International Journal of Engineering Research and Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 2, April - 2012

Persian Signature Verification using Convolutional Neural Networks

Hurieh Khalajzadeh
Intelligent Systems Laboratory (ISLAB), Faculty of Electrical & Computer Engineering
K.N. Toosi University of Technology, Tehran, Iran
h_khalajzadeh@ee.kntu.ac.ir

Mohammad Mansouri
Intelligent Systems Laboratory (ISLAB), Faculty of Electrical & Computer Engineering
K.N. Toosi University of Technology, Tehran, Iran
mohammad.mansouri@ee.kntu.ac.ir

Mohammad Teshnehlab
Intelligent Systems Laboratory (ISLAB), Faculty of Electrical & Computer Engineering
K.N. Toosi University of Technology, Tehran, Iran
teshnehlab@eetd.kntu.ac.ir

Abstract

The style of people's handwritten signature is a biometric feature used in person authentication. In this paper, an offline signature verification scheme based on Convolutional Neural Network (CNN) is proposed. CNN focuses on the problems of feature extraction without prior knowledge on the data. The classification task is performed by Multilayer perceptron network (MLP). This method is not only capable of extracting features relevant to a given signature, but also robust with regard to signature location changes and scale variations when compared to classical methods. The proposed method is evaluated on a dataset of Persian signatures gathered originally from 22 people. The simulation results reveal the efficiency of the suggested algorithm.

1. Introduction

There is an increasing interest in trustworthy identity verification. Biometric authentication is as more trustable alternative to password based security systems. This method is gaining popularity as it is relatively hard to be forgotten, stolen, or guessed. Several biometric features have been studied and proved useful, including biological characteristics such as fingerprint, face, iris, and retina pattern or behavioral traits such as signature and speech. In compare with conventional methods of identification such as employing PIN-codes, passwords, magnet, or smart cards; biometric characteristics offer several advantages which are listed here. They are significant for each individual, are always available, cannot be transferred to another person, cannot be forgotten or stolen and are always variable. However, because most biological characteristics are unchangeable, a more serious problem occurs when they are copied. So, one will hesitate to use the disclosed biological features [1, 2].

Signature verification is an active research area in the field of pattern recognition due to its usability in many areas associated with security and access control. Signature authentication is low cost biometric system where awareness and uniqueness of person is necessary [2, 3]. There are two main research fields in this area: signature recognition (or identification) and signature verification. The signature recognition problem consists on identifying the author of a signature. In this problem a signature database is searched to find the identity of a given signer. This task is different from signature verification. Verification defines the process of testing a signature to decide whether a particular signature truly belongs to a person or not. In this case, the output is either accepting the signature as valid or rejecting it as a forgery. Automatic signature verification is a well-known and very active research field with important applications. Different techniques have already been applied in signature verification such as fuzzy logic [4], geometric features [5, 6], global characteristics [7], genetic algorithms [8], neural networks [9-11] and hidden Markov models [12]. In comparison, the signature recognition problem is more complex than the signature verification problem. So, rather little research effort has been focused on automatic signature recognition [13].

Depending on the data acquisition method and involved application, existing signature verification systems are generally classified either online or offline approaches. In general, online signature verification systems present a better performance than the offline signatures verification systems. In the online approach the system uses not only the signature but also the dynamic information obtained during the signing process. However, online signature verification system necessitates the presence of the signer at both time of obtaining the reference signature and the verification process which is not welcome by many applications. Thus offline verification methods have more practical application areas than that of the online signature verification methods. The offline approach only uses the digitalized image of a signature extracted from a document called static information. So it does not require any special processing devices. But preprocessing is more difficult and time consuming in offline systems due to unavailability of the dynamic information. Developing an efficient and accurate offline signature verification system is a challenging task as signatures are sensitive to geometric transformations, interpersonal signature collected in course of time, complex background of the signature, skilled forgery, non availability of time taken to sign, lack of sufficient signatures samples for training the system, noise introduced by scanning device, difference in pen width, ink pattern and etc [14].

Convolutional neural networks are feed-forward networks with the ability of extracting topological properties from the input image without any preprocessing needed. Therefore, CNNs could be useful to overcome the preprocessing problems of offline signature verification task. This paper presents an offline signature verification system using a CNN for extracting the features and a MLP for classification of its extracted features. Proposed system is tested on 176 Persian signatures gathered from 22 people. The simulation results expose the prosperity of using CNNs in the task of offline signature verification.

