Writer Independent Manipuri Offline Signature Verification using Transfer Learning Technique of Convolutional Neural Network

Teressa Longjam, Dakshina Ranjan Kisku

Abstract: Automatic Signature Verification system is used to verify whether a signature is genuine or forged. Forged Signatures are those signatures that a person produced by imitating the signature of another person. Automatic Signature Verification is very important as a person's handwritten signature is used everywhere to authenticate themselves and there is not very much difference between a genuine signature and the imitation of it, i.e. a forged signature. In this work, signature verification is done using different pre-trained Convolutional Neural Networks (CNNs). Convolutional Neural Network has powerful learning ability, and it can be used to distinguish between a genuine and a forged signature automatically. In this experiment, Manipuri signature dataset was used, the dataset was prepared originally and it contains 729 genuine signatures and 243 forged signatures. Features were extracted from pre-trained networks and classification was done using binary Support Vector Machine (SVM) classifier and the performances of the networks were compared. And according to the experiment we achieved a classification accuracy of 84.7 using VGG19 features, accuracy of 86.8 using VGG16 features and accuracy of 81.9 using Alexnet features.

Keywords: Forged signatures, Genuine Signatures, Transfer learning, Writer independent signature verification.

I. INTRODUCTION

Handwritten signatures are the most widely used biometric trait to authenticate the identity of a person. It is used to authenticate documents in many places such as places where financial, legal and commercial works are done. Because of these reasons the verification of a signature becomes very important in order to detect whether a signature is genuine or forged. Forged signatures are mainly produced to do some illegal activities and there are human experts who verified whether a written signature is genuine or forged. The manual way to verify whether a signature is genuine or not is time-consuming, so researchers are trying to automate the process by using many techniques. Machine learning and many other pattern recognition and classification techniques are used for verifying a genuine signature.

Some of the previous works are based on only simulated forgery [1], [2] and some are based on simulated forgery with the other two types of forgery called simple forgery and random forgery. Simulated forgery is the forgery done by imitating the genuine signature. A simulated forged signature is almost similar to the genuine signature in shape, size, and style. In the work done by L.G. Hafemann et.al. [1], they propose different formulation of feature learning for offline writer independent signature verification, they were able to propose a system which was able to perform verification for even unseen users. Another similar work was done by S. Dey et.al. [2], they did not use any feature set for classifying genuine and forged signature but they propose a writer independent Siamese CNN for classification of genuine and forged signatures. A simple forgery is done without having any knowledge about the genuine signature. The forger knows the name of the person but never shows his/her signature, so he/she just writes the name of the person in free hand in his/her own style then the forgery is a simple forgery. Random forgery is the simplest, here the forger knows nothing, he/she write randomly anything and say it is a signature of a person then it is a random forgery. Verification of simple and random forgery is fully writer dependent, i.e. the pattern matching and verification is done depending on the person to which the signature belongs. While verification of simulated forgery can be done based on writer or completely independent to the writer. If writer independent approach is used then the system should be able to distinguish between the features of a genuine signature and the signature written by imitating the genuine signature. Structural features cannot be used in this case because genuine and simulated forgeries are almost similar structurally. D. Bertolini et.al. [3], used graphometric feature set to distinguish between genuine and forged signature and an ensemble of classifiers were used for the classification purpose. In their work, genuine and random forgeries were used to search for best-fit classifiers using genetic algorithm and they used simulated and simple forgery for optimizing the classifier set.

In writer dependent signature verification system [4], [5], [6], for each person registered there is one system that will classify whether the signature belongs to the person (Genuine) or not (Forged). And for the writer independent

* Correspondence Author
Teressa Longjam*, Computer Science and Engineering Department, National Institute of Technology Manipur, Imphal, India. Email: teressalongjam@gmail.com
Dakshina Ranjan Kisku, Computer Science and Engineering Department, National Institute of Technology Durgapur, Durgapur, India. Email: drkisku@cse.nitdgp.ac.in

signature verification system, only one system is used to classify whether a signature is genuine or forged (simulated forged). Comparing to writer dependent signature verification system, writer independent signature verification system is more suitable to real-life scenarios. In the work done by D.R. Kisku et. al. [6] and T. Longjam et.al. [4], a set of local and global features were extracted and the extracted features for each user were used to train a classifier. So in these works, for every user there was a system that classifies whether a signature is genuine or forged. In another work done by M.A. Ismail et. al. [5], signature recognition system was proposed using local and global features. In their work, the system finds out the writer in their database to which the input sample signature belongs.

