# Learning Iris Biometric Digital Identities for Secure Authentication. A Neural-Evolutionary Perspective Pioneering Intelligent Iris Identification

N. Popescu-Bodorin *Member, IEEE* and V. E. Balas *Senior Member, IEEE*

**Abstract** This chapter discusses 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 inter-class comparisons performed for the test database (Bath Iris Image Database). It is shown here that when using digital identities evolved by a *logical* and *intelligent* artificial agent (Intelligent Iris Verifier/Identifier) the separation between inter- and intra-class scores is so good that it ensures *absolute safety* for a very large percent of accepts (97%, for example), i.e. recognition is no longer a statistical event, or in other words, the statistical aspect of iris recognition becomes residual while the logical binary aspect prevails. In this way, iris recognition theory and practice advance from *inconsistent verification* to *consistent verification/identification*.

## 1 Introduction

Nowadays, after years of important studies and contributions, such as those of Wildes [21] and Daugman [3, 5], or the newer developments undertaken at CASIA by Ma *et al.* [10] and Tan *et al.* [20], at the University of Bath by Monro *et al.* [11, 12], Rakshit and Monro [18, 19], at NIST by Grother *et al.* [7] - who summarized the evaluation of iris recognition technologies competing in Iris Challenge

Nicolaie Popescu-Bodorin
Artificial Intelligence and Computational Logic Laboratory, Department of Mathematics and Computer Science, Spiru Haret University, Bucharest, Romania, e-mail: bodorin@ieee.org

Valentina E. Balas
Faculty of Engineering, Aurel Vlaicu University, Arad, Romania, e-mail: balas@drbalas.ro

Evaluation [9], and also at the University of Notre Dame by Baker *et al.* [1], Bowyer *et al.* [2], Hollingsworth *et al.* [8], after a lot of things being done and being said about iris recognition, it could appear the temptation to believe that iris recognition is a closed domain. We *strongly* disagree with this point of view.

So far, iris recognition theory tells in short that the similarity of some uint8[1] codes (unwrapped iris segments obtained through segmentation, unwrapping and normalisation of the iris captured in an eye image) is decidable in the space of binary iris codes (a space of binary matrices obtained by compressing uint8 codes into binary codes).

Is this *theory* logically consistent (sound)? Nobody asked, as far as we know, but certainly, no answer to this question was ever published, and consequently, *inconsistent iris verification* - a field of experimental science and engineering - took the place and the name of *iris recognition* - a field of science which is supposed to deliver proofs and certitudes concerning the results obtained experimentally. For quite a while (ten years at least), different authors published for different iris recognition approaches a single type of demonstration proving how good these approaches are and identifying upper bounds for whatever False Accept Rate meant in their biometric system. These kinds of demonstrations have at least three logical faults that must be corrected:

- Firstly, a case of False Accept is an objective situation, and therefore, the Fals Accept Rate (FAR), is on its turn, an *objective measure*, and therefore, only in a logically inconsistent practice of iris recognition a relation between FAR at verification and FAR at identification could be formulated (estimated / established) as being a non-identical function.
- Secondly, confusing a *binary iris code* with a *digital identity* does not match a logical restriction that a biometric system must satisfy in terms of entropy: a recognizer object encodes more entropy than any of the recognized objects.
- At last but not the least, *proving an upper bound for the False Accept Rate* (as a value or as a dynamic) *while keeping the space of digital identities stationary is a logical non-sense*, because it means to establish a limitation for the speed with which *the explosion of a contradiction* expands in the internal logic of a biometric system. Of course, this is not a problem if the biometric system does not have to prove a binary consistent internal logic (this cloud be the case if the internal logic of the biometric system is allowed to be an *inconsistent* or a *paraconsistent* 2-valent or n-valent fuzzified logic of *beliefs*). Still, in a stationary space saturated with imbricate clusters (each cluster being a cloud of binary iris codes coming from the same eye of the same person), the process of finding a suitable location for a new cluster to be inserted without colliding it with the other clusters that are already there, only gets harder and harder, and finally impossible, and therefore, if a False Accept occurred, and if the number of enrolled users continues to grow, the trivial expansion of the contradiction within the internal logic of the biometric system can only accelerate.

[1] unsigned 8-bit integer

The motivation behind one of our previous papers [13] 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 [13] is said that it was 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. It is 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.

All of these ideas [13] were succesfully validated in our current work whose results follow to be presented here. Now we know that the classical neural architetures (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/Adviser Module within NPB Iris Recognition Generic Experimental Model [14] and used to find all the novelties which follows to be discussed here. Also, using the infrastructure described there [14] enabled us to draw one of the most important conclusions which led us to the current neural-evolutionary perspective: 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.

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 taken for the same eye of the same person) 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 would not be true, then one solution for defining a suitable encoding of the biometric identities should exist in terms of finding some binary matrices as centroids for the sets of iris codes extracted for the same eye of the same person. Still, this hypothesis has not been validated in our experience so far. Hence we have assumed that the dimension of the stored identities must differ with at least one or-

der 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 to store 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 [7] in his proprietary iris code format, and also the necessity of this change.

