TEXTURE ANALYSIS USING LOCAL TERNARY PATTERN FOR FACE ANTI-SPOOFING

Sajida Parveen[1,*], Sharifah Mumtazah Syed Ahmed[1,2], Nidaa Hasan Abbas[1], Nadeem Naeem[1] and Marsyita Hanafi[1,2]

[1]Faculty of Engineering, Department of Computer and Communication Systems Engineering
Universiti Putra Malaysia. Serdang, Selangor D. A. 43400.
[2]Research Centre of Excellence for Wireless and Photonics Network (WiPNET),
Universiti Putra Malaysia. Serdang, Selangor D. A. 43400.

ABSTRACT: *This paper proposes a new face anti-spoofing approach based on analysis of texture characteristics. Photo images are used for spoofing the face recognition and verification system. These photos are similar to the images of a live person which are exhibiting quite different contrast and texture characteristics when compared to real face images. Various feature extraction methods for texture classification including local Binary Patterns emerge as one of the most popular method because of its simplicity and classification accuracy. However, in homogenous regions, the order of the pixel with respect to its neighbors is quite noisy which can affect the performance of Local Binary Pattern. This paper demonstrates the use of local Ternary Pattern (LTP) in face liveness detection system to overcome this problem. The LTP approach is tested on three publicly available NUAA Photograph Imposter database, CASIA Face Anti-Spoofing Database and REPLAY-ATTACK database. Moreover, different experiments are performed by applying different sizes of neighbor pixels and radius of the patches. The test results are compared with the LBP operator and other state-of art work. The proposed face anti-spoofing method performs better than conventional texture based methods.*

Keywords**:** Face anti-spoofing, Local Ternary Pattern (LTP), Local binary Pattern (LBP), Texture analysis, Non-intrusive and Liveness detection

INTRODUCTION

The individual's behavior and biological characteristics form the basis of their biometric profile. The increase in the need to improve privacy and securing the user information has facilitated the adoption of Biometrics. The recent increase in the identity theft along with recent security breaches in systems like PSN have increased the importance of using physical and behavioral characteristics including facial, fingerprints, signature, retinal vein, voice and iris to enhance security [1]. However, this list includes only the partial measures that include gait, ear shape, optical skin reflectance, body odor and head resonance as well as further technologies to enhance security [2]. In biometric systems, it will be devastating to have a security breach as it will defeat the purpose of its adoption. The most common type of biometric attacks includes spoofing that incorporates the usage of artificial or counterfeit features of original data by using masks, gummy fingers or by using a recorded sample of the biometric system. When the biometric trait is obtained from sources other than the user, it is deemed as a spoof. Therefore, in order to deter these spoof attacks, it is imperative to have a mechanism that continuously detects these spoof attacks and takes measures to secure the biometric system. This spoof detection system can help in differentiating between a real user and a fake based on their source. Liveness detection is the process through which the key life vital signs are determined by the biometric system [3].

In order to fulfill multiple biometric checks, biometric traits rely on human face for identification, recognition, surveillance, law enforcement, and human computer interaction systems. However, due to the fact that faces are easily available online or can be sourced from illegitimate sources, they do not present as a reliable means of identity check. Digital cameras, Google Images, Facebook and many other social and internet websites can be used to collect target face images. In addition to this, these images can be enhanced in a large variety of mediums by using latest technologies like 3D image processing and LCD screens to name a few. This makes it harder to differentiate real faces from fake ones due to large number of ways they can be manipulated to present themselves are original ones [4].

Due to the nature of Texture analysis of extracting the protruding features, it is is broadly used in face spoof detection systems. In this paper, Local Ternary Pattern (LTP) is used as a feature descriptor to improve the anti-spoofing rate.

The studies on face liveness detection have been enormously researched to overcome the problem of spoofing attacks. The objective of this paper is to find the fissures in the current scenario and methods applied. For this objective, the reported research work is reviewed in details. The previous studies found that Intrusive and Non-Intrusive are two categories of methodologies on face liveness detection [5]. In the Intrusive technique, clients are required to react to the framework in an obliged way, for example, showing a few activities, expressing words, and pivoting their head in a specific bearing. The intrusive approach usually requires the users to respond to some actions specified by the system. By using head movement [6] the rotation of users in a certain direction according to the random instruction generated by the system is estimated by the algorithm. Another procedure is lip development [7], in which the clients are requested to begin expressing the particular digit succession provoked arbitrarily from 0 to 9 and every lip development is perceived consecutively. Utilizing optical stream, the ten lip developments of clients are sorted into ten unique classes prepared by SVM classifier. However, liveness confirmation with lip development without sound can be assaulted video or distinctive photo successions. Correspondingly, some multi-modular methodologies likewise utilize intuitive way of using so as to talk three attributes like face, voice, and lip

developments to enhance acknowledgment exactness and security. Moreover, in [8] a face liveness checking method measures the level of synchronization between lips and voice separated from video includes half and half combination of acoustic and visual discourse connection highlights.

