Journal of Engineering Sciences
Vol 11, Issue 4 , April/2020
ISSN NO:0377-9254

DEEP TEXTURE FEATURES FOR ROBUST FACE SPOOFING DETECTION

Vunnam Umamaheswari[1] , Baddigam Indu Sree[2], Muppalla Suma[3], Nelluri Lekhana[4], V.Sasikala[5]

[1,2,3,4]IV B.Tech, Department of Information Technology, Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur-522009, Andhra Pradesh, India.

[5]Asst.Professor, Department of Information Technology, Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur-522009, Andhra Pradesh, India.

kala.sasiv88@gmail.com

ABSTRACT

Biometric systems are quite common in our everyday life. Face anti-spoofing is crucial to prevent face recognition systems from a security breach. Previous deep learning approaches formulate face anti-spoofing as a binary classification problem. Many of them struggle to grasp adequate spoofing cues and generalize poorly. Nowadays criminals are developing techniques to accurately simulate physical, physiological, and behavioral traits of valid users, process known as spoofing attack. Most of state-of-the-art anti spoofing techniques for face recognition applications extracts handcrafted texture features from images, mainly based on the efficient local binary patterns (LBP) descriptor, to characterize them.

Keywords: Deep Learning, Deep Texture Features, Spoofing Method, PCA, LBP, LDA, Gabor Filter.

1. INTRODUCTION

Biometric systems are increasingly common in our everyday activities. People recognition through their own physical, physiological or behavioral traits inhibits most of the frauds often committed in security systems based on knowledge (passwords) or tokens (cards, keys, etc.). However, nowadays criminals are already developing techniques to accurately simulate the biometric characteristics of valid users, such as face, fingerprint and iris, to gain access to places or systems, process known as spoofing attack[1][2]. In this context, robust countermeasure techniques must be developed and integrated into the traditional biometric applications in order to prevent such frauds. Despite face being a promising trait due to its convenience for users, universality and acceptability, traditional face recognition systems can be easily fooled with common printed facial photographs, which nowadays can be obtained by criminals on the worldwide network, especially due to the dissemination of social medias and networks[3][4]. Spatial image information is extremely important in tasks involving faces, such as face detection and face recognition[5][6].

Face ID is the most generally utilized technique in applications, for example, PC/smart phone login, recognizable proof cards, and outskirt and identification control. Appearance of the face is used in this biometric feature as a key to distinguish a person among group of individuals. Though it has various disadvantages, including variations in illumination and head pose, still it can be utilized with other biometric characteristics like fingerprints, finger-veins, palm-veins, etcetera to guarantee the high accuracy rate of recognition systems. Various components of a face recognition process are shown in Fig. 1 [7][8].

Firstly, to capture the image of users, they must exhibit their faces in front of capturing devices. In this manner, the face restriction and highlight extraction steps are performed to separate picture highlights from the info face picture. At long last, a matching algorithm is performed to perceive the approved client in the information picture[9][10].

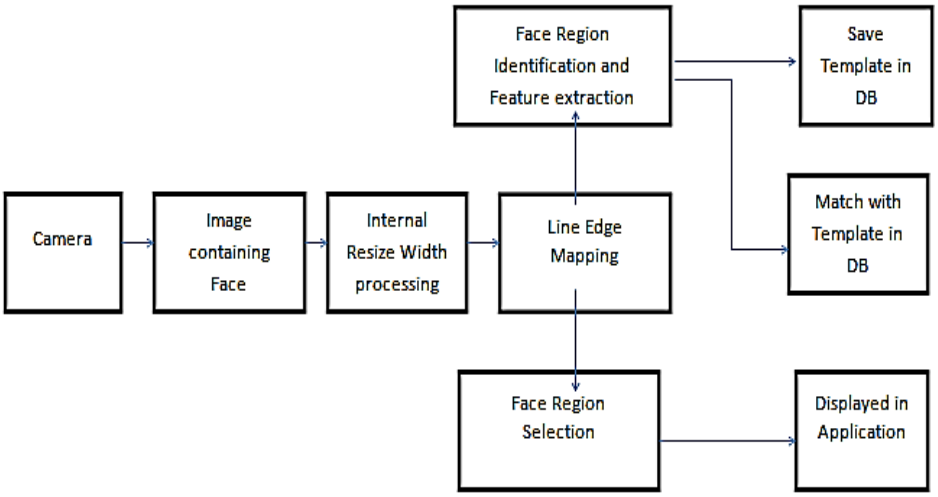

Fig. 1 Components of Face Recognition System

However, a face recognition system can be attacked by various means such as (a) printed photos, (b) displayed image or motion video; (c) plastic surgery; (d) sketch; (e) make-up and accessory wearing; (f)3D mask; or (h) synthetic photograph or video, generated using computer graphics. To take care of this issue, the presentation attack detection (PAD) strategies have been looked into for such systems. Past investigations are ordered into two classes of feature extraction methods, training-based and non-training-based[11][12] .

