FACIAL ACCESS CONTROL BASED ON VG-RAM WEIGHTLESS NEURAL NETWORKS

Jairo Lucas de Moraes, Alberto F. De Souza, Claudine Badue

Departamento de Informática, Universidade Federal do Espírito Santo
Av. Fernando Ferrari, 514 – 29060-970 – Vitória-ES – Brazil

Abstract

We present and evaluate a system for access control that uses only facial biometrics as access key. Our system first detects a face in an image, then tries to recognize the face, and finally decides on grating or not access based on a belief computed during the face recognition process. We use the Viola-Jones approach for face detection, Virtual Generalizing Random Access Memory Weightless Neural Networks (VG-RAM WNN) for face recognition, and Bayesian inference for access control.

We simulated the access control to a given resource for a universe of 50, 100 and 200 users. For the set of 200 users, the system was able to correctly authenticate 93.0% of the users with a False Acceptance Rate (FAR) of only 0.8%; for the set of 100 users, 90.3% of the users with a FAR of 1.8%; and for the set of 50 users, 93.1% of users with a FAR de 4.8%.

Keywords: *Access control, facial biometrics, VG-RAM weightless neural networks, Bayesian inference*

1. Introduction

The process of electronic recognition of the identity of individuals has become increasingly commonplace. Its use goes from the access of garages of buildings via magnetic cards to the login into banking sites via identification numbers or electronic passwords. Today, at various levels of transparency, individuals coexist with automatic recognition processes in their day-to-day activities.

According to Hong and Jain [1], traditional approaches for personal recognition are based on "something that you know", such as a personal identification number, or "something that you have", such as an identification card. Unfortunately, for many applications, these methods may not be secure enough to ensure proper personal recognition, because they lack the capability to differentiate between a genuine individual and an impostor who fraudulently acquires the access privilege.

Biometric systems—which include devices to capture biometric information, such as face images, iris images, fingerprints, etc., and databases and software for storage and management of this information [2]—perform the automatic recognition of individuals based on their physiological and/or behavioral characteristics, that is, the individuals themselves become the "identification key", which makes the process more transparent and less prone to fraud. Due to their wide application in various areas, such as public safety, continuous authentication on computer networks, access control, etc., biometric systems are gaining increasing attention from researchers in academia and industry [3, 4, 5].

Among the various alternative biometric information forms that can now be caught by input devices of personal recognition systems, face images are one of the most convenient. Video capture devices are non-invasive, inexpensive, and easy to use. Moreover, the continuous increase of processor performance over the several last decades allowed the use of more sophisticated, robust, reliable and fast algorithms for face detection and recognition.

In this paper, we evaluate the feasibility of a system for access control using only facial biometrics as access key. In this case, access control would no longer be based on "something that you know" or "something that you have", but on the individual itself. To evaluate the feasibility of an access control system based only on facial biometrics, we developed a prototype of this system that operates fully automatically, being able to detect a face in an image and then perform the recognition of that face, with no human intervention. We use a well known approach proposed by Viola and Jones [6] for face detection and Virtual Generalizing Random Access Memory Weightless Neural Networks (VG-RAM WNN) for face recognition [7, 8]. Lastly, we employed Bayesian inference for the access control decision process.

Many techniques for face recognition have been proposed in the literature [4, 5]. However, instead of the access control problem, most of them have been employed to address: the *face identification problem*, where the system always returns a face that has the most similar features to the input face, even though the input face is not in the knowledge base; or the *face verification problem*, where the system receives an identification number along with facial biometric data and reports whether or not it belongs to the claimed identification number. Different

from the approaches presented in [4, 5], we employ a face recognition technique to address the *access control problem* using only facial biometrics as access key; in this case, the system receives facial biometric data only and reports whether or not it belongs to a user that has access to a particular resource or environment.

Although there are currently face based access control systems commercially available, as far as we could examine in the literature, the combination of techniques we have employed to tackle the problem is unique, and the results we have obtained are promising. Using our prototype, the access control to a given resource was simulated for 50, 100 and 200 users. For the set of 200 users, the system was able to correctly authenticate 93.0% of the users with a False Acceptance Rate (FAR) of only 0.8%; for the set of 100 users, the system was able to correctly authenticate 90.3% of the users with a FAR of 1.8%; and for the set of 50 users, the system correctly authenticated 93.1% of users with a FAR of 4.8%.

