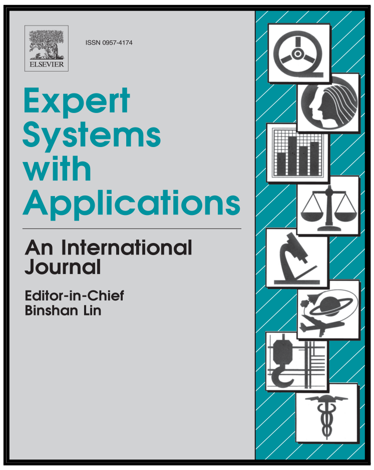
Accepted Manuscript



New Off-line Handwritten Signature Verification Method based on Artificial Immune Recognition System

Yasmine Serdouk, Hassiba Nemmour, Youcef Chibani

PII: S0957-4174(16)00002-6
DOI: 10.1016/j.eswa.2016.01.001
Reference: ESWA 10451

To appear in: *Expert Systems With Applications*

Received date: 11 January 2015
Revised date: 12 November 2015
Accepted date: 1 January 2016

Highlights

- A new system for Handwritten Signature Verification is proposed.
- The Artificial Immune Recognition System is proposed to achieve the verification task.
- Two new features that are Gradient Local Binary Patterns and Longest Run Features are proposed.
- Results obtained on CEDAR and GPDS-100 corpuses reveal the effectiveness of the proposed methods.

New Off-line Handwritten Signature Verification Method based on Artificial Immune Recognition System

Yasmine Serdouk*, Hassiba Nemmour, Youcef Chibani

Communicating and Intelligent System Engineering Laboratory,
Faculty of Electronic and Computer Sciences,
University of Sciences and Technology Houari Boumediene (USTHB),
Bab Ezzouar El-Alia BP. 32. 16111, Algiers, Algeria

Email: {yserdouk, hnemmour, ychibani}@usthb.dz

Abstract

Natural Immune System offers many interesting features that inspired the design of Artificial Immune Systems (AIS) used to solve various problems of engineering and artificial intelligence. AIS are particularly successful in fault detection and diagnosis applications where anomalies such as errors and failures are assimilated to viruses that should be detected. Thereby, AIS seem suitable to automatically detect forgeries in signature verification systems. This paper proposes a novel method for off-line signature verification that is based on the Artificial Immune Recognition System (AIRS). For feature generation, two different descriptors are proposed to generate signature traits. The first is the Gradient Local Binary Patterns that estimates gradient features based on the LBP neighborhood. The second descriptor is the Longest Run Feature, which describes the signature topology by considering longest suites of text pixels. Performance evaluation is carried out on CEDAR and GPDS-100 datasets. The results obtained showed that the proposed system has promising performance and often comfortably outperforms the state of the art.

Keywords: Artificial Immune Recognition System, Gradient Local Binary Patterns, Longest Run Features, Signature Verification.

*Corresponding author. Tel: +213 561122950.
Email address: `yserdouk@usthb.dz` (Yasmine Serdouk)

1. Introduction

Biometrics is the science which identifies persons on the basis of their biological or behavioral features. Currently, various identification systems employing fingerprints, hand geometry, retina, iris, or faces provide very interesting performances. Nevertheless, in some specific applications using paper documents such as bank checks and contracts, handwritten signature remains the oldest and the main identification tool. Many successful studies have been reported on this subject. However, because of speed and robustness requirements, signature verification remains an open research issue (Impedovo, Modugno, Pirlo, & Stasolla, 2008). There are two approaches for developing such systems, the on-line verification and the off-line verification (Plamondon & Srihari, 2000; Impedovo, Modugno, Pirlo, & Stasolla, 2008). In the former, signatures are acquired via an electronic device such as tablets and an instrumented stylus that captures temporary information such as the x-y coordinates, velocity or acceleration (Plamondon & Srihari, 2000). In the off-line verification, such information cannot be recovered since signatures are prewritten on a paper. Consequently, it is less accurate but it has more practical application areas. On the other hand, the verification itself may be attempted in either writer-dependent or writer-independent context. In the writer-dependent case, the system is trained by using genuine signatures or both genuine and forgeries of a specific writer (Rivar, Granger, & Sabourin, 2013). This means that the training process should be repeated each time a new signer is presented to the system. The writer-independent scenario develops a generic system that can be tested on any new writer (Kumar, Sharma, & Chanda, 2012). Precisely, the system is developed using dissimilarities between genuine and forged signatures of some writers and tested on dissimilarities of other writers.

Note that since signatures are strong variable entities, even for human experts, their verification is not a trivial matter (Vargas, Ferrer, Travieso, & Alonso, 2011). For this reason, the signature verification has been widely investigated during the past years. The literature reports a lot of research works using various feature generation and verification methods (Plamondon & Srihari, 2000; Impedovo, Modugno, Pirlo, & Stasolla, 2008). Presently, we are focused on the writer-dependent off-line signature verification. In this approach, the best off-line signature verifiers (when tested on publicly available databases and against skilled forgeries) deliver error rates of approximately 9-10% (Kovari & Charaf, 2013). Such scores reveal that more theoretical advances should be done in the signature verification field in order to reach real-life verification systems.

In this work, a new off-line signature verification method based on the Artificial Immune Recognition System (AIRS) is proposed. Artificial immune systems are a new computational research area inspired by simulated biological behavior methods like neural networks and genetic algorithms. Recall that to protect the bodies, biological immune system develops adaptive mechanisms (white blood cells) that allow the detection of foreign substances such as viruses. This process includes the detection of both unchanging organisms as well as un-encountered organisms (Bayar, Darmoul, Hajri-Gabouj, & Pierreval, 2015). These characteristics attracted researchers on pattern recognition who suggested that this principle can help to solve various expert and intelligent systems issues such as fault or anomaly detection. Then, several artificial immune algorithms such as the AIRS, which was developed by (Watkins, 2001), achieved high performance in various pattern recognition problems. AIRS was successfully used for thyroid diagnosis (Kodaz, Ozsen, Arslan, & Gunes, 2009), fault detection (Laurentys, Palhares, & Caminhas, 2011) and watermarking (Findik, Babaoglu, & Ulker, 2011).

Keeping in mind that a verification system should efficiently discriminate forged signatures that are seen as dangerous invaders to the verification mechanism, we suggest that AIRS can give an interesting solution for off-line signature verification. Recall that AIRS has been used in various handwriting recognition applications, such as handwritten character recognition (Chen, Liang, Yang, Peng, & Zhong, 2010), handwritten Russian uppercase letter recognition (Yang, 2011), as well as Arabic word recognition (Nemmour & Chibani, 2013 'a').

