UDC 004.932.72
DOI: 10.30987/conferencearticle_61c997ee310750.12735248

PROBLEMS OF BIOMETRIC IDENTIFICATION IN ACCESS SYSTEMS

Umidjon Yu. Akhundjanov, PhD student, axundjanov@mail.ru

Valery V. Starovoitov, Chief Researcher, Dr. Sci., Professor

United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Belarus, Minsk

Abstract. Handwritten signature recognition is a biometric method that can be used in many aspects of life when it is necessary to use personal signatures, for example, when cashing a check, signing a credit card, authenticating a document, etc. Innovative approaches to solving static signatures that have been introduced into the literature increase every year.

Keywords: recognition, biometrics, handwritten signature.

INTRODUCTION

Biometric authentication systems are among the most reliable and effective methods of verifying the user's identity. Biometric data includes, for example, fingerprints, photos of the retina and iris, a picture of the geometry of the face, samples of voice and handwriting, three-dimensional photography, etc. [1].

In general, biometric identification systems are divided according to the principle of operation into two main types: static and dynamic.

1) **Static (physiological characteristics)**

- *Fingerprints*
- *The iris of the eye*
- *Retina of the eye*
- *Vein pattern*
- *Face*
- *Hand geometry*
- *Heart rate*
- *DNA*

2) **Dynamic (behavioral characteristics)**

Handwriting and signature dynamics

- *Heart rate*
- *Voice and speech rhythm*
- *Gesture recognition*
- *Speed and features of working on the computer keyboard*
- *Gait*

The problem of verifying a handwritten signature is related to image recognition problems. The main difficulties with signature recognition are related to the fact that a legitimate user can sign in different ways, depending on their emotional and mental

САПР и моделирование в современной электронике. С. 69 – 72.

state, or even have several variants of their signature. An attacker can also attempt to forge a signature [2].

Handwriting examinations can effectively detect forgery, but these types of examinations are expensive and cannot be carried out in real time within the framework of authentication systems.

Static (off-line), offline handwriting recognition is performed after a sample text has been created and recorded in digital form. The optically captured image data is then converted into a bitmap. Offline signature processing has about 40 functions, including the analysis of the center of gravity, edges, and curves for authentication. In the off-line method, stable dynamic characteristics are absent due to the uniqueness of the signature difference due to age, illness, geographical location and, perhaps, to some extent, the emotional state of the person, exacerbates the problem. Thus, the offline signature recognition method is complex.

DATA COLLECTION

Data collection can be performed in two ways: first of all, signature databases are available from open sources (via the Internet). If necessary, images are obtained by scanning signatures.

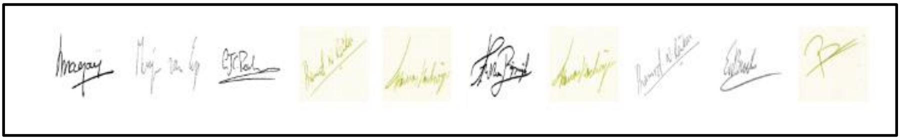

Figure 1 – Example of raw images of signatures.

IMAGE PREPROCESSING

When preprocessing an image, various operations are performed on the caption image, such as converting a color image to gray, removing noise, determining a threshold value, thinning, detecting borders, and cropping. When binarized, the color image is converted to a black-and-white image, meaning the caption pixel will be "1 "and the background pixel will be"0".

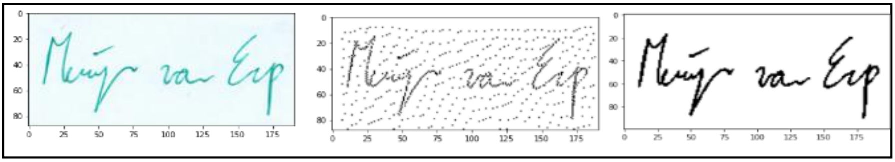

Figure 2 – Pre-processing examples

Feature extraction

At the feature extraction stage, we extract some features of the signature image. Different algorithms are used to extract features. The extracted signature image features at this stage are inputs to the learning and recognition stages. Features can be classified as global, grid, and masking.