This paper is organized as follows. After this introduction, in Section 2 we present our prototype of an access control system based only on facial biometrics. In Section 3, we describe our experimental methodology, in Section 4, we analyze our experimental results and, in Section 5, we discuss them. Our conclusions follow in Section 6.

2. Access Control Based on Facial Biometrics

We developed a prototype of an access control system based only on facial biometrics. Our system operates fully automatically in three steps: (i) detection of a face in an image; (ii) recognition of the detected face; and (iii) Bayesian inference for determining if the access should be granted. In the first step, given an arbitrary image, the system determines whether or not there are faces in the image and, if so, it returns the image location and extent of each face. In the second step, given a detected face, the system returns the most similar face, among those enrolled in the knowledge base, along with a matching score, that quantifies the similarity between the detected face and the most similar face in the knowledge base. In the third step, given the matching score and using the Bayes' rule, the system computes a probability measure that indicates the degree of belief of the system in that the detected face belongs to an individual with granted access.

The system final decision is regulated by a threshold: if the degree of belief of the system in that the detected face belongs to an individual with granted access is less than the threshold, than he/she is rejected as an impostor; otherwise, he/she is accepted as an individual with granted access (or genuine individual for short).

In the following, we describe each of these three steps.

2.1. Face Detection

We use the well known object detection technique proposed by Viola and Jones [6] for the task of face detection. This technique uses integral images for fast feature extraction, AdaBoost [9] for classification, and a method for combining the classifiers in a cascade, which allows background regions of the images to be quickly discarded while spending more computation on promising face-like regions.

We have used the Viola-Jones approach to detect faces and also the eyes within the faces. The knowledge of the eyes' position is important for proper face recognition, since it allows a more precise reference for the face recognition system to operate. We found the correct detection of the eyes hard to obtain in some cases. Because of that, our face detection sub-system tries and recognizes the cases were it was not possible to correctly detect the eyes and, in such cases, approximates their position as a previously computed average position.

2.2. Face Recognition

We use Virtual Generalizing Random Access Memory Weightless Neural Networks (VG-RAM WNN) [10, 11] for face recognition. VG-RAM WNN is an effective machine learning technique that offers simple implementation and fast training and test [10]. In previous works [7, 8], we evaluated the performance of VG-RAM WNN on face recognition using well known face databases. Our experimental results showed that, even when training with a single face image per individual, VG-RAM WNN are robust to various facial expressions, occlusions and illumination conditions, showing better performance than many well known face recognition techniques. This has motivated us to use VG-RAM WNN for the face recognition step of our access control system.

2.2.1. VG-RAM WNN

RAM-based neural networks, also known as *n*-tuple classifiers or weightless neural networks, do not store knowledge in their connections but in Random Access Memories (RAM) inside the network's nodes, or neurons. These neurons operate with binary input values and use RAM as lookup tables: the synapses of each neuron collect a vector of bits from the network's inputs that is used as the RAM address, and the value stored at this address is the neuron's output. Training can be made in one shot and basically consists of storing the desired output in the address associated with the input vector of the neuron [12].

In spite of their remarkable simplicity, RAM-based neural networks are very effective as pattern recognition tools, offering fast training and test, in addition to easy implementation [10]. However, if the network input is too large, the memory size becomes prohibitive, since it must be equal to 2^n, where n is the input size. Virtual Generalizing RAM (VG-RAM) Weightless Neural Networks (WNN) are RAM-based neural networks that

only require memory capacity to store the data related to the training set [11]. In the neurons of these networks, the memory stores the input-output pairs shown during training, instead of only the output. In the test phase, the memory of VG-RAM WNN neurons is searched associatively by comparing the input presented to the network with all inputs in the input-output pairs learned. The output of each VG-RAM WNN neuron is taken from the pair whose input is nearest to the input presented—the distance function employed by VG-RAM WNN neurons is the Hamming distance. If there is more than one pair at the same minimum distance from the input presented, the neuron's output is chosen randomly among these pairs.