## 2 Terminology and problem formulation

All data and all techniques reported in this chapter are about authentication of persons based on comparing iris biometric binary templates to learned (enrolled) digital biometric identities. A *digital identity* is a collection of data (a memory) stored for each enrolled user of a biometric system.

The identities are learned when the biometric 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 *digital 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 *digital identity* are found to be sufficiently similar) or could reject it.

The claims could be *positive* - "*I am*", or *negative* - "*I am not*", *honest* (the enrolled user claims its own identity, or if he is not enrolled claims that he isn't) or *forged* (the user claims 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.

[2] The informed readers should appreciate if the domain of Iris Recognition is or is not still in its infancy, if such things about iris codes and biometric digital identities are told here for the first time.

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, or iris images (or iris codes), some of them are used to learn identities (*learning dataset*), and all others (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 binary 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 binary 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 (enrolled) *digital identity*.

The simplest biometric system is based on single-enrollment: there is only one binary template enrolled under an ID number, the training function is the identical function, and consequently, the enrolled *digital identity* for the person who owns that ID number coincides with the single enrolled *binary 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 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) because identification and verification are considered to be 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) and it is not valid in Consistent Biometry - as is further shown here.

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 [13]-[15], 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 questions to be answered here is the following:

- *Why to choose a multi-enrollment system?*

*- How to select the enrolled binary templates (learning dataset)?*
*- How to learn a biometric digital identity?*
*- 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:

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.

Baker, Bowyer and Flynn [1] documented the problem of template aging. In this context, multi-enrollment is a recommended policy for ensuring a smooth variation of the iris identities over time.

## 3 Proposed method

There are three simple and logical basic ideas underlying our evolutionary approaches to iris recognition:

Firstly, we always follow the idea of a large-scale distributed (geographically scattered) biometric system organized as a network with one or more central units and a lot of peripheral terminals. We follow this idea because we think that the future large-scale systems for iris based biometric identification will be hosted on hardware resources (IBM, Sun) dedicated to and fully compatible with virtualization and cloud computing technologies.

Secondly, we consider naturally that a recognizer must encode much more entropy than the recognized objects. Exactly how much? We don't know *a priori*. This is the reason why, in our models, a *digital identity is free to evolve* during its training up to a stage where it encodes enough entropy such that the recognition of the learning examples to take place at a certain level of quality comparable with the quality of recognition measured for human subjects during a Turing Test. A software enabled to replicate at a certain degree the human performances in iris recognition is further referred to as an *intelligent agent for iris recognition*.

At last but not the least, in our view, iris recognition is a problem of *consistent* or *inconsistent* logic. For example, practicing iris recognition for iris images in which not even the pupil is recognizable is just an inconsistent and vague verification (that we called *possibilistic and inconsistent iris hunting*), and not a logically consistent achievement in *iris recognition*. These cases fall into the following inconsistent logic in which the agent says: *I couldn't say where the pupil is, but I'm sure that this person is George*, or even better, into the following fuzzy, modal, and possibilistic

logic of *beliefs* in which the agent says: *it is impossible for me to say where the pupil is, but I believe it could be (very) possible that this person to be George*. Hence, involuntary humour is reachable for certain artificial intelligent agents (not too smart, indeed) - on one hand, but on the other, *iris recognition* and *iris hunting* are two very different things.

### *3.1 Logical framework: Consistent Biometry*

Our concern is doing iris recognition in a logically consistent manner (i.e. intelligent iris identification) or at least with a coarse, predictable and controllable loss in consistency (intelligent iris verification). To achieve these, the primer condition is a consistent procedure of enrollment in the dataset of training examples.

Assuming that a low-quality training could guarantee excellent learning performances, or in evolutionary terms, supposing that insufficiently precisated adaptation stress could guarantee the evolution of a very specialized individual, are too optimistic hypothesis for us to follow. Instead of accepting them, we let the following possibilistic but consistent deduction to lead us:

$$consistent(A) \rightarrow [not(enrolled(I)) \rightarrow impossible(identification(I))]\,,$$

i.e.

$$[possible(identification(I)) \rightarrow (enrolled(I))]\ OR\ [inconsistent(A)]\,,$$

i.e.

$$[inconsistent(A)]\ OR\ [impossible(identification(I))]\ OR\ [enrolled(I)]\,.$$

where A and I encode the agent and an individual, respectively. Nothing changes essentially if the same deduction is made for the verification. Therefore:

$$[inconsistent(A)]\ OR\ [impossible(verification(I))]\ OR\ [enrolled(I)]\,.$$

The following two formulae:

$$[not(enrolled(I)) \rightarrow impossible(identification(I))]\,,$$

$$[not(enrolled(I)) \rightarrow impossible(verification(I))]\,,$$

will be further referred to as the *Principle of Consistent Biometry*, or the first axiom of Consistent Biometry (CBA1).

