Securing Cloud Data using Face Recognition and Deep Learning

B.Konda Reddy, Ch.Nikhil, Manoj Kolluri, K.Ruth Ramya, Venkata Naresh Mandhala

Abstract**: *In this paper, we propose the face recognition using deep learning approach. Face recognition is used to determine an individual and for authentication purpose, face recognition is used to catch criminals and any approach used for face recognition is not 100% accurate. The main problem of face recognition is intensity, illumination, pose. During this paper the peace of mind and protection to the cloud data is well-found by scrambling the cloud data with human face as a key. The human face can encipher the cloud data that present within the cloud.***

Index Terms**: *Cloud Storage, face recognition, Binary Signal.***

I. INTRODUCTION

In face recognition, however, large scale public datasets are lacking and, for the most part thanks to this issue, most of the current advances within the neighborhood continue to be restricted to net giants like Face book and Google etc. for instance, the primary recent face consciousness methodology by means of Google [1]was once skilled mistreatment two hundred million photographs and eight million distinctive identities. The dimensions of this dataset is almost 3 orders of magnitude large than any publically presented face dataset. Unnecessary to mention, building a dataset this massive is on the some distance facet the abilities of most worldwide analysis teams, considerably in academe. This paper has 2 goals. The most important one is to recommend a procedure to shape a pretty giant face dataset whilst requiring solely a limited extent of person-power for annotation. To the present vogue we have a tendency to advocate a way for assembling face records mistreatment facts sources supplied on the net. we have a tendency to use this manner to create a dataset with over 2 million faces, The 2nd aim is to lookup various CNN architectures for face identification and verification, collectively with exploring face alignment and metric learning, mistreatment the novel dataset for training. Several current works on face attention have planned different variants of CNN architectures for faces, and that we assess a quantity of these modelling decisions so as to filter what's indispensable from moot details.

The result might also be a lot of easier and on the other hand correctly accomplishing shut to revolutionary results on all widespread image and video face recognition

Face recognition may want to be a classical and representative laptop vision drawback, and a wide variety of face recognition techniques are projected inside the literature [2], [3],[4][27]. Generally, there are 2 necessary approaches for a good face recognition system: face illustration and face matching. Face illustration pursuits to extract discriminative function descriptors to structure face images/videos extra dissociable, and face matching is to style tremendous classifiers/models to differentiate extraordinary face samples[27]. Sensible face attention systems are from time to time struggling from quite a few versions like occlusions, poses, illuminations, expressions and resolutions that sometimes cause giant intra-class variations. Hence, a way to get sturdy face representations that are invariant and sturdy to a number of real-world variants is quintessential task in face awareness systems[27]. Existing face illustration approaches is mainly classified into 2 categories: holistic characteristic illustration [3], [4] and native characteristic illustration [2].

II. RELATED WORK

In this section, we generally discuss briefly about three related topics: 1) feature learning for face recognition and 2) binary code learning.

A. *Feature learning*

Representative characteristic getting to know techniques embody disbursed auto-encoders [5], convolutional neural networks [6], freelance topological house evaluation [8],[27] and reconstruction freelance section analysis [10][27]. Feature mastering has conjointly been with success utilized for face recognition. As an example, Cao et al. [9] bestowed a learning-based (LE) characteristic illustration approach through making use of the bag-of-word (BoW) framework. Hussain et al. [7][27] deliberate a region quanta sample (LQP) technique through modifying the LBP technique with a realized writing strategy. Lei et al. [11] deliberate a discriminated face descriptor (DFD) approach by using gaining knowledge of a photo filter victimization the LDA criterion to get LBP-like options. Sun et al. [13] planned a deep convolutional neural networks method to discover out face representations. Recently, Taigmanet. al. [12] brought a Deep Face method that analyze supervised face illustration with four,000,000 tagged face samples by using victimization the deep convolutional neural networks. Parkhiet. al. [14][27] bestowed A deep convolutional neural networks technique with the triplet loss perform, the place 2.6M tagged face images had been accustomed train the deep model. However, most of those strategies study real-valued face characteristic descriptors. For face recognition, binary picks rectangular measure extra sturdy to native modifications in face pictures as an end result of little variations brought on by means of various expressions and illuminations are often eradicated by means of quanta binary codes.