Figure 1 shows the lookup table of a VG-RAM WNN neuron with three synapses (X_1, X_2 and X_3). This lookup table contains three entries (input-output pairs), which were stored during the training phase (entry #1, entry #2 and entry #3). During the test phase, when an input vector (input) is presented to the network, the VG-RAM WNN test algorithm calculates the distance between this input vector and each input of the input-output pairs stored in the lookup table. In the example of Figure 1 the Hamming distance from the input to entry #1 is two, because both X_2 and X_3 bits do not match the input vector. The distance to entry #2 is one, because X_1 is the only non-matching bit. The distance to entry #3 is three, as the reader may easily verify. Hence, for this input vector, the algorithm evaluates the neuron's output, *Y*, as class 2, since it is the output value stored in entry #2.

Lookup Table	X_1	X_2	X_3	Y
entry #1	1	1	0	label 1
entry #2	0	0	1	label 2
entry #3	0	1	0	label 3
	↑	↑	↑	↓
input	1	0	1	**label 2**

Figure 1: VG-RAM WNN neuron lookup table

2.2.2. Face Recognition with VG-RAM WNN

Our VG-RAM WNN architecture for face recognition has a single bidimensional array of $m \times n$ neurons, *N*, where each neuron, $n_{i,j}$, has a set of synapses, $W = (w_1, w_2, ... w_{|W|})$, which are connected to the network's bidimensional input, Φ, of $u \times v$ inputs (see Figure 2 and Figure 3). The synaptic interconnection pattern of each neuron $n_{i,j}$ follows a bidimensional Normal distribution with variance σ^2 centered at φ_{μ_k,μ_l} where $\mu_k = \frac{i.u}{m}$ and $\mu_i = \frac{j.v}{n}$; i.e., the coordinates *k* and *l* of the elements of Φ to which $n_{i,j}$ connects via *W* follow the probability density functions:

$$\omega_{\mu_k,\sigma^2}(k) = \frac{1}{\sigma\sqrt{2\Pi}} e^{\frac{-(k-\mu_k)^2}{2\sigma^2}}$$

$$\omega_{\mu_l,\sigma^2}(l) = \frac{1}{\sigma\sqrt{2\Pi}} e^{\frac{-(l-\mu_l)^2}{2\sigma^2}}$$

where σ is a parameter of the architecture (Figure 2). This synaptic interconnection pattern mimics that observed in many classes of biological neurons [13], and is created when the network is built and does not change afterwards.

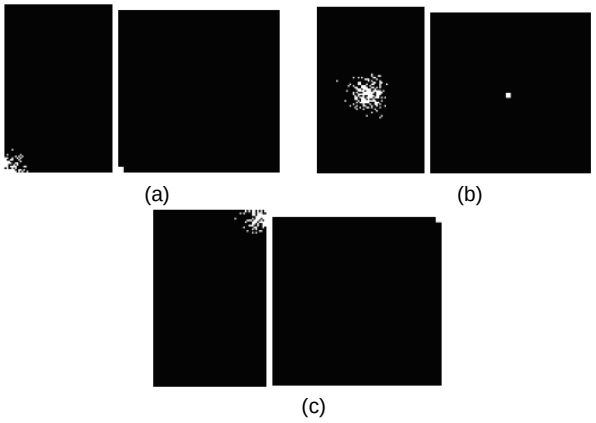

Figure 2: The synaptic interconnection pattern of our VG-RAM WNN architecture for face recognition. (a) Left, input Φ: in white, the elements $\varphi_{k,l}$ of the input Φ that are connected to neuron $n_{1,1}$ of *N* via $\Omega_{1,1,\sigma}(W)$. Right, neuron array *N*: in white, the neuron $n_{1,1}$ of *N*. (b) Left: in white, the elements $\varphi_{k,l}$ of Φ connected to $n_{\frac{m}{2},\frac{n}{2}}$ via $\Omega_{\frac{m}{2},\frac{n}{2},\sigma}(W)$. Right: in white, the neuron $n_{\frac{m}{2},\frac{n}{2}}$ of *N*. (c) Left: in white, the elements of Φ connected to $n_{m,n}$ via $\Omega_{n,n,\sigma}(W)$. Right: in white, the neuron $n_{m,n}$.