The blend of more than one biometric attribute coordinated into one framework is an ingenious procedure to upgrade the security level of a face anti spoofing system [9]. Broad exploration led to modify the most ideal approach to consolidate data from a few biometric attributes; whether it is at the feature extraction level or at the decision level. Multi-level Liveness Verification (MLLV) system [10] revealed the static and element relationship between the voice and face. In [11] combination of thermal imaging and skin flexibility of human face is utilized as a part in which clients are requested to chew and move brow at the same time. The connection coefficients were ascertained between the pictures caught by nonexclusive web camera sensor and thermal sensor. The face skin versatility was ascertained by utilizing segregate examination to separate the human skin from different materials such as gelatin, rubber, cadaver, and clay. Another methodology [12] depended on a mix of eye squints and scene setting. The creators used outside face intimation of scene connection called reference scene which is like the foundation. At the point when a human stands before a settled camera of a face recognition system, the detection model separated the information and reference scene. This method is secured against replica, photograph, and 3D attacks yet might be helpless against video attacks. The blend of eye flicker and 3D properties of face, for example, mouth development and eye squinting were extricated utilizing 3D Gaussian and raster flow.

Further, a client's association is not required in the non-intrusive strategy. Non-intrusive methodology uses the unconstrained physiological exercises of face including properties of 3D geometry, eye flickering, skin surface, non-inflexible distortion, and thermgrams. It investigates the physiological exercises of face, for example, properties of 3D geometry assessed [13] by utilizing optoelectronic 3D filtering that depended on the supposition that a genuine face has a characteristic for 3D structure and the printed face picture and computer screen did not demonstrate surface ebb and flow. The optical flow fields dissected that a face is a sporadic 3D object which implies the optical flow field produced by head movement and outward appearances are unpredictable [14]. Sparse logistic regression model and partial least squares regression are utilized to dissect the properties of 3D articles to separate the live and spoof pictures or recordings [15, 16, 17 and 18].

The eye squinting is another physiological activity that comprises of two persistent sub-activities from open to close and close to open. The sham can likewise deliver eye flicker movement by showing the recordings of unique live face. To conquer this kind of attack, an eye flicker based face liveness detection methodologies are proposed by utilizing adaptive boosting algorithm [19], the conditional random field (CRF) [20 and 21], and hamming distance [22]. Another methodology is the eye development with the structure data is utilized for the grouped live and fake countenances taking into account Fourier spectra assumptions in which high recurrence segments of photograph were not exactly live face [23]. Texture analysis is additionally a physiological quality utilized for face liveness detection. Local Binary Pattern (LBP) is a strategy based on Texture Analysis. It is a straightforward yet extremely effective texture descriptor which marks the pixels of a picture by limit the area of every pixel and considers the outcome as a binary numbers as 0s or 1s. LBP texture descriptor has as of late gotten to be prevalent because of its prejudicial force and computational straightforwardness. The Local Binary Pattern (LBP) and multi-scale Local Binary Pattern has been proposed to dissect the capability of texture elements of the face [24, 25 and 26]. Along with multi-scale operator to LBP based approach has been used to detect the structure of the facial micro-textures in faces anti-spoofing [27]. In [28] the characteristics of contrast and texture of captured and recaptured face images have been calculated. Local binary pattern variance (LBPV) is used for feature extraction and (DoG) filter is used to obtain a special frequency band that gives substantial information to discriminate between live face and photo images. An additional LBP related approach based on the local binary pattern operator is used from three orthogonal planes (LBP-TOP) that syndicate space and time information into a single descriptor with multi resolution strategy using photographs and videos [29]. Furthermore, the variation of LBP comes in the form of Local Graph Structure (LGS) for face anti-spoofing application. The texture information is extracted from the divided local region of the face images and then combines into global descriptor [30]. Recently, a technique appears in the shape of using camera focus function [31]. It has been proved that the variations of pixel values by focusing two images sequentially taken in different focuses can identify the fake faces.

