Learning Iris Biometric Identities for Secure Authentication. A Neural-Evolutionary Approach Pioneering Intelligent Iris Identification[1]

NICOLAIE POPESCU-BODORIN, *Member, IEEE*
Mathematics and Computer Science Department
Spiru Haret University of Bucharest
Bucharest, ROMANIA
http://fmi.spiruharet.ro/bodorin/

Abstract: - This paper discuss the latest trends in the field of evolutionary approaches to iris recognition, approaches which are compatible with the task of multi-enrollment in a biometric authentication system based on iris recognition, and which are also able to ensure strong discrimination between the enrolled users. A new authentication system based on supervised learning of iris biometric identities is proposed here. It is the first neural-evolutionary approach to iris authentication that proves an outstanding power of discrimination between the intra- and the inter-class comparisons performed for the test database (Bath Iris Image Database).

Key-Words: - iris recognition, iris authentication, iris biometrics, iris biometric authentication.

1 Introduction

Nowadays, after years of important studies and contributions, such as those of Wildes [1] and Daugman [2],[3], or the newer developments undertaken at CASIA [4],[5], University of Bath [6]-[9], NIST [10],[11] and Notre Dame University [12]-[14], could appear the temptation to believe that iris recognition is a closed domain. We *strongly* disagree with this point of view. The motivation behind one of our recent works [15] was the belief that the major improvements in iris recognition will come from the field of artificial intelligence. One challenge defined in that paper (namely C8:"*Build an exploratory supervised intelligent agent for iris recognition*") is how to find a way of automating the process of searching for new methods for iris segmentation and for iris matching. In the same paper [15] we said that it is not clear at all why the neural approaches to iris encoding and matching usually do not lead to the same performances as those obtained in the classical approaches based on the direct comparison of binary iris codes. We also said there that in terms of artificial intelligence, a way to find new methods for iris encoding and matching could be to define a neural network architecture or a heuristic algorithm able to replicate currently available iris recognition results obtained by comparing the iris codes directly. Such an approach would assume that each enrolled identity is stored as a trained memory or as a feature vector and would be able to classify candidate iris codes as well as possible by preserving or improving the quality of the separation between genuine and imposter score distributions in terms of False Accept/Reject Rates.

This paper is a successful proof of all of these ideas. Now we know that the classical neural architectures (from Multi-Layer Perceptron to Self Organizing Maps) are too general to be well adapted for achieving biometric purposes. We also know that genetic programming can be used to create (or to optimize) program sources for well specified goals. Genetic programming techniques were integrated into the Analyzer/Advisor Module within NPB Iris Recognition Generic Experimental Model [16] and helped us finding all the novelties which follows to be discussed here. Also, using the infrastructure described in [16] enabled us to draw the most important conclusions which led to the current neural-evolutionary approach: in order to be of high quality, the process of learning biometric identities must be supervised, must be adaptive, and must keep separate tracks of the rewards and punishments occurred during instruction by encoding the history of positive and negative events into two different memory tables. Regardless the type of neural networks used in our simulations (and in the last three years we did more than ten thousands simulations on Bath Iris Image Database), when the learning process encodes experience on unspecialized neurons (punishments an rewards are memorized on the same memory table), the obtained model rapidly lost its power of generalization: the learning data were correctly recognized but the correct classification of test data failed too often.

[1] **Draft Manuscript in Preparation for a Joint S.V. Chapter with V.E. Balas**

We also know now that in order to be the main member of a one-to-many relation with the candidate iris codes (one identity/one memory should be able to recognize multiple instances of binary iris codes) an identity must have a bigger informational entropy than the candidate binary iris codes, in the same way in which a class encodes more entropy than its own members. If this wouldn't be true, then one solution for defining a suitable encoding of the biometric identities should exists in terms of finding some binary matrices as centroids for the sets of iris codes extracted for the same person. But this hypothesis has not been validated in our experience so far. Hence we assumed that the dimension of stored identities must differ with at least one order from that of the candidate iris codes. Even so, finding these centroids in a richer space (of increased entropy) through k-means or SOM type algorithms would mean storing a memory on unspecialized neurons.

On the other hand, strictly from the point of view of artificial intelligence, it is absolutely logical that *a recognizer (classifier/discriminator) object encodes more entropy than each of the recognized (classified/discriminated) objects*[2]. The difference between them is nothing more, nothing less and nothing else than (computed) *intelligence* - or in other words, encoded (quantized) entropy obtained by extracting knowledge from data through specific computational means. Hence now we understand in our own way the motivations behind the recent changes made by Daugman [10] in its own proprietary iris code format, and also the necessity of this change.

2 Terminology and Problem Formulation

All data and all techniques reported in this paper are about authentication of persons based on comparing iris biometric binary templates to learned (enrolled) biometric identities. An *identity* is a collection of data (a memory) stored for each enrolled user of a biometric system. The identities are learned when the system runs in calibration mode, from a set of iris biometric templates (binary iris codes) further referred to as "*learning dataset*" (the learning data contain correctly labeled binary templates). After the learning is done, the system goes into regular exploitation mode. In this stage, different users (enrolled or not) will expose their iris to the acquisition device which will process the current iris image up to a binary code. By claiming an identity - "I am the enrolled user number 354", the user asks the system to verify the matching between the binary template extracted from the current image of his iris (*candidate iris code*) and the identity stored under the unique ID number 345. As a result, the biometric system could accept the claim (if the candidate iris code and the claimed identity are found to be sufficiently similar) or could reject it. The claims could be positive – "I am", or negative "I'm not", honest (the enrolled user claims its own identity, or if he is not enrolled claims that he isn't) or forged (the user claim something false hoping to cheat the system).