Revised Manuscript Received on April 25, 2019.

B. Konda Reddy, Ch. Nikhil, Computer Science Engineering, Koneru Lakshmaiah Education Foundation, Guntur, India.

Manoj Kolluri, Electronics and Computer Science Engineering, Koneru Lakshmaiah Educationl Foundation, Guntur, India.

K. Ruth Ramya, Venkata Naresh Mandhala, Department of Computer Science Engineering, Koneru Lakshmaiah Education Foundation, Guntur, India.

B. *Binary code learning*

Different varieties of computer code learning techniques are previously published in recent years [15], [16], [17][27]. For instance, Weiss et al. [17] planned a binary committal to writing gaining knowledge of strategy for photo search. Norouzi et al. [19] elevated it by using a triplet rating loss optimisation criterion. However, most existing laptop code mastering strategies region unit developed for climbable similarity search [15][27]. whereas binary preferences like LBP are utilized in face recognition, most of them are unit handsewn. There are some latest work that employs laptop code getting to know for face illustration and attention [18], [20], [21][27]. For instance, Zhang et al. [21] and Rastegariet al. [20][27] learned binary codes supported variants of the fisher criterion. However, these binary codes vicinity unit realized holistically and no longer in function level. a lot of recently, Lu et al. [18][27] introduced a compact binary feature descriptor (CBFD) that discovered binary face descriptors at the function level. However, CBFD carried out function and codebook getting to know one by one, in order that some beneficial information or codebook studying should additionally be compromised inside the finalisation stage[27].

III. BIOMETRICS

Client identifying proof is essential for securing knowledge from unlawful access. Human face conveys explicit temperament for everybody. It was absolutely seen that there's a vital distinction between one individual face to other individual's face. Afterwards, the discourse flag is what is more as same as human distinctive mark as appeared below figure to create a consumer recognizable proof framework, biometrics acknowledgment system is inevitable.

Biometrics face acknowledgment strategy automatically understands the discourse of a personal upheld the alternatives exists in his/her face flag. There are various accessible procedures of face recognition like hidden Markov model (Hmm), Eigen face technology etc., [15].

Network Architecture and training

This section is a description of the CNN method used in our experiments and their training. Inspired by way of [24],the networks are “very deep”, in the experience that they include a lengthy sequence of convolutional layers. Such CNN models have very these days executed present day performance in many such tasks as the Image-Net ILSVRC 2014 project [23], as nicely as in many different tasks [22,24].

Process of Learning a face classifier

Initially, the deep architectures f are bootstrapped by using thinking about the problem of recognizing

N = 2;622 unique individuals, setup as a N-ways classification problem. The CNN

associates to every education picture `t ; t = 1; : : : ;T a rating vector xt = Wf(`t)+b 2 RN by

means of a final fully-connected layer containing N linear predictors 2RN_D; b 2RN, one

per identity. After learning, the classifier layer (W;b) can be removed and the rating vectors f(`t) canbe used for face biometric authentication using the Euclidian distance to match them. However, the scores is extensively increased by means of standardization.

Learning a face embedding the usage of triplet

Triplet-loss teaching goals at getting to recognize rating vectors that operate appropriate in the ultimate application, i.e. identity verification via the use of comparing face descriptors in Euclidean space. This is related in spirit to “metric learning”, and, like many metric gaining expertise of approaches, is used to learn a projection that is at the identical time one-of-a-kind and compact, attaining spatiality discount at same time. Our triplet-loss coaching scheme is related in spirit to that of [1]. The output f(`t ) 2 RD of the CNN, pre-trained as defined in Section 4.1, is l2-normalised and projected to a L_D dimensional area the use of an affine projection xt =W0f(`t)=kf(`t)k2, W0 2 RL_D. While this aspects is comparable to the linear predictor realized above, there are two key differences. The first one is that L 6=D is no longer equal to the range of classification identities, however it is the (arbitrary) dimension of the descriptor embedding (we set L = 1; 024). The 2nd one is that the projectionW0 is skilled to minimize the empirical triplet loss

E(W0)=å(a;p;n)2Tmaxf0;

a□kxa□xnk22+kxa□xpk22g;

xi=W0f(`i)

kf(`i)k2(1)

Note that, differently from the previous section, there is no bias being discovered right here as the differences in (1) would cancel it. Here a _ 0 is a constant scalar representing a learning margin and T is a sequence of teaching triplets. A triplet (a; p;n) consists of an anchor face image a as properly as a exquisite p 6= a and terrible n examples of the anchor’s identity. TheprojectionW0 is realized on target datasets such as LFW and YTF honouring their guidelines.