The contribution of this paper is twofold. First, the AIRS is used for solving the off-line signature verification where it is trained according to the writer-dependent approach. For each writer, an AIRS is developed by considering genuine and forged signature classes. Second, to obtain a robust signature characterization, a combination of topological and gradient features, is proposed. For the topological characterization, the Longest Run Feature, which highlights the pixel distribution in various directions is proposed. Then, gradient information based on Local Binary Neighborhood is extracted by using the so-called Gradient Local Binary Pattern. This paper is arranged as follows: Section 2 presents the background to signature verification methods. Section 3 provides a brief review of AIRS. Section 4 introduces the proposed signature verification system. Experimental results are reported and discussed in section 5. The last section gives the main conclusions of this work.

2. Background

In both on-line and off-line approaches, the verification system is composed of two main steps that are feature generation and verification. In the on-line verification, the feature generation is the key component since the verification itself can be carried out through similarity measures. With modern tablets, signatures are registered as a set of discrete points from which various basic dynamic features are captured, such as x-y coordinates, pen-top, pen-down, pressure, velocity, and acceleration. Thereafter, features can be locally computed for each point in the time sequence or global if they are calculated from the whole signature sequence (Doroz, Porwik, & Orczyk, 2015). In (Doroz, Porwik, & Orczyk, 2015), authors employ ten of such dynamic features associated to various similarity coefficients. Also, several research works were focused on developing robust features from on-line signature sequences while employing the Dynamic Type Warping (DTW) or other similarity measures to achieve the verification task (Fischer, Diaz, Plamondon, & Ferrer, 2015). Furthermore, recent works based on SVM and random forest classifiers propose feature combination associated to time functions that parametrize pen pressure, coordinates and inclination angles (Parodi & Gomez, 2014).

In the off-line signature verification approach which constitutes the purpose of the present work, signatures are extracted from digitized documents using a scanner or a camera, and stored as two dimensional gray level images. To cope with the lack of dynamic information, complex image processing techniques are required to extract signature traits. For the feature generation, a large number of methods were utilized to extract pertinent information about signatures. First techniques were based on statistical features like geometric moments as well as global image transformations such as the wavelet transform, Radon transform, Ridgelet transform, Contourlet as well as the Curvelet transform (Deng, Mark Liao, Ho, & Tyan, 1999; Soleymanpour, Rajae, & Pourreza, 2010; Radhika, Venkatesha, & Sekhar, 2011; Hamadene, Chibani, & Nemmour, 2012; Nemmour & Chibani, 2013 'b'). Also, in (Kumar & Puhan, 2014), authors propose the use of Chord moments for feature generation. Experiments conducted on CEDAR dataset by using SVM gave promising performance. Currently, attentions are focused on the use of local features, which are intended to be more robust to the global shape variation induced by ballistic and fast movement during the signature writing (Kiani, Pourreza, & Pourreza, 2009). In this respect, various structural, directional and curvature features provided satisfactory results (Huang & Yan, 2002; Justino, Bortolozzi, & Sabourin, 2005). In (Bertolini, Oliveira, Justino, & Sabourin, 2010) authors proposed a set of grid features including pixel density, pixel distribution, slant and curvature to train an ensemble of SVM classifiers. Experiments showed that distribution-based and slant-based systems can provide satisfactory discrimination between genuine and forged signatures. Also, satisfactory performance has been reported using grid-based Histogram of Oriented Gradients (Yilmaz, Yanikoglu, Tirkaz, & Kholmatov, 2011). In recent past years, textural features, especially Local Binary Patterns (LBP), gained an important interest for signature characterization (Vargas, Ferrer, Travieso, & Alonso, 2011). Various forms of LBP, such as Center Symmetric LBP (CS-LBP), Local Derivative Patterns (LDP), Rotation Invariant Uniform LBP (LBPriu) and Orthogonal Combination of LBP (OC-LBP), were utilized for off-line signature verification (Vargas, Ferrer, Travieso, & Alonso, 2011; Ferrer, Vargas, Morales, & Ordonez, 2012; Serdouk, Nemmour, & Chibani, 2014). Moreover, several research works present LBP-based verification, as one of the most powerful systems for off-line signature verification, where efforts are focused on developing approaches to strengthen such systems (Ferrer, Diaz-Cabrera, & Morales, 2015; Galbally et al., 2015).

Regarding the verification step, first techniques were based on similarity measures and template matching (Hunt & Qi, 1995). Thereafter, efficient classifiers and learning machines such as Bayes classifiers, artificial neural networks, Hidden Markov Models and SVM, were employed (Kalera, Srihari, & XU, 2004;

Fang & Tang, 2005; Shanker & Rajagopalan, 2007). Recent researches on signature verification reveal that similarity measures still remain very successful for on-line verification (Doroz, Porwik, & Orczyk, 2015), whereas SVM constitutes the best verifier for the off-line approach (Guerbai, Chibani, & Hadjadji, 2015; Ferrer, Diaz-Cabrera, & Morales, 2015; Galbally et al., 2015). Indeed, various works showed that SVM outperforms hidden Markov models and neural networks in terms of accuracy and efficiency (Justino, Bortolozzi, & Sabourin, 2005; Martinez, Sanchez, & Velez, 2006).

Despite all these efforts, verification scores obtained on benchmark datasets are suboptimal and need to be improved (Murshed, Bortolozzi, & Sabourin, 1995 'a'; Murshed, Bortolozzi, & Sabourin, 1995 'b'; Justino, Bortolozzi, & Sabourin, 2005; Martinez, Sanchez, & Velez, 2006). Various references proposed hybrid systems as well as classifier ensembles to deal with the complexity of this task (Batista, Granger, & Sabourin, 2012). In (Ferrer, Diaz-Cabrera, & Morales, 2015; Galbally et al., 2015), authors propose an ink deposition model to produce synthetic images that help improving the off-line verification. Synthetic signature images aim at integrating on-line information that are not present in regular static signatures (e.g., pressure, speed or pen-ups trajectory). Different results obtained for synthetic random and skilled forgeries evince that signature verification is still an ongoing and very attractive research field. In this work, Artificial Immune Recognition System, which gives high performance in some pattern recognition tasks, is proposed to carry out the off-line signature verification. This classifier is associated to two new features that are introduced to highlight local topological and gradient traits of handwritten signatures.

3. Overview of the Artificial Immune Recognition System (AIRS)

Artificial immune systems are inspired from the natural immune system which uses antibodies (B-Cells) to recognize dangerous invaders that are known as antigens. Recently, they have been employed as expert systems in various purposes including feature generation, pattern recognition, machine learning and data mining (Kodaz, Ozsen, Arslan, & Gunes, 2009). Timmis and Neal proposed the first resource limited artificial immune algorithm based on Artificial Recognition Balls (ARB), which have the same meaning as B-Cells (Timmis & Neal, 2001). Then, Watkins proposed the Artificial Immune Recognition System (AIRS) (Watkins, 2001). AIRS is a resource limited algorithm that imitates immune metaphors such as antibody-antigen binding, affinity maturation, clonal selection process, resources competition and memory cell acquisition (Kodaz, Ozsen, Arslan, & Gunes, 2009). In AIRS, each training or test sample is an antigen. Antibodies are the Memory Cells (MC) of the system, which constitute representative data of each class. An ARB corresponds to the feature vector of an antibody with its class label and its resources number. AIRS training develops new antibodies (or memory cells) that effectively describe the different classes of interest. Thereby, ARBs compete with each other for a fixed resources number in order to keep those with high affinities to the training antigen. Here affinity expresses similarity between patterns through Euclidian distance. New memory cells are extracted from the remaining ARBs in the system to form the MC pool which will be used to classify test antigens. AIRS training algorithm is detailed in the following sections.