From the perspective of Artificial Intelligence, CBA1 tells that an intelligent agent who knows and practices a consistent biometric theory could neither verify nor identify an unenrolled individual, simply because it wasn't trained with samples

taken from that individual. In order to be verified or identified by an intelligent distributed biometric system any user must enroll himself at one terminal of the system, must be *known* by the system.

The formulae:

$$[enrolled(I) \rightarrow possible(identification(I)],$$

$$[enrolled(I) \rightarrow possible(verification(I)],$$

will be further referred to as the *Positive Possibilistic Axiom of Consistent Biometry*, or the second axiom of Consistent Biometry (CBA2).

The following two formulae:

$$[enrolled(I) \leftrightarrow possible(identification(I)],$$

$$[enrolled(I) \leftrightarrow possible(verification(I)],$$

will be further referred to as the *Fundamental Theorem of Consistent Biometry* (FTCB). It tells that even in a computational perspective the identification and verification are different (being based on one-to-all and one-to-one comparisons, respectively), in a consistent biometric theory they have the same logical meaning. Hence, in CB there is no need to invent different quality measures for verification and identification as proposed in [5].

FTCB also tells that a biometric system in which the identification is not possible is an inconsistent verifier whose output is more likely a fuzzy inconsistent belief about the identities represented by the codes which are currently compared rather than a consistent biometric decision. The theorem also suggests that the *modes* of enrollment will determine the *modes* of identification and verification: accurate enrollment - reliable biometric decision, low-quality enrollment - unreliable biometric decision.

Hence, in a consistent biometric theory, *possibility* is the only guaranteed mode for both identification and verification. Advancing verification/identification from *possible* to *accurate*, or to *necessary* is a matter of calibrating the enrollment, a matter of customizing the enrollment procedures in order to achieve enough quality.

It is obvious now why we said that *consistent enrollment* is the primer condition for practicing iris recognition in a logically consistent manner (intelligent iris identification) or at least with a coarse, predictable and controllable loss in consistency (intelligent iris verification).

### *3.2 Internal logic, knowledge and self-awareness representation for intelligent systems*

Humans can invent the formal theory of Consistent Biometry. The only problem is how to implement this knowledge into an artificial intelligent agent. In order to transfer logical knowledge to an artificial agent, it must have an inference engine (it has to know at least a formal theory of binary logic) which in the case of our Intelligent Iris Verifier/Identifier is the *Computational* formalization of *Cognitive Binary Logic* (CCBL, [16]). The internal logical language (logical dialect) in which our Intelligent Iris Verifier/Identifier thinks, decides and talks about itself, about logic and about iris recognition in the context of Consistent Biometry is *the Cognitive Dialect* [17] - a logical language supporting *self-reference ambiguity*, a formal language native in CCBL designed to reveal that *auto-referential deductive discourses in CCBL are non-paradoxical*, and to support the *soundness* and *completeness* of the deductive discourse in CCBL regardless if it is auto-referential or not.

The close relationship that exists between the *self-reference ambiguity* in CCBL and the *self-awareness* is illustrated in the following situation: the truth does not depend on who is talking, and therefore, 'p' is a symbol used by us when we talk about a given propositional variable, is a symbol used by an artificial intelligent agent when it 'talks' about a given propositional variable, or is a symbol used by a propositional variable when talking about itself, all at once. This looks a little bit strange at first sight, but it comes very naturally: the most rudimentary intelligent agent is a bit storing the truth value of propositional variable 'p', and the next simple intelligent agent is a logical circuit: '$1 \rightarrow p$', telling that '*p is true*', and obviously, $p \leftrightarrow (1 \rightarrow p)$. This is the beginning of the self-awareness: 'p' is equivalent to '*p is true*'. Hence, who could say that '*p is true*' ? All of us, and even 'p', and obviously, the truth value of 'p' does not depend on who is talking about 'p'. If we now cease to exist, the propositional variable will continue to talk about itself (in a silent non-contradictory auto-referential deductive discourse, [16]) waiting to be heard, waiting to be discovered. This is the essence of CCBL: a self-reference formal deductive discourse (theory) written *with* and *about* the propositional variables of binary logic. Therefore, we said that *self-reference sentences are native and non-paradoxical in CCBL*, and therefore, *CCBL is a suitable inference engine for all of those intelligent agents that aim to be consistent in binary logic* - in general, for our Intelligent Iris Verifier/Identifier which aims to auto-control its evolution toward a logically consistent understanding of iris recognition by stepping always through and always to a logically consistent state - in particular. Of course, human understanding (or *the common belief*) about self-reference sentences formulated in semantically closed languages is a different thing.

In short, the Cognitive Dialect is the language that enables the Intelligent Iris Verifier/Identifier *to know* CCBL and Consistent Biometry, *to decide* how to create (evolve) a consistent theory of iris recognition dynamically over an extending vocabulary of digital identities, *to become* and *to stay aware* of its logical status

(at least). This is why we tell that *Cartesian argument is valid even in Artificial Intelligence*.