MATERIALS AND METHODS

Face images captured from printed photos may visually look very similar to the images captured from live faces. Nevertheless, the surface properties of real and fake faces were different such as prints, e.g. pigments, printing quality defects, and image blur. The Local Binary Pattern operator is introduced for liveness detection by inspiring such micro texture pattern [27]. LBP cannot adequately deal with the range of appearance variations that commonly occurred in unconstrained natural images due to illumination, and partial occlusions and it generates the noise in uniform and near-uniform image regions. This research proposes Local Ternary Pattern for the face liveness detection system to overcome this limitation and increase the performance of system.

In this work, for performing the face liveness detection, three publicly available databases are used. The detail of Databases is given in section IV. The images of all these databases are rich in texture variations (printed photo, digital display screen, HD screen and etc).

For the facial feature extraction, the new method known as Local Ternary Pattern (LTP) [32] is introduced in this research work for face anti-spoofing method. Also, for comparison of the proposed method, the most famous existing texture based method named as local binary pattern is adopted. The details of both feature descriptors are given in below subsections.

1. Local Binary Pattern (LBP)

Local Binary Pattern (LBP) is a method based on texture analysis [33]. It is a simple yet very resourceful texture operator which labels the pixels of an image by threshold the neighborhood of each pixel and considers the result as a binary number as shown in Fig 1. It appears to be a unifying approach to the traditionally divergent statistical and structural models of texture analysis. The threshold equation is given below

$$a_i = \begin{cases} 1 & if\ p_i > c \\ 0 & if\ p_i \le c \end{cases}, (1 \le i \le P) \qquad (1)$$

Where c is the intensity value of the center pixel and p_i is the intensity value of the neighborhood pixels. The weighted sum function is represented by:

$$LPB_{P,R} = \sum_{i=1}^{P} a_i \times 2^{i-1}, (a_i \in \{0,1\}) \qquad (2)$$

Where P is the number of neighbor pixels, R is the radius of neighborhood and is gray valued function and a_i is gray valued function. The researchers have calculated $LBP_{8,\ 2}$ features on whole image of 64×64 pixel dimension form NUAA database and computed the histogram in 59 bins as shown in Fig.2.

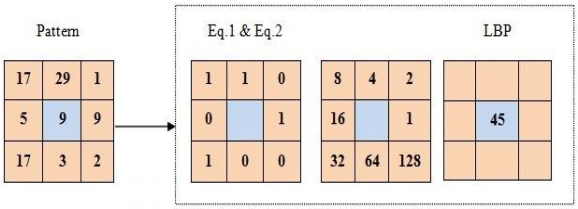

Fig.1 Local Binary Pattern calculation process

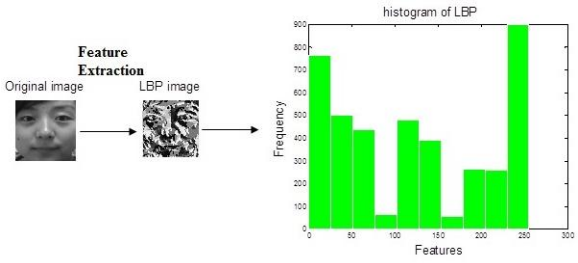

Fig.2 Feature calculation and obtained histogram of Local Binary Pattern on sample image

2. Local Ternary Pattern (LTP)

The Local Ternary Pattern (LTP) operator is an extension of LBP is used. Due to the ternary threshold function, it is more resistant to noise and reliable for uniform pattern [33]. The threshold equation for three variables is given below.

$$a_i = \begin{cases} 1 & if \quad p_i > c + t \\ 0 & if \quad c - t \le p_i \le c + t, (1 \le i \le P) \\ -1 & if \quad p_i < c - t \end{cases} \qquad (3)$$

Where the intensity value of the center pixel represent with c, p_i is the intensity value of the neighborhood pixels and t represents the threshold value that is used to direct the sensitivity of the ternary pattern against the noise with central pixels.

