Protection of iris samples with the Glass Maze Algorithm

Edlira Martiri
University of Tirana
Albania
edlira.martiri@unitir.edu.al

Enkeleda Ibrahimi
Security Analyst, Vodafone AL
Albania
enkeleda.ibrahimi@vodafone.com

Abstract

Considering the increasing usage of biometrics as an authentication method by many institutions in order to replace or enhance traditional security systems, it raises a need to create and improve biometric recognition systems. In this work we will discuss about iris recognition systems and implement a novel technique of template protection based on key-binding. It is a scheme that uses neural networks which nodes are fed by the binary representations of the iris. Keys are encoded according to the idea of Trugenberger, i.e. applying the spin glass and the Hopfield neural network. The system is implemented on a database of 86 subjects to show its applicability.

1 Introduction

The increasing demand for security, deriving from past and recent events worldwide, has brought to the front the necessity to use techniques for the identification of individuals. Modern societies tend to attribute this increasing importance to systems that provide this type of service by offering safety and protection towards information. For this reason, the use of biometric systems has been encouraged by many public and private institutions in order to replace or enhance traditional security systems. In essence, the objective is to establish the identity of a subject based on what he is (face, fingerprints, voice, etc), not on what he has (smartcards), or what he knows (passwords).

A biometric recognition system is used to identify a person through the measurement of physiological or behavioral characteristics and the comparison with other previously validated and stored references within a database. These characteristics can be behavioral, such as voice, handwriting or typing style, or physiological such as iris, fingerprint, hand, face, etc. Considering that the recognition performance of a biometric system is achieved, one challenge is to protect our characteristics in the database where they reside, or when they pass through communication channels. To this aim, different protection mechanisms have been designed to protect the biometric template, the digital representation of our biometric characteristics. In this work we will discuss about iris recognition systems and a novel technique of template protection based on key-binding. It is a scheme that uses neural networks which nodes are fed by the binary representations of the iris. For the key it is used the theory of spin-glasses where it was tested on a small scale database.

2 Biometric recognition

When designing a system for user authentication we have to take into consideration three main factors: the level of security, the convenience and the cost of authenticators. An authenticator [Ogo03] can be a password (knowledge-based authenticators), a token (object-based authenticators), and biometric (ID-based authenticators). The third type of authenticator, biometrics, is different from the other two since they depend on the human body traits and features. Biometric Systems nowadays use different biometric characteristic types in order to identify individuals. The biometric signal that is obtained from the capturing device can be stable over time such as our fingerprints or alterable when it depends on human behaviors such as the voice [Ogo03]. The former are called physiological, and the later behavioral biometrics. Klosterman et al. explain that biometric traits are not secrets and cannot be used in the same way as passwords or tokens are. They present in [Klo00] six differences between them which are listed below: 1. *Biometrics is not secrets.* 2. *Biometrics is not completely accurate.* 3. *Biometrics can be continuously monitored.* 4. *Biometrics is expensive to compute.* 5. *Biometrics is unique per-individual measures.* 6. *Biometrics is not universally desirable.* In any

case it is necessary to emphasize that there is no system clearly better than the other, the choice therefore appears to be a compromise between the qualities of the properties associated with the selected characteristic and production costs. These properties include [Rath11]: universality, uniqueness, permanence, performance, acceptability, collectability, circumvention.

One of the robust biometric characteristics widely used are irises. The pigmentation and the radial arrangement of the fibers of the iris are unique characteristics to each individual (the iris has 266 unique features, while the fingerprint has only 90) [Kal13], [Kha13] and it is also proved that the irises of twins homozygotes are completely different from one another (unlike the DNA that is very similar). Even in the same individual the iris of the right eye is different from the iris of the left eye [Dau14]. In light of all these considerations, the choice of the iris as a characteristic of a biometric system implies an efficient system.

Recognition systems based on iris have been used with success in distinct sectors, such as the border check-in, or control of refugees. The iris recognition technique consists of five steps: acquisition, segmentation, normalization, feature extraction and the comparing step [Dau14].