### 3.3 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 [15] (Second version of Circular Fuzzy Iris Segmentation) which is a two step segmentation procedure. Firstly, the pupil is found (Fig. 1 in [14]). Secondly, the image is unwrapped through a pupil-centric polar coordinate transform (Fig. 2 in [14]) and the limbic boundary is approximated (Fig.1.a. in [15]). 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 chapter are the following two: Log-Gabor Encoder (LGE, [15]) and an encoder based on Haar Wavelet (noise filtering) and Hilbert Transform (phase encoding), abbreviated HH1 and introduced in [15].

### 3.4 Selecting and aligning the enrollment templates

The criterion used here for selecting the enrolled binary 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 (Monte-Carlo Simulation), through randomization of selected indices:

$$S_5 = min\{ \parallel [M_s, 2 \times S_s^{1/2}] - [M_{10}, 2 \times S_{10}^{1/2}] \parallel \mid s \in C_{10}^5 \}$$

where $C_{10}^5$ is the set of all 5-combinations taken from those first 10 images, ($M_S$, $S_S$) 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, excepting the cases of failed segmentation (3 failures in a total of 1000 eye images), for each eye represented in the database, there are 5 images for training and 15 images 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 generated with LGE [15] were tested for angular alignment using rotations in range of $\pm 5.625$ hexadecimal degrees ( $\pm 8$ pixels for unwrapped uint8 iris segments of dimension 512x32) with respect to the witness. The corrections were applied on the collection of unwrapped uint8 iris segments which have been further used to generate binary iris codes of dimension 256x16 using HH1 encoder [15].

### *3.5 Learning evolutionary digital biometric identities*

Learning biometric identities is a problem of *artificial intelligence* and *evolution*. Why is that? Fig. 1 shows an instant picture of a biometric system, but the truth is that a biometric system, in order to be *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 on its turn, it is impossible to achieve without *intelligence*[3]. Otherwise, if the enrollment is not accompanied by adaptation, it is just

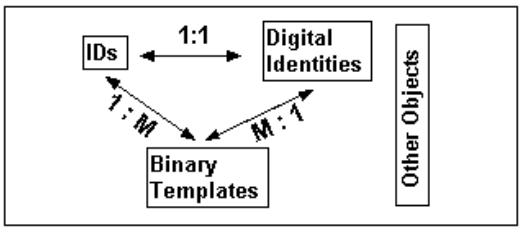


**Fig. 1** An instant picture of a biometric system frozen in time: a relational collection of *ID numbers*, *binary templates* (sub-collection of hypostases / samples taken for the recognized objects), *digital identities* (recognizer objects), optional strings and, possibly, other objects.

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 [3] (see the formula (16) and the subsequent example of that formula in [3]). Still, it seems that the correct in-

[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.

terpretation (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 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 satisfy 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 [3]) was 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 stationary biometric system in which the *consistent enrollment* (*adaptation* / *learning*) is not guaranteed, the chances for facing inconsistency in the form of False Accept grow nearly linearly

[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.

with the number of trials (with database size). By contrast, a LCBS behave totally different. The next section of the paper will show that, at least for moderate database sizes (such is the case of Bath Iris Image Database), an *intelligent iris verifier* is also reliable as an *identifier*.

Since we are bonded to a logically consistent approach to iris recognition we could also reformulate Daugman's conclusions with even more precaution: in a stationary biometric system in which the *consistent enrollment* is not guaranteed, in which a *local* iris recognition theory is known only through the experimental measurements onto a given current vocabulary of binary iris codes, there could appear *statistical motivations* (reasons, but not in the sense of an argument in consistent binary logic) *to believe* that chances for facing inconsistency in the form of False Accept grow nearly linearly with the number of trials. If these *motivations would be valid logical arguments* in binary logic, and if the statistically motivated *belief* that the chances of False Accept grow nearly linearly with the number of trials *would be a proved theorem*, then and only then *the statistical decision landscape* proposed by Daugman [3] could have the chance to be a consistent 2-valued formal logic theory of iris recognition. Until then, it is at most an inconsistent theory of statistically motivated *beliefs* about iris verification validated by observing measurements over a given vocabulary of binary iris codes.

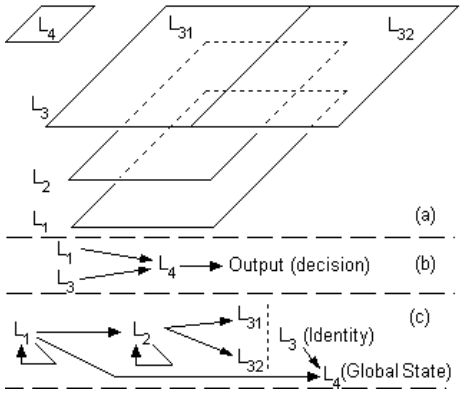


**Fig. 2** (a) - ANN structure. (b) - Information flow during verification: the input consists in a candidate template (one binary template from the *test dataset*) loaded on $L_1$ and an enrolled digital identity loaded on $L_3$.
**(c)** - Information flow during training: the input is the current learning example (enrolled iris binary code) and the output is a digital identity which follows to be written in a database.