VG-RAM WNN synapses can only get a single bit from the input. Thus, in order to allow our VG-RAM WNN to deal with images, in which a pixel may assume a range of different values, we use *minchinton cells* [14]. In the proposed VG-RAM WNN architecture, each neuron's synapse, w_t, forms a minchinton cell with the next, w_{t+1} ($w_{|W|}$ forms a minchinton cell with w_1). The type of the minchinton cell we have used returns 1 if the synapse w_t of the cell is connected to an input element, $\varphi_{k,l}$, whose value is larger than the value of the element $\varphi_{r,s}$ to which the synapse w_{t+1} is connected, i.e., $\varphi_{k,l} > \varphi_{r,s}$; otherwise, it returns zero (see the synapses w_1 and w_2 of the neuron $n_{m,n}$ of Figure 3).

The input face images, *I*, of $\xi \times \eta$ pixels (Figure 3) must be transformed in order to fit into the network's input, Φ. The images are rotated, scaled, and cropped (Figure 4) automatically in three steps: (i) the position of the face in the image is found; (ii) based on the face position, the positions of the eyes are found (Figure 4(b));

and (iii) based on the positions of the face and eyes, the image is rotated, scaled and cropped to fit into Φ. Before being copied to Φ, the transformed image is filtered by a Gaussian filter to smooth out artifacts produced by the transformations (Figure 4(c)).

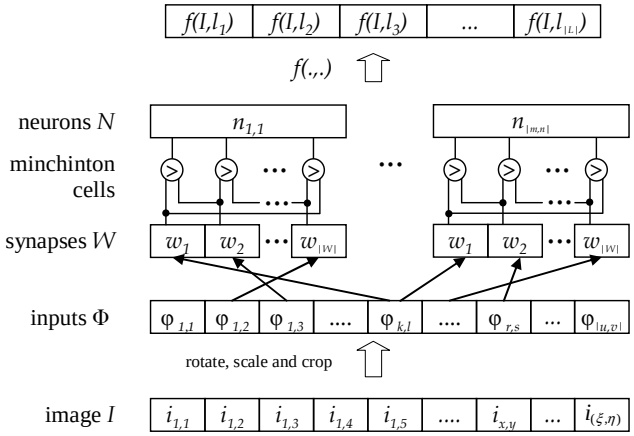

Figure 3: Schematic diagram of our VG-RAM WNN architecture for face recognition

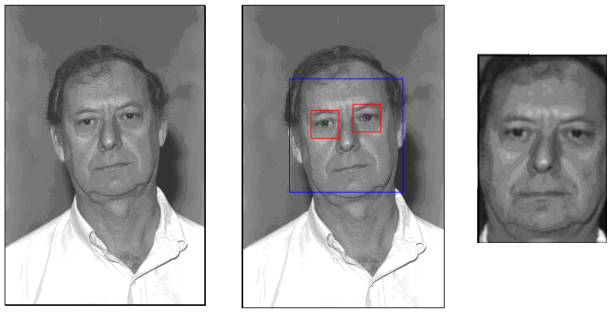

Figure 4: Face image and its preprocessing. (a) Original image; (b) positions of the face and eyes in the image; and (c) rotated, scaled, cropped and filtered image.

During training, the face image I_x of a person p is transformed and filtered, its pixels are copied to the VG-RAM WNN's input Φ, and all $n_{i,j}$ neurons' outputs are set to the value of the label $l_p \in L=\{l_1, \ldots l_{|L|}\}$ associated with the face of the person p ($|L|$ is equal to the number of known persons). All neurons are then trained to output this label with this input image. This procedure is repeated for all images I_x of the person p and, likewise, for all persons in the training dataset. During testing, each face image I_y is also transformed, filtered, and copied to the VG-RAM WNN's input Φ. Then, all neurons' outputs are computed and the number of neurons outputting each label $l_p \in L=\{l_1, \ldots, l_{|L|}\}$ is counted. The network output is given by the label l_p with the largest count along with the percentage of neurons that presented l_p as output for the face image I_y. This percentage is a matching score, $f(I_y, l_p)$, which quantifies the similarity between the face image I_y and the most similar one in the knowledge base that is indexed by the label l_p.