(1) Acquisition

During this process the "captured" image of the subject must serve as input to the recognition system. The aspects to be kept in mind at this stage regard the type of acquisition device.

(2) Segmentation

The region of the iris can be approximated by two circles, one for the outlined iris / sclera and another, internal to the first, for the contour of the iris / pupil. Eyelashes and eyelids can sometimes occlude the upper and lower parts of this region and for this reason, in addition to locating the region of interest, are used techniques to exclude these parts [Mal03]. Two techniques used to implement iris segmentation are Hough transform and Daugman method.

Hough transform

It is an algorithm commonly used in image processing to determine the parameters of geometric figures within a simple picture [Illi88]. In the context of iris recognition this algorithm can be used to derive radii and centers contours corresponding to the iris and the pupil. The Hough transform can be seen as a transformation of a point from the plane (x, y) of the image to the space of the parameters, in base of the geometric figure to identify [Mal03].To identify better the circles that represent the contour between iris and sclera the algorithm extracts the region of interest [Mal03].

$$(y' \cdot cos\vartheta' - x' \cdot sin\vartheta')^2 = a \cdot (x' \cdot cos\vartheta' + y' \cdot sin\vartheta') \quad (1)$$

where y' and x' indicate the peak coordinates and ϑ' is the rotation angle relative to the horizontal axis.

Daugman method

It requires the use of an integro-differential operator constructed to locate the circular regions of iris and pupil, and arches that define the contours of the eyelids. If they have circular shape, the operator is defined as:

$$max_{r,x_0,y_0}|G_\sigma(r) \cdot \frac{\delta}{\delta r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \quad (2)$$

where I is the intensity value of the image at the point of coordinates (x, y), r is the radius, s is the track and G is a Gaussian filter defined as [Dau14]:

$$G_\sigma(r) = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{(r-r_0)^2}{2\sigma^2}} \quad (3)$$

(3) Normalization

Inconsistencies between different dimensional images are mainly due to expansion or contraction of the iris, caused by contraction or expansion of the pupil in variable lighting conditions [Mal03]. Rubber Sheet Model of Daugman This normalization model, represents every point extracted from the iris in a space defined from the coordinates (r, ϑ), where r is included in [0, 1] and ϑ is the angle in the interval $[0, 2\pi]$. The normalization of points from the Cartesian plane to polar coordinates is modelled as:

$$I(x(r,\vartheta), y(r,\vartheta)) \longrightarrow I(r,\vartheta) \quad (4)$$

$$x(r,\vartheta) = (1-r) \cdot x_p(\vartheta) + r \cdot x_i(\vartheta) \quad (5)$$

$$y(r,\vartheta) = (1-r) \cdot y_p(\vartheta) + r \cdot y_i(\vartheta) \quad (6)$$

where, x_p and y_p indicate the coordinates of the points on the pupil contour for a certain angle ϑ [Mal03].

(4) Feature Extraction

To provide an overview of the procedures required for the extraction and encoding of the biometric feature, we describe one of the methods discussed in the literature. This algorithm explained in [Kah10] works as follows: (1) The normalized template is divided in rows where every row represents the intensity values inside of a circular track. (2) The frequency response of the mono-dimensional Log-Gabor filter is calculated by means of the formula:

$$G(f) = e^{\frac{-(log(\frac{f}{f_0}))^2}{2(log(\frac{\delta}{f_0}))^2}} \quad (7)$$

where f_0 is the central frequency.

(3) For every extracted intensity function is calculated the FFT (Fast Fourier Transform) which is then multiplied with the frequency response of the Gabor filter. (4) After calculating the Inverse FFT of the filtered data, it is then quantized in phase by using four levels. Phase quantization is obtained by valuing the complex amplitude values by means of two binary masks, one for the real part and one for the imaginary part. The mask relative to the real part will contain 1 if the real part of the filtered data is greater than zero, and so the mask associated to the imaginary part.