In this work, Manipuri handwritten writer independent signature verification is done using Convolutional Neural Networks. Manipuri is a language spoken mainly by Manipuri, a group of people who lives in Manipur and in some parts of Myanmar and Bangladesh. The script used to write the Manipuri language is called Meitei Mayek [7]. Genuine signatures written using Meitei Mayek script are collected from 81 individuals and another set of signatures, forged signatures, are also collected. By using the genuine signatures volunteers were instructed to imitate, to get the set of forged signatures. Alexnet, VGG16, and VGG19 were used to conduct the experiments. The pre-trained networks were used to extract features of the collected signatures and later used for the classification purpose. The block diagram of the proposed work is shown in Fig. 1.
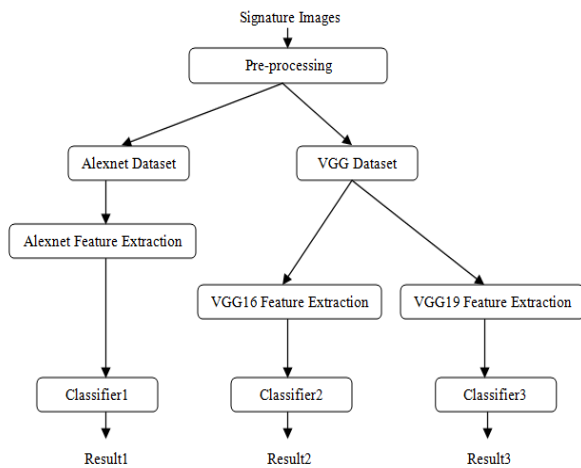

Fig. 1. Block diagram of the proposed work.

II. DATASET

A signature collecting template is used to collect the signatures. The template consists of 9 boxes, so from each person 9 genuine signatures were collected. From 81 individuals, signatures were collected, so all together we collected 729 genuine signatures. The same template was used for collecting the second set of signatures, i.e. forged signatures. For each person 3 simulated forged signatures were collected from volunteers, so altogether we collected 243 forged signatures. Our dataset consists of two classes of signatures, 729 signatures belong to the genuine class and

the other remaining 243 belong to the forged class.

III. PREPROCESSING

Collected signature templates are scan using a scanner with dpi 300 in order to convert it to digital images. A sample signature collecting template is shown in Fig. 2. Signatures collecting template contains 9 boxes, so the first step of pre-processing is to crop a scanned image to get 9 images, 1 image for each box. After getting 9 images, each image is again cropped to get an image containing only the area of interest, i.e. the signature part. Fig. 3. shows a signature image showing only area of interest.

The median filtering algorithm is then applied to all the cropped images to remove noise. And at last the images are normalized according to the pre-trained networks. That is for Alexnet the images are normalized to 227X227 and for VGG the images are normalized to 224X224, such that we have 2 databases of Manipuri signatures (Genuine and Forged), one for Alexnet and another for VGG.
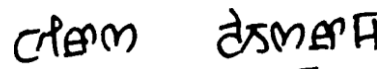

Fig. 2. Signature collecting template.

Fig. 3. A Meitei mayek signature.

IV. CLASSIFICATION USING TRANSFER LEARNING

Transfer learning is a process where a pre-trained CNN is used to extract features of images to be classified and the extracted features are used to train another classifier. In this work three networks, pre-trained Alexnet, VGG16, and VGG19, are used to extract features from the images and SVM classifier is used for the classification purpose.

A. Feature extraction using Alexnet

Alexnet is a CNN proposed by Alex K. et. al. [8] and won ImageNet LSVRC 2012 competition. The network has eight layers, five convolution layers and after that three fully connected layers. Every convolutional and every fully connected layer is followed by one activation layer. Other layers are normalization and drop out.

Signature images from the Alexnet dataset are fed into the pre-trained network and the output of the seventh layer is extracted and it becomes the features of the images.

B. Feature extraction using VGG16

The size of the input image of VGG16 is 224X224, so for VGG16, we used the VGG dataset. The network was proposed by K. Simonyan et.al. [9]. The network consists of twelve convolution layers and

four fully connected layers. All the layers work with activation function ReLU. At first after every two convolutional layers there is max pooling. But for the last six convolutional layers, after every three convolutional layers there is max pooling.

The output of the last second fully connected layer is used as the features of the signature images.