2.1 False Accept/Reject, True Accept/Reject

A *False Reject* happens when the biometric system fails to recognize correctly an honest positive claim or a forged negative claim.

A *False Accept* occurs when the biometric system fails to recognize correctly an honest negative claim or a forged positive claim.

A *True Reject* happens when the biometric system recognize correctly an honest negative claim or a forged positive claim.

A *True Accept* occurs when the biometric system recognize correctly an honest positive claim or a forged negative claim.

When a biometric system is simulated using a database of eye/iris images (or iris codes), some of them are used to learn identities (*learning dataset*), and all of the other (which form the *test dataset*) for testing the quality of the learning, i.e. the power of generalization achieved through learning. During a simulation, the templates within the *test dataset* play the role of *candidate iris codes* and those within the learning dataset are *training examples* or, in other words, *enrolled templates*.

A training function or a training procedure (a feature extractor / a learning rule) is a computational routine that somehow assemble the information available in all training examples into a new data structure, namely the digital (enrolled) identity.

The simplest biometric system is based on single-enrollment: there is only one template enrolled under an ID number, the training function is the identical function, and consequently the enrolled identity for the person who owns that ID number coincides with the single enrolled template.

In a multi-enrollment biometric system, at least two binary templates are enrolled under the ID number of the user. The training function/procedure

[2] We will let the informed reader to appreciate if the domain of Iris Recognition is or is not still in its infancy, if such things about iris codes and biometric identities are told here for the first time.

is no longer trivial and the digital identity learned from the enrolled templates will differ from them.

The definition given above for the False Accept/Reject cases are our definitions. Daugman proposed a different interpretation of these measures. For example, in his view the False Accept Rate in *identification* (one-to-many comparison) is different than the False Accept Rate in *verification* (one-to-one comparison). In his view, identification and verification are two different things. Daugman supposed that the difference between identification and verification is mainly the type of comparison allowed in the system: one-to-many comparisons are allowed in identification systems and only one-to-one comparisons are allowed in verification systems. This assumption inevitably leads to logical inconsistencies (because in this context *verification* means enrollment without proper validation).

As a precaution, in our authentication system one-to-all comparisons are not just allowed, but mandatory each time when a negative claim such "I'm not enrolled" occurs. The moment when a new enrollment takes place is a crucial one for preserving logical consistency of the biometric system. This is why, in our approaches [15]-[17], the False Accept/Reject Rates are considered to be global quality measures for a recognition technique when it is tested on a given database and are always computed by making the statistics of *all-to-all* comparisons (exhaustive testing on the database). The possibility to enroll the same person twice, just because one-to-all comparison would be formally not allowed, does not exist in our models.

The first set of question to be answered here is the following:

- *Why to choose a multi-enrollment system?*
- *How to select the enrollment templates (how to delimitate/build the learning dataset)*?
- *How to learn a digital biometric identity from the binary templates enrolled under the same ID number?*
- *How to match a digital identity to a candidate iris binary code or vice versa?*

2.2 Why multi-enrollment?

There are two main reasons for choosing multi-enrollment. Firstly, multi-enrollment ensures that the biometric identity will be trained with different hypostases of the same iris (different pupil dilations, illumination, blur, distortions, and occlusions). As a result, the digital identity will be much able to overcome *intraclass variability* and to recognize more hypostases of the same iris while still preserving the higher similarity scores possible.

Secondly, Baker, Bowyer and Flynn [12] documented the problem of template aging. Multi-enrollment is a recommended policy for ensuring a smooth variation of the iris identities over time.

3 Proposed Method

3.1 Iris segmentation and encoding

The segmentation and encoding techniques must be used in order to extract a binary iris code for each eye image from the database. The segmentation procedure used here is CFIS2 [17] (Second version of Circular Fuzzy Iris Segmentation) which is a two step segmentation procedure. Firstly, the pupil is found (Fig.1 in [16]). Secondly, the image is unwrapped through a pupil-centric polar coordinate transform (Fig.2. in [16]) and the limbic boundary is approximated (Fig.1.a. in [17]). The result is an unwrapped iris segment, further used as an input for the encoding procedure, through which a binary iris code is generated.

The encoders used in this paper are the following two: Log-Gabor Encoder (LGE, [17]) and an encoder based on Haar Wavelet (noise filtering) and Hilbert Transform (phase encoding), abbreviated HH1 and introduced in [17].

3.2 Selecting and aligning the enrollment templates

The criterion used here for selecting the enrolled templates (learning dataset) was pupil dilation. In order to ensure that each identity will be trained with different hypostases of more dilated or contracted pupil, the following selection procedure was practiced: there are 20 images for each eye in the database; hence, excepting the cases of failed segmentation, there are 20 binary iris codes in the template database. Five of them, chosen from the first ten, were used as learning examples. Those five binary iris codes are associated with five eye images chosen such that to preserve (as much as possible) the diversity of pupil dilation as it was measured in the set of the first 10 images. For each subject in the eye image database, the following optimization problem was solved heuristically, through randomization of selected indices:

$$S_5 = \min_{s \in C_{10}^5} \left(\| [M_s \,,\, 2*S_s^{1/2}] - [M_{10} \,,\, 2*S_{10}^{1/2}] \| \right)$$

where (M_S, S_S) and (M_{10}, S_{10}) are the means and the standard deviations of the vectors:

(PupilRadii)./(IrisRadii)

computed for the current selection of indices s, and for the first 10 images corresponding to the same eye, respectively (where './' signifies component to

component division).