(5) The binary codification of the iris

After being segmented and normalized, it is obtained by placing in columns the two binary masks. This template is called the Iris Code.

In Fig. 1 are presented the noise detection of an iris and the segmentation process. The normalization following it, will provide a binary template, as presented in Fig. 2

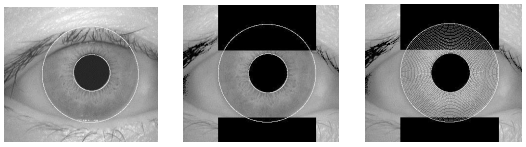

Figure 1: Normal iris; noise removal; and segmentation

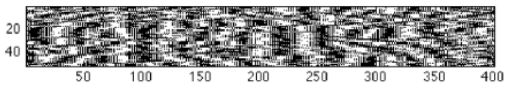

Figure 2: Binary representation of an iris code.

3 Hopfield networks

One of the major contributions to the study of artificial neural networks has been given by the work of Hopfield (from 1982 to 1985 with a series of papers) who studied a network whose units resemble the perceptron. The Hopfield network consists of a certain number of nodes totally connected between them but without auto-connections. The value of output of each node can be 0 or 1 (using the 'step'), or 1 or -1 (using the "sign" function: the output of the unit is 1 if the activation is positive and -1 if the activation is negative). The Hopfield network does not have a layer of input and an output, since each node acts both as input and output [Flo93]. One of the merits of the original work of Hopfield was to describe the dynamics of the network in terms of energy. Each state of the network represents a certain value of global energy. The central property of an energy function is that it always decreases (or remains constant) when a system evolves according to its dynamic rule.

The energy landscape of Hopfield networks presents a hilly view and the rule of adaptation of synaptic weights associates each pattern with an energy minimum. In the test phase the network starts from a state energy high enough which corresponds to a new pattern and slopes down towards the most similar vault. However, energy presents many minima many which do not correspond to any of the stored patterns: the most simple of them is a combination of three original patterns, while a more complex situation can be seen if a local minimum is not correlated to any pattern. These are called spin-glasses state, in correlation to the property of spin glasses in statistical mechanics. Basically, if we consider N-units (or neurons) indexed 1..N, the neuron i can be considered connected to the neuron j with a synaptic weight of $W(i,j)$, where $W(i,i) = 0$ and $W(i,j) = W(j,i)$. In every instant of time t, the neuron possess a potential of $X(t,i)$ which can have one of the two values: 1 or -1. A certain potential distribution is called state of the system. Considering that time is discrete, at instant $t+1$ the neuron assumes a potential that depends on the weighed sum of all the other neurons [Ami85].

$$X(t+1,i) = f(\sum_j (W(i,j)X(t,j)) \tag{8}$$

where f is the sign function mentioned above. Taking an initial state $X(0,i)$, the system evolves in a deterministic way, passing from one state to another showing a very particular discrete dynamic system. Such system, in a finite number of steps arrives in a fixed point. The fixed point can be one of the minima points P and Hopfield proofed that these fixed points correspond to the energy function introduced by him:

$$H(X) = -\sum_{i,j} (W(i,j)X(i)X(j)) \tag{9}$$

His idea was to model the surface of the energy in such a way that its minima should correspond to the states that the machine must acquire. If there are m-configurations to store/memorize it is sufficient to calculate:

$$W(i,j) = \sum_t (M(t,i)M(t,j) \tag{10}$$

where $M(x,y)$ is the x-configuration ($x = 1, ..., m$).

The surface of the energy can be imagined made of holes (the local minima) with different depths and surrounded of a vault, called the attraction vault. The initial status is represented by a certain position on

this surface and it must "fall into" one of these holes. Probably this will happen with a well-determined hole, but if there are holes less deep and narrower vaults, then it would be enough to "shake" a little bit the surface and the point would fall into another vault whose depth is deeper. But what does it mean to "shake" the surface? How is it possible to change the energetic values of the points? At this point we can see an interesting connection between Hopfield Neural Networks and magnetism.