2.3. Access Control

We employed Bayesian inference for addressing the problem of access control. Given a face image I_y, our access control system maps the matching score $f(I_y, l_p)$—that quantifies the similarity between the face image I_y and the most similar image in the knowledge base, indexed by label l_p (Section 2.2.2)—into a probability measure, which indicates the degree of belief of the system in that the face image I_y belongs to a genuine individual. The system final decision is regulated by a threshold for the probability measure: if the probability measure is smaller than the threshold, the user associated with the face image I_y is rejected as an impostor; otherwise, the user is accepted as a genuine individual. The value of the threshold can either be specified by the system operator or automatically tuned using a validation dataset (not a part of the training dataset or the test dataset [15]), by varying the value of the threshold until the performance of the access control system is optimized on the validation dataset. The probability measure is computed using the Bayes' rule as described in the following.

The probability measure of interest, $p(A|B)$, is computed as the probability that a given face image, I_x, belongs to a genuine individual ($p(A)$), given that the neural network returned a matching score, $f(I_x, l_p)$, within an interval $b_i \in B=\{b_1, \ldots, b_{|B|}\}$ ($p(B)$). The random variable A may take two values: 1, if the given face image I_x belongs to a genuine individual; or 0, if the given face image I_x belongs to an impostor. The random variable B may take a continuous value within one of the intervals of $B=\{b_1, \ldots, b_{|B|}\}$.

The probability $p(A|B)$ can be computed using the Bayes' rule, i.e.:

$$p(A \mid B) = \frac{p(B \mid A) \times p(A)}{p(B)}.$$

The probability $p(A)$ can be estimated as the percentage of genuine individuals in the **training and validation datasets**. The probability $p(B)$ can be estimated as the percentage of times the neural network outputs a matching score within each interval of $B=\{b_1, \ldots, b_{|B|}\}$ for images in the **validation dataset**. Finally, the probability $p(B|A)$ can be estimated (using the **validation dataset**) as the percentage of matching scores within each interval $b_i \in B=\{b_1, \ldots, b_{|B|}\}$, given that the network returned genuine individuals.

3. Experimental Methodology

To evaluate our access control system we have used the Color Face Recognition Technology (FERET) database (http://face.nist.gov/colorferet). For that, we divided it into several datasets and used them to train, validate and test the performance of our system according to widely used biometric performance metrics.

3.1. Datasets

The Color FERET database contains a total of 11,338 face images with 512 by 768 pixels. They were collected by photographing 994 individuals at various angles over the course of 15 sessions between the years of 1993 and 1996. Among 13 different poses available in the database (frontal face and head turned from 15 to 75 degrees right and left), we considered 2 frontal face images of 991 individuals: the regular frontal face image, named *fa* in the database, and the alternative frontal face image, *fb*, taken shortly after the corresponding *fa* image. Figure 5 shows the regular frontal face image, *fa*, and the alternative frontal face image, *fb*, of one individual of the Color FERET database.

Figure 5: Regular frontal face image, *fa*, and alternative frontal face image, *fb*, of one individual of the Color FERET database

We derived three datasets using the frontal face images *fa* and *fb* of 991 individuals of the FERET database, namely CA1, CA2, e CA3.

3.1.1. CA1 Dataset

To obtain CA1, we partitioned the full dataset (*fa* and *fb* of 991 individuals of the FERET database) into 10 subsets of 100 individuals (the last subset has only 91 individuals). The first of these subsets was further partitioned into training and validation subsets—the training subset comprises the *fa* images of the first 50 individuals, while the validation subset comprises the *fb* images of all 100 individuals. Each of the remaining 9 subsets was partitioned into training and test subsets—the training subset comprises the *fa* images of the first 50 individuals, and the test subset comprises the *fb* images of all 100 individuals of the subset (91 in the last subset).

3.1.2. CA2 Dataset

To obtain CA2, we partitioned the full dataset into 5 subsets of 200 individuals (the last subset has only 191 individuals). The first of these subsets was partitioned into training and validation subsets—the training subset comprises the *fa* images of the first 100 individuals, while the validation subset comprises the *fb* images of all 200 individuals. Each of the remaining 4 subsets was partitioned into training and test subsets—the training subset comprises the *fa* images of the first 100 individuals, and the test subset comprises the *fb* images of all 200 individuals of the subset (191 in the last subset).