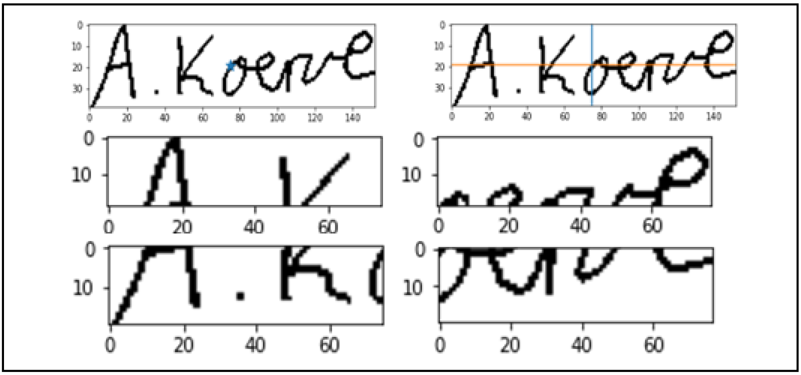

Figure 3 – Feature extraction examples

Classification

When a new signature is used, its characteristics are extracted and compared to those already stored in the database. If the characteristics match, it is classified as genuine, otherwise-as a fake.

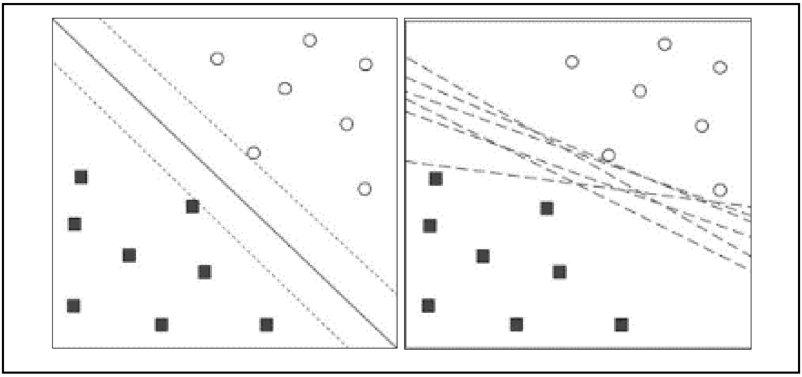

Figure 4 – SVM (support vector machine) classification

Consider them:

1) Arbitrary forgery: A signature written by a person who does not know the form of the original signature is an arbitrary forgery.

2) Accidental forgery: A signature written by a person who does not know the form of the original signature is an accidental counterfeit.

3) Qualified counterfeit: The third type, called qualified counterfeit, is represented by a suitable copy of the genuine signature model.

4) Imitation of a forgery: the forger has access to a sample of the genuine signature with which he practices making copies.

5) Cut and paste forgery: An authentic signature is cut from one document and placed on a forged document and then copied. If the lighting and resolution are set correctly, the document will look authentic.

CONCLUSION

It should be noted that a lot of work has already been done in the field of signature verification, but there are still many problems in this area. There are basically two problems with the signature verification method. The non-repetitive nature of variations in the caption image due to illness, age, and geographical location. To some extent, due to the emotional state of the person, there is a variation of the signature. Another problem is related to security considerations. It is very difficult to make the signature database of the original documents available for signature verification. More research is needed in the field of offline signature verification and online signature verification, although the accuracy obtained with the available systems is not very good.

The described aspects are still the objects of research on the base, and, therefore, the practical application of identification by handwritten signature in automated systems is still problematic.

REFERENCES

1. Behrouz Vaseghi, Somayeh Hashemi."Off line signatures Recognition System using Discrete Cosine Transform and VQ/HMM,"Australian Journal of Basic and Applied Sciences, ISSN 1991-8178,6(12): 423-428, 2012

2. Ахунджанов У. Ю. Статическая преобразование подписи с применением классификаторов SVM / KNN // Современные проблемы и их решения информационно-коммуникационных технологий и телекоммуникаций: Сборник докладов республиканской научно-технической онлайн конференции. Фергана: 2020. – С.12 – 14.

Материал принят к публикации 23.09.21.