The rest of the paper is organized as follows. Section 2 presents an introduction to CNNs. Section 3 discusses the proposed CNN-based signature verification system. Section 4 is about the dataset which is used in experiments. Section 5 summarizes the experiments and results. Finally, in Section 6 conclusive remarks are resumed.

2. Convolutional Neural Networks

Yann LeCun and Yoshua Bengio introduced the concept of CNNs in 1995. A convolutional neural network is a feed-forward network with the ability of extracting topological properties from the input image. It extracts features from the raw image and then a classifier classifies extracted features. CNNs are invariance to distortions and simple geometric transformations like translation, scaling, rotation and squeezing.

Convolutional Neural Networks combine three architectural ideas to ensure some degree of shift, scale, and distortion invariance: local receptive fields, shared weights, and spatial or temporal sub-sampling [15]. The system is usually trained like a standard neural network by back propagation. CNN layers are an alternation of convolutional layers and subsampling layers. A convolutional layer is used to extract features from local receptive fields. It is organized in planes of neurons called feature maps. In a network with a 5×5 convolution kernel each unit has 25 inputs connected to a 5×5 area in the previous layer, which is the local receptive field. A trainable weight is assigned to each connection, but all units of one feature map share the same weights. This feature which allows reducing the number of trainable parameters is called weight sharing technique and is applied in all CNN layers. LeNet5 [15], a fundamental model of CNNs proposed by LeCun, has only 60,000 trainable parameters out of 345,308 connections. In order to extract different types of local features, a convolutional layer is composed of several feature maps. A reduction of the resolution of the feature maps is performed through the subsampling layers. In a network with a 2×2 subsampling filter such a layer comprises as many feature map numbers as the previous convolutional layer but with half the number of rows and columns. Each unit *j* in mentioned network is connected to a 2×2 receptive field, computes the average of its four inputs y_i which are outputs from the corresponding feature map of the previous layer, multiplies it by a trainable weight w_j and adds a trainable bias b_j to obtain the activity level v_j:

$$v_j = w_j \frac{\sum_{i=1}^{4} y_i}{4} + b_j \tag{1}$$

In the rest of this section a particular convolutional neural network identified as LeNet5 is described. LeNet5 takes a raw image of 32×32 pixels as input. It is composed of seven layers: three convolutional layers (C1, C3 and C5), two subsampling layers (S2 and S4), one fully connected layer (F6) and the output layer. These layers are connected as shown in Fig. 1.

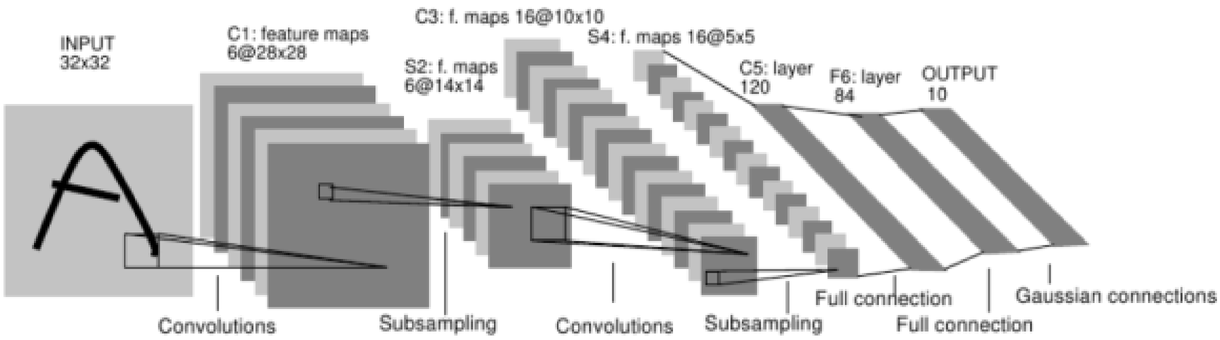

Figure1. LeNet-5 architecture [15]

The first convolution layer is composed of six feature maps of 32 × 32 units. The following subsampling layer (S2) reduces by 2 the resolution, while the next convolutional layer (C3) extends the number of feature maps to 16. As shown in table 1 the choice is made not to connect every feature map of S2 to every feature map of C3. Each unit of C3 is connected to several receptive fields at identical locations in a subset of feature maps of S2 [15, 16].