The binary threshold function h_i for the upper pattern is computed as:

$$h_i = \begin{cases} 1 & if \quad a_i = 1 \\ 0 & otherwise \end{cases}, (1 \le i \le P) \qquad (4)$$

The binary threshold function l_i for the lower pattern is calculated:

$$l_i = \begin{cases} 1 & if \quad a_i = -1 \\ 0 & otherwise \end{cases}, (1 \le i \le P) \qquad (5)$$

The weighted sum function for upper pattern can be expressed as:

$$LTPh_{P,R} = \sum_{i=1}^{P} h_i \times 2^{i-1}, (h_i \in \{0,1\}) \qquad (6)$$

The weighted sun function for lower pattern can be expressed as:

$$LTPl_{P,R} = \sum_{i=1}^{P} l_i \times 2^{i-1}, (l_i \in \{0,1\}) \qquad (7)$$

Ternary functions of lower and higher patterns are calculated along with the binary threshold and concatenated the both values to make a ternary function as shown in Fig 3. The graphical representation of calculated histograms of equation (6) and (7) are shown in Fig4.

Once the histograms are computed from feature extraction process then a Support Vector Machine (SVM) classifier is used. The SVM classifies the fake and real face images. The SVM classifier is first trained by using different datasets of positive (real faces) and negative (fake faces) samples. For training

data (x_i, y_i) for $i = 1 \ldots N$ with $x_i \in R^d$ and $y_i \in \{1, -1)$, learn a classifier $f(x)$ such that

$$f(x_i) = \begin{cases} \ge 0 & y_i = +1 \\ < 0 & y_i = -1 \end{cases} \qquad (8)$$

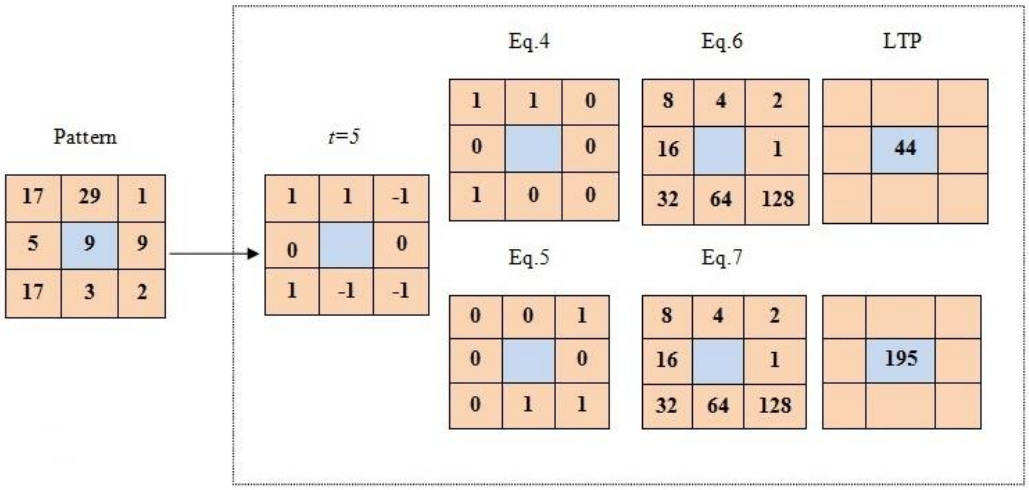

Fig.3 shows calculation of LTP operators with upper and lower binary code

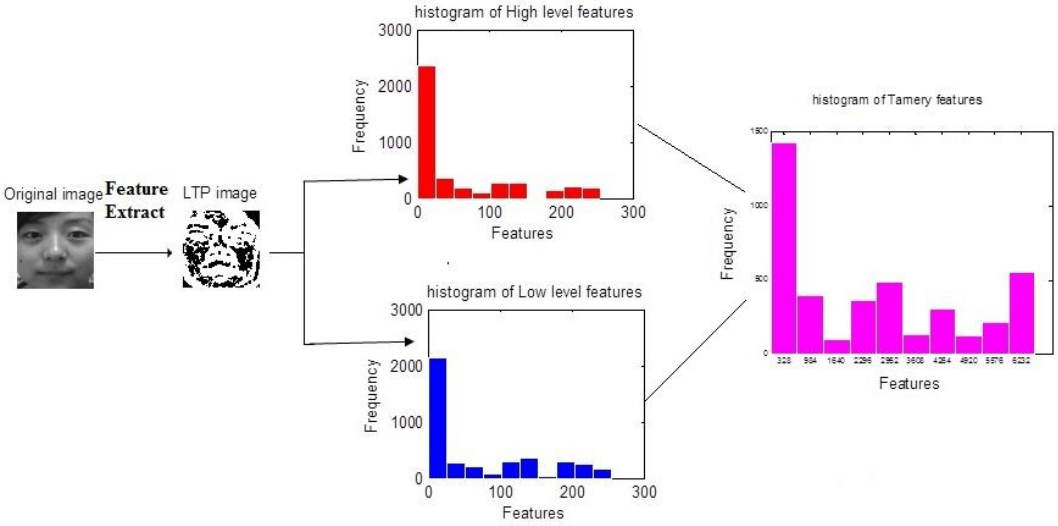

Fig.4 Features calculation and obtained histograms of Local Ternary Pattern on sample image

i.e $y_i f(x_i) > 0$ for correct classification. For our experiment we are using the linear kernel of SVM classifier [35] that can be express as follow:

$$f(x) = w^T x + b \qquad (9)$$

Where, w is known as weight vector and b is the bias.

