An Efficient Face Spoofing Detection Technique for Big Data

Shivakumar Dalali
Research Scholar,
Department of CSE
Don Bosco Institute of
Technology, Bangalore-74.

Suresh L., PhD
Principal & Supervisor,
Cambridge Institute of
Technology, Bangalore-36.

ABSTRACT
Big data refers to huge information whose quantity is beyond the capacity of the system to manage, process and capture. On the basis of the biological and behavioral characteristics of the human, information gathered from which person can be recognized and referred as biometrics. Example includes finger print, face, voice and behavioral analysis etc. Among these, face recognition will not make use of any physical contact with the biometrics system; it is more secure and effective. Hence face recognition becomes one of the best technologies in the biometrics field. Although plenty of efforts have been carried out in the field of face recognition, this work has mark with many challenges in general settings. The criteria behind the successful face recognition systems are developed only under constrained situations with small sized data bases. Hence there is necessary to work under general setting that fit to big data for face recognition. This paper, aims to increase performance and accuracy of face recognition by considering face spoofing attack (veracity). Result analysis of our proposed work ensures increase in accuracy compared to other methods.

Keywords
Big data, Biometrics, Face recognition system, veracity

1. INTRODUCTION
Basically biometric are of two types i.e. Physical biometrics and behavioral biometrics. Physical biometrics deals with natural physical characteristics such as Retinal scan, Fingerprints scan, Hand geometrical scan, DNA analysis, Iris scan and facial identification of a person. It is used for either verification or identification. Behavioral biometrics measures the characteristics (Speaker recognition, Signature, Keystroke, gait and behavioral) which are acquired naturally over a time and it is used for verification. Face is one of the most acceptable physical biometrics because human beings are using this method of credentials in their visual activity and face image acquiring is non-intrusive. The physical attributes, dimensions and proportions of a person's face are unique. Facial recognition systems will gauge and analyze the overall shape, structure and proportions of the face [1][2]. The major hurdle in current face recognition technique is to handle changeable face images such as arbitrary in depth rotations. The varied face images are distinguished and are unable to recognize [3][4].

On the other side, face Recognition has much potential in many applications because of the passive biometric techniques. Biometric sensor presentation attacks are becoming a serious problem in Biometrics [5]. Presentation attack is authorizing a person to gain access to facilities or services by presenting a photo of a person and is also known as spoofing [10][12]. Face recognition algorithm have been constructed to operate on a wide selection of data types such as 2D-gray scale images, color images, different face images, different intensities, in addition fusion of different modalities [6][7]. If there is a large database, will have to verify or identify more subjects or templates. The algorithm is the main key component which builds the template; as this feature distinguishes biometric recognition system with others, which uses the facial features or patterns for authentication purpose [8]. There are many pros to leverage biometrics to Big Data, of which is the elimination of unauthorized access and security. Big data systems are characterized by Volume, Variety, Veracity and a Velocity [9]. In turn, we can make better decisions for acquiring, growing, retaining and managing customer relations. This becomes an important concern when large civilian and enterprise systems such as online face detection, recognition, surveillance camera image on fly analysis use of face recognition for authentication for all of their daily transaction [11]. Face spoofing detection is an important parameter in biometric systems which concerned to one of the big data characteristic's known as veracity. This paper proposes methods of detecting spoofing (veracity) attacks.

2. LITERATURE SURVEY
Ms.S.S.Ghatge et.al [01] proposed a method to show that a challenge exists for robust face recognition in an abandoned environment. The most critical aspect in face recognition is finding the efficient features to represent the face. Here author extract the local feature by using LBP which are insensible to variation of illumination. Using K-mean and distance metric classifier Performance of the LBP is compared with Local ternary pattern (LTP).

Raikoti Sharanabasappa et.al [02] proposed an efficient algorithm for Human face recognition, which is based on unique security architecture and generally viewed as the most flexible model. Where document security uses subsequently generated templates and face features as encryption, decryption keys. The face instances are used for training samples in the public key cryptography.