Table1. The Interconnection of the S2 Layer to C3 Layer [15]

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	X				X	X	X			X	X	X	X		X	X
1	X	X				X	X	X			X	X	X	X		X
2	X	X	X				X	X	X			X		X	X	X
3		X	X	X			X	X	X	X			X		X	X
4			X	X	X			X	X	X	X		X	X		X
5				X	X	X			X	X	X	X		X	X	X

The subsampling layer S4 acts as S2 and reduces the size of the feature maps to 5×5. The last convolutional layer C5 differs from C3 as follows. Each one of its 120 feature maps is connected to a receptive field on all feature maps of S4. And since the feature maps of S4 are of size 5×5, the size of the feature maps of C5 is 1 × 1. Thus C5 is same as a fully connected layer. The fully connected layer (F6) contains 84 units connected to the 120 units of C5. All the units of the layers up to F6 have a sigmoid activation function of the type:

$$y_j = \varphi(v_j) = A\tanh(Sv_j) \tag{2}$$

Where vj is the activity level of the unit. A and S are two constant parameters for the sigmoid function.

Finally, the output layer is an Euclidean RBF layer of 10 units (for the 10 classes) whose outputs yj are computed by

$$y_j = \sum_{i=1}^{84} (y_i - w_{ij})^2, \quad j = 0, \ldots, 9. \tag{3}$$

Where yi is the output of the ith unit of the layer F6. For each RBF neuron, yj is a penalty term measuring the fitness of its inputs yi to its parameters wij. These parameters are fixed and initialized to −1 or +1 to represent stylized images of the characters drawn on a 7×12 bitmap that are targets for the previous layer (hence the size 84 for the layer F6). Then the minimum output gives the class of the input pattern [16].

3. Proposed Method for signature verification

3.1. Feature extraction

Convolutional neural network is used to extracting features in this paper. The proposed CNN which is depicted in Fig. 2 takes a raw image of 180×240 pixels as input. Input images are normalized between 0 and 1 and are given to a CNN. The CNN is composed of nine layers: five convolutional layers, and four subsampling layers. Multilayer perceptron network is used for classifying the outputs of CNN instead of radial basis function network which is used in LeNet5 network. Output layer or the last layer of the CNN is given to a MLP network as the input. Number of feature maps and dimention of convolutional and subsampling filters are obtained experimentaly for all

International Journal of Engineering Research and Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 2, April - 2012

of layers. The structure of multilayer perceptron network is discribed in next subsection.

The first convolutional layer of the proposed CNN has six feature maps, each of which has a resolution of 174 × 234, with a receptive field of 7 × 7. The second layer, or the first subsampling layer, contains six feature maps of size 87 × 117, with a receptive field of 2 × 2. The third layer is another convolutional layer and has 16 feature maps with size 80 × 110, with a receptive field of 8 × 8. The fourth layer contains 16 feature maps as well, each of which is of size 40 × 55. The fifth convolutional layer has 30 feature maps, each of which has a resolution of 34 × 48, with a receptive field of 7 × 8. The sixth layer contains 30 feature maps of size 17 × 24, with a receptive field of 2 × 2. The seventh layer is another convolutional layer and has 50 feature maps with size 10 × 18, with a receptive field of 8 × 7. The eighth layer contains 50 feature maps as well, each of which is of size 5 × 9. The ninth layer is a convolutional layer with 120 feature maps, again with a receptive field of 5 × 9.

All convolutional neural network neurons compute their input by calculating the weighted sum and feeding the result to the equ.2 in which A is chosen to be 1. The number of parameters in this method is 412,166. Since the input dimension is 180×240 (43200) pixels, parameter number is comparable with conventional neural networks such as MLP.