C. Feature extraction using VGG19

VGG19 was proposed by K. Simonyan et.al. [9]. The network consists of nineteen layers, sixteen convolutional layers, and three fully-connected layers. At the starting of the network, after two convolutional layers there is a max-pooling and then again after two convolutional layers there is another max pooling. And at the end after every four convolutional layers there is max pooling.

The signature images of the VGG dataset are fed into the network and the output of the last second fully connected layer was extracted as the features of the images.

D. Classification using SVM

For classification, both the two datasets are split into training data and testing data. 70% of the dataset was used for training and the remaining for testing.

Three SVM classifiers [10] were trained using features extracted by Alexnet, VGG16, and VGG19 respectively. After training the classifiers, they are used for classification. During the classification process the classifier classifies whether the input test signature image is a genuine signature or a forged signature.

V. RESULT AND DISCUSSION

The performances of the classifiers are given in terms of the classification accuracy, false acceptance rate (FAR) and false rejection rate (FRR). Accuracy of a classifier is defined as the ratio of number of true classification to the total number of test signatures, FAR is the rate of falsely accepted forged signatures and FRR is the rate of falsely rejected genuine signatures.

The classifier that uses Alexnet features provides an accuracy of 81.9, FAR of 30 and FRR of 13.9. Using VGG16 we get an accuracy of 86.8, FAR of 38 and FRR of 4.6. And lastly by using VGG19 we get an accuracy of 84.7, FAR of 20 and FRR of 13.The performances of the classifiers are shown in Table 1 and Figures 4, 5 and 6.

Table- I: Table showing performances of the three classifiers.

CNN used for feature extraction	Accuracy	FAR	FRR
Alexnet	81.9	30	13.9
VGG16	86.8	38	4.6
VGG19	84.7	20	13

From the above result, we can see that the accuracies of all three classifiers when using different features are almost the same. But there is a huge difference between FAR and FRR when we used features extracted from VGG16. It is because the features are able to well describe the pattern of genuine signatures but not able to distinguish a forged signature from a genuine one. If we see FAR of all classifiers, VGG19 features gave us the best result. And if we see FRR, then VGG16 features are way better than the other two types of features.
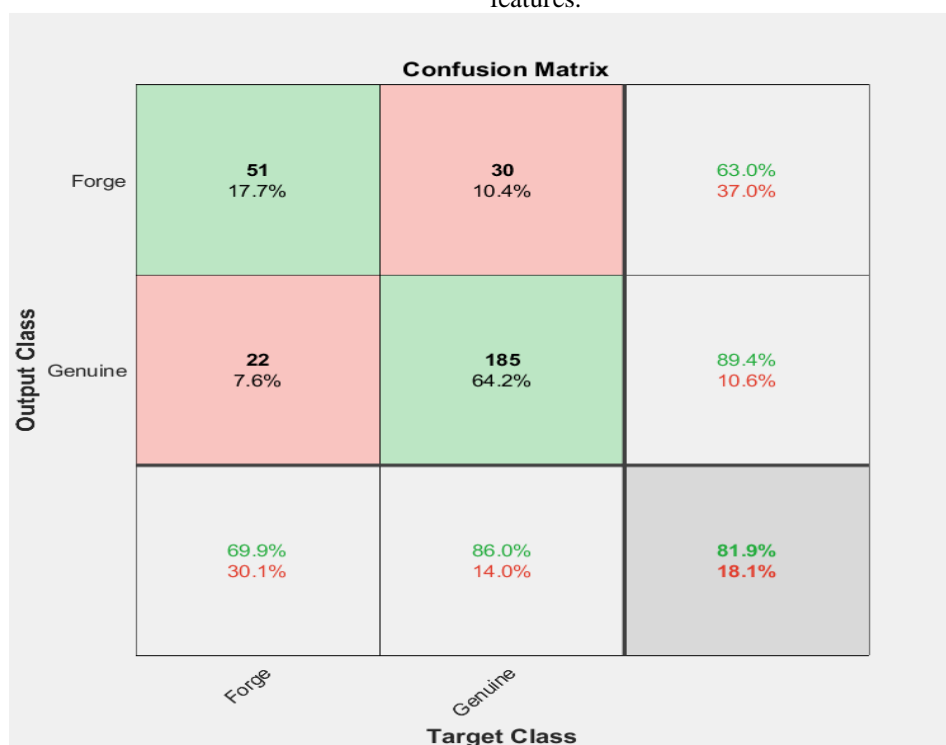