### *3.6 Artificial neural network support for consistent enrollment*

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

i) The learning process does not 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 is not, 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.

ii) The learning process resumes each time when a new enrollment occurs (enrollment triggers evolution).

iii) 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 Fig. 2. 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 is not (the negative discriminator). If the current stage is a verification (a test), the global activation ($ga$) will be the number:

$$ga = \{L_{31}, L_1\} - \{L_{32}, L_1\},$$

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 braces 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 $L_4$.

### *3.7 The importance of being aware*

When a biometric system loses its logical consistency, among the regular *sheep* [22], an entire *biometric menagerie* appears within it: *the goats* - characterized by their low genuine scores (difficult to match through a genuine comparison), *the lambs* - those "vulnerable to impersonating" (Yager, [22]), and *wolves* - which are "exceptionally successful at impersonation and prey upon lambs" (Yager, [22]), but this is not all. Yager and Dunstone [22] brought more animals in the biometric farm, animals called worms, chameleons, phantoms, and doves.

It happens that we have studied a lot of logical aspects concerning iris recognition and we saw that if the recognition theory is 3-valent, fuzzy and inconsistent (like $TSC_2$ in Fig. 6), there exists a supra-theory of recognition with $2^3 = 8$ values of truth (three of them being those previously considered) which is, on its turn, inconsistent and (even much) fuzzy. Hence, increasing the number of the fuzzy values of truth will not repair the inconsistency. Anyway, from the point of view of Consistent Biometry doing that is as logical as looking at a macroscopic explosion through

a microscope[5]. In the context of Consistent Biometry, the most important aspect of self-awareness is that a logically consistent intelligent agent for iris recognition must stay aware of its logical status, must be able to detect any enrollment that could jeopardize its logical status, and must evolve in such a way that all enrolled identities to preserve the quality of being *sheep*. In Consistent Biometry, *reliability* is synonym for *logical consistency*.

## *3.8 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 a 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,
18: **End**;
18: **Output:**
$d$ (current decision) for testing mode OR
$L_3$ (current trained identity) for training mode.

[5] The *natural* logical framework of logically consistent iris recognition is Binary Logic. Inconsistent enrollment (i.e. inconsistent extension of the current vocabulary of binary iris codes) introduces the contradiction in the internal logic of biometric system. Naturally, the contradiction will explode in an exponential number of 'words' (or 'animals', i.e. insufficiently precisated values of truth) and finally in pure inconsistency: more and more enrolled users will become *lambs* and *wolves* simultaneously, or the False Reject Rate will increase making the system unreliable.

### *3.9 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 understanding* of their nature 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 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, 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 illustrated in Fig. 3 and further stated in (C 7.1.1). 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 *in mass evolution* of an entire population of individuals

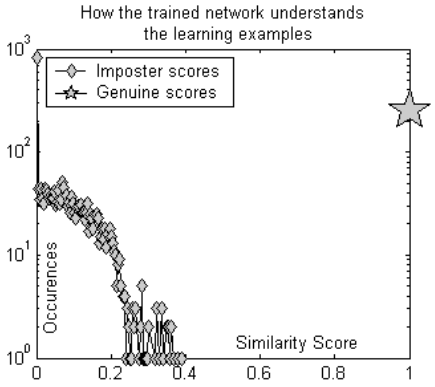


**Fig. 3** The manner in which an Intelligent Iris Verifier recognizes the binary iris codes on which was trained (learning 50 identities from 250 genuine comparisons, and 2‘450 imposter comparisons). The figure illustrates the behavior of a *trained* Intelligent Iris Verifier whose understanding is very close to the human understanding proved during a Turing Test.

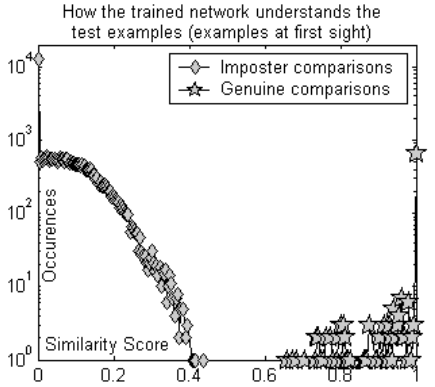


**Fig. 4** The manner in which an Intelligent Iris Verifier recognizes binary iris codes that it has not seen during the training stage (50 learned identities tested through 747 genuine comparisons and 36603 imposter comparisons). The Intelligent Iris Verifier proves its power of generalization. The figure is also an example of fuzzified but still consistent understanding of the binary logical values.