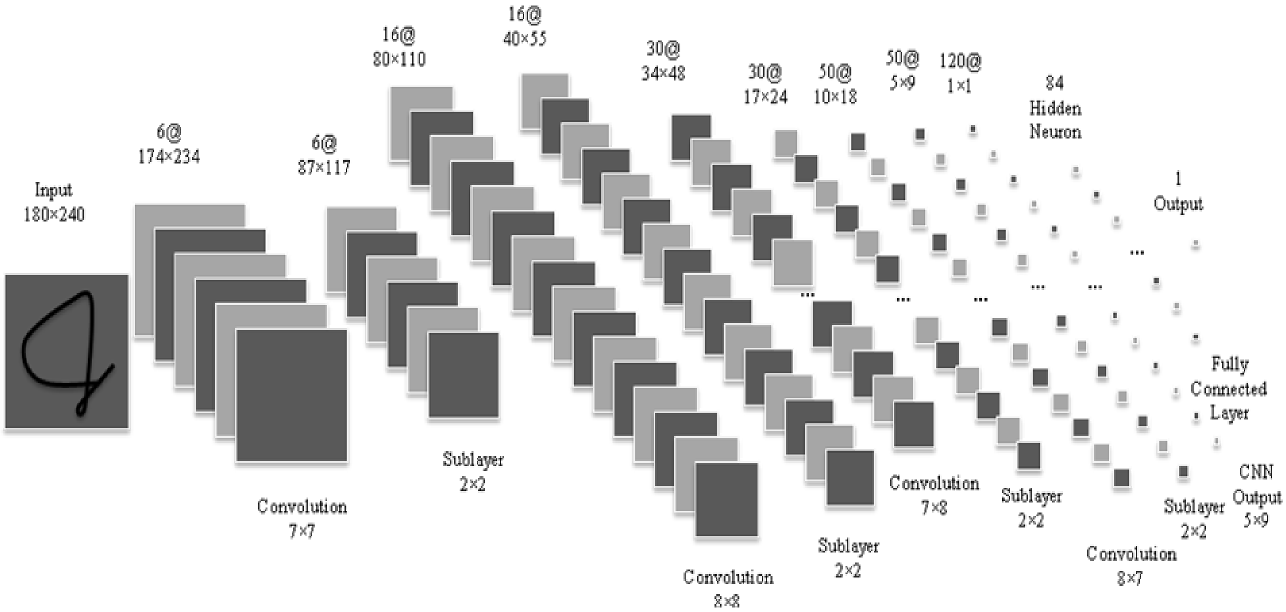

Figure2. Proposed CNN for persian signature verification

3.2. Classification

A MLP network is used to classify the features which are extracted with the applicability of the CNN model. Last layer of the CNN is considered as the input layer for the MLP network. This layer is followed by a hidden layer with 84 neurons, which is fully interconnected with the previous layer. Finally, the last layer of this network is a layer with one neuron which is target of the network. The target is considered as 0 or 1. It indicates wether the input signature is related to the desired person or not. Targets 0 and 1 signifiy the original and forgery signatures respectively. The MPL network using to classify the features is depicted in the 3 last layers of Fig. 2.

4. Data

In this research, 176 original Persian signatures from 22 people are used. For each person, 8 signatures are considered for training, testing, and validation of the algorithm. Some signature images used in this paper are shown in Fig. 3. The size of the images is 640×480.

Figure3. Some Signature images used in the experiment

5. Experiments and Results

A variety of experiments are performed and results are presented in this paper. Different numbers of feature maps and dimentions of convolutional and subsampling filters are considered and the best of them is selected. All experiments were performed with 176 signatures from 22 people. There was no overlap between the training and testing sets. The performance of the suggested method during the training session for the training, testing and the validation dataset is illustrated in Fig. 4. The training was stopped when the minimum error for the validation dataset was achieved.

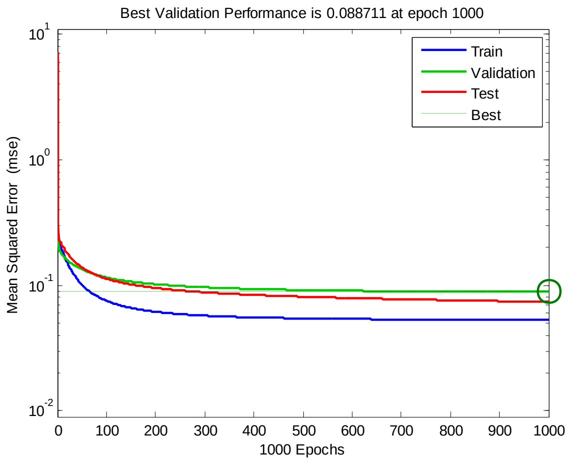

Figure4. Performance of the proposed CNN structure

Experiments are performed 10 times for 1000 epochs. The average of 99.86 is resulted for validation performance. The error is fixed after the average of 785 epochs.