After selecting the enrolled templates, for each eye represented in the database, there are 5 images for training and 15 images for testing. Hence, excepting the cases of failed segmentation (3 failures in a total of 1000 eye images), there are 20 binary iris codes in the template database: 5 of them used for training and the other for testing.

From each set of 5 images used for training, the first one is considered to be the unrotated witness, in order to unify the angular alignment of the entire set of images taken for the same eye. The iris codes were tested for angular alignment using rotations in range of ± 5.625 hexadecimal degrees with respect to the witness.

3.3 Learning biometric identities

Learning biometric identities is a problem of *artificial intelligence* and *evolution*. Why is that? Let us take an instant picture of a biometric system. We'll see there a *relational collection* of *ID numbers* (unique numerical identifiers of the users), *binary templates* (sub-collection of hypostases / samples taken for the recognized / classified / discriminated objects), *digital identities* (discriminator / classificator / recognizer objects), optional strings and, possibly, other objects (Fig.1).

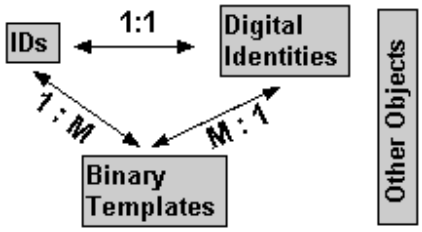

Fig.1. A biometric system frozen in time

3.4 The differences between an intelligent biometric system and a regular one.

Figure 1 shows an instant picture of a biometric system, but the truth is that a biometric system, in order to be *logically complete* and *logically consistent*, must be a *non-stationary* system, must be a system which adapts / changes itself over time. As a logical consequence, our opinion is that in a biometric system, it is mandatory to consider that the time is ticking when a new enrollment occurs - the enrollment being the stress factor that demands adaptation, which in its turn, is impossible to achieve without intelligence[3]. Otherwise, if the enrollment is not accompanied by adaptation, it is just a matter of logical consequence to expect that *contradictions* will be reached very rapidly. The proof of this thing is of colossal importance for the future of biometry, and it was already made in the year 2000 by Daugman, in [2] (see the formula (16) and the subsequent example of that formula in [2]). Still, it seems that the correct interpretation (the logical meaning) of Daugman's demonstration lied misunderstood, unexplored and unexploited, ever since. In Daugman's view, a *verification* system is based on one-to-one (binary candidate to claimed identity) comparisons. Hence, by design, Daugman's *verifier* systematically fails to adapt itself when a new enrollment occurs.

On the other hand, in a *logically consistent biometric system*[4] (LCBS), one hypostasis of the adaptation triggered by enrollment is a recalibration made in a certain way such to preserve a comfortable distance between the inter-class and intra-class distribution of scores computed for all enrolled users (this implicitly means allowing all-to-all comparisons). We called this recalibration "*consistent enrollment*". "Consistent enrollment" and "adaptation" are two equivalent semantic labels:

- the former is a name for a binary value of truth (consistent/inconsistent) in a second order binary logic language over the set of enrolments, or even a name for a modal and fuzzy value of truth in a second order 3-valent modal logic language (consistent / inconsistent / unknown) – in case in which we aim to model incertitude.

- the latter is a name of a generic group of methods of Artificial Intelligence enabled to change the current state of the biometric system to a new state in which the system comfortably discriminate between the newly enrolled identity and all the older ones, previously enrolled.

In a LCBS, if the current enrollment jeopardizes system consistency, it will be dropped immediately in a quarantine where it stays until the system evolve (recalibrate itself) to a new state adapted to

[3] This is a simple, informal, but intuitive proof telling that the future of biometry as a science (including iris recognition) will be inevitably shared between the theories and applications of logic, artificial intelligence, evolutionary computation and non-stationary systems. The concept of logically sound, logically complete, intelligent, adaptive, evolutionary (non-stationary) biometric systems, which is introduced here for the first time, will prove to be a milestone in iris recognition. We are currently working on this.

[4] A logically consistent biometric system is one whose internal logic is consistent - meaning that a false affirmation of biometry will never be proved (will never be computed / observed) in the system. For example, in a logically consistent biometric system (which is an idealized concept), the False Accept is not possible.

comfortably discriminate between the newly enrolled identity and all the older ones, previously enrolled. On short, a LCBS stays consistent through adaptation (supervised and consistent enrollment). If the current enrollment fits the current safety limits of the system, the adaptation is the identical function mapping the current state of the system to itself.

Neither *consistent enrollment* nor *adaptation* are among the possibilities of Daugman's *verifier*. This is why it is naturally to assume that Daugman's verifier will face, eventually, situations of logical inconsistency expressed by Daugman as verification *false accepts*. Daugman established a formula which correlates *verification false accepts* and *identification false accepts* in a given number of trials. His conclusion (pp.6 in [2]) is that "*when searching a database of size N an identifier needs to be roughly N times better than a verifier to achieve comparable odds against a False Accept*" and "*even for moderate database sizes, merely 'good' verifiers are of no use as identifiers*".

We propose the following reformulation: in a biometric system in which the *consistent enrollment* (adaptation / learning) is not guaranteed, chances for facing inconsistency in the form of False Accept grows nearly linear with the number of trials (with database size).

By contrast, logically consistent biometric systems (LCBS) behave totally different. The next section of the paper will show that *an intelligent verifier* is also an *identifier*, a system which proves that at least for moderate database sizes (such is the case of Bath Iris Image Database) an intelligent verifier is also reliable as an identifier.