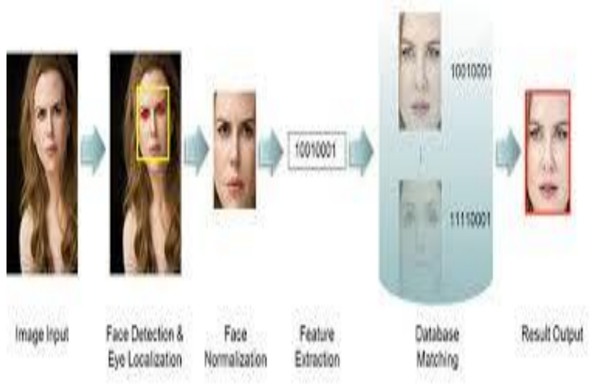

Figure1: The Human face Recognition System

IV. LITERATURE SURVEY

The methodology employed in this paper is native Binary Feature Learning. Algorithms are PCA and HMM. One of the simplest and most high-quality PCA employed in face consciousness systems is that the alleged Manfred Eigen face approach. This strategy transforms faces into a little set of integral characteristics, Manfred Eigen faces that are the foremost necessary factors of the preliminary set of gaining information of snap shots (training set). Recognition is performed by jutting a brand new image within the Manfred

Eigen face mathematical space, when that the character is categorized by approach of evaluating its position in Manfred Eigen face space which perform of famed people [25]. The advantage of this strategy over totally different face recognition structures is in its simplicity, speed and unfitness to tiny or gradual modifications on the face. The effort is affected to files which will be accustomed apprehend the face. Namely, the images should be vertical frontal views of human faces. the entire focus technique involves 2 steps: A. low-level formatting technique B. Recognition methodology The low-level formatting technique involves the subsequent operations: i. Acquire the initial set of face pictures referred to as coaching set. ii. Calculate the Manfred Eigen faces from the employment set, maintaining exclusively absolutely the best Eigenvalues. These M pictures define the face house. As new faces are fully fledged, the Manfred Eigen faces is updated or recalculated. iii. Calculate distribution during this M-dimensional house for every regarded man or girl by suggests that of jutting his or her face footage onto this face-space. The opposite methodology is HMM (Hidden Markov Models) which is a collection of applied math models accustomed represent the applied math homes of a sign. associate degree HMM may be a doubly framework with associate degree underlying framework that's now not noticeable, but is ascertained via the other set of random ways that turn out a sequence of situated symbols. Associate degree HMM contains a finite set of states, each of that is said with a flat probability distribution; transitions between these states ar ruled by suggests that of a collection of possibilities. Hidden Andrei Markov Models are specifically famed for his or her package in 1D sample awareness like speech recognition, musical rating analysis, and sequencing issues in bioinformatics. additional recently they need been applied to additional complicated second issues and this appraise focuses on their use within the space of automatic face recognition, observance the evolution of the employment of Hidden Andrei Markov model from the early-1990’s to the present day

V. PROPOSED SYSTEM

We have to give training to the machine in number of situations of authenticated user face such as face with colourful background, face without background, face in lightning condition and face in dim light condition etc. After the training of machine the machine is now capable enough to recognize authenticated user face in any situation and then generate key for the user face which acts as key to decrypt the encrypted cloud data which was encryptedusing the encryption algorithm.After encryption send the encrypted file to cloud storage and when ever if the user tries to access it then he have to use the face as password and the face password is compared with the password which was fixed earlier and after matching of the password the face is used as a decryption key for encrypting the file to get access.In this way we are providing security to the data file stored in cloud.If the unauthorised user tries to access the file then at verifying the password there is dissimilarities in features of unauthorised user and hence the file is not accessed. The results are given in the below graph. There is training accuracy, validation accuracy, training loss and validation loss are represented and in that graphs the red line represents the validation and blue line represents training.