Dr. Pramod Kumar et.al [03] Face recognition has tricky problem in the image analysis and computer vision field and has interest over the past few years cause of its applications in diverse domains. This manuscript focuses on the face recognition types based on 2D system and 3D system & details of 3D recognition procedures.

Mohammad Reza [04] has proposed a competent method; where face recognition is done under illumination variations. Competent method is based on the fractal analysis (FA) and

the log function to produce a logarithmic fractal dimension (LFD) image and it is illumination invariant. The FA method is a very effective edge enhancer technique to extract and enhance facial features such as eyebrows, eyes, mouth and nose. After extensive experiments proposed method shows best recognition accuracy using an image per subject for training after compared to different state-of-the-art methods.

S. S. Shylaja et.al [05] has proposed an efficient method for identification and verification systems like surveillance and access control. The primary goal of such systems is that only legitimate users can access the resources. Inept person detection systems may vulnerable by allowing impostors. An automated face recognition biometric system finds its enormous application under these circumstances. This manuscript investigates the use of different new approaches for educating low-dimensional depiction of a face image using the idea of transmutation and its variants.

N. K. Ratha, Pankanti &J. H. Connell S. [09] was proposed a paper a biometric-based identity analytics based on Big Data approach. This motivates to leverage biometrics to big data. Countrywide identity proof and portable safe payment methods require very large-scale biometric systems, and they are becoming main stream. Compared to other Big Data systems, biometric systems also face the challenges of different V's that occupy the efficient managing of the complicated life cycle and operations of authentication information. Enormous enrolment, database-size (volume), requirements uses a potentially noisy, fraudulent (veracity), rapid transaction response-time (velocity), & multiple (variety) biometric identifiers.

This paper describes techniques to addressing the above challenges in a variety of various and practical biometrics applications such as 1) indexing methods which allow accessing in close to constant time (velocity) irrespective of the size (volume) of the biometric database, 2) merging multiple (variety) biometrics to address threat and precision concerns, and 3) integrity ensuring (veracity) of biometric databases by deleting multiple second copy records as well as protecting against thievery of biometric identifiers. While sharing many commonalities with generic Big Data system-design issues, biometric systems also provide a rich case study involving how these issues manifest and are addressed in a unique, domain-specific way. By virtue of dealing with some of the most critical entities, namely identity and entitlement, biometric systems are likely to emerge as among the most critical of the Big Data systems.

3. METHODOLOGY

The proposed work is divided into training and testing phase as shown in the figure 1. The training phase reads the image from the database folder as per the query text. Perform image pre-processing like color conversion, image resizing on the image. Blurry feature and chromatic moment feature is extracted from the image for spoofing detection. Weber local descriptor (WLD) is used to extract the feature from the image. The WLD uses ratios to calculate its two components, differential excitation and orientation. Save those trained images in the database. In testing phase images are taken as input and pre-processed. After pre-processing, features can be extracted. These features are further in lined with knowledge based for recognizing images and spoofing image using ART Classifiers. In order to make face spoofing detection (veracity) robust following strategies are used.

3.1 Pre-Processing

Pre-processing is required to clean the samples which may be subjected to various types of noise, inferences and prepare the samples into appropriate format for feature extraction or biometric analysis. Here pre-processing is used in order to remove out the face area from the background and then normalize the face image so that all the face images in the database will be of equal size i.e. image resizing and better for face detection. The fixed size chosen for resizing is 256×256. The input image is converted to gray for further processing and the grey conversion equation is given as below:

$$G=Y=0.2989*R+0.5870*G+0.1148*B \quad (1)$$

3.2 Face Detection by Viola Jones Algorithm

The complexity coupled with face detection at varying conditions like location, scale, orientation (in-plane rotation), occlusions, facial expression, and lighting conditions. Face detection finds the presence and location of a face inside an image. Using appropriate face modeling and segmentation need to be distinguished from other patterns in the image. Face detection approach should also considers an account of variation of facial gestures like illumination (shadowing, and self-shadowing, color), the imaging process (focus, resolution, perspective effects, imaging noise), viewing geometry and occlusion. The face detection algorithm proposed by Viola and Jones is deployed in the proposed methodology for better face feature extraction. This algorithm for face detection will get particular Haar features of a human face, once the features with all these properties are obtained then only this particular algorithm will keep track for the next stage and next level of the process and a rectangular section of an original images and its driver called a sub-window is acquired. Main step in this process is to obtain the sub-window, which is cropped for the calculation of pixels and location of the pixels. The integral image at location (x, y) contains the sum of the pixels above and to the left of (x, y).