3.4. Artificial neural network support for consistent enrollment.

By design, our neural network for biometric purposes fits into the following restrictions:

- The learning process doesn't rely on unspecialized neurons. Discriminator memory is trained only on positive examples. To match this rule, each enrolled identity (a trained memory) stores information for both positive and negative discrimination in separate zones. It memorizes what an iris is, but also what it isn't, both types of information being extracted only from positive learning examples, i.e. only from those enrollment templates stored under the ID of currently trained memory.
- The learning process resumes each time when a new enrollment occurs (enrollment triggers evolution).
- The neural network (ANN) works in two modes: *learning* and *testing*. During the training stage, the neural network acts as a feature extractor by learning digital identities from the enrollment templates, whereas in the second mode, the ANN is used either as a verifier, or as an identifier.

The minimal architecture of an artificial neural network for iris biometric purposes is described in the following figure:

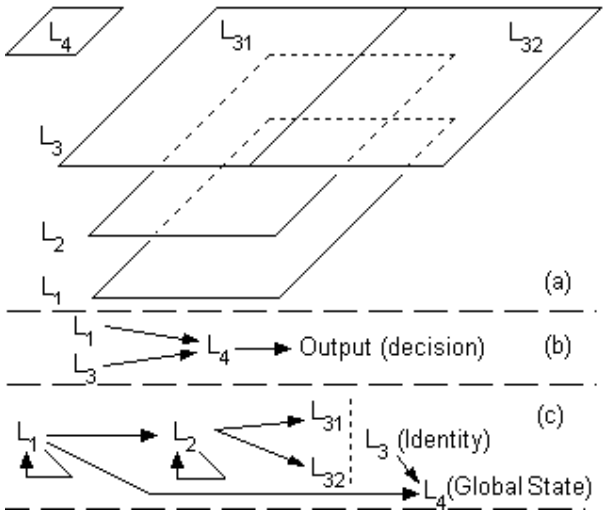

Fig.2. ANN Structure (a), Information flow during verification (b), Information flow during training (c).

The first layer of the ANN is responsible to load and to keep the current learning example. The third layer will encode the digital identity. It consists of two parts: L_{31} is a positive discriminator which learns what the current example is, whereas L_{32} learns what it isn't (the negative discriminator).

If the current stage is a learning/training step, the input of the ANN is the current learning example (enrolled iris binary code) and the output is a digital identity which follows to be written in a database.

If the current stage is a verification (a test), the input consists in a candidate template (one binary template from the *test dataset*) and in an enrolled digital identity loaded on L_3. The global activation (ga) in this case will be the number:

$$ga = \left\langle L_{31}, L_1 \right\rangle - \left\langle L_{32}, L_1 \right\rangle, \quad (1)$$

i.e. the difference between a neural excitation (voting for similarity between the candidate stored in L_1 and the enrolled identity stored in L_3) and a neural inhibition (voting for dissimilarity), where the angular parentheses signify partial activation functions (the positive activation and the negative activation – or inhibition, respectively). In this case, the output is a binary value depending on the relation between the global activation value and two thresholds (one for recognition, one for non-recognition) written in L_4.

3.5. The prototype of Intelligent Iris Verifiers

The procedure describing how a simple prototype of intelligent iris biometric system works is the following:

ANN Based Evolutionary Intelligent Iris Verifier:
(N. Popescu-Bodorin, January 2011, IIV Description)

1: **Global State**: thresholds, mode (testing or training);
2: **Primary Input:** chosen mode (testing OR learning);
3: **Secondary Input:** (L_1,L_3) for testing OR L_1 for training;
4: **If** testing mode is on,
5: Compute decision: d = ga;
6: **Else,** (Evolution triggered by enrollment: Quarantine, then Individual Evolution or Systemic Evolution or Failure)
7: **Quarantine** the current enrollment
Begin enrollment simulation and analysis
8: **Try** (for a while) to evolve new identity in the generation of all identities previously enrolled,
9: OR **Fail** AND **Try** (for a while) to evolve (in a space of higher entropy) a new generation of identities - including the identity which attempts to enroll,
10: OR **Fail** AND:
11: **Keep** the current enrollment quarantined
12: **Apply** whatever custom routine is associated to the failure event,
13: OR **Succeed** AND:
14: **Finish** enrollment simulation and analysis;
15: **Qualify** the current enrollment as being consistent,
16: **Change** the global state of the biometric system to the newly simulated consistent state;
17: **End;**
18: **Output: d** (current decision) for testing mode OR
19: L_3 (current trained identity) for training mode.

3.5. Evolutionary network – the key factor in achieving superior levels of intelligence.

Fig.3 shows the exact histograms of all intraclass / interclass scores obtained by comparing *all* enrolled identities *to all* binary codes from the *learning dataset* (50 eyes – 50 identities, 5 training images for each eye, 250 binary iris codes) and it gives us an image about the properties which qualify a biometric system as being *intelligent* and *trained*. It can be seen there that, with respect to the *learning dataset*, our system proves a crisp understanding of what it means to be a genuine comparison (it qualifies such comparisons with unitary similarity score), and a fuzzy understanding of what it means to be an imposter comparison - because it qualifies such comparisons with (fuzzy) similarity scores belonging in [0,1/2). Still, for 33.3% of all imposter pairs formed with training examples, the system performs a crisp recognition (by mapping these pairs to the null similarity score).