3.1.3. CA3 Dataset

To obtain CA3, we partitioned the full dataset into 2 subsets; the first with 400 individuals and the second with 591 individuals. The first of these 2 subsets was partitioned into training and validation subsets—the training subset comprises the *fa* images of the first 200 individuals, while the validation subset comprises the *fb* images of all 400 individuals. The second was partitioned into training and test subsets—the training subset comprises the *fa* images of the first 200 individuals and the test subset comprises the *fb* images of all remaining individuals in the subset.

3.2. Metrics

We evaluated the performance of our access control system according to two standard metrics for biometric recognition systems [16]:

- False Acceptance Rate (FAR), which is defined as the probability of an impostor being accepted as a genuine individual. It can be estimated as the ratio between the number of false positives and the total number of negatives (true negatives plus false positives).
- False Reject Rate (FRR), which is defined as the probability of a genuine individual being rejected as an impostor. It can be estimated as the ratio between the number of false negatives and the total number of positives (true positives plus false negatives).

There is a tradeoff between FAR and FRR. A larger FAR leads to a smaller FRR, while a larger FRR leads to a smaller FAR. In fact, both FAR and FRR are functions of the system threshold *t*. On the one hand, if *t* is decreased to make the system more tolerant, then FAR increases (and FRR decreases); on the other hand, if *t* is increased to make the system more secure, then FRR increases (and FAR decreases). The tradeoff between FAR and FRR is usually depicted in a receiver operating characteristic (ROC) curve, which is a plot of FAR against (1 - FRR) for various threshold values.

4. Experimental Results

In this section, we present the experiments employed to evaluate experimentally the performance of our access control system with 50, 100 and 200 users. To run these experiments, we used the Viola-Jones implementation that is part of the OpenCV library (http://sourceforge.net/projects/opencvlibrary/) and publicly available training datasets for face and eyes detection. We have set the parameters of our VG-RAM WNN to the best values obtained in previous works [8].

In order to use our system, its is necessary to estimate the values of the terms of the Bayes' rule ($p(A)$, $p(B)$ and $p(B|A)$), and to select a threshold for $p(A|B)$ (see Section 2.3). To estimate the values of the terms of the Bayes' rule and to select a threshold for $p(A|B)$ for the case of 50 users, we used the training and validation subsets of the first subset of the CA1 dataset.

In the first subset of the CA1 dataset, the number of users (genuine individuals) is equal to the size of the training subset: 50 individuals; while the number of non-users (impostors) is equal to the size of the validation set minus the number of users: 100 - 50 = 50 individuals. Therefore, $p(A)$ (the probability that a given face image, I_x, belongs to a genuine individual) is equal to 0.5 (the number of users divided by the total number of individuals: 50/100).

To obtain an estimate of $p(B)$ with the first subset of CA1, we train the network with its training set, examine the network output with the validation set, and compute the percentage of times the neural network outputs a matching score within each interval of $B=\{b_1, \ldots, b_{|B|}\}$.

To estimate $p(B|A)$, we compute the percentage of matching scores within each interval $b_i \in B=\{b_1, \ldots, b_{|B|}\}$ for which the network returned genuine individuals.

To select a threshold for $p(A|B)$, we varied its value, plotted a ROC curve and chose a threshold that gives acceptable values of FAR and FRR. The graph in Figure 6 shows the ROC curve of the first subset of CA1 for the threshold values shown in Table 1.

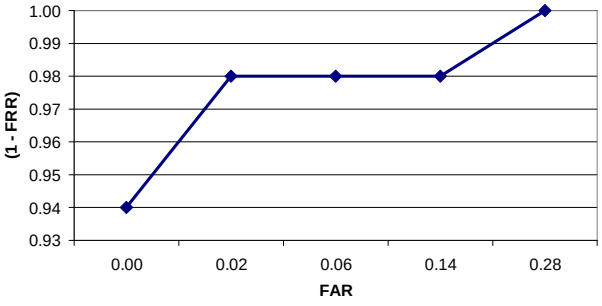

Figure 6: ROC curve of the first subset of CA1

As the graph in Figure 6 shows, our system can achieve a FAR equal to 0% with a FRR of 6% ((1 - FRR) = 0.94) for a threshold of 0.70 (see first data line of Table 1). For a threshold of 0.50, our system can achieve a FAR equal to 2% with a FRR of 2% (a rather small Equal Error Rate - EER).