$$II(x,y) = \sum_{x' \le x, y' \le y} i(x,y) \quad (2)$$

More rectangles will be present in the Haar features these rectangles are subjected for detecting the face images candidates by scanning and finding for present stage and the weight will be generated. By considering the area of the obtained rectangles in the Haar functions, the area is computed in a very easy way by utilizing integral image. The coordinates of a rectangle and any of its corners can be used to get sum of all pixels above to its left of the location which uses integral image.

3.3 Feature Extraction for Varieties

WLD can be defined as a Weber Local Descriptor which is based on the concept of Weber's Law. The flow chart demonstrated in Figure 2 is based on the Weber's law in which the input image for the WLD is represented as differential excitations like histogram with gradients orientations. This will use to calculate and provide many different parameters like robustness for elimination of noises from the images and it will mainly work for the change that happens during illumination process in the images.

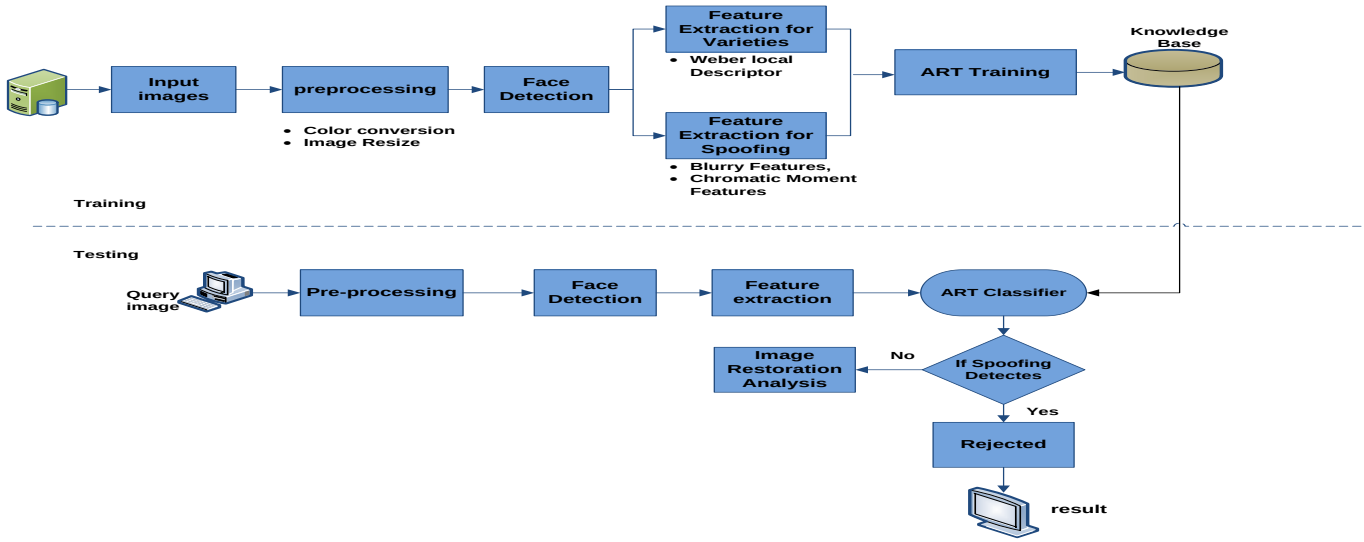


Fig 1 : Block Diagram of Face Spoofing Detection Technique for Big Data.

Edges from the images are also identified effectively and it provides the graceful representation of images.