All of these facts (described in the previous paragraph and also in Fig.3) are related to the lines 8-10 within the functional description of the *ANN Based Evolutionary Intelligent Iris Verifier* (further referred to as "**IIV** description"). The evolution of IIV does not alter its ANN structure. The learning rule is the one that changes under the pressure of

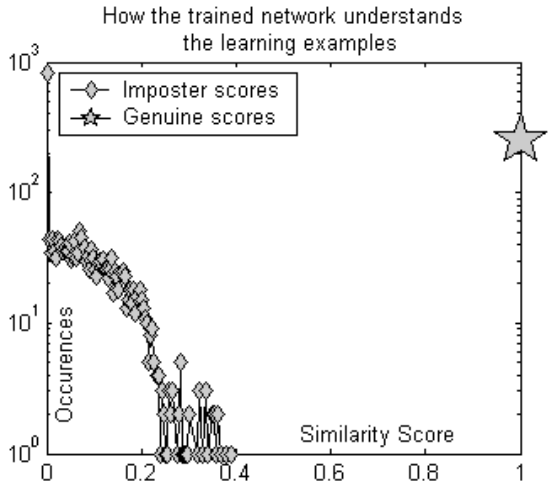

Fig.3. The manner in which an Intelligent Iris Verifier recognizes the binary iris codes on which was trained (learning 50 identities from 250 genuine comparisons, and 2'450 imposter comparisons).

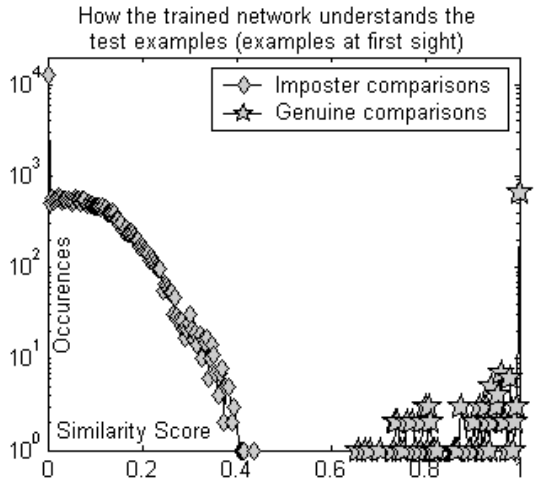

Fig.4. The manner in which an Intelligent Iris Verifier recognizes binary iris codes that it has not seen during the training stage (50 learned identities tested through 747 genuine comparisons and 36'603 imposter comparisons).

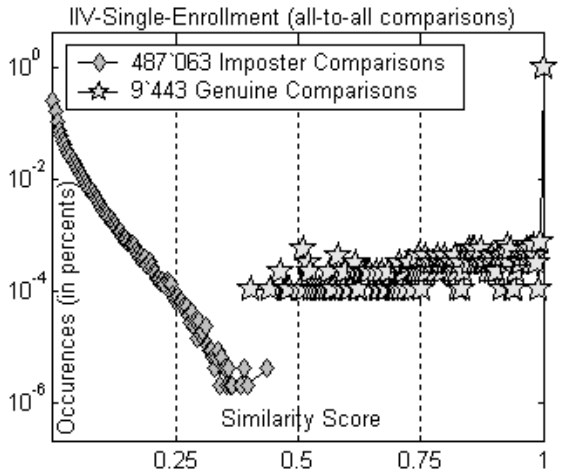

Fig.5. The manner in which the identities evolved by the Intelligent Iris Verifier "**filters**" the apparent statistical landscape [2] (induced by compressing uint8 iris images to binary iris codes) and recovers the fuzzy meaning of two concepts: "genuine" and "imposter" comparisons.

those new enrollment requests that have the potential to jeopardize system consistency. Even if is unusual, this comes very naturally: if the current space of identities becomes incompatible with an imposed safety standard, the identities must migrate in a new space, and consequently, the customized arithmetic formal language underlying the computation of the identities must be evolved to an extension of its, an extension enabled to describe the computation of the migrated identities. Previously, we said that for IIV the time is ticking when a new enrollment occurs. Hence, the system ages, and now we see that as it ages, it becomes a more experienced learner by evolving/updating its own learning rule.

Among the parts of our Intelligent Iris Verifier (see "other objects" in Fig.1), we designed a dictionary of searchable arithmetic expressions which allows us to construct learning rules, in real time. Each learning rule is further implemented on the hidden layer L_2 of the ANN (see Fig.2).

To "evolve a new identity in the generation of all identities previously enrolled" (line 8 in IIV description) means that without changing the learning rule the system computes an identity from the set of 5 binary codes currently submitted to enrollment. Then the system tests if the enlarged set of identities is compatible with the restrictions of (C 7.1.1), illustrated in Fig.3. If the test succeeds, the evolution materializes through the creation of a new individual in the current space of identities. This is what we called *individual evolution* - an asynchronous differentiation of a single individual of a given population, made by training his memory to store the consciousness of individuality.

If the test fails (see for example the genuine comparisons scored other than unitary in Fig.4), then the failure triggers the change of learning rule, which on its turn leads to the evolution of all enrolled identities. This is what we called *systemic evolution* - a synchronous "*mass evolution*" of an entire population of individuals which redefine their identities on new coordinates that fits within the dynamic consciousness of an extending group.

Hence, the lines 8 and 9 from IIV description tell that the *adaptation* is achieved through *individual* or *systemic* evolution.