Resnet-50 may be a convolutional neural network that's trained on over 1,000,000 pictures from the Image Net info. The network is fifty layers deep and might classify pictures into a thousand object classes, like keyboard, mouse, pencil, and plenty of animals. As a result, the network has learned wealthy feature representations for a good vary of pictures. We used this Resnet50 architecture in our model and we build the model with fine tuning and transfer learning methodology. We created a sequential model and we created some layers to the neural network. The layers are to perform flip, normalisation, zoom and add some blur to the pictures which were captured. These layers are used to train the neural network. The layers used for test and validation are normalization and zoom layers. In this way we will train the vgg16 neural network and after that test and validate the users whether they are authenticated or not. If the user is not authenticated then the user will not get accessed to the file and thus we provide security to the file using face recognition as a key feature. The steps involved in this model is better explained with the block diagram as mentioned below

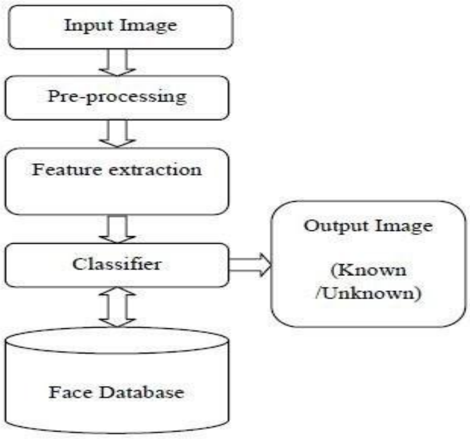

Figure2: Face detection and classification

The algorithm for the model generated by us is as follows

Algorithm:

```
1. Start
2. Create directories Test, Train, Validation folders in Model directory and create a duplicate of model directory as dummy directory with same folders
3. Camera is capturing the pictures as
For I in range(100):
Iq=0
Return_value,image=camera.read()
Cv2.imwrite('dummy/train/'+a+'/'+str(i)+'.png', image)
Facechop('dummy/train/'+a+'/'+str(i)+'.png',iq)
4. The face chop will chop the face and writhe those chopped images in to model directory of trained folder
5. For I in range(15):
Iq=0
```

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Return_value,image=camera.read()
Cv2.imwrite('dummy/test/'+a+'/'+str(i)+'.png', image)
Facechop('dummy/test/'+a+'/'+str(i)+'.png',iq)
The face chop will chop the images of test folder in dummy directory and write those images to test folder of model directory

6. For I in range(15):
Iq=0
Return_value,image=camera.read()
Cv2.imwrite('dummy/validation/'+a+'/'+str(i)+'.png', image)
Facechop('dummy/validation/'+a+'/'+str(i)+'.png',iq)
The face chop will chop the images of validation folder in dummy directory and write those images to validation folder of model directory

7. Train the model with the captured photos using vgg16 neural network with hidden layers flat, dense on the photos

8. The more the training the more will be the accuracy and after training save the trained model

9. Check the model whether it is correctly working or not by giving authenticated face if yes then it will encrypt the file and this file is stored in cloud and the user need to download the file and give authentication of his face to access the content of the file by decrypting it

10. The authentication will fail if other face is given as input and the file is not accessed to that user

VI. Results

The training is done for the model and we will save that model and this model is used during validation process. We will generate the graph which will show the training accuracy and validation accuracy and while training there will be some triplet loss and that will be shown in another graph which shows training loss and validation loss. We have to give at least hundred photos for training to the model and we have to run at least thirty epochs to get the output accurately. We used tensor flow, Keras and Opencv libraries in python and we used a vgg16 neural network to create a model.