2. LITERATURE SURVEY

The different visual patterns of each facial region encode rich and discriminative information necessary to distinguish a face from other objects, and also from other faces. Regarding face spoofing detection, some works based on handcrafted features have mentioned that different spoofing cues can be extracted from different facial regions[13][14]. Recently, deep learning architectures have emerged as good alternatives for solving complex problems and have reached state-of-the-art results in many tasks due to their great power of abstraction and robustness, working with high-level features, self-learned from the training data[39]. Among the proposed deep learning architectures, Convolutional Neural Networks (CNN) have appeared as one of the most important classes of deep neural networks able to deal with digital images with great performances[15][16].

Some CNN based state-of-the-art methods were recently proposed for face spoofing detection. However, none of them take into account the different visual aspects of each facial region and, consequently, the different local spoofing cues that could be learned by the neural networks to improve their performances[17][18]. All proposed methods work on whole faces, in a holistic way, or with random and small patches, i.e., they train the neural networks with samples extracted from random regions of the faces, all together. This can degrade the performance of the training algorithm since the back propagation method [36]can be distracted by the different visual information extracted from random regions of the face, instead of learning the real differences between real and fake faces in each facial region, with similar visual aspects, differing only by spoofing cues[37][38]. In this context, we propose a novel CNN architecture trained in two steps for a better performance in face spoofing detection[19][20]: (i) the local pre-training phase, in which each part of the model is trained on each main facial region, learning deep local features for attack detection and initializing the whole model in a great position in the search space (the network learns to detect multiple and different spoofing cues from all the facial regions)[35]; (ii) the global fine tuning phase, in which the whole model is fine-tuned based on the weights learned independently by its parts and on whole real and fake facial images, in order to improve the model generalization [21][22][41].

Results obtained on two major datasets used for the evaluation of face spoofing detection techniques,

3. RELATED METHODS

A. Different types of feature descriptors

Face spoofing detection can be done by various ways, using different descriptors. Some of the descriptors based on global approaches are described as:-

1. Local Binary Pattern (LBP) [42]
2. Gabor Filter [43]
3. LDA (Local Descriptor Analysis)
4. PCA (Principle Component Analysis)

Table I depicts the comparative analysis of the above mentioned image feature descriptors along with their benefits and limitations[23][24].

Considering the various descriptors, LBP is used here to extract the texture information. Local binary pattern (LBP) is significantly intended for analysis and description of texture of images. It is for the most part utilized on account of its fantastic light invariance property and low computational unpredictability. The major aspect of working of LBP operator is a 3 x 3 pixel matrix[25][26]. In this matrix, center pixel is considered as threshold [34]and is surrounded by eight neighbours. Being threshold value, center pixel allows its surrounding pixels to be marked as 1 or 0, former value if their gray value is higher or equal than center pixel, and otherwise they are given latter value. At last, a code is obtained whose decimal equivalent is computed and placed at center pixel. Fig. 2 delineates the LBP operator[27][28].

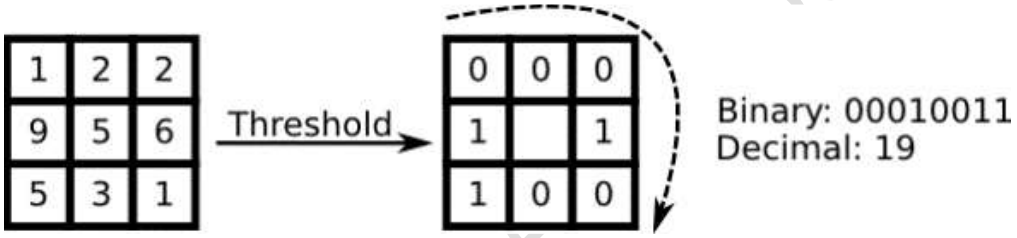

Fig. 2 Basic LBP operator

Table I: Comparison of various image feature descriptor

Feature Descriptor	Pros	Cons
PCA	The dimension of data is reduced, easy to use and learn the whole image of face taken into consideration.	Time required to find Eigen values is more so it is more time consuming. It is affected by lighting conditions.
LBP	Used in texture description, fast and efficient computation, moving objects by subtracting background of image.	Face localisation are not detected, large regions increase the error rate, can be used in binary and gray image only.
LDA	Identify individuals of same faces, grouped individual faces with same features ,lighting variations solved because it is used within class	More complex method, difference between classes affect within class.
GABOR FILTER	Captures spatial frequency, localisation, and orientation.	Sensitive to illumination changes.