One of our previous affirmations (see the challenge C 7 in [15]) is that we still consider the iris encoding and iris matching as being two open problems in iris recognition. Now it is time to refine this topic by bringing new elements into the spotlight: at each enrollment demanding systemic evolution, in order to find the new learning rule (that

new rule adapted to the enlarged set of identities) the following sub-problems of (C7) must be solved:

(C 7.1): *Find evolutionary methods for iris encoding;*

(C 7.1.1)*: Given the current enlarged set of identities, given the dictionary of arithmetic expressions, find a function which satisfies the restrictions:*
- *It must be well-formed through concatenation between legal arithmetic 'genes' from the dictionary.*
- *It must prove a crisp understanding of what it means a genuine comparison, i.e. all genuine pairs formed with elements of learning dataset must be mapped to unitary scores (see the histogram of all genuine comparisons in Fig.3).*
- *It must prove a fuzzy but still consistent understanding of what it means an imposter comparison, i.e. all imposter pairs formed with elements of learning dataset must be mapped to scores in* [0, 1/2).

Fig.4 shows the exact histograms of all intraclass / interclass scores obtained by comparing *all* enrolled identities *to all* binary codes from the *test dataset* (examples at first sight). It gives us a visual representation for the quality of the training by showing how much power of generalization the trained Intelligent Iris Verifier proves:
- For 34.14% (12`498) of all imposter pairs formed with test examples, IIV performs a *Crisp Reject* by mapping these pairs to the null similarity score.
- For 65.86% (24`105) of all imposter pairs formed with test examples, IIV performs a *Fuzzy Reject* by mapping these pairs to scores within (0, 1/2).
- For 87.82% (656) of all genuine pairs formed with test examples, IIV performs a *Crisp Accept* by mapping these pairs to unitary score.
- For 12.18% (91) of all genuine pairs formed with test examples, IIV performs a *Fuzzy Accept* by mapping these pairs to scores within (1/2, 1).

Summarizing, IIV achieves 100% correct recognition of 39`053 unique imposter pairs (2`450 pairs formed with evolved identities and elements of the *learning dataset*, 36`603 pairs formed with enrolled identities and the elements of *test dataset*). It also achieves 100% correct recognition of 997 unique genuine pairs (250 pairs formed with evolved identities and elements of the *learning dataset*, 747 pairs formed with enrolled identities and the elements of *test dataset*)

4 New safety standards for logically consistent biometric purposes

Definitions (N. Popescu-Bodorin):

1) A biometric system has/gives/is/induces:

i) a **consistent crisp binary safety model** - if it is able to prove crisp understanding of two words (concepts) – *imposter* and *genuine* comparisons, by scoring them all into {0, 1}.

ii) a **fuzzified binary safety model** - if it is able to prove a fuzzified binary understanding of intra-class and inter-class comparisons, by scoring them all into [0, 1].

iii) a **consistent fuzzified binary safety model** - if it is able to prove a fuzzy but still consistent binary understanding of inter-class and intra-class comparisons, by scoring them into [0, 0.5] and (0.5, 1], respectively.

2) A fuzzified binary safety model proves:

i) **True Accept Consistency**, if the scores associated to Accept can not be obtained by comparing different irides.

ii) **True Reject Consistency**, if any pair of irides scored as a fuzzy reject is in fact a pair of different iris images.

It can be seen in Fig.4 that the proposed *Intelligent Iris Verifier* (which is a multi-enrollment system) has a *consistent fuzzified binary model* which can be transformed in a *consistent crisp binary safety model* through a simple defuzzification of the similarity score.

Solving optimization problems like (C 7.1.1) means heuristic optimization through genetic algorithms. There are many solutions to (C 7.1.1) but relatively few of them prove generalization capacities (few of them are *logically and semantically consistent solutions*). There is not enough space here for detailing the reasons why Daugman's *verifier* [2], Hollingsworth-Bowyer-Flynn *best bits matcher* [14], Dong-Tan-Sun *best bits matcher* [18], and our previously proposed multi-enrollment systems [17] also, all of them are strongly unoptimal solutions of the problem (C 7.1.1). In fact, all of them are weak solutions for drastically weakened optimization problems derived from (C 7.1.1). We won't hesitate to write on demand a separate paper on this topic. Here, it is

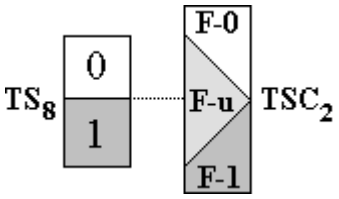

Fig.6. Transporting the binary truth values of the affirmations about the similarity between uint8 codes of dimension d (from TS_8) to fuzzy values (F-1 - Fuzzy 1, F-0 - Fuzzy 0, F-u - Fuzzy unknown) or fuzzy modal values (Most Probable Identical Codes, Most Probable Different Codes, Uncertain) of truth from TSC_2. See Proposition 1 and the subsequent comments.

more important to formulate the following new challenge:

(C 7.1.2): *Given a logically and semantically consistent iris verifier as solution of (C 7.1.1), evolve a model for fuzzy intelligent understanding of iris identification while preserving consistency as much as possible.*

The results obtained by answering this new challenge are illustrated in Fig.5.