3.1. Initialization

In this step, data are normalized such that Euclidian distance scales in the range [0, 1]. Then, an Affinity Threshold (AT) is computed according to the following equation:

$$AT = \frac{\sum_{i=1}^{n-1} \sum_{j=i+1}^{n} affinity(ag_i, ag_j)}{n(n-1)/2} \tag{1}$$

ag_i: feature vector of the i^{th} antigen (training sample).
$affinity$: Euclidian distance.
n: number of antigens.

AT is used in the condition of a memory cell replacement in the training routine. The initialization step is achieved by seeding of initial Memory Cells (MC) pool and initial ARBs pool. In other words, for each class of interest (two classes in our case), at least one training sample is randomly selected to be used as prototype of its class in the MC and ARBs pools.

3.2. Training process

The training of each antigen (training sample) is a one-shot process as described in Algorithm 1.

Algorithm 1. Antigen training in AIRS

---

1. *MC-Match selection:* This step performs the antigen-antibody binding by computing stimulations between the antigen and all antibodies in the Memory Cells (MC) pool as:

$$ST(ag_i, MC) = 1 - ED(ag_i, MC) \tag{2}$$

   ED: Euclidian distance.
   MC: Memory cell.
   The antibody giving the highest stimulation is called the Memory Cell-Match or *MC-Match*.

2. *Clonal expansion and affinity maturation:* Generate a set of mutated clones of *MC-Match* and add them to the ARBs pool.

3. *Metadynamics:* ARBs that belong to the same class of the present antigen, undergo a resource allocation and a selection process.

   - Resource allocation: Each ARB is supplied by a resources number to express how much its stimulation to the antigen is high.

   - Clonal selection: It is carried out based on ARBs competition for a fixed global resources number in order to keep only ARBs with actually high stimulations.

4. *Stopping condition:* Calculate the average stimulation of ARBs of each class to check the stopping condition. If average stimulations are lower than a user-defined stimulation threshold, repeat steps 2, 3 and 4.

5. *MC-Candidate Selection:* Select the ARB with highest stimulation in the antigen class. This ARB is the Memory Cell-Candidate (*MC-Candidate*).

6. *Update the MC pool: MC-Candidate* is added to the MC pool if it has higher stimulation to the present antigen than *MC-Match*. In this case, if the Euclidian distance between *MC-Candidate* and *MC-Match* is lower than a threshold proportional to the AT, the *MC-Match* is removed from the MC pool.

3.3. Classification step

Once the training of all antigens is completed by performing steps of Algorithm 1, the evolved MC pool can be used for classifying test samples. Specifically, the classification is achieved through a K-Nearest Neighbors decision computed over the MC pool.

4. Proposed signature verification system

The flowchart of the proposed signature verification system is depicted in Fig. 1. Specifically, the training stage is evolved as a two-class classification problem, which aims to separate genuine signatures from skilled forgeries. Initially, signature images are converted into binary format by using Otsu's method. Then, they are sent to the feature generation module in order to extract pertinent information. Feature vectors of all signatures constitute the set of antigens of both genuine and forged classes. AIRS is trained over these antigens to build a set of Memory Cells (MC pool) describing the variability in the two classes. The MC pool is employed in the verification stage. Precisely, each questioned signature undergoes the same binarization and feature generation processes. Then, a set of affinities are calculated with respect to all memory cells. Finally, the questioned signature is assigned either to the genuine or forged class based on the K-Nearest Neighbor classification.

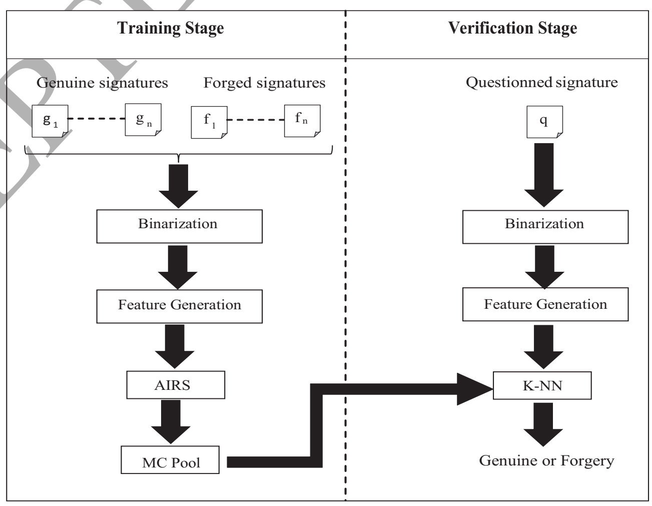


Figure 1: Flowchart of AIRS-based handwritten signature verification

Furthermore, two features describing gradient and topological properties are introduced to characterize handwritten signatures. Gradient features are obtained by using the gradient local binary patterns, which combines the gradient information with texture features derived from uniform patterns. As topological traits, we propose the Longest Run Feature, which considers the length of the longest pixel succession in various directions.

4.1. Gradient Local Binary Patterns

The Gradient LBP (GLBP) was recently introduced for human detection (Jiang, Xu, Yu, & Goto, 2013). The basic idea consists of using the LBP neighborhood to compute the histogram of oriented gradients. Recall that Local Binary Patterns (LBP) are utilized in statistical and structural analysis of textural patterns, based on the gray level distribution. For each pixel, LBP is obtained by comparing its gray level value with those of its neighbors that are taken through a radius R (Ojala, Pietikainen, & Harwood, 1996). So, considering the eight neighbors, which means that R=1, the LBP code is calculated as follows:

$$LBP(x, y) = \sum_{p=0}^{7} s(g_p - g_c) \tag{3}$$

with:

$$s(l) = \begin{cases} 1 & l \geq 0 \\ 0 & l < 0 \end{cases} \tag{4}$$

g_c: gray level value of the central pixel $P(x, y)$.
g_p: gray value of the p^{th} neighbor.

The global signature LBP feature corresponds to the histogram of all possible codes. In various pattern recognition applications, LBP were employed to introduce the texture information within other descriptors such as wavelet transforms and Gabor filters (Zhang et al., 2005; Vargas, Travieso, Alonso, & Ferrer, 2010). Recently, the LBP neighborhood was exploited to improve gradient features for human detection (Jiang, Xu, Yu, & Goto, 2013). This yields the GLBP descriptor that is adapted here for describing signatures. The GLBP calculation on a signature image is summarized in Algorithm 2.