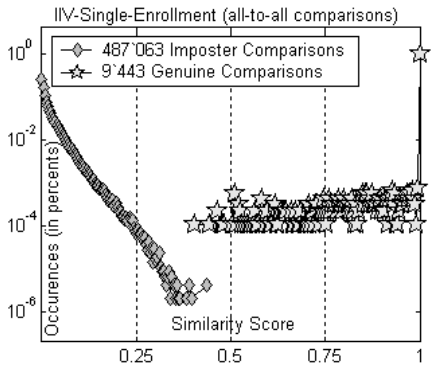


**Fig. 5** The manner in which the identities evolved by the Intelligent Iris Verifier ‘*filters*’ the apparent *statistical decisional landscape* [3] (induced by compressing uint8 iris images to binary iris codes) and recovers the fuzzy meaning of two concepts: ‘*genuine*’ and ‘*imposter*’ comparisons. From statistical safety to absolute safety: 97% of the genuine comparisons are not even questionable through reasonable statistical doubts.

which redefine their identities on new coordinates in a space *large enough* to host the dynamic consciousness of an extending group in which the ground policy is to preserve the differentiation between its members. Hence, the lines 8 and 9 from

IIV description tell that the *adaptation* is achieved through *individual* or *systemic* evolution.

In a geometrical view, the *individual evolution* gives the start point for a trajectory which will host the digital identity of a certain enrolled person along the time. Of course, we may consider that a given identity computed at a certain moment is a discrete point in the current space of all enrolled identities, case in which, the movement of this point along the time describes the trajectory of the given identity, but also, we may see the given identity not like a clear discrete point, but as a fuzzy one, as a density of possible (and probable) points situated in a disk centred on the given identity, case in which, the movement of the identity describes a tube of possible and probable trajectories. The *systemic evolution* must maintain the flow of all these trajectories/tubes (corresponding to all enrolled persons) as laminar (untangled) and as smooth as possible. These conditions are not easy to satisfy because, by its nature, the flow of identities is non-stationary: a new spring appears within it each time when a new enrollment occurs.

One of our previous affirmations (see the challenge C 7 in [13]) 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 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 intra- and inter-class 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:

i) 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. Hence, in these cases, IIV proves a *crisp understanding* of what it means to be an imposter comparison (or an imposter pair).

ii) 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). Hence, in these cases, IIV proves a *fuzzy understanding* of what it means to be an imposter comparison (or an imposter pair).
iii) For 87.82% (656) of all genuine pairs formed with test examples, IIV performs a *Crisp Accept* by mapping these pairs to unitary score. Hence, in these cases, IIV proves a *crisp understanding* of what it means to be a genuine comparison (or a genuine pair).
iv) 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). Hence, in these cases, IIV proves a *fuzzy understanding* of what it means to be genuine comparison (or a genuine pair).

Summarizing the data presented in Fig. 3 and Fig. 4, 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*).

## *3.10 New safety standards for logically consistent biometric purposes*

**Definition 1.** (N. Popescu-Bodorin)

1. A biometric system has/gives/is/induces:
   i) a *consistent and crisp binary safety model* - if it is able to prove crisp understanding of two words (concepts) - *imposter* and *genuine* comparisons, by scoring them into $\{0, 1\}$.
   ii) a *fuzzified binary safety model* - if it is able to prove a fuzzified binary understanding of intra- and inter-class comparisons, by scoring them all into [0, 1].
   iii) a *consistent and fuzzified binary safety model* - if it is able to prove a fuzzy but still consistent binary understanding of inter- and intra-class comparisons, by scoring them into [0, 0.5] and (0.5, 1], respectively.
2. A fuzzified binary safety model for iris recognition 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 and fuzzified binary safety model* which can be transformed into a *consistent and crisp binary safety model* through a simple defuzzification of the similarity score.

### *3.11 New challenges - new results*

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 [3], Hollingsworth-Bowyer-Flynn best bits matcher [8], Dong-Tan-Sun best bits matcher [6], and our previously proposed multi-enrollment systems [15] 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, but here, it is 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 logico-arithmetical 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 at dimension $256\times16$ with Haar-Hilbert encoder HH1, [15]) 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 [15]) is consistent. The exact meaning of this term will be illustrated below. Until then, its opposite is discussed:

**Proposition 1.** *(N. Popescu-Bodorin)*
*Let us consider these:*
*a) $d$ is a given dimension (*$256\times16$ *for example).*
*b) $C_8$ is the set of all uint8 codes of dimension $d$.*
*c) $C_2$ is the set of all binary codes of dimension $d$.*
*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 $d$).*
*e) $TS_2$ 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

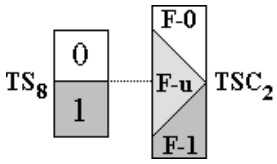


**Fig. 6** Transporting the binary truth values of the affirmations about the similarity between uint8 codes of dimension d (from $TS_8$) to fuzzy values of truth in $TSC_2$.

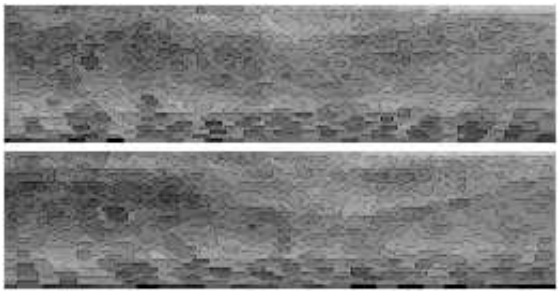

**Fig. 7** True Reject Consistency: IIV-SE agent classifies correctly (rejects) the hypostases of the same iris if they are very different. Are these two hypostases of the same iris sufficiently similar to be scored with a Fuzzy Accept? IIV-SE agent tells that these two hypostases cant be matched, and this is the truth.