It can be seen there that the identities evolved by IIV "attract" the binary iris codes (generated with Haar-Hilbert encoder HH1 [17]) into a space where recognition is no longer a statistical event, but a logical one, with precise (and natural, and observable) causality, a space in which a *simple iris recognition "theory" written in binary logic, or in a fuzzified binary logic,* (see pp. 121 in [17]) is *consistent*. The exact meaning of this term will be illustrated below. Until then, its opposite is discussed:

Proposition 1 (N. Popescu-Bodorin):

Let's consider these:
d is a given dimension (512x32, for example).
C_8 is the set of all uint8 codes of dimension d.
C_2 is the set of all binary codes of dimension d.
TS_8 is a consistent and complete theory of similarity over C_8 (a theory over a second order language of binary valued affirmations about the similarity between uint8 codes of dimension d.
TS_2 is a consistent and complete theory of similarity over C_2 (a theory over a second order language of binary valued affirmations about the similarity between binary codes of dimension d.

Then:
There is no way to define an isomorphism between TS_8 and TS_2.

The elementary argument for the above proposition is the difference between the numbers of elements in the sets TS_8 and TS_2. Behind this simple fact is a deeper understanding of what happens with the Boolean algebras underlying TS_8 (or C_8) and TS_2 (or C_2). It is known that any Boolean algebra generates a subsequent logic which is called here *the intrinsic logic* of that Boolean algebra. If *f* is a surjective function from C_8 to C_2 which completely covers C_2 and transports the Boolean algebra (underlying the complete and consistent TS_8 theory) from C_8 into a Boolean algebra TSC_2 over C_2 then the *intrinsic logic* of the transported Boolean algebra is inevitably *fuzzy* (or modal), *inconsistent* and *incomplete*. Fig.6 shows what is happening in such a case: the crisp binary values of truth from TS_8 are inevitably fuzzified by a binary compression. The fuzzy understanding of similarity is inconsistent because there are different uint8 codes that matches equal chances to be or not to be qualified as being similar in TSC_2 (if F-u means equally probable) or matches null chances to be qualified as being non-similar in TSC_2 (if F-u means "any other way that F-0 and F-1").

Hence, when a space of uint8 matrices is compressed to a space of binary matrices of the same dimension, there is always a biometric truth from the initial space which is no longer observable in the compressed space. Consequently, the biometric theory migrated into the compressed space (TSC_2) is incomplete.

On the other hand, in the above example a pair of codes is seen in TSC_2 differently than it is in reality (in TS_8). Consequently, the biometric theory transported in the compressed space is inconsistent (it can prove something unreal).

Therefore, logically consistent biometric *identification* in TS_8 (for the elements of C_8) will never be achievable in the space of binary compressed codes underlied by the transported biometric theory TSC_2. On the other hand, in TSC_2 *verification* [2] is possible, but still logically inconsistent, despite the existence of a suitable choice of the code dimension which induces a statistical decision landscape [2] over a given set of binary iris codes.

Poor acquisition discipline is a kind of compression, or even worst, a way of losing the original information because of a mixed effect of: overwriting the original with ambient noise, occluding some areas, improper quantization, etc.

Hence, poor discipline in image acquisition is a ticket to inconsistency. It will never be compatible with a complete and consistent theory or with a consistent practice of iris recognition.

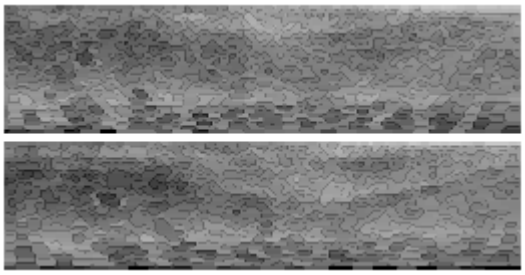

Fig.7. True Reject Consistency: IIV-SE agent classifies correctly (rejects) those hypostases of the same iris which are very different. Are these hypostases of the same iris sufficiently similar to be scored with a Fuzzy Accept? IIV-SE agent tells that these two hypostases can't be matched – and this is the truth, they are different.

Let us return now to the fact that iris recognition theory, as is seen by the IIV-Single-Enrollment (IIV-SE) agent, is *consistent*. In its numerical language (see Fig.5), IIV-SE tells us that:

- For 97% (9`160) of all (9`443) genuine comparison, it performs a *Crisp Accept* by mapping these comparisons to the unitary similarity score.
- For 2.93% (276) of all (9`443) genuine comparisons, IIV-SE performs a *Fuzzy Accept* by mapping these comparisons to scores within (0.5, 1).
- For 0.0741% (7) of all (9`443) genuine comparisons, IIV-SE performs a *Fuzzy Reject* by mapping these comparisons to scores within (0.4023, 0.5].
- For 100% (487`063) of all imposter comparisons, IIV-SE performs a *Fuzzy Reject* by mapping these comparisons to similarity scores within (0, 0.4368).

There are two important aspects regarding the results of all-to-all comparisons computed by IIV-SE agent:

- Firstly, as the number of comparisons grows (the database enlarges) the logarithmic histogram of all impostor scores runs for nearly vertical asymptotic trends in 0 and 0.5. This behavior ensures that any accept produced by the system is a True Accept, or in other words, IIV-SE proves ***True Accept Consistency***. Hence, what seemed like a property that only an idealized system may have (LCBS – a theoretical concept of a Logically Consistent Biometric System), it is now ascertained on the basis of a test with real data from University of Bath Iris Image Database (UBIID, Fig.5). Obviously, while tested on UBIID, IIV-SE has not produced any False Accept.
- Secondly, the apparent cases of False Reject are in fact cases of True Rejects, or in other words, IIV-SE proves ***True Reject Consistency***. Because of accumulated errors (pupil center, iris center, pupillary boundary, and limbic boundary) it is possible to encounter the situation in which two unwrapped uint8 irides are two very different hypostases of the same iris. A consistent matching technique can not overcome localization and segmentation errors. Hence, it is naturally that IIV-SE rejects this kind of pairs. Such an example is given in Fig.7. For that pair of very different hypostases of the same iris IIV-SE agent computes a similarity score of 0.4023. This proves two things: the index of genuine comparisons can be accidentally altered through accumulated errors of iris preprocessing - on the one hand, and IIV-SE is sufficiently intelligent to detect these cases – on the other hand.