4 Spin Glasses

There exists an isomorphism between the model of Hopfield and the Ising model of the magnetism at 0 degrees. The Ising model describes a system made of atoms which can be considered as tiny magnets that interact with each other until they reach equilibrium [Mez86]. These are scattered randomly and the function that describes the model of Ising has the same form of the model of Hopfield [Ami85]. In physics 'disorder' may indicate imperfect structures or impurities in a material. It is the counterpart of order since sufficient amount of randomness, of imperfections and inconsistencies may destroy the symmetries that dramatically simplify certain physical descriptions [Mez86]. For most the history of 'disorder' was pushed into a corner and scientists have been dedicated for decades to the study of ordered systems [Pen98]. One of the most successful attempts to understand the disordered systems is the study of the so-called 'spin-glass'. The composition of this material is a mixture of iron and copper atoms, but its magnetic properties are very complex and are unpredictable.

The 'spin' is the mechanical quantum which originates the magnetic properties and the 'glass' indicates the presence of disorder in the orientation of the spin [Men98]. The spin-glass is an excellent disordered system, applied in complex problems and in a plethora of subjects. Their characteristics, their dynamics and their complexity are as result of the magnetic interactions between the atoms that compound them. If a block of this alloy which certain atoms act as magnets is exposed to an outer magnetic field, the momenta inside of it tend to align in a particular direction [Mez86]. Sometimes it can be seen the same reaction as a consequence of strong internal effects [Men98]. As a result of this, the effect is named ferromagnetism and can be seen even in other materials (nickel, cobalt, etc.). A spin glass can have a lot of states of low energy, which are not separable easily in the same way that energy is stored in the surface of the Hopfield network. To obtain a state of low energy the temperature of the spin glass is raised and the direction of the spin is easily invertible. As a result the probability is higher to come out of holes that are not so deep. The temperature is introduced by means of a probabilistic technique. As in [Tru11] the formula that guides the evolution of the system is $P(X(t+1),i)=1)=\varphi(\sum_j(W(i,j)X(t,j))$, where $P(x)$ is the probability that at time $t+1$ the i-neuron takes the value of 1. The function φ is not the sign function any more, but:

$$\varphi(z)=\frac{1}{1+e^{\frac{-z}{T}}} \tag{11}$$

where T represents the temperature. If $z \to \infty$), $\varphi(z)=1/2$, and the system is chaotic. The higher the temperature the more agitated the system is and it is easier to go out of small energetic holes. What the technique suggests is to undergo through a series of alternating heating and cooling [Spr13]. These are called evolutions of the system and this kind of system gives very good results in different applications.

4.1 The idea of Trugenberger

In his paper Trugenberger gives the idea of applying the spin glass and the *Hopfield NN* to encode keys as a local minimum configuration. The key is used to protect fingerprints in a similar way as the fuzzy vault technique does [Jue02]. This process passes through some steps. The first one is quantization where the fingerprint is represented as a set of $M(x_i,y_i)$ minutiae coordinates which create a configuration of the Hopfield NN. But, since in the Hopfield model we need a binary representation of data, Trugenberger creates this input by taking into consideration N-squares of pixels from the fingerprint image and to each of them is associated one neuron. If inside the square there is at least one minutiae, the state of the neuron is 1, and if there are no minutiae, then the state of the neuron is -1. Before passing to the second step let's suppose that every column of the iris code, which is a vector of binary values, is represented by one neuron. If the total number of bits '*1*' is more than or equal two the number of bits '*0*' than the neuron will take status *1*, otherwise the neuron will take status *0*. This is a configuration and we call it σ^{iris}. As in the fingerprint case, the enrolled iris becomes one particular state configuration: σ_i^{iris}.