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 crisp values of truth from $TS_8$ became the fuzzy values F-1, F-0, F-u (i.e. Fuzzy 1, Fuzzy 0 and Fuzzy unknown, respectively) or fuzzy modal values MPI, MPD, U (Most Probable Identical codes, Most Probable Different codes, and Uncertain, respectively). 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 underlain by the transported biometric theory $TSC_2$. On the other hand, in $TSC_2$ *verification* [3] is possible, but still logically inconsistent, despite the existence of a suitable choice of the code dimension which induces a *statistical decision landscape* [3] 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.

### *3.12 Logical consistency vs. safety*

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:

i) For 97% (9‘160) of all (9‘443) genuine comparison, it performs a *Crisp Accept* by mapping these comparisons to the unitary similarity score. Hence, in these cases, IIV proves a *crisp understanding* of what it means to be a genuine comparison (or a genuine pair). For 97% of the genuine comparisons, the recognition is done in terms of *absolute safety* (*absolute security*): 97% of the genuine comparisons are clearly above any doubts (eventualy) motivated through a statistical game of chances; 97% of the genuine comparisons are clearly outside any statistical decision landscape [3]. This is the main quality of our results. They prove that a logically consistent approach to iris recognition qualifies almost all Accept cases as being *absolutely safe* / *absolutely secure* / *necessary True Accepts* / *indubitable True Accepts*.

ii) 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). Hence, in these cases, IIV proves a *fuzzy understanding* of what it means to be to be a genuine comparison (or a genuine pair).
iii) 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]. Hence, in these cases, IIV proves a *fuzzy understanding* of what it means to be an imposter comparison (or an imposter pair) wrong placed under the intra-class index as a consequence of eye image preprocessing.
iv) 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). Hence, in these cases, IIV proves a *fuzzy understanding* of what it means to be an imposter comparison (or an imposter pair).

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

i) 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.

ii) 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.

### *3.13 Comparison to a result previously obtained by Daugman*

We must clarify here if the result presented in Fig. 5 is or isn't the first of its kind. The answer is negative: a result previously obtained by Daugman and presented in Fig. 10 from [4] also reveal a *weak statistical aspect of recognition*, but Daugman omitted to give the correct interpretation of this fact. Now we know for sure that Daugman obtained that result by doing other things than just comparing only binary iris codes to each other using Hamming distance. Surely he used at least another one element (just as we did in our approach by introducing the *digital identity*) in order to 'attract' the binary codes in a space in which statistical aspect of recognition is weak.

Hence our result is not the first of its kind but it is much better because we managed to give the correct interpretation for the result previously obtained by Daugman, and we also managed to advance from a *weak statistical aspect of recognition*[6] to a *residual statistical aspect of recognition*[7].

The difference between our result and the result previously obtained by Daugman comes from a different understanding of what it means *to recognize*:

- Daugman sustained the idea of a statistical decision landscape of recognition (iris recognition is viewed as a game of chances, inevitably logically inconsistent).

[6] Daugman said in [4] that "more than half of such image comparisons achieved an HD of 0.00, and the average HD was a mere 0.019", hence in our terms, he said that in more than half of such image comparisons his verifier proved a crisp understanding of what it means to be a genuine pair.

[7] IIV-SE system proposed by Bodorin proves a crisp understanding of what it means to be a genuine pair in 97% of cases.

Still, Fig. 10 from [4] shows how close to the truth was Daugman when he did that experiment.

- We are sustaining the idea of a logically consistent approach to recognition based on cognitive investigation which aims to link the causes to the effects by thinking in Horn clauses, or by following *cognitive implications*, or by exploring *deductive discourses* [16]: recognition or non-recognition happens because precise conditions are or aren't fulfilled. By defining iris recognition as a problem of logic we allowed a custom designed intelligent agent (Intelligent Iris Verifier/Identifier, which knows *Computational Cognitive Binary Logic* and *Consistent Biometry*), to evolve (to create) a vocabulary of digital identities (corresponding to all enrolled users) and a (complex) piece of knowledge - a consistent formal biometric theory over this vocabulary.

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 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 fully erroneous segmentation. Overall efficiency of the segmentation procedure (CFIS2, [15]) can be now reevaluated at 99%.

## *3.14 Another question*

Before ending, we must answer one more question: what made possible the results presented here? The answer is surprisingly simple: for us, iris recognition is another facet of Binary Logic, or in other words, iris recognition is another hypostasis of a more general problem, namely *logical and intelligent artificial understanding of data* where *logical* means *based on Böhm-Jacopini theorem*. We did nothing more than searching for a logical and intelligent manner of understanding (quantizing!) some signals encoded in the iris texture. But what it is really important is that we managed to create an artificial intelligent agent able to achieve some sub-goals of this complex task '*by himself*' (referring a self-aware artificial intelligent agent as a person is something absolutely legal in his formal language). IIV agent discovers and learns gradually a logico-arithmetical formal theory in which *iris identification* is provable (computable). Hence the present chapter marked the moment in which *Computational Inventics* departs from fiction once for good.