Algorithm 2. GLBP calculation

For each pixel in the signature image, GLBP feature is obtained as:

1. Compute LBP code,
2. Compute width and angle values from the uniform patterns such as (see Fig. 2):
   - The width value corresponds to the number of "1" in LBP code,
   - The angle value corresponds to the Freeman direction of the middle pixel within the "1" area in LBP code,
3. Compute the gradient at the 1 to 0 (or 0 to 1) transitions in uniform patterns,
4. Width and angle values define the position within the GLBP matrix, which is filled by the gradient information.

The size of the GLBP matrix is defined by all possible angle and width values. Specifically, there are eight possible Freeman directions for angle values while the number of "1" in uniform patterns can go from 1 to 7. This yields 7×8 GLBP matrix, in which gradient features are accumulated. Finally, the L2 normalization is applied to scale features in the range [0, 1] (Dalal & Triggs, 2005; Tang & Goto, 2010).

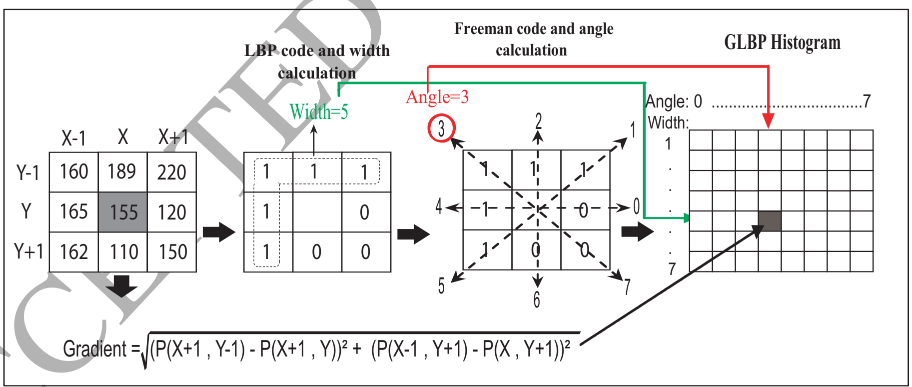


Figure 2: Calculation of GLBP feature for a central pixel

4.2. Longest Run Feature

Longest Run Feature (LRF) is based on counting text pixels through horizontal, vertical and diagonal directions. For each direction, the longest suite of text pixels is selected. More precisely, if we consider the horizontal direction, along each line, the size of the longest succession of signature pixels is captured. Then, the sum of all sizes constitutes the LRF value along the horizontal direction. The same features are then computed for the remaining directions as shown in Fig. 3. Note that LRF has been employed as a local feature through uniform grid partitioning for handwritten digit recognition (Das et al., 2012). Presently, we investigate its applicability to highlight the global signature topology. Once computed, LRF features are normalized according to the image size in each direction.

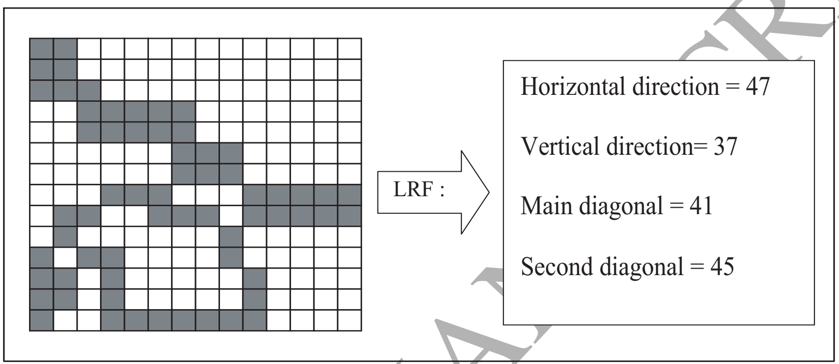


Figure 3: Illustration of LRF computation

5. Experimental results

The proposed signature verification system is evolved using the writer dependent scenario, where a specific system is implemented for each signer. The performance evaluation is based on False Rejection Rate (FRR), which gives the percentage of genuine signatures that are rejected by the system and the False Acceptance Rate (FAR), which is the percentage of forged signatures accepted by the system. Also, the Average Error Rate (AER) is considered to provide the global verification error. Experiments are carried out on two datasets that are CEDAR and GPDS-100.

5.1. CEDAR signature corpus

CEDAR dataset[1] contains signatures of 55 volunteer signers belonging to versatile cultural backgrounds (Kumar, Sharma, & Chanda, 2012). For each

[1]CEDAR Dataset is available on: http://www.cedar.buffalo.edu/NIJ/publications.html/

signer, there are 24 genuine signatures and 24 skilled forgeries. So, this yields 1320 genuine and the same number for skilled forgeries. Genuine signatures were written during 20 minutes apart while the forgeries were simulated by asking about 20 skillful forgers to reproduce the signatures of the database. All signatures were scanned at 300 dpi in 8-bit gray level. In the present work, signature images were binarized using Otsu's method in order to facilitate the calculation of Longest Run Features.

5.2. GPDS-100 signature corpus

GPDS corpus was collected by Grupo de Procesado Digital de Senales[2]. The first collection contained signatures for 100 writers with 24 genuine and 30 skilled forgeries. This leads to 2400 genuine signatures and 3000 forgeries in the whole dataset. Genuine signatures were collected on the same day where signers filled up a form with 24 boxes of different sizes. Forgeries were collected on a form of 15 boxes by asking each forger to imitate 3 signatures of 5 randomly selected signers. Once signature forms were collected, each form was scanned with a Canon device using 256 level gray scales. Thereafter, they were converted to black and white using a global threshold that was computed using Otsu's method. The resulting binary image is then passed through a median filtering to eliminate anomalies such as minor discontinuities as well as salt and pepper noises (Ferrer, Alonso, & Travieso, 2005).

5.3. Training protocol

In experiments, the signature corpus is divided into three equal subsets. Two subsets are used in the system development (training and parameter selection) while the third constitutes the test set for the performance assessment. Thereby, 16 genuine signatures and 16 forgeries are used in the model training and parameter selection. The remaining signatures (8 genuine + 8 forgeries for CEDAR) and (8 genuine + 14 forgeries for GPDS-100) are used to test the verification performance. Before validating this protocol, we tested various development sets in which, the number of samples per class was varied from 5, 8, 10 to 16. AER variations of a randomly selected signer from the two databases

[2]GPDS Dataset is available on: http://www.gpds.ulpgc.es/download/index.htm/.

are reported in Fig. 4. As expected, with a small training set, the AER takes high values while it can be significantly reduced with large training sets.

