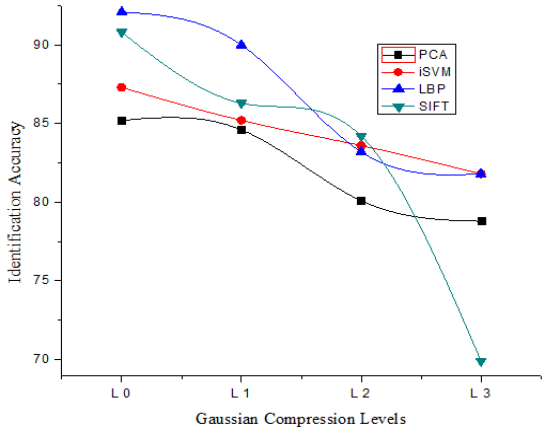

Figure 13. Graph of identification accuracy for 30 % colour Imposed

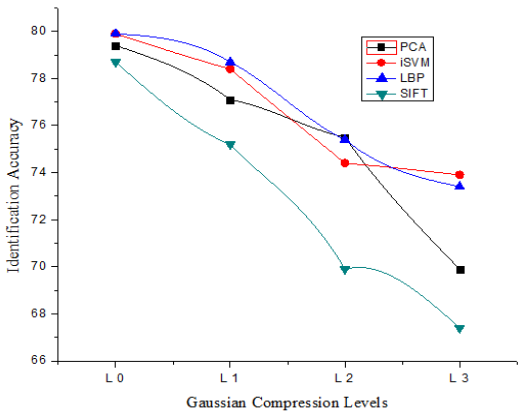

Figure 14. Graph of identification accuracy for 60 % colour Imposed

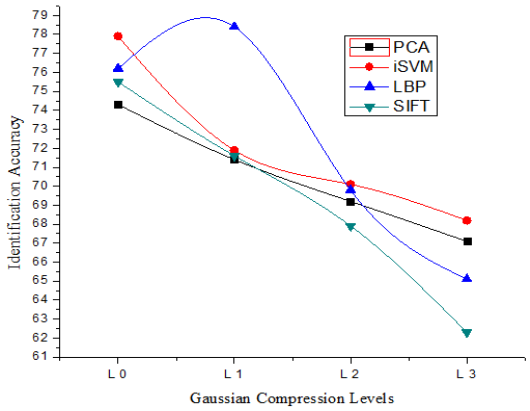

Figure 15. Graph of identification accuracy for ~ 100 % colour imposed

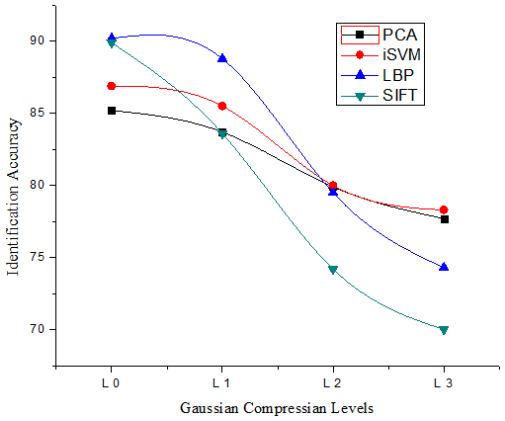

Figure 16. Graph of identification accuracy for 30 % masked

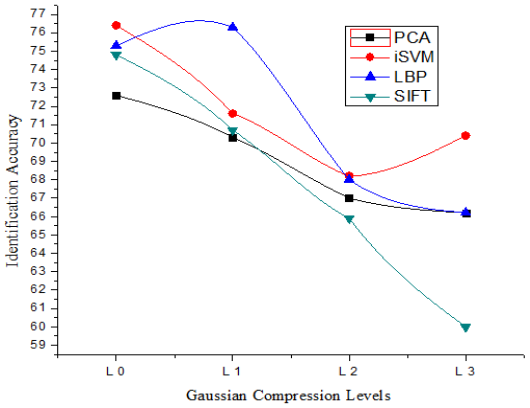

Figure 17: Graph of identification accuracy for 60% 100 % masked

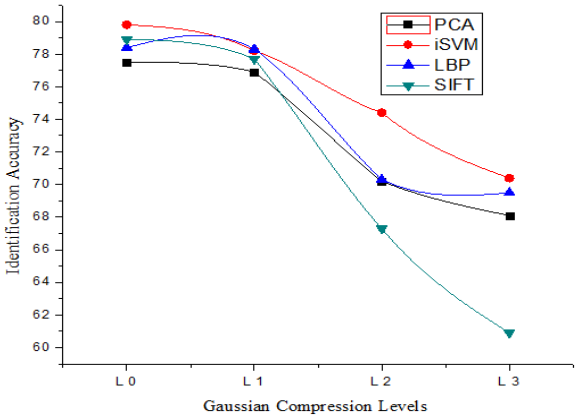

Figure 18: Graph of identification accuracy for ~ masked

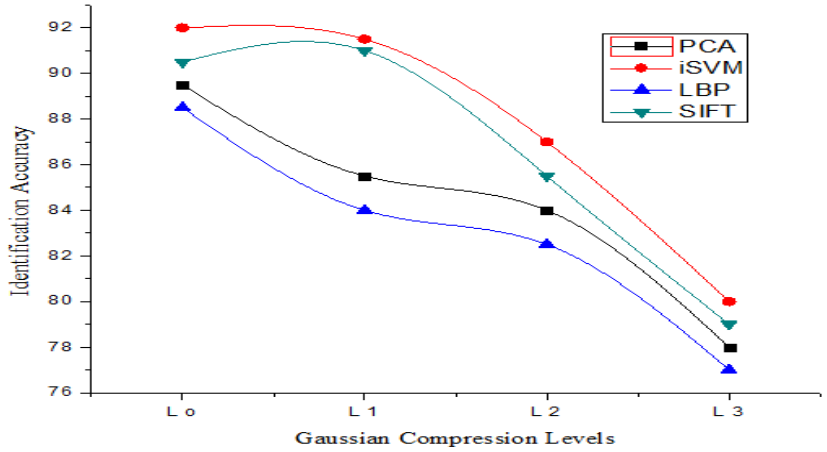

Figure 19. Graph of identification accuracy for Dummy Face Images at multiple Gaussian Levels

Table 1: Percentage identification accuracy of the algorithms for different size of images

Algorithms	Tampering Type	L_0	L_1	L_2	L_3
PCA	Real Face	93.4	92.1	87.6	85.1
	Colour Imposed 30 %	85.2	84.6	80.1	78.8