IIV-SE achieves consistent iris recognition (True Accept Consistency, True Reject Consistency) and an objective evaluation of the image database: UBIID database contains good quality images on which consistent practice of iris recognition is possible. This means that on UBIID, both IIV systems described here (multi / single enrollment) are both consistent *biometric verifiers* and consistent *biometric identifiers*. We are wishful to cooperate for testing if and what other databases match these properties (i.e. prove an acquisition standard compatible with a logically consistent approach to iris recognition) but we will never again waste our time searching for truth in logically inconsistent worlds such is the theory of iris recognition when "no matter how low quality" replaces a credible standard of image acquisition.

IIV-SE also achieves an objective evaluation of iris segmentation: besides the three cases of failed segmentation, IIV-SE detects another seven cases of erroneous segmentation. Overall efficiency of the segmentation procedure (CFIS2, [17]) can be now reevaluated at 99%.

4 Conclusion

This paper is a successful proof that future of iris recognition (including iris-based identification) will be inevitably marked by multi-enrollment, and by the newly proposed concepts of consistent, intelligent, adaptive, evolutionary biometric systems. It is also clear that the future of biometry as a science (including iris recognition) will be inevitably shared between the theories and applications of logic, artificial intelligence, evolutionary computation and non-stationary systems. All of these are necessary instruments in

achieving secure iris-based or biometric-based identification.

Acknowledgement

We thankfully acknowledge the University of Bath and Prof. D. Monro for granting us access to the iris database.

References:

[1] R. Wildes, *Iris Recognition - an emerging biometric technology*, Proc. of the IEEE, vol. 85, no. 9, pp. 1348-1363, Sep. 1997.

[2] J. Daugman, Biometric Decision Landscapes, Technical Report No. TR482, University of Cambridge, 2000.

[3] J. Daugman, *New methods in iris recognition*, IEEE Trans. Systems, Man, Cybernetics B 37(5), pp 1167-1175, Oct. '07.

[4] L. Ma, T. Tan, Y. Wang, D. Zhang, *Personal Identification Based on Iris Texture Analysis*, IEEE TPAMI, Vol. 25, No. 12, pp.1519-1533, 2003.

[5] T. Tan and L. Ma, *Iris Recognition: Recent Progress and Remaining Challenges*, Proc. of SPIE, Vol. 5404, pp. 183-194, 12-13 Apr 2004, Orlando, USA.

[6] D. M. Monro, S. Rakshit, *Rotation Independent Iris Matching by Motion Estimation*, Proc. IEEE Int. Conf. on Image Processing, Sep. 2007.

[7] D. M. Monro, S Rakshit, D. Zhang, *DCT-Based Iris Recognition*, IEEE TPAMI, Vol.29, No.4, pp. 586-595, 2007.

[8] S. Rakshit, D. M. Monro, *Robust Iris Feature Extraction and Matching*, Proc. IEEE Int. Conf. on DSP, Jul. 2007.

[9] S. Rakshit, D. M. Monro, *Pupil Shape Description Using Fourier Series*, Workshop on Signal Processing Applications for Public Security and Forensics, April 2007.

[10] P. Grother, E. Tabassi, G. Quinn and W. Salamon, *Interagency report 7629: IREX I - Performance of iris recognition algorithms on standard images*, N.I.S.T., October 2009.

[11] Iris Challenge Evaluation, http://iris.nist.gov/ice/, January, 2011.

[12] S. E. Baker, K. W. Bowyer, P. J. Flynn, *Empirical evidence for correct iris match score degradation with increased time-lapse between gallery and probe matches*, Proc. 3rd IEEE Int. Conf. on Biometrics, L.N.C.S., Vol. 5558, pp. 1170-1179, 2009.

[13] K.W. Bowyer, K. Hollingsworth, P.J. Flynn, *Image understanding for iris biometrics: a survey*, Computer Vision and Image Understanding, vol. 110, no. 2, pp. 281-307, 2008.

[14] K.P. Hollingsworth, K.W. Bowyer, P.J. Flynn, *The best bits in an iris code*, IEEE TPAMI, Vol. 31, No. 6, pp. 964-973, June 2009.

[15] N. Popescu-Bodorin, V. E. Balas, *AI Challenges in Iris Recognition. Processing Tools for Bath Iris Image Database*, Proc. WSEAS 11th Int. Conf. on Automation & Information, pp. 116-121, WSEAS Press, June 2010.

[16] N. Popescu-Bodorin, *Exploring New Directions in Iris Recognition*, 11th Int. Symp. on Symbolic and Numeric Algorithms for Scientific Computing, CPS-IEEE Computer Society, pp. 384-391, 2009.

[17] N. Popescu-Bodorin, V. E. Balas, *Comparing Haar-Hilbert and Log-Gabor based iris encoders on Bath Iris Image Database*, Proc. 4th Int. Conf. on Soft Computing Applications, pp. 191-196, IEEE Press, July 2010.

[18] W. Dong, T. Tan, Z. Sun, *Iris Matching Based on Personalized Weight Map*, Accepted for publication in IEEE-TPAMI (to appear in 2010).