B. Convolutional Neural Networks (CNN)

Convolutional Neural networks are considered as deep learning architectures which contain various layers where filters like convolution and sampling are employed as the input to two dimensional images data [29][30]. The final outcome of the initial layer is used as the input to the consecutive one till it reaches the top of the network. These type of networks give the simple topology in comparison to other fully connected networks [44] [45]. After the operation of convolution and sampling layers that are totally in contact can be indulged at the top for the classification[31][32].The layered network of CNN is revealed in Fig. 3.

Practically, for a two-dimensional image in each network layer, Convolutional filters are applied through which different channels of the original inputs are obtained [46] [47]. Pooling which is also known as the sampling operations are done to get different kind of translational and scale invariance and decrease the quantity of data that is considered high level representation of original image is obtained at the top of the network which is more robust then the raw pixels information for various applications[33][34].

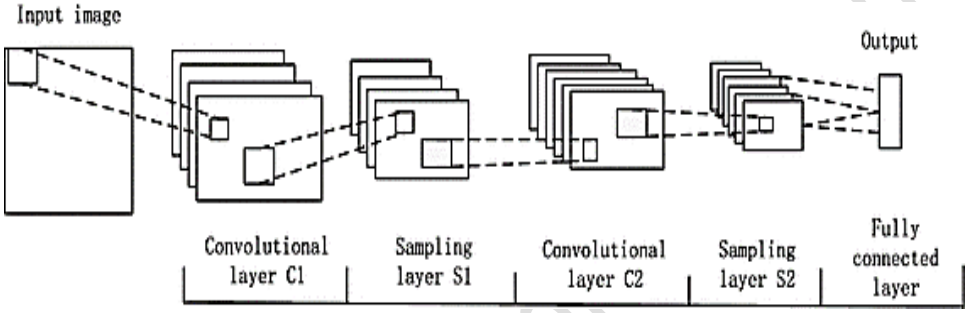

Fig. 3 Layers in Convolutional Neural Networks

4. PROPOSED METHOD

Face Track is an efficient system to perform liveness detection by tracking face changes of users.

Face Track collects face positions and uses the derived trajectories to draw a conclusion. It requires no special hardware, and can therefore be used on any device equipped with a camera and a display. Face Track is also robust in environmental condition changes, such as light intensity and face-camera distance [48] [49]. Fig 4 describes the flow of process followed in the experimental program for the evaluation of efficient face recognition. First of all, data acquisition of the training videos is done. The video can be converted into frames. In this step, images from the given database are selected to be processed further. The training images here are referred as the knowledge base of the given dataset. This knowledge base consists of original as well as fake images.

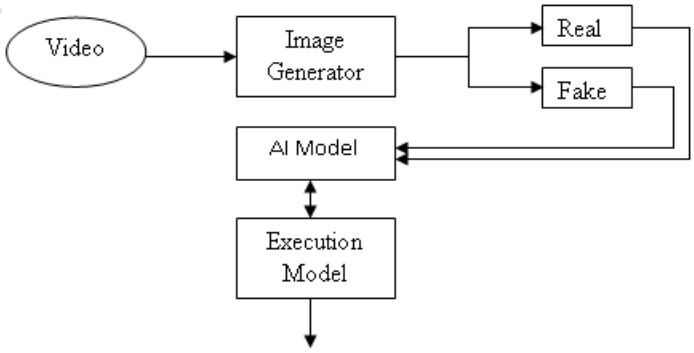

Fig 4: Flow of process of proposed method

Journal of Engineering Sciences
Vol 11, Issue 4 , April/2020
ISSN NO:0377-9254

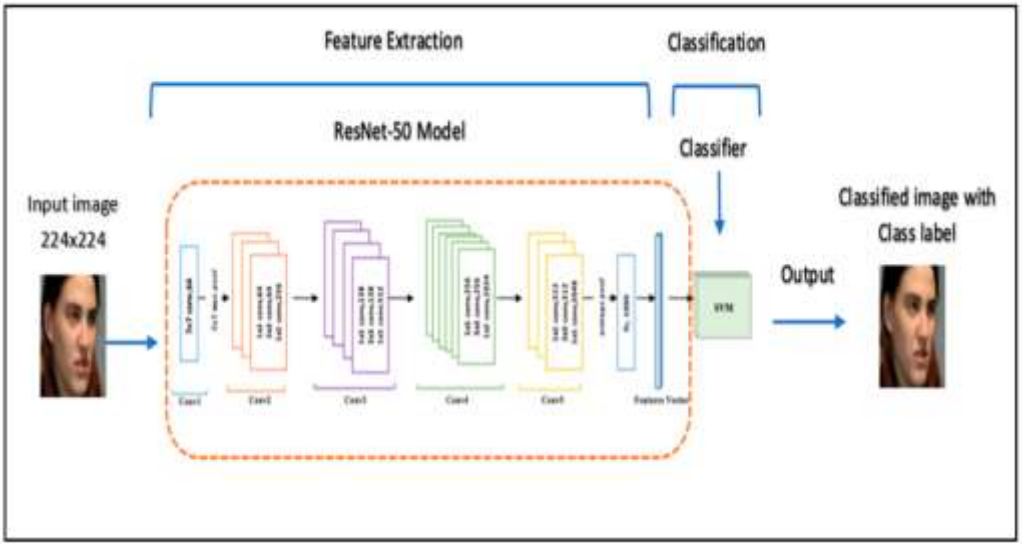

Figure 5: Proposed Architecture with CNN Layers

The major texture descriptors, the real LBP with new advancement of Gene-LBP method is created to extract the feature and optimize the extracted feature with the help of three operators namely selection, crossover and mutation. These operators must work in conjunction with one another in order for the algorithm to be successful.

After training, test images are selected and pre processed in the same manner as that of training images. Then, the feature vectors of test images are also extracted. For classification, the feature vectors of training images, testing images and class label are transferred to CNN Classifier which is trained to calculate the class of novel face. It divides face image in patches and create an image histogram to each patch, which at the end are combined. The final stage is face detection in which the classifier will distinguish between the ―Real‖ or ―Fake‖ face spoofing detection. Apart from this, various performance parameters are calculated to compare the results of the proposed method with various state of art spoofing detection techniques.

LBP-Based Convolutional neural network:

The LBP net presents the following configuration, from bottom to top, mainly inherited from Lenet 5:

a) The first layer is modified, as said, by incorporating the LBP descriptor in the convolution step.
b) Rectified Linear Unit layer, that performs an inner product followed by a rectification (–ve) negative values on the originated signals.
c) Fully Connected (FC) layer, with two nodes, which also performs an inner product and classification (attack or not attack attempt) of the input image using the softmax function.

❖ The convolution operation can be written as:

$$Ci(p) = \forall q \in N(p) LBP(I(q)) \cdot Ki(j) \text{------(1)}$$

q belonging to the neighborhood of pixel;

p = (xp,yp), i.e., q ∈ N(p) in original image I (also considering p∈N(p));

Ci(p) means the value in the corresponding position to p in the output feature map Ci,

with i = 1,2,...,20; and Ki(j).

❖ . The max-pooling operation can be written as:

$$Pi(r) = \max\{Ci(s)\} \forall s \in N(r) \text{ -------(2)}$$

s=(xs,ys), represents the value in position s belonging to the neighborhoods;

r = (xr,yr), i.e., s∈N(r), in feature map;

Ci (generated in the previous convolution step), with i=1,2,...,20 (also considering r ∈N(r));

Pi(r) means the value in the corresponding position to r in the new output feature map Pi.

❖ At the top of the network there are a Rectified Linear Unit (ReLU) and a Fully Connected (FC) layers. The ReLU layer actuates by performing an inner product

with the 13 × 13 structures and by rectifying the signal obtained, not propagating negative values, following Eq. 3:

ReLU(t) = max{0;t} (3)

where t corresponds to the weighted sum of the signals from the neurons of the previous layer of the LBPnet (values in the 13 × 13 feature maps).

- Inner product operation and applying the softmax function for defining their activations, which is

sk = e^uk/(e^u0+e^u1) -------(4)

Sample Code:

```
# construct the argument parser and parse the arguments
ap = argparse.ArgumentParser()
ap.add_argument("-d", "--dataset", required=True,
	help="path to input dataset")
ap.add_argument("-m", "--model", type=str,
required=True,
	help="path to trained model")
ap.add_argument("-l", "--le", type=str,
required=True,
	help="path to label encoder")
ap.add_argument("-p", "--plot", type=str,
default="plot.png",
	help="path to output loss/accuracy plot")
args = vars(ap.parse_args())
# initialize the initial learning rate, batch size, and number of
# epochs to train for
INIT_LR = 1e-4
BS = 8
EPOCHS = 50
# grab the list of images in our dataset directory, then initialize
# the list of data (i.e., images) and class images
	print("[INFO] loading images...")
	imagePaths =
	 list(paths.list_images(args["dataset"]))
	data = []
	labels = []
for imagePath in imagePaths:
# extract the class label from the filename, load the image and
# resize it to be a fixed 32x32 pixels, ignoring aspect ratio
	label = imagePath.split(os.path.sep)[-2]
	image = cv2.imread(imagePath)
	image = cv2.resize(image, (32, 32))
# update the data and labels lists, respectively
	data.append(image)
	labels.append(label)
```

5. RESULTS

The NUAA photo data base is collected using several webcams from an electronic market. The database is collected in three forms in an interval of two weeks between two sessions and the condition of every single session is different. The 15 subjects that are given were numbered from 1 to 15 and every single session takes the images of together the subjects that are live with their photographs. The sample images from the three sessions are obtained from the database. The left side reveals the actual image of human whereas the right one is the photograph of the person. There will be alterations in appearance for the recognition system. Database contains all the colour images with the same value of pixels. Each subject from every session use webcams to capture series of data images. During image capturing, each subject sees webcam with neutral expression. In this way live human looks like a photo.

Fig. 6 Example of face image dataset

In order to collect the sample of the photo, highly defined photo for each subject use camera to take two by third of the overall region of the picture. There are different ways in which the photos are generated, firstly photos are printed on piece of paper with common size.

Fig. 7 Example of Dissimilar Attacks in Image Datasets

It implies that if an intruder wants access to the authorised system, then using these dissimilar attacks it could have been possible. However, anti-spoofing techniques ensure that these attacks can be detected and corrected efficiently.

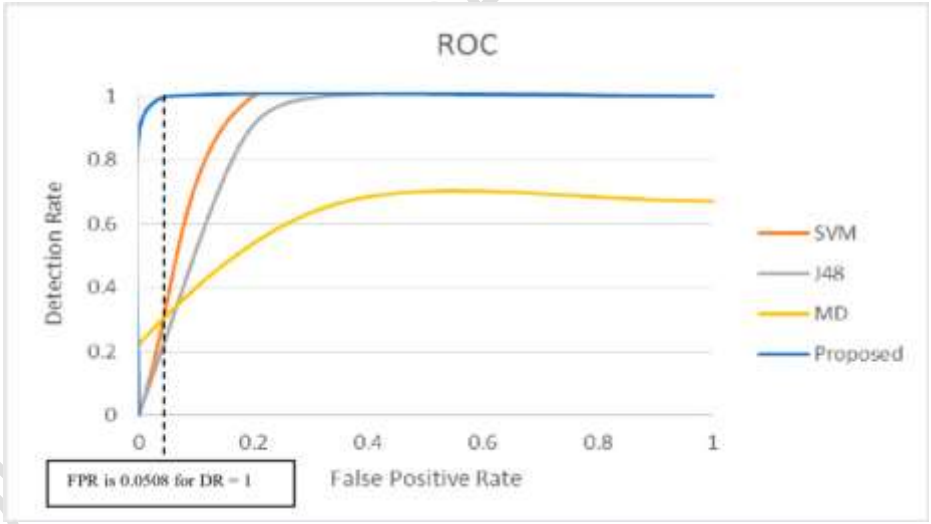

Fig : 8 ROC curve

Regarding the ROC curves, Fig. 7 shows the True Acceptance Rate (TAR) versus the False Acceptance Rate (FAR) of: (i) SVM; (ii) J48; (iii) MD; (iv) the best method of the original paper of the NUAA dataset - this best approach works on Different images

6. CONCLUSION

In this brief, two LBP-based Convolutional Neural Networks, LBPnet and n-LBPnet, are proposed for spoofing detection in face recognition systems, which presented great results on the NUAA spoofing dataset, outperforming other assessed state-of-the-art

techniques. With the highest ROC curves, low EER as well as high accuracy, the proposed LBPnet and n-LBPnet networks configure effective alternatives for spoofing detection in real face recognition applications of nowadays. Besides of presenting great results, the proposed methods are more efficient than other state-of the-art techniques that combine lots of handcrafted informationto detect attacks. Our approaches use the LBP descriptor with a single neighborhood, a forward bottom-up pass and simple softmax neurons at the top for detecting spoofing attempts quickly, being more suitable for real time applications. Based on all this it is possible to conclude that deep texture features are rich sources of information for face spoofing detection, propiciating better results than handcrafted ones (or even combination of them, which may become impractical). The integration of the LBP descriptor in a deep learning architecture is a suitable and robust alternative to prevent such criminal activities.

References

[1]. Lakshman Narayana Vejendla and A Peda Gopi, (2019)," Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology", Revue d'Intelligence Artificielle , Vol. 33, No. 1, 2019,pp.45-48.

[2]. Gopi, A.P., Jyothi, R.N.S., Narayana, V.L. et al. (2020), "Classification of tweets data based on polarity using improved RBF kernel of SVM" . Int. j. inf. tecnol. (2020). https://doi.org/10.1007/s41870-019-00409-4.

[3]. A Peda Gopi and Lakshman Narayana Vejendla, (2019)," Certified Node Frequency in Social Network Using Parallel Diffusion Methods", Ingénierie des Systèmes d' Information, Vol. 24, No. 1, 2019,pp.113-117.. DOI: 10.18280/isi.240117

[4]. Lakshman Narayana Vejendla and Bharathi C R ,(2018),"Multi-mode Routing Algorithm with Cryptographic Techniques and Reduction of Packet Drop using 2ACK scheme in MANETs", Smart Intelligent Computing and Applications, Vo1.1, pp.649-658. DOI: 10.1007/978-981-13-1921-1_63 DOI: 10.1007/978-981-13-1921-1_63

[5]. Lakshman Narayana Vejendla and Bharathi C R, (2018), "Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS", Modelling, Measurement and Control A, Vol.91, Issue.2, pp.73-76. DOI: 10.18280/mmc_a.910207

[6]. Lakshman Narayana Vejendla , A Peda Gopi and N.Ashok Kumar,(2018)," Different techniques for hiding the text information using text steganography techniques: A survey", Ingénierie des Systèmes d'Information, Vol.23, Issue.6,pp.115-125.DOI: 10.3166/ISI.23.6.115-125

[7]. A Peda Gopi and Lakshman Narayana Vejendla (2018), "Dynamic load balancing for client server assignment in distributed system using genetic algorithm", Ingénierie des Systèmes d'Information, Vol.23, Issue.6, pp. 87-98. DOI: 10.3166/ISI.23.6.87-98

[8]. Lakshman Narayana Vejendla and Bharathi C R,(2017),"Using customized Active Resource Routing and Tenable Association using Licentious Method Algorithm for secured mobile ad hoc network Management", Advances in Modeling and Analysis B, Vol.60, Issue.1, pp.270-282. DOI: 10.18280/ama_b.600117

[9]. Lakshman Narayana Vejendla and Bharathi C R,(2017),"Identity Based Cryptography for Mobile ad hoc Networks", Journal of Theoretical and Applied Information Technology, Vol.95, Issue.5, pp.1173-1181. EID: 2-s2.0-85015373447

[10]. Lakshman Narayana Vejendla and A Peda Gopi, (2017)," Visual cryptography for gray scale images with enhanced security mechanisms", Traitement du Signal,Vol.35, No.3-4,pp.197-208. DOI: 10.3166/ts.34.197-208

[11]. A Peda Gopi and Lakshman Narayana Vejendla, (2017)," Protected strength approach for image steganography", Traitement du Signal, Vol.35, No.3-4,pp.175-181. DOI: 10.3166/TS.34.175-181

[12]. Lakshman Narayana Vejendla and A Peda Gopi, (2020)," Design and Analysis of CMOS LNA with Extended Bandwidth For RF Applications", Journal of Xi'an University of Architecture & Technology, Vol. 12, Issue. 3,pp.3759-3765. https://doi.org/10.37896/JXAT12.03/319.

[13]. Chaitanya, K., and S. Venkateswarlu,(2016),"DETECTION OF BLACKHOLE & GREYHOLE ATTACKS IN MANETs BASED ON ACKNOWLEDGEMENT BASED APPROACH." Journal of Theoretical and Applied Information Technology 89.1: 228.

[14]. Patibandla R.S.M.L., Kurra S.S., Mundukur N.B. (2012), "A Study on Scalability of Services and Privacy Issues in Cloud Computing". In: Ramanujam R., Ramaswamy S. (eds) Distributed Computing and Internet Technology. ICDCIT 2012. Lecture Notes in Computer Science, vol 7154. Springer, Berlin, Heidelberg

[15]. Patibandla R.S.M.L., Veeranjaneyulu N. (2018), "Survey on Clustering Algorithms for Unstructured Data". In: Bhateja V., Coello Coello C., Satapathy S., Pattnaik P. (eds) Intelligent Engineering Informatics. Advances in Intelligent Systems and Computing, vol 695. Springer, Singapore

[16]. Patibandla, R.S.M.L., Veeranjaneyulu, N. (2018), "Performance Analysis of Partition and Evolutionary Clustering Methods on Various Cluster Validation Criteria", Arab J Sci Eng ,Vol.43, pp.4379–4390.

[17]. R S M Lakshmi Patibandla, Santhi Sri Kurra and N.Veeranjaneyulu, (2015), "A Study on Real-Time Business Intelligence and Big Data",Information Engineering, Vol.4,pp.1-6.

[18]. K. Santhisri and P.R.S.M. Lakshmi,(2015), " Comparative Study on Various Security Algorithms in Cloud Computing", Recent Trends in Programming Languages ,Vol.2,No.1,pp.1-6.

[19]. K.Santhi Sri and PRSM Lakshmi,(2017), "DDoS Attacks, Detection Parameters and Mitigation in Cloud Environment", IJMTST,Vol.3,No.1,pp.79-82.

[20]. P.R.S.M.Lakshmi,K.Santhi Sri and Dr.N. Veeranjaneyulu,(2017), "A Study on Deployment of Web Applications Require Strong Consistency using Multiple Clouds", IJMTST,Vol.3,No.1,pp.14-17.

[21]. P.R.S.M.Lakshmi,K.Santhi Sri and M.V.Bhujanga Ra0,(2017), "Workload Management through Load Balancing Algorithm in Scalable Cloud", IJASTEMS,Vol.3,No.1,pp.239-242.

[22]. K.Santhi Sri, P.R.S.M.Lakshmi, and M.V.Bhujanga Ra0,(2017), "A Study of Security and Privacy Attacks in Cloud Computing Environment", IJASTEMS,Vol.3,No.1,pp. 235-238.

[23]. R S M Lakshmi Patibandla and N. Veeranjaneyulu, (2018), "Explanatory & Complex Analysis of Structured Data to Enrich Data in Analytical Appliance", International Journal for Modern Trends in Science and Technology, Vol. 04, Special Issue 01, pp. 147-151.

[24]. R S M Lakshmi Patibandla, Santhi Sri Kurra, Ande Prasad and N.Veeranjaneyulu, (2015), "Unstructured Data: Qualitative Analysis", J. of Computation In Biosciences And Engineering, Vol. 2,No.3,pp.1-4.

[25]. R S M Lakshmi Patibandla, Santhi Sri Kurra and H.-J. Kim,(2014), "Electronic resource management using cloud computing for libraries", International Journal of Applied Engineering Research, Vol.9,pp. 18141-18147.

[26]. Ms.R.S.M.Lakshmi Patibandla Dr.Ande Prasad and Mr.Y.R.P.Shankar,(2013), "SECURE ZONE IN CLOUD", International Journal of Advances in Computer Networks and its Security, Vol.3,No.2,pp.153-157.

[27]. Patibandla, R. S. M. Lakshmi et al., (2016), "Significance of Embedded Systems to IoT.", International Journal of Computer Science and Business Informatics, Vol.16,No.2,pp.15-23.

[28]. AnveshiniDumala and S. PallamSetty. (2020),"LANMAR routing protocol to support real-time communications in MANETs using Soft computing technique", 3rd International Conference on Data

Engineering and Communication Technology (ICDECT-2019), Springer, Vol. 1079, pp. 231-243.

[29]. AnveshiniDumala and S. PallamSetty. (2019),"Investigating the Impact of Network Size on LANMAR Routing Protocol in a Multi-Hop Ad hoc Network", i-manager's Journal on Wireless Communication Networks (JWCN), Volume 7, No. 4, pp.19-26.

[30]. AnveshiniDumala and S. PallamSetty. (2019),"Performance analysis of LANMAR routing protocol in SANET and MANET", International Journal of Computer Science and Engineering (IJCSE) – Vol. 7,No. 5, pp.1237-1242.

[31]. AnveshiniDumala and S. PallamSetty. (2018), "A Comparative Study of Various Mobility Speeds of Nodes on the Performance of LANMAR in Mobile Ad hoc Network", International Journal of Computer Science and Engineering (IJCSE) – Vol. 6, No. 9, pp. 192-198.

[32]. AnveshiniDumala and S. PallamSetty. (2018),"Investigating the Impact of IEEE 802.11 Power Saving Mode on the Performance of LANMAR Routing Protocol in MANETs", International Journal of Scientific Research in Computer Science and Management Studies (IJSRCSMS) – Vol.7, No. 4.

[33]. AnveshiniDumala and S. PallamSetty. (2016),"Analyzing the steady state behavior of RIP and OSPF routing protocols in the context of link failure and link recovery in Wide Area Network", International Journal of Computer Science Organization Trends (IJCOT) – Vol. 34 No 2, pp.19-22.

[34]. AnveshiniDumala and S. PallamSetty. (2016),"Investigating the Impact of Simulation Time on Convergence Activity & Duration of EIGRP, OSPF Routing Protocols under Link Failure and Link Recovery in WAN Using OPNET Modeler", International Journal of Computer Science Trends and Technology (IJCST) – Vol. 4 No. 5, pp. 38-42.

[35]. VellalacheruvuPavani and I. Ramesh Babu (2019) ,"Three Level Cloud Storage Scheme for Providing Privacy Preserving using Edge Computing",International Journal of Advanced Science and Technology Vol. 28, No. 16, pp. 1929 – 1940.

[36]. VellalacheruvuPavani and I. Ramesh Babu,"A Novel Method to Optimize the Computation Overhead in Cloud Computing by Using Linear Programming" ,International Journal of Research and Analytical Reviews May 2019, Volume 6, Issue 2,PP.820-830..

[37]. Anusha Papasani and Nagaraju Devarakonda,(2016),"Improvement of Aomdv Routing Protocol in Manet and Performance Analysis of Security Attacks", International Journal Of Research in Computer Science & Engineering ,Vol.6,No.5, pp.4674-4685.

[38]. Sk.Reshmi Khadherbhi,K.Suresh Babu , Big Data Search Space Reduction Based On User Perspective Using Map Reduce ,International Journal of Advanced Technology and Innovative Research Volume.07, IssueNo.18, December-2015, Pages: 3642-3647

[39]. B.V.Suresh kumar,Sk.Reshmi Khadherbhi ,BIG-IOT Framework Applications and Challenges: A Survey Volume 7, Issue VII, JULY/2018 pg.no 1257-1264

[40]. P.Sandhya Krishna,Sk.Reshmi Khadherbhi,V.Pavani, Unsupervised or Supervised Feature Finding For Study of Products Sentiment ,International Journal of Advanced Science and Technology, Vol 28 No 16 (2019).

[41]. S.Sasikala, P.Sudhakar, "interpolation of CFA color Images with Hybrid image denoising", 2014 Sixth International Conference on Computational Intelligence and Communication Networks, DOI 10.1109/.53 193 DOI 10.1109/CICN.2014.53, pp. 193-197.

[42]. K.Santhi Sri, Dr.Ande Prasad (2013), "A Review of Cloud Computing and Security Issues at Different Levels in Cloud Computing" , International Journal on Advanced Computer Theory and Engineering Vol. 2,pp 67-73.

[43]. K.Santhi Sri, N.Veeranjaneyulu(2018), "A

Vol 11, Issue 4 , April/2020
ISSN NO:0377-9254

Novel Key Management Using Elliptic and Diffie-Hellman for Managing users in Cloud Environment", Advances in Modelling and Analysis B,Vol.61,No.2,pp 106-112.

[44]. K.Santhi Sri, N.Veeranjaneyulu(2019), "Decentralized Key Management Using Alternating Multilinear Forms for Cloud Data Sharing with Dynamic Multiprivileged Groups", Mathematical Modelling of Engineering Problems,Vol.6,No.4,pp511-518.

[45]. S.Sasikala, P.Sudhakar, "interpolation of CFA color Images with Hybrid image denoising", 2014 Sixth International Conference on Computational Intelligence and Communication Networks, DOI 10.1109/.53 193 DOI 10.1109/CICN.2014.53, pp. 193-197.

[46]. Me. Jakeera Begum and M.Venkata Rao, (2015), "Collaborative Tagging Using CAPTCHA" International Journal of Innovative Technology And Research, Volume No.3, Issue No.5,pp,2436 – 2439.

[47]. L.Jagajeevan Rao, M. Venkata Rao, T.Vijaya Saradhi (2016), "How The Smartcard Makes the Certification Verification Easy" Journal of Theoretical and Applied Information Technology, Vol.83. No.2, pp. 180-186.

[48]. Venkata Rao Maddumala, R. Arunkumar, and S. Arivalagan (2018)"An Empirical Review on Data Feature Selection and Big Data Clustering" Asian Journal of Computer Science and Technology Vol.7 No.S1, pp. 96-100.

[49]. Singamaneni Kranthi Kumar, Pallela Dileep Kumar Reddy, Gajula Ramesh, Venkata Rao Maddumala, (2019), "Image Transformation Technique Using Steganography Methods Using LWT Technique" ,Traitement du Signalvol 36, No 3, pp. 233-237.