Table 1: Effect of threshold on FAR and (1 - FRR)

Threshold	FAR	(1 - FRR)
0.70	0.00	0.94
0.50	0.02	0.98
0.35	0.06	0.98
0.25	0.14	0.98
0.09	0.28	1.00

Figure 7 presents the results in Table 1 in graph form (Figure 7(a)), together with equivalent results for CA2 ((Figure 7(b)) and CA3 (Figure 7(c)). As the graphs of Figure 7 show, with 50 users, our system presents an ERR of ~2%, with 100 users an ERR of ~9%, and with 200 users an ERR of ~9% as well.

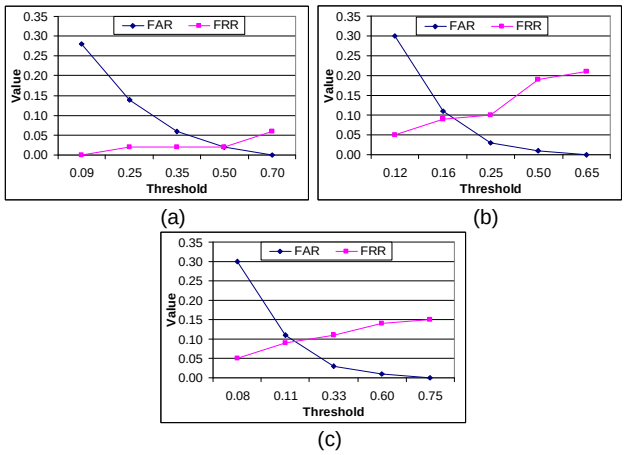

Figure 7: FAR and FRR of the first subset of CA1 (a), CA2 (b) and CA3 (c).

Table 2 presents the performance of our system for 50, 100, and 200 users obtained summarizing the performance derived from the 9 pairs of training and test subsets of CA1, the 4 pairs of training and test subsets of CA2, and the training and test subset of CA3. In order to obtain the results of Table 2, we run experiments with the validation sets of CA1, CA2 and CA3 to try and find the thresholds that favor better (smaller) FAR. In most cases of access control, this is the case, i.e., one prefers a smaller false acceptance rate even if it increases the false rejection rate (or decreases (1 - FRR)).

Table 2: Performance of the access control system for CA1, CA2 and CA3

Data Set	Threshold	FAR	(1 - FRR)
CA1	0.50	0.048	0.931
CA2	0.25	0.018	0.903
CA3	0.33	0.008	0.930

As Table 2 shows, with 50 users, the system correctly authenticated 93.1% of users with a FAR of 4.8%. With 100 users, the system was able to correctly authenticate

90.3% of the users with a FAR of 1.8%. Finally, with 200 users, the system was able to correctly authenticate 93.0% of the users with a FAR of only 0.8%.

5. Discussion

An important aspect of our system is that, in order to select the threshold for $p(A|B)$, it is necessary to use a set of impostors. Actually, the ratio between the size of this set and the size of the set of genuine individuals affects the FAR and FRR of the system. In our experiments we used a ratio equal 1, but this ratio must be estimated for each possible scenario of use of the system in order to properly select a threshold for $p(A|B)$.

Although currently there are many commercially available systems for access control via face recognition, we could only find a single paper about the subject in the literature, [17]. However, the access control system via face recognition proposed by Bryliuk and Starovoitov in [17] employs standard weighted multilayer Perceptron neural networks, instead of weightless neural networks, and train with several image samples per individual. Also, they do not use Bayesian inference to decide about grating the access. Finally, their best FAR and FRR for EER is ~12% with a rather smaller face dataset—40 individuals (http://www.cam-orl.co.uk/facedatabase.html).

6. Conclusions and Future Work

We present a facial access control system based on VG-RAM weightless neural networks (WNN). Our system uses the Viola-Jones approach to detect faces and eyes within these faces in images, forward positions of detected faces and eyes to VG-RAM WNN for recognition of previously trained faces, and employs Bayesian inference for granting or not access to a given resource or environment.