The next step is the key generation. This key that will be bounded is created by modifying a certain amount k of columns of the iris configuration. Let's call it σ_i^{key}. The two configurations σ_i^{iris} and σ_i^{key} are considered that belong to the same subject if their Hamming distance is equal to k.

5 Experiments

During verification, the correct iris will evolve toward one fixed point, which is the key and if it is not, then

the evolution will emerge a completely different key. According to Trugenberger the number k of patterns for fingerprints is chosen as $\alpha = k/N$ with values between 0.051 and 0.138. We will use in our case $\alpha = 0.1$.

Practically, we generated 86×7 iris codes and each one of them is made of 20 rows and 480 columns. We divided it into blocks of 20×20 having as a result 24 blocks. These blocks will let us create e Hopfield NN made of 24 nodes. If we feed the genuine configuration it always converges to it, otherwise it converges to the nearest one in terms of Hamming distance. The recognition performance based on the Equal Error Rate of the system is 5.3%.

6 Conclusions

In this work we discussed about iris recognition systems and a novel technique of template protection that uses neural networks. It is a scheme in which nodes are fed by the binary representations of the iris. For the key it is used the theory of spin-glasses where it was tested on a small scale database. As future work, it still needs a deeper verification of the Neural Network with different number of nodes. For a more accurate recognition performance a database with a larger number of subjects needs to be tested.

Acknowledgements

The authors want to thank the Norwegian Biometrics Laboratory at NTNU, Norway, and the reviewers of RTA-CSIT'16 for their helpful comments.

References

[Ami85] Amit, D., Gutfreund, H., Sompolinsky, H., Spin-glass models of neural networks, The American Physical Society, 1985.

[Dau14] Daugman, J., How Iris Recognition Works, IEEE Trans. CSVT 14(1), pp. 21 30.

[Flo93] Floreano, D., Nolfi, F., Reti neurali: algoritmi di apprendimento, ambiente di apprendimento, architettura, Giornale italiano di psicologia / a. Xx, febbraio - 15-50. 1993

[Illi88] Illingworth, J., Kittler, J., A survey of the hough transform Computer vision, graphics, and image processing 44, 87-116 (1988)

[Jue02] Juels, A., Wattenberg M., A fuzzy vault scheme. In Proc. IEEE Int. Symposium on Information Theory, 2002.

[Kah10] Kahlil, A., Abou-Chadi, Generation of iris codes using 1d log-gabor filter. IEEE, 2010.

[Kal13] Kale, J., Pardeshi K., Nirgude V., Improved Iris Recognition using Discrete Fourier, Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 93-97 (2013)

[Klo00] Klosterman, A., Ganger, G., "Secure continuous biometric-enhanced authentication", 2000. Computer Science Department. http://repository.cmu.edu/compsci/2113

[MaL03] Masek, L., Recognition of Human Iris Patterns for Biometric Identification, School of Computer Science and Software Engineering, The University of Western Australia, 2003

[Men98] Mencuccini, Silvestrini, "Fisica: elettromagnetismo e ottica", Liguori Editore, Italy, 1998.

[Mez86] Mezard, M., Parisi G., Spin Glass Theory and Beyond, World Scientific Publications, Singapore, 1986.

[Ogo03] O'Gorman L., "Comparing passwords, tokens and biometrics for user authentication", Proceedings of IEEE, vol. 91, no. 12, 2003, doi:10.1109/jproc.2003.819611, pp. 2021-2040.

[Pen98] Penrose, R., Shadows of the Mind: A Search for the Missing Science of Consciousness, Oxford University Press. ISBN 0-19-853978-9, 1998.

[Rath11] Rathgeb, C., Uhl, A., A survey on biometric cryptosystems and cancelable biometrics, EURASIP Journal on Information Security 2011.

[Spr13] Springer, M., Protection of Fingerprint Data with the Glass Maze Algorithm, BIOSIG, 2013.

[Tru11] Trugenberger, C., The Glass Maze: Hiding Keys in Spin Glasses. BIOSIG 2011: 89-102