## 4 Conclusion

The present chapter announced the technological advance from *inconsistent iris verification* to *consistent iris identification* and it showed that the future iris-based *identification* will be inevitably marked by multi-enrollment, and by the newly proposed concept of consistent, intelligent, adaptive, evolutionary biometric system. 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*, simply because *secure* means *logically consistent*, because *adaptation* of a biometric system means *logical and intelligent evolution* in response to *enrollment*.

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

## References

1. Baker, S. E., Bowyer, K. W., and Flynn, P. J.: 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.
2. Bowyer, K.W., Hollingsworth, K., and Flynn, P.J.: Image understanding for iris biometrics: a survey, Computer Vision and Image Understanding, vol. 110, no. 2, pp. 281-307, 2008.
3. Daugman, J.: Biometric Decision Landscapes, Technical Report No. TR482, University of Cambridge, 2000.
   http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-482.pdf
4. Daugman, J.: How Iris Recognition Works, IEEE Trans. on Circuits and Systems for Video Technology, vol. 14, No. 1, Jan. 2004.
5. Daugman, J.: New methods in iris recognition, IEEE Trans. Systems, Man, Cybernetics, B 37(5), pp 1167-1175, Oct. 2007.
6. Dong, W. , Tan, T., and Sun, Z.: Iris Matching Based on Personalized Weight Map, Accepted for publication in IEEE-TPAMI (to appear in 2010).
7. Grother, P., Tabassi, E., Quinn, G., and Salamon, W.: Interagency report 7629: IREX I - Performance of iris recognition algorithms on standard images, N.I.S.T., Oct. 2009.
8. Hollingsworth, K.P., Bowyer, K.W., and Flynn, P.J.: The best bits in an iris code, IEEE TPAMI, Vol. 31, No. 6, pp. 964-973, June 2009.
9. Iris Challenge Evaluation, N.I.S.T., http://iris.nist.gov/ice/ Cited 20 February 2011.
10. Ma, L., Tan, T., Wang, Y. and Zhang, D.: Personal Identification Based on Iris Texture Analysis, IEEE TPAMI, Vol. 25, No. 12, pp.1519-1533, 2003.
11. Monro, D. M. and Rakshit, S.: Rotation Independent Iris Matching by Motion Estimation, Proc. IEEE Int. Conf. on Image Processing, Sep. 2007.
12. Monro, D. M., Rakshit, S., and Zhang, D.: DCT-Based Iris Recognition, IEEE TPAMI, Vol.29, No.4, pp. 586-595, 2007.
13. Popescu-Bodorin, N., and Balas, V. E.: AI Challenges in Iris Recognition. Processing Tools for Bath Iris Image Database, Proc. $11^{th}$ Int. Conf. on Automation and Information, pp. 116-121, WSEAS Press, June 2010.
14. Popescu-Bodorin, N.: Exploring New Directions in Iris Recognition, $11^{th}$ Int. Symp. on Symbolic and Numeric Algorithms for Scientific Computing, CPS - IEEE Computer Society, pp. 384-391, 2009.

15. Popescu-Bodorin, N., and Balas, V. E.: Comparing Haar-Hilbert and Log-Gabor based iris encoders on Bath Iris Image Database, Proc. $4^{th}$ Int. Conf. on Soft Computing Applications, pp. 191-196, IEEE Press, July 2010.
16. Popescu-Bodorin, N., and State, L.: Cognitive Binary Logic - The Natural Unified Formal Theory of Propositional Binary Logic , Recent Advances in Computational Intelligence, pp. 135-142, WSEAS Press, April 2010.
17. Popescu-Bodorin, N., and Balas, V. E.: From Cognitive Binary Logic to Cognitive Intelligent Agents, Proc. $14^{th}$ Int. Conf. on Intelligent Engineering Systems, pp. 337-340, CPS - IEEE Computer Society, May 2010.
18. Rakshit, S. and Monro, D. M.: Pupil Shape Description Using Fourier Series, Workshop on Signal Processing Applications for Public Security and Forensics, Apr. 2007.
19. Rakshit, S. and Monro, D. M.: Robust Iris Feature Extraction and Matching, Proc. IEEE Int. Conf. on Digital Signal Processing, Jul. 2007.
20. Tan, T. and Ma, L.: Iris Recognition: Recent Progress and Remaining Challenges, Proc. of SPIE, Vol. 5404, pp. 183-194, Apr. 2004.
21. Wildes, R.: Iris Recognition - an emerging biometric technology, Proc. of the IEEE, vol. 85, no. 9, pp. 1348-1363, Sep. 1997.
22. Yager, N., Dunstone, T.: The Biometric Menagerie, IEEE TPAMI, vol.32, no.2, pp.220-230, Feb. 2010.