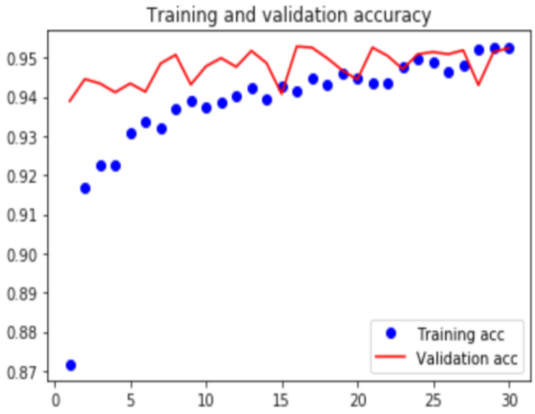

Figure3: Training and validation accuracy

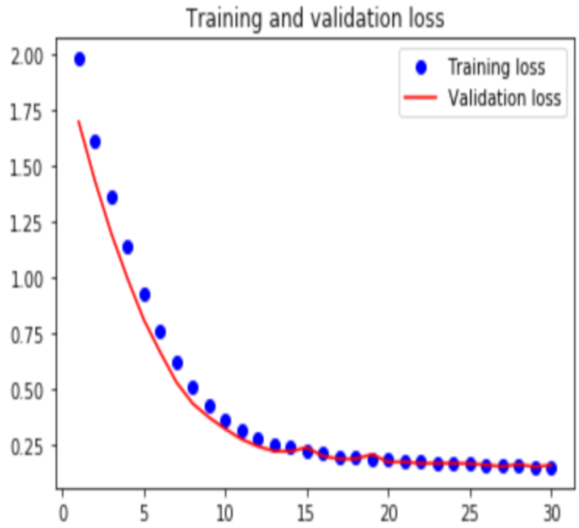

Figure4: Training and validation loss.

VII. RESULTS & COMPARISON WITH OTHER BIOMETRIC SYSTEMS

SN o.	Features	Security Perspective	Developed, utilized or proposed methods	Success rate	Data set

1	Face / Palm-print	Propose a one of a kind cancellable biometric format age formula using Gaussian	Randomized vectors and the single direction of modulus hashing Gaussian irregular	vector/PCA/ LDA average confront eer for pca 0.05 %/Normal face eer for lda 0.03 % /average palm print eer for lda 0.2 %/normal palm print eer for lda 0.05 %	orl/yale/indian face/ polyu/casia
2	Face	Presentation of another method to secure the face biometrics amid acknowledgment, utilizing the purported cancellable biometric	2dpcA	The enhanced exactness to 3 % from the first data	oRl
3	Face	Present the novel of biometric assurance strategy to produce secure facial biometric formats utilized in factual based acknowledgment algorithms	2dpcA	recognized exactness 3 % and 4.5 % over the first and other changed data	oRl
4	Fingerprint	Proposed the novel of a paired length-settled component age strategy for fingerprint	bcH / reed–solomon/ ldpc	4.58 % zero far	FvC2002 db2
5	Fingerprint	The spotlight is on the biometric cryptosystem execution and the assessment depends on the quantity of unique mark surface descriptors	Gabor filter/ Lbp	eer of the unique finger impression descriptors for the finger code, lbpP8, lbP16, lbp24, bBPu2, lbpr, and ldp are 10.96 %, 22.79 %, 19.54 %, 24.6 %, 22.88 %, 29.56 %, what's more, 15.95 %, respectively	FvC2000 db2a
6	iris	The identification of the printed-iris assaults/oppose assaults dependent on the superb printing	svm / LbP / direct kernel / gabor / so-bel Filter	fgr 2.25 / FfR 0.25 / Hter 1.25	miche database / mobio-counterfeit Database
7	mouse dynamics	The examination of the biometric confirmation framework Under the different diverse examination strategies /test static versus dynamic trust models	svm / AnN / multi classifier fusion (mcf) / libSvm	FMR 0.37 % / FNMR 1.12 %	their framework depend on the information of 28 clients centring on the diverse mouse occasions
8	Face/finger print/ Iris	The proposed calculation ceaselessly refreshes the choice procedure utilizing on the web learning	fusion algorithms	FAR 0.01 %	wvu / lea