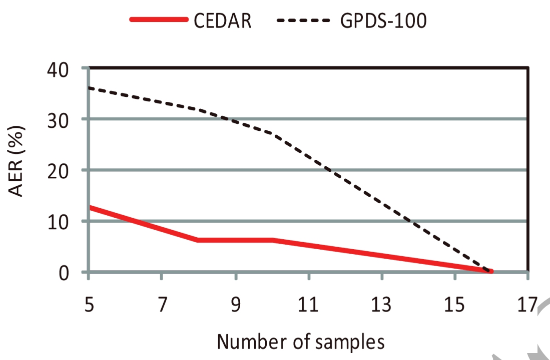


Figure 4: AER variations for various development sets

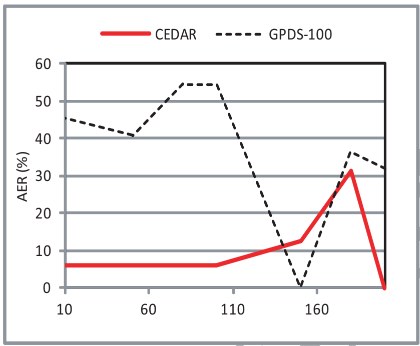
5.4. Parameter selection for AIRS

To implement AIRS classifier, user-defined parameters should be experimentally tuned (see Table 1). Hence, for each signer several run-passes were executed in order to find optimal values that allow the best verification accuracy. In a first time, one parameter was varied while keeping fixed values for the others. Then, a second round of experiments was performed in order to optimize the tuning of all parameters at once. Obtained results showed that four parameters, namely, the clonal rate, resources number, the mutation rate and the hyper-mutation rate, substantially control AIRS behavior. So, to illustrate the influence of parameters, Fig. 5 depicts AER variations achieved for randomly selected signers from the two datasets. Note that experiments were conducted using GLBP-based system so that the feature vector has a large size (56 components instead of LRF, which has 4 values). Also, the remaining parameters take the same values for all writers.

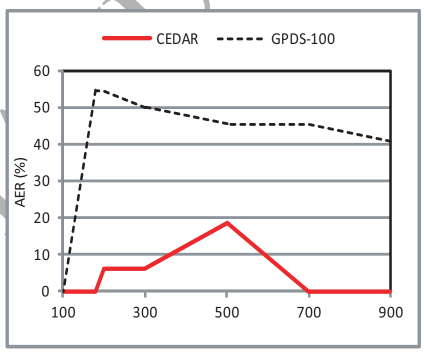
Since there is no rule that could be followed to find the best selection, each parameter was varied by considering the largest meaningful range of values. Specifically, the clonal rate was taken in the range [10, 200], while resources number was varied between 100 and 900 with a step of 50. For the mutation rate, which is the mutation probability of a given feature, small values were considered because a high probability yields clones that are too much different

Table 1: AIRS parameters description

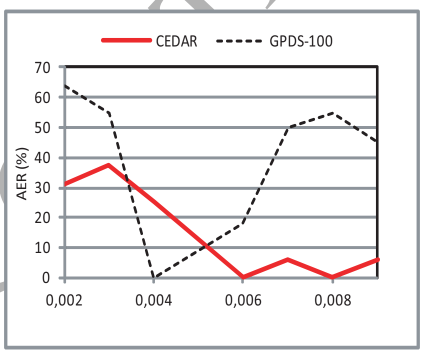
Parameter	Definition
Mutation rate	The probability that any given feature of an ARB will be mutated (it is taken between 0 and 1).
Hyper-mutation rate	Integer which determines the number of mutated clones, that a given memory cell is allowed to inject into the cell population.
Clonal rate	An integer that controls the number of generated mutated clones.
Affinity threshold scalar	Scalar used in the MC-Candidate and MC-Match comparison.
Stimulation threshold	Stopping threshold that is compared to the average stimulation (a real ranged between 0 and 1).
Resources number	An integer used to limit the total number of mutated clones in the ARBs pool.



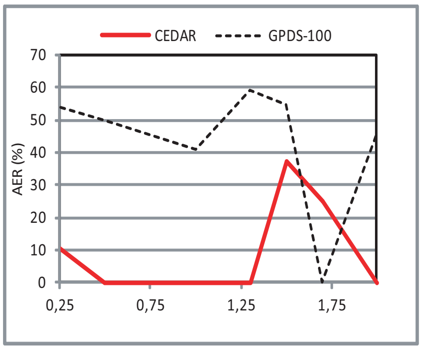
(a) Clonal rate



(b) Resources Number



(c) Mutation Rate



(d) Hyper-mutation rate

Figure 5: AER variations according to AIRS parameters

from the MC-Mach. Therefore, this parameter was taken in the range [0.002, 0.01] with a step of 0.01. Finally, the hyper-mutation rate scales between 0.25 and 2.

Roughly speaking, GPDS results reveal higher sensitivity to parameter values, since the AER variation reaches 60%. Also, for each parameter there is only one value that gives an optimal AER. For this reason, finding the optimal parameters selection for GPDS corpus is not a trivial task. On the other hand, CEDAR signatures allow more freedom when selecting parameters since for each of them, several values provide similar AER. Besides, compared to GPDS, the CEDAR verification task seems to be easier since the AER takes a small range of variations that is about 38%. This fact is depicted in Fig. 6, which shows the superposition between genuine and genuine signatures as well as genuine and forged signatures for the considered writers. As can be seen, for CEDAR data the superposition indicates a weak intra-class variability versus a high inter-class variability between genuine and forgeries. On the contrary, we note similar inter-class and intra-class variability for GPDS signatures, which evinces a more complicated discrimination.

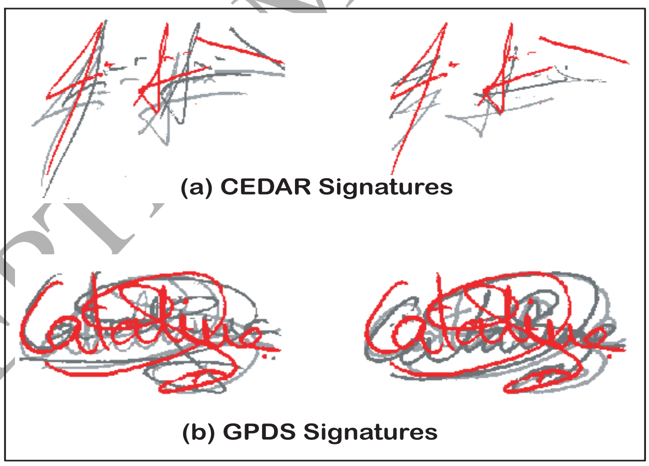


Figure 6: Superposition of a genuine signature (In red) with other signatures. Left hand: superposition with two genuine signatures, Right hand: superposition with two forgeries

From this first set of experiments, we noted that the clonal rate affects both the AER as well as the training time since it controls the number of generated mutated clones. So, the more the clonal rate is big the more the training duration is long. Therefore, this parameter was selected to allow the best tradeoff between AER and training duration.