	Colour Imposed 60 %	79.4	77.1	75.5	69.9
	Colour Imposed ~100 %	74.3	71.4	69.2	67.1
	Masked 30%	85.2	83.7	79.9	77.7
	Masked 60%	77.5	76.9	70.2	68.1
	Masked ~100%	72.6	70.3	67.0	66.2
iSVM	Real Face	95.0	92.3	87.7	86.3
	Colour Imposed 30 %	87.3	85.2	83.6	81.8
	Colour Imposed 60 %	79.9	78.4	74.4	73.9
	Colour Imposed ~100 %	77.9	71.9	70.1	68.2
	Masked 30%	86.9	85.5	80.0	78.3
	Masked 60%	79.8	78.2	74.4	70.4
	Masked ~100%	76.4	71.6	68.2	67.1
LBP	Real Face	94.6	95.3	91.9	81.8
	Colour Imposed 30 %	92.1	90.0	83.2	81.8
	Colour Imposed 60 %	79.9	78.7	75.4	73.4
	Colour Imposed ~100 %	76.2	78.4	69.8	65.1
	Masked 30%	90.2	88.8	79.5	74.3
	Masked 60%	78.4	78.3	70.3	69.5
	Masked ~100%	75.3	76.3	68.0	66.2
SIFT	Real Face	93.9	91.7	87.4	80.3
	Colour Imposed 30 %	90.8	86.3	84.2	69.9
	Colour Imposed 60 %	78.7	75.2	69.9	67.4
	Colour Imposed ~100 %	75.5	71.6	67.9	62.3
	Masked 30%	89.9	83.6	74.2	70.0
	Masked 60%	78.9	77.7	67.3	60.9
	Masked ~100%	74.8	70.7	65.9	60.0

iii) In this experiment, only non live face (dummy face of 200 subjects) images are considered to evaluate the recognition accuracy. For this purpose we have set 6 poses of each dummy as gallery images and 4 poses of corresponding dummy face as probe images. Finally, obtained the results described in the Table 2 and plotted graph in Figure 13.

Table 2: Recognition accuracy of the algorithms for different size of dummy face images

60/40 % Gallery/Probe	Gaussian Compression Levels			
	L_0	L_1	L_2	L_3
PCA	89.5	85.5	84	78
iSVM	92	91.5	87	80
LBP	88.5	84	82.5	77
SIFT	90.5	91	85.5	79

6. 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 category of algorithms. The reason behind these variations are described as –

- Figures 3, 4, 5 and 6 demonstrate that identification accuracy of all mentioned algorithms decrease as we increase the Gaussian level of compression.

- It is clearly visible from figures 3, 4, 5 and 6 that the performance of all mentioned algorithms decreases on increasing the tampering area of facial surface.
- The graphs of figures 7 to 9, it is shown that the identification accuracy of LBP is more than all other algorithms because local texture on imposing the synthetic colour shows the best performance for identification.
- In the case of masked face the graphs shown from figures 10 to 12 demonstrate that the identification accuracy of used algorithms is unpredictable. It also declares that the feature of masked face varies with compress the image and algorithm to algorithm.
- From the above results it is unpredictable that which type of algorithm will be well suited for the tampered face recognition of particular type of tampering.
- The above results also demonstrate that on every level of compressed image it is not possible to select any particular algorithm for particular type of tampering.
- It is clear from figure 13 that the performance of identification of SIFT is very close to iSVM in every case compressed image because SIFT works on local feature as a descriptor and in dummy face images, there are no any change in local features of on image compression.
- 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.

7. CONCLUSION AND FUTURE DIRECTIONS

Generally face recognition algorithms are developed based upon their facial properties. The categories of algorithms are the holistic feature based, local feature based, texture based and intelligent based. Therefore, in this paper we have selected one algorithm of each category to evaluate the identification accuracy and done number of experiments for tampered face to select the category of algorithm for particular type of tampering but the results of our experimental are very fluctuating nature in all cases of tampering and 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. To meet our hypothesis we have developed one technique based on gradient method [40] for face tampering detection but more research is to be done for vitality or tampering detection.

REFERENCES

[1] Aruni Singh, Sanjay Kr. Singh and Shrikant Tiwari,(2013) "Fake Face Database and Proprocessing", *An International Conference* CCSIT- 2013 (Springer-LNICST), Paper Id-98.

[2] Murali Mohan Chakka, Andre Anjos, S_ebastien Marcel, Roberto Tronci, Daniele Muntoni, Gianluca Fadda, Maurizio Pili, Nicola Sirena, Gabriele Murgia,Marco Ristori, Fabio Roli, Junjie Yan, Dong Yi, Zhen Lei, Zhiwei Zhang, Stan Z.Li, William Robson Schwartz, Anderson Rocha, Helio Pedrini, Javier Lorenzo-Navarro, Modesto Castrill_on-Santana, J.Maatta, Abdenour Hadid, Matti Pietikainen Idiap Research Institute, Ambient Intelligence Laboratory, Chinese Academy of Sciences, University of Campinas, Universidad de Las Palmas de Gran Canaria, University of Oulu, (2011) "*Competition on Counter Measures to 2-D Facial Spoofing Attacks*".

[3] Li, J.; Wang, Y. & Tan, T. & Jain, A., (2004) "Live Face Detection Based on the Analysis of Fourier Spectra" , Biometric Technology for Human Identification", *Proceedings of SPIE*, Vol. 5404, pp. 296-303,.

[4] Tan,X., Li,Y., Liu, J., Jiang, L.,(2010) "Face liveness detection from a single image with sparse low rank bilinear discriminative model", *Proc. 11th European Conf. on Computer vision: Part VI. ECCV'10*, 2010, pp. 504–517, available at http://portal.acm.org/citation.cfm?id=1888212.1888251

[5] Y.Li, X. Tan,(2009) "An anti-photo spoof method in face recognition based on analysis of Fourier spectra with spark logistic regression", *In Chinese conference in Pattern Recognition*.

[7] K. Kollreider, H. Fronthaler, J. Bigun,(2008) "Verifying liveness by multiple experts in face biometrics", *In Computer society conference on Computer Vision and pattern Recognition Workshops IEEE*, pp 1-6.

[6] K. Kollreider, H. Fronthaler, J. Bigun,(2005) "Evaluating liveness by face images and the structure tensor", *Fourth IEEE Workshop on Automatic Identification Advanced Technologies,* Buffalo, New York, pp. 75–80.

[8] W. Bao, H. Li, N. Li and W. Jiang,(2009) "A Liveness Detection Method for Face Recognition Based on Optical Flow Field".

[9] M.D. Marsico, M. Nappi, D. Riccio and J.L. Dugelay, "Moving Face Spoofing Detection via 3D Projective Invariant".

[10] W.R.Schwartz, A. Rocha and H. Pedrini, "Face Spoofing Detection through Partial Least Squares and Low Level Descriptors".

[11] H.K.Jee, S.U.Jung and J.H.Yoo,(2006)"Liveness Detection for Embedded Face Recognition System", *World Academy of Science, Engineering and Technology*.

[12] Li, J.; Wang, Y. & Tan, T. & Jain, A.,(2004)"Live Face Detection Based on the Analysis of Fourier Spectra, Biometric Technology for Human Identification", *Proceedings of SPIE*, Vol. 5404, pp. 296-303.

[13] 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 (Springer)*, Vol. 116/2012, 211-222.

[14] Gao, X., Ng, T.T., Qiu, B., Chang, S.F.,(2010) "Single-view recaptured image detection based on physics-based features", *IEEE Int. Conf. on Multimedia & Expo (ICME)*, pp. 1469–1474.

[15] B. Peixoto, C. Michelassi and A. Rocha,(2011)"Face Liveness Detection under bad illumination conditions", *18th IEEE International Conference on Image Processing*.

[16] J.Maatta, A.Hadid and M.Pietikainen,(2012)"Face Spoofing detection from single image using texture and local shape analysis", *IET Biometrics*, Vol.1, Iss. 1, pp. 3-10, doi:10.1049/iet-bmt.2011.0009.

[17] Gang Pan, Zhaohui Wu and Lin Sun,(2008)"Liveness Detection for Face Recognition", *Recent advancement in Face recognition*, pp. 109-124.

[18] Viola P., Jones M.J.,(2001), "Rapid Objet Detection using Boosted cascade of simple Features", *Proc. IEEE CS Conference in Computer Vision and Pattern Recognition*, Vol. 1, Page: 511-518, Kauaii-Hawaii.

[19] L. Sun, G. Pan, Z.Wu and S. Lao,(2007) "Blinking-Based Live Face Detection Using Conditional Random Fields", *ICB 2007*, LNCS 4642, pp. 252–260.

[20] Socolinsky, D.A.; Selinger, A. & Neuheisel, J. D.,(2003). "Face Recognition with Visible and Thermal Infrared Imagery", *Computer Vision and Image Understanding*, vol.91, no. 1-2, pp. 72-114.

[21] Frischholz, R.W. & Dieckmann, (2000)"*U. Bio ID: A Multimodal Biometric Identification System*", IEEE Computer, Vol. 33, No. 2, pp.64-68.

[22] Chetty, G. & Wagner, M.,(2006)"*Multi-level Liveness Verification for Face-Voice Biometric Authentication*" *, Biometric Symposium 2006*, Baltimore, Maryland.

[23] Girija Chetty,(2009)"*Biometric Liveness Detection Based on Cross Modal Fusion*", *12th International Conference on Information Fusion Seattle*, WA, USA.

[24] R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Siren, G. Murgia and M. Ristori, "Fusion of Multiple clues for photo-attack detection in face recognition systems", *IEEE transaction*.

[25] B. Biggio, Z. Akhtar, G. Fumera, G.L.Marcial and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attack", *IET biometrics*, doi: 10:1949/iet-bmt.2011.0012, ISSN 2047-4938.

[26] "Image Processing for Artist Identification", (2007), *First International Workshop on Image Processing for Artist Identification Brushwork in the paintings of Vincent van gogh*.

[27] D.B. Megherbi and Y. Miao,(2009)"A Distributed Efficient Face Image Screening and Retrieval With Affine Transformation, Disguised and Varying Facial Expressions".

[28] I. Pavlidis and P. Symosek, (2000)"The Imaging Issue in an Automatic Face/Disguise Detection System".
[29] H.S. Bhatt, S. Bharadwaj, R. Singh and M. Vatsa, " On Matching Sketches with Digital Face Image", IEEE transaction.
[30] P. Belhumeur, J. Hespanha, D. Kriegman, (1997). "*Eigenfaces vs. Fisherfaces: class specific linear projection*," *IEEE Transactions on PAMI*, 19(7), 711-720.
[31] M. Turk and A. Pentland, (1991), "*Eigenfaces for Recognition*," J. Cognitive Neuroscience, 3(1).
[32] L.Sirvoich and M.Kirby, (1987) "A low dimensional Procedure for Characterization of Human Faces", *J.Optical SOC.* Am. A, Vol. 4, No. 3, 519-524.
[33] Amari S. and Wu S., "Improving Support Vector Machine classifiers by modifying kernel", PMID: 12662656, Neural N/W 12(6): 783-789.
[34] W.Liejun, Q.Xizhong, Z.Taiyi, "Facial Expression recognition using Support Vector Machine by modifying Kernels", *Information Technology Journal*, 8: 595-599.
[35] Ojala, T., Pietikiainen, M., Harwood D.,(1996) "A comparative study of texture measures with classification based on feature distributions*", Pattern Recognition 29***,** pp:51–59.
[36] David G. Lowe,(2004) "Distinctive image features from scale-invariant keypoints", *International journal of computer vision, 60*.
[37] J.Krizaj, V.Struc, N.Pavesic: "Adaptation of SIFT Features for Robust Face Recognition".
[38] P.J. Bert, E.H.Adelson,(1983) "The Laplacian Pyramid as Compact Image Code*", IEEE Transaction on Communication,* Vol. COM-31, No.4.
[39] Bai, J., Ng, T.T., Gao, X., Shi, Y.Q.,(2010) "Is physics-based liveness detection truly possible with a single image?" *, IEEE Int. Symp. on Circuits and Systems (ISCAS),* pp. 3425–3428.
[40] Aruni Singh, Shrikant Tiwari and Sanjay Kumar Singh,(2013) "Face Tampering Detection from Single Face Image using Gradient Method", *International Journal of Security and its Applications (IJSIA)*, Vol. 7, No. 1.

Author's Profile

Aruni Singh Assistant Professor in the Department of Computer Sc. & Engineering, KNIT, Sultanpur, India. His research interests include Biometrics, computational intelligence, machine learning. Currently pursuing Ph.D. at the Indian Institute of Technology, Banaras Hindu University, Varanasi, India.

Sanjay K. Singh is Associate Professor in Department of Computer Engineering, Indian Institute of Technology (I.I.T.), B.H.U., Varanasi, India. He is currently doing research in Biometrics.