According to Weber's law the proportion of the background intensity to the increment threshold is constant. Three main steps involved in WLD are as follows: Finding differential excitations, gradient orientations and building the histogram. For calculating differential excitation $\varepsilon(x_c)$ of a pixel x_c first intensity differences with its neighbors x_i, $i = 1, 2, \ldots, p$ are calculated as follows:

$$\Delta Ii = Ii - Ic \tag{3}$$

Then the ratio of total intensity difference of x_c with its neighbors x_i to the intensity of x_c is determined as follows:

$$f_{ratio} = \sum_{i=0}^{P-1} \left(\frac{\Delta I_i}{I_c}\right) \tag{4}$$

In order to increase the robustness of WLD against noise arctangent function is the main thing used here which results in:

$$\sum(Xc) = arctan\left[\sum_{i=0}^{p=0} \left(\frac{\Delta Ii}{Ic}\right)\right] \tag{5}$$

The differential $\varepsilon(x_c)$ excitation may be positive or negative. Next main component of WLD is gradient orientation. For a pixel (x_c) the gradient orientation is calculated as follows:

$$\theta(x_c) = \arctan\left[\left(\frac{I_{73}}{I_{51}}\right)\right] \tag{6}$$

Where $I_{73} = I_7 - I_3$ is the intensity difference of two pixels on the left and right of the current pixel (x_c) and $I_{51} = I_5 - I_1$is the intensity difference of two pixels directly below and above the current pixel. The gradient orientations are quantized into T dominant orientations as:

$$\phi_t = \frac{2t}{T}\pi \tag{7}$$

$$where\ t = \left(\left\lfloor \frac{\theta'}{\frac{2\pi}{t}} + \frac{1}{2} \right\rfloor, T\right) \tag{8}$$

Where $\theta' \epsilon [o, 2\pi]$and is defined in terms of gradient orientation computed.

3.4 Feature Extraction for Spoofing

The process where the third party tries to authenticate another device or the system on a user network to impact the attacks upon the hosts of network, to grab the information from the network, to spread malware or to gain control on the access is referred as a spoofing attacks. In order to accomplish this attacks there are several methods, among those IP address spoofing attacks, ARP spoofing attacks and DNS server spoofing attacks are the most common ones.

The response of real time face spoofing detection in real time applications like mobile and other media will work on the decision made on the basis of limited number of frames. By considering this criterion, our methodology is designed to propose discriminative features, these features are very much able of differentiating between the original and the spoof faces on the basis of single frame. There will be other types of distortions present in spoofing images of a face such as a geometric distortion and artificial texture patterns, example paper wrapping. However these distortions usually vary with the illumination dependent. For an instance consider geometric distortion which varies with illumination but the artificial textured patterns can separated by high quality cameras. Hence, focusing can be on the four general sources for image distortion in spoof face images and design, which corresponds to feature for face spoofing detection.

3.5 Blurriness Features

Usually spoof faces are captured with smart cameras from out of focus because of their quantity and sizes of the available images causes blurry features in the captured images. With the spoofing media's like screen where the picture captured from the mobile phones and printed papers where the images get printed, the

attackers should keep the camera which they are using for process in very focused way in accordance to conceal the medium where the spoofing attacks takes place. All because of these mentioned reasons the images are tend to defocused and the considered images becomes blur, these blurred images are considered as one more cue for the process of anti-spoofing technology. The blurriness feature uses Algorithm SIFT (Scale Invariant feature Transform) can be used to extract a feature for a spoof image.

Scale Invariant Feature Transform algorithm introduced by Lowe in the year of 2004 to resolve the problem of image rotation, deformation of affine, noise, change in viewpoint, scaling factor, illumination change and strong robustness. The SIFT algorithm mainly has four steps, such as scale space extrema detection, key point localization, assignment of orientation and description generation. This technique initially identifies the location and by using a scale space extrema in Difference Of Gaussian (DOG) function with various value of σ for scale of key points, this function convolves the image in space scale spitted by k (constant factor) as shown below,

$$D(x, y, \sigma) = G(x, y, k\sigma) - G(x, y, \sigma) \times I(x, y) \qquad (8)$$

Where, I denote an image and G gives a Gaussian function. The Gaussian image will get subtract to produce a difference of Gaussian, and then the Gaussian image is sub sampled by the factor of 2 and generate a DOG for the sampled image. To detect a local minima and maxima of $D(x, y, \sigma)$ pixel will compare a 3×3 neighborhood. The key point's candidates will localize and refine by eliminating the key points when they reject the low contrast points. In orientation assignment step, key points can obtain on the basis of local image gradient. In description generation step will calculate the local image descriptor for a single key points on the basis of magnitude of image gradient.