We evaluated our system using the Color FERET database in scenarios that simulate the use of our system with 50, 100 and 200 enrolled users. Our experimental results show that, tuning the system to favor a better (smaller) False Acceptance Rates (FAR), in the case of 50 users, it is able to correctly authenticate 93.1% of users with a FAR of 4.8%. With 100 users it can correctly authenticate 90.3% of the users with a FAR of 1.8%, and with 200 users it can correctly authenticate 93.0% of them with a FAR of only 0.8%.

As future work we plan to deploy our system in a real case scenario and examine its performance using live video.

7. Acknowledgements

We would like to thank Conselho Nacional de Desenvolvimento Científico e Tecnológico-CNPq-Brasil (grants 309831/2007-5, 620185/2008-2, 314485/2009-0) and Fundação de Amparo à Pesquisa do Espírito Santo-FAPES-Brasil (grant 48511579/2009) for their support to this research work.

8. References

[1] L. Hong and A. Jain. Integrating Faces and Fingerprints for Personal Identification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 12:30-36, 1998.

[2] R. Vetter. Authentication By Biometric Verification. Computer, 43(3):28-29, 2010.

[3] M.H. Yang, D.J. Kriegman, and N. Ahuja. Detecting Faces In Images: A Survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(1):34-58, 2002.

[4] W. Zhao, R. Chellappa, J. Phillips, and A. Rosenfeld. Face Recognition: A Literature Survey. ACM Computing Surveys, 35(4):399-458, 2003.

[5] A.S. Tolba, A.H. El-Baz, and A.A. El-Harby. Face Recognition: A Literature Review. International Journal of Signal Processing, 2(2):88-103, 2005.

[6] P. Viola and M. Jones. Robust Real-Time Object Detection. In Proceedings of the 2nd International Workshop on Statistical and Computational Theories of Vision - Modeling, Learning, Computing and Sampling, p. 1-25, Vancouver, Canada, 2001.

[7] A.F. De Souza, C. Badue, F. Pedroni, E. Oliveira, S. S. Dias, H. Oliveira, and S. F. Souza. Face Recognition With VG-RAM Weightless Neural Networks. Lecture Notes in Computer Science, 5163(1):951-960, 2008.

[8] A.F. De Souza, C. Badue, F. Pedroni, S.S. Dias, H. Oliveira, and S. F. de Souza. VG-RAM Weightless Neural Networks for Face Recognition. In: Face Recognition, p. 171-186, InTech, 2010.

[9] Y. Freund and R.E. Schapire. A Decision-Theoretic Generalization of On-line Learning and An Application to Boosting. In Proceedings of the Second European Conference on Computational Learning Theory (EuroCOLT '95), p. 23-27, 1995.

[10] I. Aleksander. From WISARD to MAGNUS: A Family of Weightless Virtual Neural Machines. In: RAM-Based Neural Networks, p. 18-30, World Scientific, 1998.

[11] T.B. Ludermir, A.C.P.L.F. Carvalho, A.P. Braga, and M.D. Souto. Weightless Neural Models: A Review of Current and Past Works, Neural Computing Surveys 2: 41-61, 1999.

[12] I. Aleksander. Self-Adaptive Universal Logic Circuits. IEE Electronic Letters, 2(8): 231-232, 1966.

[13] E.R. Kandel, J.H Schwartz, and T.M. Jessell. Principles of Neural Science, Prentice-Hall International Inc, 2000.

[14] R.J. Mitchell, J.M. Bishop, S.K. Box, and J.F Hawker. RAM - Based Neural Networks, World Scientific, chapter Comparison of Some Methods for Processing Grey Level Data in Weightless Networks, p. 61-70, 1998.

[15] F. Sebastiani. Machine Learning in Automated Text Categorization. ACM Computing Surveys, 34(1):1-47, 2002.

[16] A. Jain, A. Ross, and S. Prabhakar. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1):4-20, 2004.

[17] D. Bryliuk and V. Starovoitov. Access Control by Face Recognition Using Neural Networks and Negative Examples. In Proceedings of the 2nd International Conference on Artificial Intelligence (ICAI'2002), p. 428-436, 2002.