RESULTS

The effectiveness of the proposed texture based face liveness detection method is evaluated on three publicly available Face Anti-Spoofing Databases named as NUAA Photograph Imposter database [18], CASIA Face Anti-Spoofing Database [36] and Idiap REPLAY-ATTACK database [37].

The SVM classifier is used to classify the original image and fake face image by using texture based calculated feature vector of LTP. The classifier is trained using a set of positive (genuine faces) and negative (fake faces) samples which are extracted from the provided training data. In order to get sufficient amount of images for building the still image based model, the frames are extracted from training and testing set videos of CASIA and REPLAY-ATTACK Database.

Furthermore, different patch size of the Local Ternary Pattern and LBP is set to compare the performance of face liveness detection method at $LTP_{(8,\ 1)}$, $LTP_{(16,\ 2)}$ *and* $LTP_{(24,\ 3)}$ *as P* sampling pixels with *R* radius for all databases. The threshold value *t=10* is used for LTP in all experiments because it performs better for texture feature descriptor for particularly face spoof detection method.

The Half Total Error Rate *(HTER)* is used as performance measurement of face liveness detection method. Such performance measure is used in this research work because most of the state-of-art approaches have been used and compared with the results obtained by *HTER.*

The evaluated results with different patch size of LBP and LTP on three public domain databases are presented in the Table 1,Table 3 and Table 5. While comparison with reported results on other techniques on these three databases are shown in Table 2, Table 4 and Table 6.

Table 1: HTER % of LTP and LBP with different patch size on NUAA database

Type	P=8,R=1	P=16,R=2	P=24,R=3
LBP	19.03	20.23	20.89
LTP	15.45	19.34	19.69

Table 2. Comparison of LTP with stare-of-art approaches on NUAA database

Approaches	HTER (%)
LBPV[28]	11.97
LBP+LDA[26]	18.32
LBP+SVM[26]	19.03
LBP+SVM*[26]	13.17
($LBP_{8,1}$+$LBP_{8,2}$+$LBP_{16,2}$) +SVM [26]	2.5
$LTP_{8,1}$+SVM [proposed]	**15.45**

Table 3. HTER % of LTP and LBP with different patch size on REPLAY-ATTACK database

Type	P=8,R=1	P=16,R=2	P=24,R=3
LBP	15.16	19.54	20.21
LTP	12.3	17.53	18.01

Table 4. Comparison of LTP with state-of-art approaches on REPLAY ATTACK database

Approaches	HTER (%)
IQA[38]	15.2
IDA+SVM [39]	7.4
LBP-TOP [29]	8.51
LBP+SVM [26]	15.16
DOG+LBP+SVM	11.1
LBP+LDA [26]	17.17
LBP+SVM* [26]	13.87
LTP+SVM [proposed]	**12.3034**

Table 5. HTER % of LTP and LBP with different patch size on CASIA database

Type	P=8,R=1	P=16,R=2	P=24,R=3
LBP	18.17	20.7	21.319
LTP	16.21	18.68	20.56

Table 6. Comparison of LTP with stare-of-art approaches on CASIA database

Approaches	HTER (%)
LBP+LDA [26]	21.01
LBP+SVM [26]	18.17
LBP+SVM*[26]	18.21
DoG-based [38]	17.0
IQA [38]	32.4
LTP+SVM [proposed]	**16.21**

DISCUSSION

1. Achieved results and discussion on NUAA database

The NUAA Photograph Imposter database [16] is consists of 12,614 images of both real client accesses and photo attacks. There are 500 images for each subject's recording. The images in the database are captured using conventional webcams, the resolution of 640×480 is comprised of 15 subjects. In this database, only one type of print based face spoof attack was introduced.