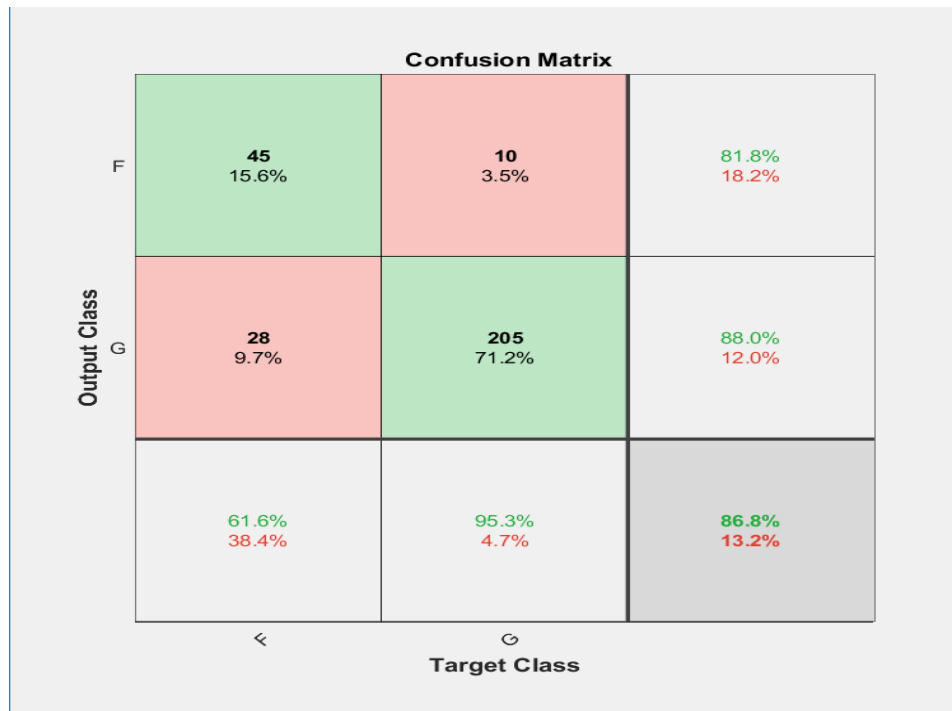Fig. 4. Confusion matrix for classification result obtained by using Alexnet features.

Fig. 5. Confusion matrix for classification result obtained by using VGG16 features.
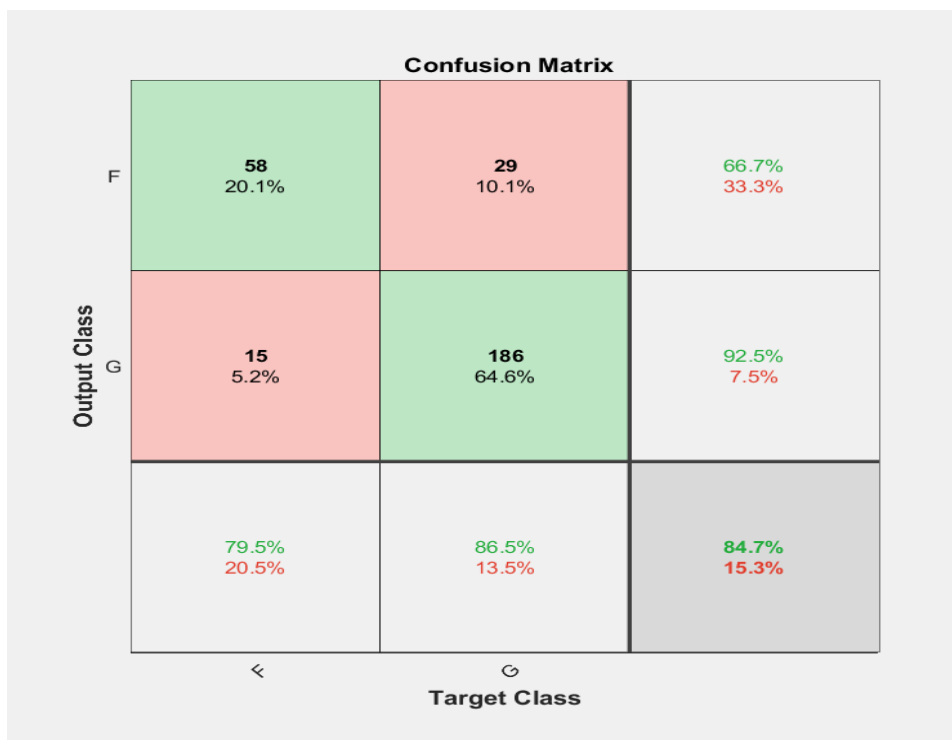

Fig. 6. Confusion matrix for classification result obtained by using VGG19 features.