5.5. Performance evaluation

The performance assessment purpose is twofold. On one hand, it aims to validate the AIRS as an effective signature verification method and on the other hand, highlight the usefulness of the proposed features for signature characterization. Table 2 reports the results obtained for individual features as well as for their combination. From this table, it is easy to see that in most cases the FAR is lower than FRR. This outcome means that the verification system discriminates more forged signatures. Also, proposed features behave differently from CEDAR to GPDS datasets. Specifically, LRF outperforms GLBP with GPDS data providing a gain of 0.59% in the AER. In return, with CEDAR database GLBP outperforms LRF with 0.68% reducing the AER to 1.94%. The best accuracy rates are obtained when considering the LRF and GLBP combination. In this case, the feature vector contains 60 components (56 GLBP features plus 4 LRF features). The combination achieves an AER of 1.59% for CEDAR and 11.73% for GPDS, respectively. For this latter, the AER is approximately the same than that derived from LRF features.

In addition to error rates, the average verification time that is required to perform the verification of one questioned signature, is reported in table 2. This includes the feature generation and the verification process. Note that all experiments have been carried out on an intel core i5 machine with 2.4 GHz and 8 GB SDRAM. As expected, LRF-based systems are much faster than the others for both databases. This is mainly due to the fact that LRF is composed of 4 values and all signature images are previously normalized to (500×500) pixels. This normalization is not adopted in the GLBP calculation, which contains 56 features. For this reason GLBP-based systems take more time especially for CEDAR samples, which have commonly larger size than GPDS data. Roughly, the verification process takes at most 3 seconds that is an acceptable duration to achieve a real time verification.

Table 2: Results obtained for the proposed system with CEDAR and GPDS-100 datasets

Dataset	Features	FRR (%)	FAR (%)	AER (%)	Verification time (seconds)
CEDAR	GLBP	2.27	1.59	1.94	2.95
	LRF	3.18	2.04	2.62	0.05
	GLBP+LRF	1.59	1.59	1.59	3.00
GPDS-100	GLBP	12.62	12.21	12.37	1.86
	LRF	16.50	9.07	11.78	0.06
	GLBP+LRF	11.00	12.14	11.73	1.92

For the purpose of investigating the performance sensitivity with respect to the variation of training and testing corpuses, experiments were replicated 8 times with different training and testing subsets. Mean and standard deviations (std) values of FRR, FAR and AER are reported in table 5.5.

Table 3: Mean and Standard deviation (Std) of the Error rates over 8 training and testing corpuses

Dataset	Features	FRR (%)		FAR (%)		AER (%)	
		Mean	Std	Mean	Std	Mean	Std
CEDAR	GLBP	3.18	1.28	4.20	3.61	3.70	2.48
	LRF	3.63	0.64	4.08	2.89	3.87	1.76
	GLBP+LRF	2.12	0.61	4.93	2.46	3.54	1.4
GPDS-100	GLBP	12.31	0.43	13.53	1.86	13.10	1.02
	LRF	18.62	3.00	9.85	1.11	13.02	1.70
	GLBP+LRF	11.38	1.33	13.16	1.75	12.52	1.11

There are two main observations. First, for all features the AER standard deviation values are scaled in the range 1% through 2.5%, which reflects a weak variation around the mean scores. Second, the inspection of mean error rates reveals similar findings to those reported in table 2. So, the random selection of training and testing samples doesn't affect the verification performance, since the proposed system provides approximately similar results.

Furthermore, AIRS behaves well with regard to both descriptors although it gives slightly better performance using LRF. Tables 4 and 5 report some state of the art results for the two datasets, obtained by considering different sets of training data as well as different verification protocols. We note that the proposed features outperform some other features that were used with SVM classifier especially for CEDAR corpus where the AER is about 3%. Also, the AIRS-based verification achieves comparable and sometimes better performance than other systems.

Table 4: Comparison with the CEDAR state of the art

Ref	Features	Classifier	#Genuine Signatures	FRR (%)	FAR (%)	AER (%)
(Kumar et al., 2012)	Surroundedness	MLP	24	08.33	08.33	08.33
(Kumar et al., 2010)	Signature morphology	SVM	24	12.39	11.23	11.59
(Guerbai et al., 2015)	Curvelet Transform	Combination of OC-SVM	12	07.41	08.25	07.83
(Chen & Srihari, 2006)	Gradient + concavity	Graph matching	16	07.70	08.20	07.90
(Chen & Srihari, 2006)	Zernike moments	Harmonic distance	16	16.60	16.30	16.40
(Larkins & Mayo, 2008)	Gradient + equimass pyramid	Adaptive features thresholding	16	07.75	07.42	07.58
(Bharathi & Shekar, 2013)	Chain code histogram	SVM	12	09.36	07.84	08.60
(Kumar and Puhan, 2014)	Chord moments	SVM	16	06.36	05.68	06.02
Proposed system	GLBP+LRF	AIRS	16	02.12	04.93	03.54

Table 5: Comparison with the GPDS-300/160/100 state of the art

Ref	Features	Classifier	#Genuine Signatures	FRR (%)	FAR (%)	AER (%)
(Kumar et al., 2012)	Surroundedness	MLP	24	13.76	13.76	13.76
(Vargas et al., 2011)	GLCM	SVM	10	24.61	04.92	12.18
(Ferrer et al., 2005)	Geometric features	Euclidian distance	16	16.39	15.50	15.94
(Guerbai et al., 2015)	Curvelet Transform	Combination of OC-SVM	12	12.50	19.40	15.95
(Bharathi & Shekar, 2013)	Chain code histogram	SVM	12	13.16	09.64	11.40
(Favorskaya & Baranov 2014)	Global traits: slant, width, length...	Structural similarity measure	15	09.62	15.82	12.72
(Ruiz-Del-Solar et al., 2008)	Local interest points	Bayesian		16.40	14.20	15.30
(Nguyen et al., 2009)	MDF,Energy, Maxima	SVM	12	17.25	17.25	17.25
Proposed system	GLBP+LRF	AIRS	16	11.38	13.16	12.52

6. Conclusion and future work

This work proposes the use of Artificial Immune Recognition System (AIRS) for off-line signature verification. AIRS is an emerging classification method inspired from the learning mechanisms of the natural immune system. It develops representative data that help to discriminate a normal behavior characterized by a given class from abnormal behavior that is characterized by a second class. Thanks to this property, AIRS is more suitable for applications with detection purposes such as anomaly detection and fault detection than other classifiers like neural networks and SVM in which the training grants the same processing for all classes. Also, its training algorithm is analytically simple since it is not based on error minimization that is commonly subject to quadratic programming resolution. Presently, the AIRS is used as the core of the proposed off-line signature verification system, where skilled forgeries are assimilated to antigens that should be detected. Besides, Gradient Local Binary Patterns and Longest Run Features are introduced to respectively highlight gradient information and pixel distribution in signature images.