The evaluated results with different patch size of LBP and LTP on NUAA database is presented in the Table 1. This experiment shows that the proposed calculated features with LTP have more ability to discriminate the fake faces as compare to the LBP features. The achieved results of HTER with different patch size have lower values in all three sets as compare to the LBP. But it is also observed that as the size of radius and number of sampling pixels increases, the error rate also increases in both of the technique. The achieved results on NUAA database exhibit that, the LTP increases the performance of face liveness detection over LBP by decreasing 1.89% of HTER in average.

Moreover, the best result is selected from Table 1 and compared with the other reported results in state-of-art methods on NUAA database. From the Table 2, it seems that the proposed method outperforms over two reported results [36] by decreasing around 3.58% and 2.87% of HTER. While in other reported results, instead of original LBP method, other modifications are also adopted. So as to compare with original LBP, LTP performed more robust for classifying fake faces from original skin.

2. Achieved results and discussion on REPLAY-ATTACK database

The Idiap REPLAY-ATTACK database [36] is consists of 1,300 video recordings of both real access and attack attempts of the 50 subjects. The spoof attacks were printed on A4 sized color photos that are displayed as real client photos and videos on mobile phone and on high definition (HD) screen. Two acquisition conditions were also maintained i.e. controlled and adverse illumination. Two types of face spoof attacks were generated likewise fixed and hand-held from different mediums under two illumination conditions.

The grand test set protocol is used for this research work, which is already defined by associated database. The obtained results of Local Ternary Pattern in Table 3 exhibit better performance than Local binary Pattern for all three different patch sizes by decreasing 2.36% of HTER in average. The results show that the performance of face liveness on REPLAY-ATTACK database detection is decreases if the number of neighborhood pixels is increased.

The best calculated result at $LTP_{(8,1)}$ is further compared with the other state-of art methods in Table 4. Local Ternary Pattern (LTP) shows lower the HTER value i.e 12.3% in contrast with most of the reported work.

3. Achieved results and discussion on CASIA Face Anti-Spoofing Database

The CASIA Face Anti-Spoofing Database [35] is consists of 600 video recordings of genuine and attack attempts of 50 subjects. This database contains three types of image quality (low, normal and high) and three face spoof attacks, which were included as warped photos, cut photos from the eye area to perform fake face attack with eye blink and HD displayed video with more diverse attacks in terms of high quality resolution, face variation with pose and expression.

The experimental results on CASIA database with different sampling and radius sizes in Table 5 showed that our proposed method improves the accuracy by reducing the

HTER by 1.58% over LBP. Especially on this database, at the lower sample and radius size gives good result which is further compared with other reported results in Table 6. According to that the proposed LTP improves the face liveness detection rate among all other reported results, which are only compared with texture based methods.

This is important to note that overall performance of LTP based face liveness detection on all three other databases is increased as compared with the traditional LBP. It is seen that more promising results are shown by decreasing HTER in comparison to the state-of-art. Moreover, different patch sizes were also adopted in this research work. With different size of radius and neighbor pixels in LTP and LBP responded in same manner along with all experiment in all databases. It is interesting to note that the HTER increases with the increase in patch size on all three databases as shown in Fig. 5. This reveals that the performance of face liveness detection is affected by setting different mapping methods. The best result is achieved on *P=8 and R=1* patch size.

CONCLUSION

The aim of this research work is to improve the performance of texture based face spoof detection system by introducing Local Ternary Pattern (LTP). The LTP features were obtained by concatenated the histogram of its higher and lower components. The face anti-spoofing experiments were conducted on three different publicly available databases namely NUAA Imposter database, REPLAY-ATTACK database and CASIA face anti-spoofing Database. Three different patch sizes were also adopted for LTP and LBP. The obtained results from both of the descriptors with different patch sizes were compared. The results showed that overall performance of LTP was found to be higher than LBP texture operator. It is also observed that particularly in this application, discriminate ability of original faces from spoof faces is inversely proportional to the size of local patch. A clear margin of the LTP performance superiority over traditional LBP method is evaluated on three publicly available databases and also compared the achieved results with other reported methods on all these three databases. The outcome shows that LTP features performed batter in face anti-spoofing and produce prominent margin by decreasing total error rate.

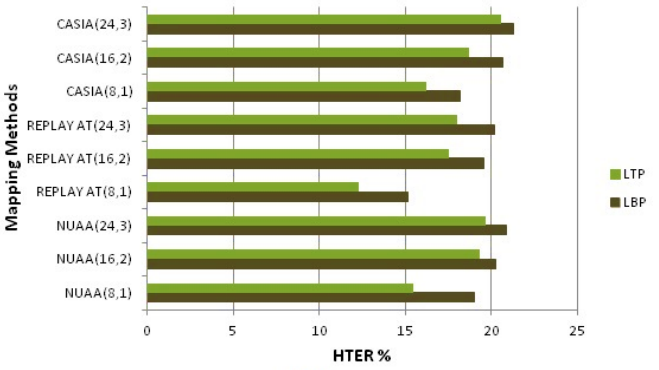

Fig 5. Effect of Different Size of *P* and *R* on Face Liveness Detection method on three public domain databases

REFERENCES

[1] Li, S. Z., "Encyclopedia of Biometrics: I-Z," *Springer Science & Business Media*, **1**: (2009)

[2] Jain, A. K., Maltoni, D., Maio, D. and Wayman, J., "Biometric Systems Technology, Design and Performance Evaluation," *London: Spring Verlag*, (2005)

[3] Jain, A. K., Ross, A. A. and Nandakumar, K., "Introduction to biometrics," *Springer Science & Business Media*, (2011)

[4] Nixon, K. A., Aimale, V., Rowe R. K., "Spoof Detection Schemes," *Handbook of Biometrics*, Springer, (2007)

[5] Parveen, S., Syed, Ahmad, S. M., Hanafi, M., Wan, Adnan, W. A., "Face anti-spoofing methods," *Current Science (00113891)* 108(8), 1491-1500 (2015)

[6] Frischholz, R. W., Werner, A., "Avoiding replay-attacks in a face recognition system using head-pose estimation," *Analysis and Modeling of Faces and Gestures IEEE International Workshop*, (2003)

[7] Kollreider, K., Fronthaler, H., Faraj, M.I., Bigun, J., "Real-time face detection and motion analysis with application in "liveness" assessment," *Information Forensics and Security, IEEE Transactions on*, ***2***(3): 548-558 (2007)

[8] Chetty, G., "Robust audio visual biometric person authentication with liveness verification," *Intelligent Multimedia Analysis for Security Applications. Springer Berlin Heidelberg*, 59-78 (2010)

[9] Schuckers, S. A., "Spoofing and anti-spoofing measures," *Information Security technical report* **7**(4): 56-62 (2002)

[10] Chetty, G. and Wagner, M., "Multi-level liveness verification for face-voice biometric authentication," *Biometrics symposium*, Baltimore, Maryland, 19-21 (2006)

[11] Kant, C. and Sharma, N., "Fake Face Recognition using Fusion of Thermal Imaging and Skin Elasticity," *International Journal of Computer Science and Communication*, **4**(1): 65-72 (2013)

[12] Kollreider, K., Fronthaler, H., Bigun, J., "Verifying Liveness by Multiple Experts in Face Biometrics," *IEEE Computer Vision and Pattern Recognition Workshops. CVPRW '08*. 23-28 (2008)

[13] Lagorio, A., Tistarelli, M., Cadoni, M., Fookes, C., Clinton, B. and Sridha, S., "Liveness detection based on 3D face shape analysis," *IEEE International Workshop on Biometrics and Forensics (IWBF)*, Lisbon, Portugal, 1-4 (2013)

[14] Bao, W., Li, H., Li, N. and Jiang, W., "A Liveness detection method for face recognition based on optical flow field," *IEEE International Conference on Image analysis and signal processing (IASP)*, 233-236 (2009)

[15] Wang, T., Jianwei, Y., Zhen, L., Shengcai, L. and Stan, Z. L., "Face liveness detection using 3d structure recovered from a single camera," *IEEE International Conference on Biometrics (ICB)*, 1-6 (2013)

[16] Kollreider, K., Fronthaler, H. and Bigun, J., "Non-intrusive liveness detection by face images," *Image and Vision Computing*, **27**(3): 233-244 (2009)

[17] Choudhury, T., Clarkson, B., Jebara, T. and Pentland, A., "Multimodal person recognition using unconstrained audio and video," *International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA'99)*, Washington DC, 176–181(1999)

[18] Tan, X., Li, Y., Liu, J. and Jiang, L., "Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model," *Computer Vision-ECCV, Springer Berlin Heidelberg*, 504-517, (2010)

[19] Pan, G., Sun, L., Wu, Z. and Lao, S., "Eye blink-based Anti-Spoofing in Face Recognition from a Generic Web camera," *IEEE 11th International Conference on computer vision (ICCV'07)*, Rio de Janeiro, Brazil, 14-20 (2007)

[20] Pan, G., Sun, L., Wu, Z. and Lao, S., "Eye blink-based Anti-Spoofing in Face Recognition from a Generic Web camera," *IEEE 11th International Conference on computer vision (ICCV'07)*, Rio de Janeiro, Brazil, 14-20 (2007)

[21] Szwoch, M. and Pieniążek, P., "Eye blink based detection of liveness in biometric authentication systems using conditional random fields," *Computer Vision and Graphics. Springer Berlin Heidelberg*, 669-676 (2012)

[22] Jee, H. K., Jung, S.U. and Yoo, J. H., "Liveness detection for embedded face recognition system," *International Journal of Biological and Medical Sciences*, **1**(4): 235-238 (2006)

[23] Li, J., Wang, Y., Tan, T. and Jain, A. K., "Live face detection based on the analysis of Fourier spectra," *in Defense and Security. International Society for Optics and Photonics*. 296-303. (2004)

[24] Hadid, A., "The local binary pattern approach and its application to face analysis," *IEEE First Workshops on Image Processing Theory, Tools and Applications (IPTA)*, 1-9 (*2008*)

[25] Chingovska, I., Anjos, A. and Marcel, S., "On the Effectiveness of Local Binary Patterns in Face Anti-spoofing," *IEEE International Conference of the Biometrics Special Interest Group (BIOSIG)*,1-7(2012)

[26] Määttä, J., Hadid, A. and Pietikäinen, M., "Face Spoofing Detection from Single Images Using Micro-Texture Analysis," *IEEE International joint conference on Biometrics (IJCB)*, 1-7 (2011)

[27] De Freitas Pereira, T., Komulainen, J., Anjos, A., De Martino, J. M., Hadid, A., Pietikäinen, M. and Marcel, S., "Face liveness detection using dynamic texture," *EURASIP Journal on Image and Video Processing*,1-15 (2014:1)

[28] Kose, N. and Dugelay, J. L., "Classification of Captured and Recaptured Images to Detect Photograph Spoofing," *IEEE International Conference on Informatics, Electronics & Vision (ICIEV)*,1027-1032 (2012)

[29] De Freitas Pereira, T., Anjos, A., De Martino J. M. and Marcel, S., "LBP−TOP based countermeasure against face spoofing attacks," *Computer Vision-ACCV Workshops, Springer Berlin Heidelberg*,121-132 (2013)

[30] Housam, K. B., Lau, S. H., Pang, Y. H., Liew, Y. P. and Chiang, M. L., "Face Spoofing Detection Based on Improved Local Graph Structure," *IEEE International Conference on Information Science and Applications (ICISA)*,1-4 (2014)

[31] Kim, S., Yu, S., Kim, K., Ban, Y. and Lee, S., "Face liveness detection using variable focusing," *IEEE International Conference on Biometrics (ICB)*,1-6 (2013)

[32] Tan, X. and Triggs, B., "Enhanced local texture feature sets for face recognition under difficult lighting conditions," *IEEE Transactions on Image Processing*, **19**(6), 1635-1650 (2010)

[33] Ojala, T., Pietikäinen, M., Mäenpää, T., "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **24**(7), 971-987 (2002)

[34] Ojala, T., Pietikäinen, M. and Harwood, D., "A comparative study of texture measures with classification based on featured distributions," *Pattern recognition*, **29**(1), 51-59 (1996)

[35] Cristianini, N. and Shawe-Taylor, J., "An introduction to support vector machines and other kernel-based learning methods," *Cambridge university press* (2000)

[36] Zhang, Z., Yan, J., Liu, S., Lei, Z., Yi, D. and Li, S. Z., "A face antispoofing database with diverse attacks," IEEE *5th International conference on Biometrics (ICB)*, 26-31 (2012)

[37] Chingovska, I., Anjos, A. and Marcel, S., "On the effectiveness of local binary patterns in face anti-spoofing," *IEEE International conference of the Biometrics Special Interest Group (BIOSIG)*, 1-7 (2012)

[38] Galbally, J. and Marcel, S., "Face Anti-spoofing Based on General Image Quality Assessment," IEEE *22nd International Conference on Pattern Recognition (ICPR)*, 1173-1178 (2014)

[39] Wen, D., Han, H., Jain, A. K., "Face spoof detection with image distortion analysis," *IEEE Transactions on Information Forensics and Security*, **10**(4), 746-761 (2015)