6. Conclusions

In this study a general CNN architecture is applied to the task of Persian signature verification. The style of people's handwritten signature is a biometric feature used in person authentication. CNNs may be expected to achieve significantly better results than standard feed-forward networks for many tasks. The key characteristic of weight sharing is appropriate when the input data is scarse. In this paper, despite the fact that input data are little in quantity and great in dimensionality good results are obtained. Furthermore, CNNs are invariance to distortions and simple geometric transformations like translation, scaling, rotation and squeezing. Another characteristic which is more important than other characteristics for the task of signature verification is the ability of CNNs in extracting features from input data. So, it would solve the preprocessing problem of offline signature verification task. Proposed method is not only capable of extracting features relevant to a given signature, but also robust with regard to signature location changes and scale variations when compared to classical methods. The simulation results reveal the efficiency of the suggested algorithm.

6. References

[1] Jonghyon Yi, Chulhan Lee, and Jaihie Kim, "Online signature verification using temporal shift estimated by the phase of gabor filter", IEEE transactions on signal processing, vol. 53, no. 2, february 2005, 776-783.

[2] Elaheh Dehghani, Mohsen Ebrahimi Moghaddam, "On-line Signature Verification Using ANFIS", Proceedings of the 6th International Symposium on

Image and Signal Processing and Analysis (2009), 546-549.

[3] Amaç Herdağdelen and Ethem Alpaydın, "Dynamic alignment distance based online signature verification", The 13th Turkish Symposium on Artificial Intelligence & Artificial Neural Networks (2004), Izmir, Turkey.

[4] Ismail, M.A., Gad, S., "Off-line Arabic signature recognition and verification", Pattern Recognition 33 (2000), 1727–1740.

[5] Fang, B., Wang, Y.Y., Leung, C.H., Tang, Y.Y., Kwok, P.C.K., Tse, K.W., Wong, Y.K., "A smoothness index based approach for off-line signature verification", Proceedings of ICDAR'99, (1999) 785–787.

[6] Hobby, J.D., "Using shape and layout information to find signatures, text, and graphics", Computer Vision and Image Understanding, 80, (2000) 88–110.

[7] Ramesh, V.E., Murty, M.N., "Off-line signature verification using genetically optimized weighted features", Pattern Recognition 32, (1999) 217–233.

[8] Scholkopf, B., Sung, K., Burges, C., Girosi, F., Niyogi, P., Poggio, T., Vapnik, V., "Comparing support vector machines with Gaussian kernels to radial basis function classifiers", AI Memo No. 1599, MIT (1996).

[9] Bajaj, R., Chaudhury, S., "Signature verification using multiple neural classifiers", Pattern Recognition (1997) 30, 1–7.

[10] Baltzakis, H., Papamarkos, N., "A new signature verification technique based on a two-stage neural network classifier", Engineering Applications of Artificial Intelligence 14 (2001) 95–103.

[11] Velez, J.F., Sanchez, A., Moreno, A.B., "Robust off-line signature verification using compression networks and positional cuttings", Proceedings of IEEE International Conference on Neural Networks for Signal Processing (NNSP '03). (2003) 627–636.

[12] Camino, J.L., Travieso, M.C., Morales, C.R., Ferrer, M.A., "Signature classification by hidden Markov model", Proceedings of IEEE International Carnahan Conference on Security Technology. (1999) 481–484.

[13] E. Frias-Martinez, A. Sanchez, J. Velez, "Support vector machines versus multi-layer perceptrons for efficient off-line signature recognition", Engineering Applications of Artificial Intelligence 19 (2006) 693–704.

[14] B H Shekar and R.K.Bharathi, "Eigen-signature: a robust and an efficient offline signature verification algorithm", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, 134-138.

[15] Y. LeCun, L. Bottou, Y. Bengio, P. Haffner, "Gradient-based learning applied to document recognition", Proc. IEEE 86 (11) (1998) 2278–2324.

[16] C. Y. Suen and G. Bloch F. Lauer, "A trainable feature extractor for handwritten digit recognition," *Pattern recognition,* pp. 1816-1824, 2007.