Experiments were conducted on public CEDAR and GPDS-100 datasets according to the writer-dependent approach. The comparison with the state of the art reveals that the proposed system can considerably surpass existing methods, notably for CEDAR dataset. However, although the AIRS training is simple, it has two main shortcomings. The first is related to set-up parameters involved for memory cells generation that need a careful tuning. This is done through several run-passes where parameters are varied until a minimal training error is achieved. The second limitation of AIRS is the use of k-NN decision in the verification stage, where the classification is evolved on memory cells without any further information from the training set.

Thereby, one experimental issue that is worth of investigation is the parameter independent implementation of AIRS. This could be done by performing simultaneous development of memory cells for all writers. In addition, AIRS performance can be significantly improved if the k-NN classification is substituted by a more reliable decision. Currently, we are planing to employ the dissimilarity training principle. This consists of replacing each signature by a vector that contains its dissimilarities with respect to memory cells. Then, dissimilarity vectors of training data will be used to develop a trainable decision function. Finally, one practical issue is related to the fact that in various real life applications, only genuine signatures are available to develop the verification system. So, an attractive idea consists of training AIRS as a one-class classifier that is devoted to recognize genuine signatures of each writer. In this case, the k-NN decision should be substituted by a suitable thresholded decision.

References

Batista, L., Granger, E., & Sabourin, R. (2012). “Dynamic selection of generative-discriminative ensembles for off-line signature verification”. *Pattern Recognition*, 45, 1326–1340.

Bayar, N., Darmoul, S., Hajri-Gabouj, S., & Pierreval, H. (2015). “Fault detection, diagnosis ans recovery using artificial immune systems: A review”. *Engineering applications of Artificial Intelligence*, 46, 43–57.

Bertolini, D., Oliveira, L. S., Justino, E., & Sabourin, R. (2010). “Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers”. *Pattern Recognition*, 43, 387–396.

Bharathi, R. K., & Shekar, B. H. (2013). “Off-line signature verification based on chain code histogram and support vector machines”. In *Int. Conference on Advances in Computing, Communications and Informatics (ICACCI’13)* (pp. 2063–2068).

Chen, S., & Srihari, S. (2006). “A new off-line signature verification method based on graph matching”. In Proceedings of *Int. Conference on Pattern Recognition (ICPR’06)* (pp. 869–872).

Chen, Y., Liang, C., Yang, D., Peng, L., & Zhong, X. (2010). “A handwritten character recognition based on artificial immune algorithm”. In Proceedings of *Int. Conference on Computer Application and System Modeling (ICCASM’10)* (pp. 273–276).

Dalal, N., & Triggs, B. (2005). “Histograms of orientated gradients for human detection”. In Proceedings of *Conference on Computer Vision and Pattern Recognition (CVPR’05)* (pp. 886–893).

Das, N., Reddy, J. M., Sarkar, R., Basu, S., Kundu, M., Nasipuri, M., & Basu, D. K. (2012). “A statistical-topological feature combination for recognition of handwritten numerals”. *Applied Soft Computing*, 12, 2486–2495.

Deng, P. S., Mark Liao, H. Y., Ho, C. W., & Tyan, H. R. (1999). “Wavelet-based off-line handwritten signature verification”. *Computer Vision and Image Understanding*, 76, 173–190.

Doroz, R., Porwik, P., & Orczyk, T. (2015). “Dynamic signature verification method based on association of features with similarity measures”. *Neurocomputing Journal*, 171, 921–931.

Fang, B., & Tang, Y. (2005). “Improved class statistics estimation for sparse data problems in off-line signature verification”. *IEEE Trans. on Systems, Man and Cybernetics*, 35, 276–286.

Favorskaya, M., & Baranov, R. (2014). “The off-line signature verification based on structural similarity”. *Smart digital futures, Edited by R. Neves-Silva et al.*, IOS Press, Netherlands, pp. 421–430.

Ferrer, M. A., Alonso, J. B., & Travieso, C. M. (2005). “Off-line geometric parameters for automatic signature verification using fixed-point arithmetic”. *IEEE trans. on Pattern Analysis and Machine Intelligence*, 27, 993–997.

Ferrer, M. A., Diaz-Cabrera, M., & Morales, A. (2015). “Static signature synthesis : A neuromotor inspired approach for biometrics”. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 37, 667–680.

Ferrer, M. A., Vargas, J. F., Morales, A., & Ordonez, A. (2012). "Robustness of off-line signature verification based on gray level features". *IEEE trans. on Information Forensics and Security*, 7, 966–977.

Findik, O., Babaoglu, I., & Ulker, E. (2011). "A color image watermarking scheme based on artificial immune recognition system". *Expert Systems with applications*, 38, 1942–1946.

Fischer, A., Diaz, M., Plamondon, R., & Ferrer, M. A. (2015). "Robust Score Normalization for DTW-Based On-Line Signature Verification". In *Int. Conference on on Document Analysis and Recognition (ICDAR'15)* (pp. 241–245).

Galbally, J., Diaz-Cabrera, M., Ferrer, M. A., Gomez-Barrero, M., Morales, A., & Fierrez, J. (2015). "On-line signature through the combination of real dynamic data and synthetically generated static data". *Pattern Recognition*, 48, 2921–2934.

Guerbai, Y., Chibani, Y., & Hadjadji, B. (2015). "The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters". *Pattern Recognition*, 48, 103–113.

Hamadene, A., Chibani, Y., & Nemmour, H. (2012). "Off-line handwritten signature verification using contourlet transform and Co-occurrence matrix". In Proceedings of *Int. Conference on Frontiers in Handwriting Recognition (ICFHR'12)* (pp. 343–347).

Huang, K., & Yan, H. (2002). "Off-line signature verification using structural feature correspondence". *Pattern Recognition*, 35, 2467–2477.

Hunt, R., & Qi, Y. (1995). "A multi-resolution approach to computer verification of handwritten system". *IEEE Trans. on Image Processing*, 4, 870–874.

Impedovo, D., Modugno, R., Pirlo, G., & Stasolla, E. (2008). "Handwritten signature verification by multiple reference sets". In Proceedings of *Int. Conference on Frontiers on Handwriting Recognition (ICFHR'08)* (pp. 19–21).

Jiang, N., Xu, J., Yu, W., & Goto, S. (2013). "Gradient local binary patterns for human detection". In Proceedings of *Int. Symposium on Circuits and Systems (ISCAS'13)* (pp. 978–981).

Justino, E. J. R., Bortolozzi, F., & Sabourin, R. (2005). "A comparison of SVM and HMM classifiers in off-line signature verification". *Pattern recognition letters*, 26, 1377–1385.

Kalera, M. K., Srihari, S., & XU, A. (2004). "Off-line signature verification and identification using distance statistics". *Int. journal of pattern recognition and artificial intelligence*, 18, 1339–1360.

