GENERATION OF CRYPTOGRAPHIC KEY FROM EYE BIOMETRIC FEATURES

Lukáš Semerád

Master Degree Programme (3), FIT BUT

E-mail: xsemer04@stud.fit.vutbr.cz

Supervised by: Martin Drahanský

E-mail: drahan@fit.vutbr.cz

Abstract: The paper discusses ways of information processing in iris and retina of the human eye. It also has a hint of possible computations of information entropy, which is still yet probably still a lot of people did not pay attention. The found methods will be further used to create cryptographic keys.

Keywords: EEICT, retina, iris, entropy

1. INTRODUCTION

We see the use of biometrics in our normal life very often. Practically, there are not used only fingerprints. The use of some biometrics was connected more to a sci-fi world. A short time for development in biometrics has not lead to an exploration of all parts of biometrics in detail yet. One of them is the question of the amount of information in eye iris and retina. Because both of them are already used as biometric characteristics, it is also interesting to know how much information contains the biometric template.

2. RETINA

The retina is a light sensitive surface on the back of the eye, consisting of a large number of nerve cells and blood vessels. The yellow spot is one place on the retina, where is the sharpest vision in the eye. Next to it is a blind spot, where no light sensitive cells could be found, because this way goes away from the vessels of the eye.

In 1935 doctors C. Simon and I. Goldstein discovered that the blood vessels in the retina are different by various people [4]. Moreover vein structure remains unchanged throughout life and is well protected from the environment. Unfortunately it is also well protected from simple sampling for biometric systems.

For high quality of the scans, it is necessary to use the medical equipment. For standard quality of the scans are sufficient to use manufactured devices, but exposure time takes several tens of seconds. Retina is transparent for infrared light, but vessels this light reflected. First functional system based on retinal scan was created by EyeDentify in 1975. Other systems are for example Retinal Technologies, Trans Pacific Int. or RaycoSecurity [1].

Positive qualities have very low probability of false positives and the extremely low percentage of false negatives. Unfortunately, various eye diseases reduce results quality and success of identification. For example glaucoma or inflammation degrades.

2.1. ENTROPY OF RETINA

Counting entropy of eye retina is performed in several ways, similar to fingerprints. We used similar method of calculation. We study every pixels of the retinal image. For each point we examine

whether there may be a fork or termination of the vessel. Theoretically we could say that this character can occur anywhere in each pixel. As we know from images and physics of retinal blood vessels, practically it is not possible. So, if we assume that one pixel to the fork occurs, in next few pixels this fact cannot happen again. According to the procedure described theoretically find out how much minutiae can be present in the retinal image. Moreover, for each occurrence we remember its position in the image, the angle of vessel, the minutiae type and thickness of the blood vessels.

Calculation entropy from properties of eye is similar to the theoretical. It is necessary to determine, how much average occurs on eye retina of the individual symbols, branching and termination vessels. Again, this will depend on image resolution and quality of scanning cameras.

First variable in the formula 2.1 is average count δ of minutiae location. Determine their location by coordinates in the polar coordinate system *(r, Θ)*. First axis is coming from inside the slices. Second coordinate is given by degree angle. It is similarly to Daugman‘s normalization coordinates of iris. Furthermore, we determine the angle ω of each vessel. Mostly, are two angles very similar, and in the direction from the blind spot. In the formula, it will symbolize a variable indicating the number of different angles, in which all vessels are likely to lying. We are interested also, of course, the total area of the sector to be used depends on the resolution. Finally, we used the thickness of the main and tangential blood vessels. Maximum thickness width of the vessels would be approximately one tenth of the width of the ring segments.

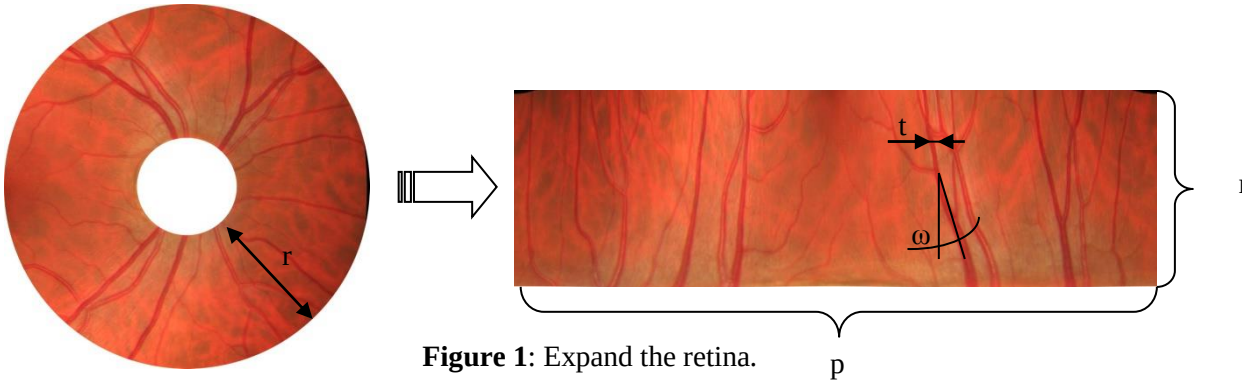

Figure 1: Expand the retina.