3.6 Chromatic Moment Features

When the original face images are subjected to comparison with the re-captured images, the faces will definitely appear with a several different color distribution. Reason for this phenomenon is that the reproduction of colors from the images are imperfect in an display and printing media where the photo is considered and known as chromatic degradation. The chromatic degradation is very effective in detecting the later recaptured face images, as the known fact that the on camera variations, illumination process the dependency is present for the absolute color distribution in an image. This paper gives an idea of detecting abnormal chromaticity in spoofed images by considering devise invariant features.

The abnormal chromaticity detection in a spoof faces initially starts with the conversion of facial image which is normalized from the RGB to HSV (Hue, Saturation, and Value). Next is to work on the deviation, skewness and mean of all the channels as a chromatic feature. Since the statistical moments in each of the channels considers features that are computed and percentage of pixels in min and max histogram bins are used as two additional features.

3.7 ART Classifier

Series of real time neural network models are considered as the ART (Adaptive Resonance Theory), which provides unsupervised, supervised learning, prediction, and detection mainly with pattern recognition. ART is designed for both analog and digital input patterns.

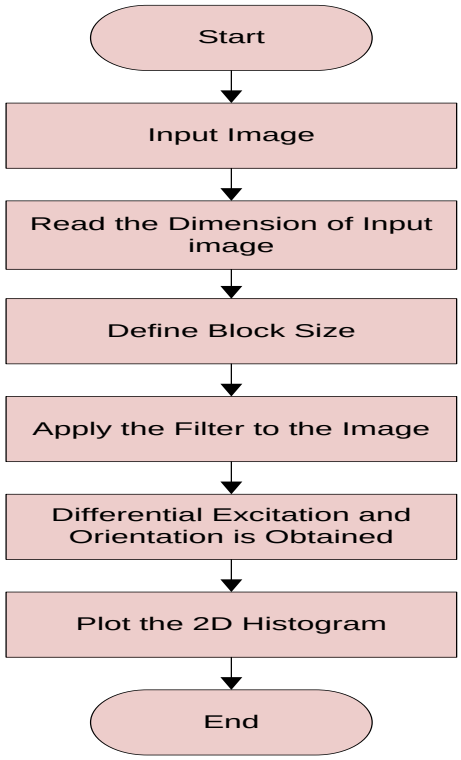


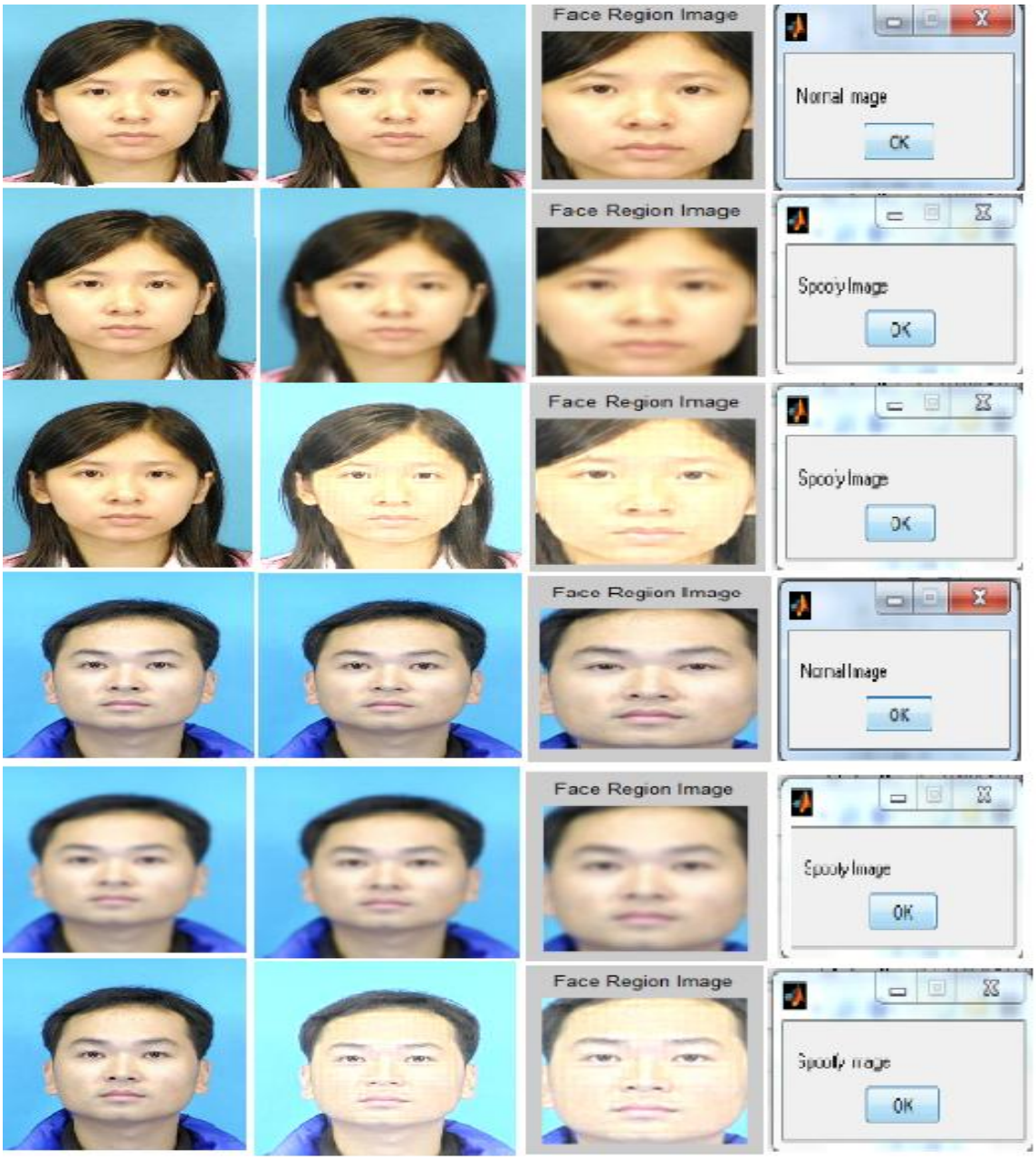
Fig 2 : WLD Flow Chart

Thus proposed system uses the ART for digital input and patterns are utilized for better level of classification which ensures better classification and recognition rate.