Kiani,V., Pourreza, R., & Pourreza, H. R. (2009). "Off-line Signature Verification Using Local Radon Transform and Support Vector Machines". *Int. Journal of Image Processing*, 3, 184–194.

Kodaz, H., Ozsen, S., Arslan, A., & Gunes, S. (2009). "Medical application of information gain based artificial immune recognition system (AIRS): Diagnosis of thyroid disease". *Expert systems with applications*, 36, 3086–3092.

Kovari. B., & Charaf, H. (2013). "A study on the consistence and significance of local features in off-line signature verification". *Pattern Recognition Letters*, 34, 247–255.

Kumar, M. M., & Puhan, N. B. (2014). "Off-line signature verification : upper and lower envelope shape analysis using chord moments". *IET Biometrics Journal*, 3, 347–354.

Kumar, R., Kundu, L., Sharma, J. D., & Chanda, B. (2010). "A writer-independent off-line signature verification system based on signature morphology". In Proceedings of *Int. Conference on Intelligent Interactive Technologies and Multimedia (IITM'10)* (pp. 261–265).

Kumar, R., Sharma, J. D., & Chanda, B. (2012). "Writer-independent off-line signature verification using surroundedness feature". *Pattern recognition letters*, 33, 301–308.

Larkins, R. & Mayo, M. (2008). "Adaptive feature thresholding for off-line signature verification". In Proceedings of *23rd Int. Conference on Image and Vision Computing New Zealand (IVCNZ'08)* (pp. 1–6).

Laurentys, C. A., Palhares, R. M., & Caminhas, W. M. (2011). "A novel artificial immune system for fault behavior detection". *Expert systems with applications*, 38, 6957–6966.

Martinez, E. F., Sanchez, A., & Velez, J. (2006). "Support vector machines versus multilayer perceptrons for efficient off-line signature recognition". *Engineering Applications of Artificial Intelligence*, 19, 693–704.

Murshed, N. A., Bortolozzi, F., & Sabourin, R. 'a'. (1995). "Off-line signature verification, without a priori Knowledge of class w2. A new approach". In Proceedings of *3rd Int. Conference on Document Analysis and Recognition (ICDAR'95)* (pp. 191–196).

Murshed, N. A., Bortolozzi, F., & Sabourin, R. 'b'. (1995). "Off-line signature verification using fuzzy artmap neural network". In Proceedings of *Int. Conference on Neural Network* (pp. 2179–2184).

Nemmour, H., & Chibani, Y. 'a'. (2013). "Artificial immune system for handwritten Arabic word recognition". In Proceedings of *Int. Conference on Innovative Computing Technology (INTECH'13)* (pp. 463–466).

Nemmour, H., & Chibani, Y. 'b'. (2013). "Off-line signature verification using artificial immune recognition system". In Proceedings of *10th Int. Conference on Electronics Computer and Computation (ICECCO'13)* (pp. 164–167).

Nguyen, V., Blumenstein, M., & Leedham, G. (2009). "Global features for the off-line signature verification problem". In Proceedings of *Int. Conference on Document Analysis and Recognition (ICDAR'09)* (pp. 1300–1304).

Ojala, T., Pietikainen, M., & Harwood, D. (1996). "A Comparative study of texture measures with classification based on featured distributions". *Pattern Recognition*, 29, 51–59.

Parodi, M., & Gomez, J. C. (2014). "Legendre polynomials based features extraction for online signature verification. Consistency analysis of feature combinations". *Pattern Recognition*, 47, 128–140.

Plamondon, R., & Srihari, S. N. (2000). "On-line and off-line handwriting recognition: A comprehensive survey". *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 22, 63–84.

Radhika, K. R., Venkatesha, M. K., & Sekhar, G. N. (2011). "An approach for on-line signature authentication using Zernike moments". *Pattern Recognition Letters*, 32, 749–760.

Rivar, D., Granger, E., & Sabourin, R. (2013). "Multi-feature extraction and selection in writer-independent off-line signature verification". *Int. Journal of Document Analysis and Recognition*, 16, 83–103.

Ruiz-Del-Solar, J., Devia, C., Loncomilla, P., & Concha, F. (2008). "Off-line signature verification using local interest points and descriptors". In Proceedings of *the 13th Iberoamerican Congress on Pattern Recognition (CIARP'08)* (pp. 20–29).

Serdouk, Y., Nemmour, H., & Chibani, Y. (2014). "Topological and textural features for off-line signature verification based on Artificial Immune Algorithm". In Proceedings of *6th International Conference on Soft Computing and Pattern Recognition (SOCPAR'14)* (pp. 118–122).

Shanker, A. P., & Rajagopalan, A. N. (2007). "Off-line signature verification using DTW". *Pattern recognition letters*, 28, 1407–1414.

Soleymanpour, E., Rajae, B., & Pourreza, H. R. (2010). "Off-line handwritten signature identification and verification using contourlet transform and support vector machines". In Proceedings of *6th Iranian Machine Vision and Image Processing (MVIP'10)* (pp. 1–6).

Tang, S., & Goto, S. (2010). "Histogram of Template for Human Detection". In Proceedings of *Int. Conference on Acoustics, Speech and Signal Processing(ICASSP'10)* (pp. 2186–2189).

Timmis, J., & Neal, M. (2001). "A resource limited artificial immune system for data analysis". *Knowledge-Based Systems*, 14, 121–130.

Vargas, J. F., Ferrer, M. A., Travieso, C. M., & Alonso, J. B. (2011). "Off-line signature verification based on gray level information using texture features". *Pattern Recognition*, 44, 375–385.

Vargas, J. F., Travieso, C. M., Alonso, J. B., & Ferrer, M. A. (2010). "Off-line signature verification based on gray level information using wavelet transform and texture features". In Proceedings of *12th Int. Conference on Frontiers in Handwriting Recognition (ICFHR'10)* (pp. 587–592).

Watkins, A. B. (2001). "AIRS: A resource limited artificial immune classifier". *Master Thesis on computer sciences*, Mississippi state university, USA.

Yang, Y. (2011). "Application of artificial immune system in handwritten Russian uppercase character recognition". In Proceedings of *Int. Conference on Computer Science and Service System (CSSS'11)* (pp. 238–241).

Yilmaz, M. B., Yanikoglu, B., Tirkaz, C., & Kholmatov, A. (2011). "Off-line signature verification using classifier combination of HOG and LBP features". In Proceedings of *Int. Joint Conference on Biometrics Compendium (IJCB'11)* (pp. 1–7).

Zhang, W., Shan, S., Gao, W., Chen, X., & Zhang, H. (2005). "Gabor binary pattern histogram sequence (LGBPHS): A novel non-statistical model for face representation and recognition". In Proceedings of *10th Int. Conference on Computer Vision (ICCV'05)* (pp. 786–791).