Approximate theoretical amount Ψ in all combination of crossing vessels will be

$$\Psi = \binom{p \cdot r}{n} \cdot \binom{\omega}{3} \cdot \binom{t+1}{2} \tag{2.1}$$

In formula 2.1, *r* is radius of ring in pixels, *p* is number of pixels in width, *n* is average amount of minutiae in picture, ω is number of possible tilt angles vessels, *t* is maximal thickness of vessels.

It can be assumed that in certain parts of the image will not appear minutiae. The formula can then be based on experimental findings improved and instead only part of the ring.

3. IRIS

Most noticeable part of the eye is the iris. Function of iris is control level of light entering to the eye. Visual texture is formed during the first two years of life. Characteristics of the iris are stabilized early after birth. Texture and features remain unchanged throughout the life of man.

The combination of colors, textures and patterns of the iris are different for each person. Iris color is caused by melanin pigment. The melanin in the iris absorbs visible light and reflects most of the infrared. More preferred capture method is currently in infrared spectrum. Loss of color information is not so important. Iris patterns are also named characters, like fingerprints. For example arched ligaments, furrows, ridges, crypts, rings, corona, freckles or zigzag lines. For the fingerprint is approximately 60 named patterns for iris it over 400 [3]. Two irises of identical twins are differ-

ent and unique [5]. Similarly, two irises of one person are different too. The most frequently used method of image processing iris is Daugman algorithm [2].

3.1. ENTROPY OF IRIS

Similarly to the retina, let us try to count the number of possible combinations Ψ occurrences of various features in the iris. For illustration, let's take only one of minutiae type - the crypt. Coordinate system of polar coordinates will be same as in retina *(r, Θ)* and its transform is shown on Figure 2. On position of occurrence we store approximate radius of one crypt and approximate shape. This pattern is very big and therefore we will proportionately reduce its size from the total area.

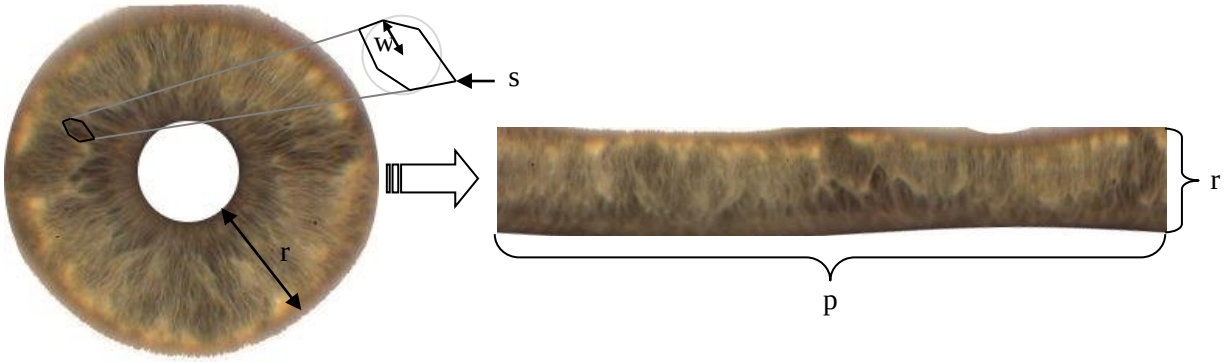

Figure 2: Iris expands (w is radius average bounding circle, s is shape of crypt).

$$\Psi = \frac{\binom{p \cdot r}{n}}{\binom{\pi \cdot \kappa^2}{n}} \cdot \binom{M + n - 1}{n} \cdot \binom{\tau + n - 1}{n} \tag{3.1}$$

κ is average radius of crypts, p is number of pixels in width, n is average number of minutiae, r is radius of iris ring in pixels, μ is maximal width of crypt (practically found value), τ is number of shape pattern types (practically found). Expression $\binom{\pi \cdot \kappa^2}{n}$ from the total area subtract area of one crypt.

4. CONCLUSION

Paper outlined information about entropy calculations, which will be in future further developed and improved. Putting concrete values into formulas will require statistical analysis a lot of samples of irises and retinas.

REFERENCES

[1] Drahanský, M., Orság, F., Doležel M. a kol., Biometrie, Brno, 2011.

[2] Daugman, J.: How iris recognition works, Proceedings of 2002 International Conference on Image Processing, Vol. 1, 2002.

[3] Ross, A. A., Hornak, L., Li X.: Analysis and synthesis of iris images, Morgantown, West Virginia, Sarvesh Makthal 2005.

[4] Simon, C., Goldstein, I.: A new scientific method if identification, New York State Journal of Medicine, 1935, p 901-906

[5] Tower, P.: The fundus oculi in monozygotic twins, Archives of Ophtalmology, 1955, p 225-239