VI. CONCLUSION

In this work, three offline signature verification systems are proposed and compared. The first system is based on features extracted from Alexnet, the next system is based on features extracted by using VGG16 and the last one is based on features extracted by using VGG19.

Three SVM classifiers were trained using three sets of features extracted from Alexnet, VGG16 and VGG19 respectively and all of them provide a good results. For this work handwritten Manipuri signatures, both genuine and forged, were used. Genuine signatures were collected from

81 individuals and forged signatures were collected from volunteers.

REFERENCES

1. L. G. Hafemann, R. Sabourin, L. S. Oliveira, "Learning Features for Offline Handwritten Signature Verification using Deep Convolutional Neural Networks", Pattern Recognition 70 (2017) 163–176.
2. Sounak Dey, Anjan Dutta, J. Ignacio Toledo, Suman K.Ghosh, Josep Llad´os, Umapada Pal, "SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification", Pattern Recognition Letters, September, 2017.

3. D. Bertolini, L.S. Oliveira, E. Justino, R. Sabourin, "Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers", Pattern Recognition 43 (2010) pp 387 – 396, Vol 43, No. 1.
4. T. Longjam, D.R. Kisku, "A Supervised Manipuri Offline Signature Verification System with Global and Local Features", 7th International Symposium on Embedded computing and system Design, 2017.
5. M. A. Ismail and Samia Gad, "Off-line Arabic signature recognition and verification", Pattern Recognition, Vol. 33, pp. 1727 – 1740 (2000).
6. D. R. Kisku, A. Rattani, P. Gupta, "A Novel Approach to Offline Signature Verification using Gaussian Empirical Rule", 6th European Conference on Information Warfare and Security (ECIW 2007), Swindon, U.K., pp. 139--150, 2007.
7. Neelakash Kshetrimayum, "A comparative study of Meetei Mayek", Conference on Typography day 2011, India.
8. Alex Krizhevsky, Ilya Sutskever, Geoffrey E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks", ImageNet Large Scale Visual Recognition Challenge, 2012.
9. Karen Simonyan, Andrew Zisserman, "Very Deep Convolutional Networks for Large-scale image recognition", ICLR 2015.
10. C. Cortes and V. Vapnik, "Support-vector networks", Machine Learning, Vol. 20, No. 3, pp. 273–297.

AUTHORS PROFILE

Teressa Longjam is currently working as a Lecturer in the Department of Computer Science and Engineering at National Institute of Technology Manipur, India. She received Bachelor of Engineering degree in Computer Science and Engineering from Manipur University, Manipur, India, in 2010, Master of Technology, in Computer Science and Engineering from Rajasthan Technical University, India, in 2013 and pursuing PhD as a part-time scholar in Computer Science and Engineering at National Institute of Technology Durgapur, India.

Dakshina Ranjan Kisku is currently an Associate Professor in the Department of Computer Science and Engineering at National Institute of Technology Durgapur, India. He obtained his B.E., M.E., and Ph.D. in Computer Science and Engineering from Jadavpur University, India. His research interests include Computer Vision, Image Processing, Biometrics, Machine Learning, Affective Computing, and Pattern Classification. He was a Researcher in the Computer Vision Laboratory at the University of Sassari, Italy from March 2006 to March 2007 and worked as a Research Associate at Indian Institute of Technology Kanpur, India from 2005 to 2006. He worked as a faculty member for several years at reputed engineering colleges in India. He has published more than 80 articles in peer-reviewed journals and conferences. He has authored and edited 12 books and book chapters on biometrics and homeland security and published one news article on healthcare biometrics. He is a recipient of the IEI Young Engineers Award, Outstanding Scientist Award, Outstanding Reviewer Award, Visvesvaraya Young Faculty Research Fellowship, MIUR Fellowship, etc. He is a Senior Member of IEEE (USA) and Fellow of the Royal Society for Public Health, UK. Besides, he regularly serves as an editorial member for several journals and reviewer for many refereed journals, conferences and edited books.