9	Face	The suggestion of a computational way to deal with the human ID dependent on the reconciliation of face and body related delicate biometric trait	Svm / Gaussian kernel / Sum / Bayesian / fuzzy logic	The distinguishing proof rate is 88 %	orlAt&t/ yale/ mUcT
10	Iris	The spotlight is on the acknowledgment, and leave the identification and highlight extraction issues in the background	ANN / Svm	The frr normal esteem is 19.80 %	casia-iris V1 database
11	Fingerprint	The Deficient execution of biometric systems for the interest of the strength and high exactness/biometric confirmation frameworks are solid in perfect situations yet can be exceptionally touchy to genuine ecological conditions	Svm/ rsvm	eer 0.13 %	fvc2006 datasets
12	Teeth	The procedure of acknowledgment exactness and to diminish the computational complexity	PCA/ LDA / Ehmm	The fdr and frr blunder rate of 8.85 %	database Comprising Of teeth pictures
13	Handwriting/ Gender/ Age	To build up the hearty forecast of the essayist's sexual orientation, age extend and handedness	svm / gmm / fuzzy / SFI	fuzzy 81.77 % gmm 69.75 % / Svm 100 % / SFI 85.18 %	IAM-1 / IAM-2 / KHATT
14	Face/teeth/ voice	To propose the upgraded multimodal individual validation framework for the cell phone security/Breaker data got from face, teeth and voice modalities to enhance performance	ehmm / 2D-dcT / MFCC / gmm / Knn / Lda	The Eer for face-teeth 2.75 % / face-voice 3.31 % / teeth-voice 4.22 % / face 5.09 %/ teeth 7.75 % / voice 8.89 %	The 1000 of biometric characteristics for database collected via a smart-phone /20 biometric traits per 50 persons
15	Face/speak	The Examination procedure of the application for existing face and speaker ID strategies to an individual recognizable proof assignment on a handheld device.	asr / Svm	The err for face 6.57% / Speak 1.54 % / fused 0.64 %	The confront and the voice information from the 35 unique individuals, and 100 of pictures and 64 discourse tests

VIII. CONCLUSION

This paper fixated on the protection problems with immense learning considered the affordable usage in Cloud computing. The task is finished with a face acknowledgment utilizing key as a security for cryptography and unscrambling of the data. The voice acknowledgment info is place away within the cloud. Therefore by death penalty this procedure the unapproved individual cannot get to or modify the data. With the goal that the safety is high.

IX. FUTURE IMPROVEMENTS

It is obvious that the results of this face recognition system are nice however there's scope for future improvement. Because of time constraints we tend to tend to weren't able to implement some objectives that got to have created the analysis work a far higher proposition. The most improvement can pursue the performances, acknowledges the time period face recognition [13]. I'd prefer to improve my code for face image recognition in addition as close up the code so as to boost performance. "In future to spice up the correction, quality based totally frame alternative, aging correction, and mark based totally matching techniques area unit typically combined to form a unified system for video based".