ART system is considered as main central feature of all the pattern matching process, in which the comparison starts with both external and internal input memory which is saved before corresponding process code. Once the resonant state is reached by an ART will provide the methodology for match-based learning. ART allows memory to change when input from the external world is close enough to internal expectations, or when something completely new occurs. This feature makes ART systems well suited to problems that require online learning of large and evolving databases. Thus by creating a hybrid model for classification, the most accurate level of classification on face recognition is achieved. This will end up with best recognition and detection rate for the proposed system.

4 EXPERIMENTAL RESULT

This section describes the overall experimental results of this phase, Figure 3 represent the step by step execution of the proposed system. Figure 3(a) represents the original image of the authorized person; this image is taken as base image for all the computations. Figure 3(b) represents the tested image, after applying viola jones algorithm the face region of this is tested and is represented as in Figure 3(c). According to the comparison done using the ART classifier, final result is displayed which is shown in Figure 3(d) for all the cases. If the tested image is same as original image the output is shown as normal image and if the tested image is different from the original image, then the output will be as spoof image as shown in Figure 3(d). Thus by looking into this effective experimental results we can say our proposed system is the more accurate and efficient one. Table 1 depicts the comparison table for the existing systems and the proposed system taking the comparison parameter as Recognition rate; similarly Table 2 depicts the comparison for the Detection Rate.



(a) (b) (c) (d)

Table 1 : Comparison of Recognition Rate with Different Methods

AUTHOR	METHOD	DATABASE USED	RECOGNITION RATE %
Michael J et.al [6]	Viola Jones	Mit+Cmu	94.1
A Suruliandi et.al[7]	Local Tetra Patterns (LTrPs)	Yale-B	96.5
Hardeep Ket.al[8]	Retinex & LOG and Local Texture Pattern (R&LOG LBP)	E Yale-B	92
Mohammad et.al [9]	logarithmic fractal dimension (LFD)	Yale-B	95.13
Proposed System	Viola Jones	Yale-B	97.8

Table 2 : Comparison of Detection Rate with Different Methods

SL.NO	METHOD	DETECTION RATE %
01	Adaboost (Haar)	97.31
02	Adaboost (LBP)	95.96
03	SVM (HOG)	92.68
Proposed system	V IOLA-Jones (Haar)	99.31

5. CONCLUSION

Uplifting current biometrics to big data has an efficient market value; hence there is an impressive attraction for research and development. In this paper we propose a design to implement robust face spoofing detection system for big data. The proposed design has enormous use in biometric authentication, nationwide identification, law enforcement and providing government services. The paper demonstrates face detection using Viola Jones method and robust pre-processing feature extraction by WLD. The main contribution of this work is to leverage current face recognition system to big data by considering characteristics of veracity. Experimental results depicts proposed methodology achieves detection accuracy of 99.31% and recognition accuracy of 97.8%, which is much better when compare to conventional methods.

Future work is to enhance the face recognition rate by considering the following strategies.

Feature extraction methods using parallelization for the velocity characteristics.

Feature extractions in face recognition with different face poses and voluminous data sets for getting good recognition rates to ensure variety and volume characteristics of big data.

6. REFERENCES

[1] Ms.S.S.Ghatge, Prof V.V.Dixit, "Face Recognition under varying illumination with Local binary pattern", Vol. 02, No. 02, 2013.

[2] Raikoti Sharanabasappa and Sanjaypande M. B." A Unique Document Security Technique using Face Biometric Template", International Journal of Advanced Science and Technology, Vol. 50, 2013.

[3] Dr. Pramod Kumar, Mrs. Monika Agarwa, Miss. Stuti Nagar," A Survey on Face Recognition System - A Challenge", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, No. 05, 2013.

[4] Mohammad Reza Faraji and Xiaojun Qi," Face Recognition under Varying Illumination with Logarithmic Fractal Analysis" ieee signal processing letters, Vol. 21, No. 12, 2014.

[5] S. S. Shylaja, K. N. Balasubramanya Murthy, and S. Natarajan, "Illumination Invariant Novel Approaches for Face Recognition", International Journal of Electrical Energy, Vol. 2, No. 2, 2014.

[6] Michael J. Jones, "Robust Real-Time Face Detection", International Journal of Computer Vision, Vol. 57, No. 02, pp. 137 – 154, 2004.

[7] K. Meena, A. Suruliandi And R. Reena Rose, "An Illumination Invariant Texture Based Face Recognition", International Journal on Image And Video Processing, Vol. 04, No. 02, 2013.

[8] Hardeep Kaur and Amandeep Kaur, " Illumination Invariant Face Recognition", International Journal of Computer Applications, Vol. 64, No. 21, pp. 975 – 8887, 2013.

[9] N. K. Ratha, J. H. Connell S. & Pankanti, "Big data approach to biometric based identity analytics", IEEE,IBM journal of Research and development, Vol. 59, No. 02, 2015.

[10] Di Wen, Hu Han, and Anil K. Jain, "Face Spoof Detection with Image Distortion Analysis", To Appear in IEEE Transactions on Information Forensics and Security, 2015.

[11] Vinay A,Vinay S Shekhar, Rituparna J, Tushar Aggrawal, K N Balasubramanya Murthya, S Natarajan, "Cloud Based Big Data Analytics Framework for Face Recognition in Social Networks using Machine Learning", 2nd International Symposium on Big Data and Cloud Computing, 2015.

[12] Jukka maatta, Abdenour Hadid, Matti Pietikainen, "Face spoofing detection From single images using Nicro texture Analysis", pp. 01 – 07, 2011..