REFERENCES

1. Fredrik, E., Peter, B.: Results and presentation of the ENFSI-DIWG 2013 facial image comparisons proficiency test. SKL Intern rapport. Document-ochin formation stekniken het en2014:08.http://media.forensicscience.eu/2014/05/FIC-test-20131.pdf
2. T. Ahonen, A. Hadid, and M. Pietikainen. Face description with local binary patterns: Application to face recognition. TPAMI, 28(12):2037–2041, 2006.
3. P. N. Belhumeur, J. Hespanha, and D. J. Kriegman. Eigenfaces vs. fisherfaces: recognition using class specific linear projection. TPAMI, 19(7):711–720, 1997.
4. M. Turk and A. Pentland. Eigenfaces for recognition. Journal ofCognitive Neuroscience, 3(1):71–86, 1991.
5. Y. Bengio, P. Lamblin, D. Popovici, and H. Larochelle. Greedy layer-wise training of deep networks. In NIPS, pages 153–160, 2007.
6. G. B. Huang, H. Lee, and E. G. Learned-Miller. Learning hierar-chical representations for face verification with convolutional deep belief networks. In CVPR, pages 2518–2525, 2012.
7. S. U. Hussain, T. Napoleon,´ F. Jurie, et al. Face recognition using local quantized patterns. In BMVC, pages 1–12, 2012.
8. A. Hyvarinen,¨ J. Hurri, and P. O. Hoyer. Independent component analysis. Natural Image Statistics, pages 151–175, 2009.
9. Z. Cao, Q. Yin, X. Tang, and J. Sun. Face recognition with learning-based descriptor. In CVPR, pages 2707–2714, 2010.
10. Q. V. Le, A. Karpenko, J. Ngiam, and A. Y. Ng. ICA with reconstruction cost for efficient overcomplete feature learning. In NIPS, pages 1017–1025, 2011.
11. Z. Lei, M. Pietikainen, and S. Z. Li. Learning discriminant face descriptor. TPAMI, 6(4):1275–1286, 2013.
12. Y. Taigman, M. Yang, M. Ranzato, and L. Wolf. Deepface: Closing the gap to human-level performance in face verification. In CVPR, pages 1–8, 2014.
13. Y. Sun, X. Wang, and X. Tang. Deep learning face representation from predicting 10,000 classes. In CVPR, pages 1891–1898, 2014.
14. O. M. Parkhi, A. Vedaldi, and A. Zisserman. Deep face recognition. In BMVC, pages 1–12, 2015.
15. Y. Gong and S. Lazebnik. Iterative quantization: A procrustean approach to learning binary codes. In CVPR, pages 817–824, 2011.
16. J. Wang, S. Kumar, and S.-F. Chang. Semi-supervised hashing for scalable image retrieval. In CVPR, pages 3424–3431, 2010.
17. Y. Weiss, A. Torralba, and R. Fergus. Spectral hashing. In NIPS, pages 1753–1760, 2008.
18. J. Lu, V. E. Liong, X. Zhou, and J. Zhou. Learning compact binary face descriptor for face recognition. TPAMI, 37(10):2041–2056, 2015.
19. M. Norouzi, D. Fleet, and R. Salakhutdinov. Hamming distance metric learning. In NIPS, pages 1070–1078, 2012.
20. M. Rastegari, A. Farhadi, and D. Forsyth. Attribute discovery via predictable discriminative binary codes. In ECCV, pages 876–889, 2012.
21. Zhang, J. R. Beveridge, Q. Mo, B. A. Draper, and P. J. Phillips. Randomized intraclass-distance minimizing binary codes for face recognition. In IJCB, pages 1–8, 2014.
22. R. Beveridge, H. Zhang, P. J. Flynn, Y. Lee, V. E. Liong, J. Lu,deAssisAngeloni, T. de Freitas Pereira, H. Li, G. Hua, et al. The ijcb 2014 pasc video face and person recognition competition. In IJCB, pages 1–8, 2014.
23. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, S. Huang, A. Karpathy, A. Khosla, M. Bernstein, A.C. Berg, and F.F. Li. Imagenet large scale visual recognition challenge. IJCV, 2015
24. Simonyan and A. Zisserman. Very deep convolutional networks for large-scale image recognition. In International Conference on Learning Representations, 2015.
25. A.W., Bolle, R.M.: Face recognition and its application. In: Zhang, D. (ed.) Biometric Solutions. The Springer International Series in Engineering and Computer Science, vol. 697,pp. 83–97. Springer, Boston (2002). 10.1007/978-1-4615-1053-6_4.
26. zhenyu Guan, Liangxu Bian, Tao Shang, Jianwei Liu, "When Machine Learning meets Security Issues: A survey", Intelligence and Safety for Robotics (ISR) 2018 IEEE International Conference on, pp. 158-165, 2018.
27. Jiwen Lu,Venice Erin Liong,Jie Zhou."Simultaneous local binary feature learning and encoding for homogenious and heterogenious face recognition",IEEE Transaction on pattern analysis and machine intelligence,2017(Volume:40,Issue:8)

AUTHORS PROFILE

Konda Reddy Battula is a Research Scholar in the department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India. He is currently Student in the department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India. Her research interests are Biometrics, Network Security and Wireless Sensor Networks. Email: itskonda11@gmail.com

Ruth Ramya Kalangi is a Research Scholar in the department of Computer Science and Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India. She is currently Assistant Professor in the department of Computer Science and Engineering, KoneruLakshmaiah Education Foundation, Guntur, Andhra Pradesh, India. Her research interests are Biometrics, Network Security and Wireless Sensor Networks. Email: ramya_cse@kluniversity.in

.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication