NATIONAL TECHNICAL UNIVERSITY OF UKRAINE
“IGOR SIKORSKY KYIV POLYTECHIC INSTITUTE”

FACULTY OF APPLIED MATHEMATICS

LIBRARY RESEARCH PAPER

The subject: “English for Professional Purposes”
On the topic: “Iris recognition”

Executed: Anna Bilous
group KP-93

Lecturer: Nataliia Chizhova

Kyiv 2021

Contents

Introduction

Since ancient times humans have been creating various algorithms and methods to authenticate an individual in order to ensure that the interlopers do not have access to secret information or can enter restricted areas. They used simple things based on verbal components like passphrases and passwords and more complex (usually material) structures such as ID cards and wristbands. However, all of them cannot be considered absolutely trustworthy: any person that discovers a password or gains ownership of the original or a perfect copy of someone’s ID card is granted access. Moreover, there are also other risks involving such methods of authentication: for example, the owner of ID card can just forget to take it with them or, to make matters worse, even lose the card.

This cannot be said about human’s biometrics: a person can’t just simply forget their fingers at home or lose their face. Also, it is almost impossible to reproduce other person’s retinal pattern or mimic their voice (at least, at the first try). Which is why with the current development of information technologies the usage of biometrics as an authentication method has become more widely-spread and has bigger potential than ever before. Biometrics can offer greater security and convenience than traditional methods for people recognition because biometric authentication can establish an unbreakable one-to-one correspondence between an individual and a piece of data.

Iris recognition is one of the latest biometric authentication processes among all other technologies in biometrics and has become a popular research in recent years. Due to its reliability and nearly perfect recognition rates, iris recognition is used in high security areas. Among its applications are border control in airports and harbors, access control in laboratories and factories, identification for Automatic Teller Machines (ATMs) and restricted access to police evidence rooms. In this technology, authentication is based on the patterns of eyes and iris. The accuracy of iris recognition is high as compared with other biometric authentication, which is why this paper focuses on this method as the most precise method of currently available out of all biometric authentication methods. This paper provides a detailed explanation of the most common algorithms used during iris recognition, as well as real-life examples of this method’s utilization.

Despite the fascinating progress in iris recognition development, the absolute replacement of the “classical” methods of authentication is unlikely: the aforementioned method has major disadvantages that still prevent its universal use. For instance, one advantage of passwords over iris recognition is that they can be re-issued, which is naturally impossible for the latter. The use of biometrics still has major weaknesses that must be taken into consideration before implementing them. One of the aims of this research paper is to cover the advantages and drawbacks of iris recognition as a method of authentication.

Overall, the purpose of this research paper is to familiarize with existing algorithms used in iris recognition method, analyze the advantages and disadvantages of iris recognition authentication over other biometric authentication methods and provide real-life examples of iris recognition systems.

1. Stages of iris recognition algorithm

The three main stages of an iris recognition system are image preprocessing, feature extraction and template matching. The first stage is divided into three steps: iris localization, iris normalization and image enhancement. The purpose of the second stage is to extract main features from the normalized iris image. The last stage compares the obtained template with templates from the database using a matching metric.

1.1. Iris image capture

Image capturing involves the usage of cameras. One of the examples is the use of a desktop camera with the help of a measure. User must maintain distance between himself and the camera (usually around half a meter). Then, the user must center his eye in order to see a ring inside the camera aperture. Some systems provide a spot of light. The user is at the wrong distance unless the light fills up the circle: if the light is larger than the circle, the user is too close, and if the light does not fill the circle completely, the user is too far. Other cameras provide a luminous circle that turns from one color to another when the user is properly set.

1.2. Image preprocessing

The purpose of this step is to obtain useful iris region from the whole image.

1.2.1. Iris localization

At this step the inner and outer boundaries of the iris are detected, which can be both approximately modeled as circles. The center of iris does not necessarily have to be concentric with the center of pupil. Iris localization is important because correct iris region is needed to generate the templates for accurate matching. An explanation of three most commonly used localization algorithms will be given.

Integro-differential operator is used for locating the inner and outer boundaries of iris, as well as the upper and lower eyelids using the first derivative. The operator computes the partial derivative of the average intensity of circle points. After convolving the operator with Gaussian kernel, the maximum difference between inner and outer circle will define the center and radius of the iris boundary. The operator is accurate because it searches over the image domain for the global maximum.

The bisection method is used to locate the center of the pupil, which is used as reference to detect the inner and outer boundaries of the iris. Firstly, edge detection is applied to the iris image to extract the edge information. For every two points on the same edge component, bisection method is applied to draw the perpendicular lines to the center point. The center point with maximum number of line intersections is selected as the center of the pupil. A virtual circle is drawn with reference to the center of the pupil and the radius is increased within a certain range. Two virtual circles with the largest number of edge points are chosen as the inner and outer boundaries of the iris.

Black hole search method is used to compute the center and area of a pupil. Since the pupil is the darkest region in the image, this approach applies threshold segmentation method to find the region. Firstly, a threshold is defined to identify the dark areas in the iris image, which are referred as “black holes”. The center of mass of these black holes is computed from the global image. The area of pupil is the total number of those black holes within the region. The radius of the pupil can be calculated from the circle area formula. However, this search method is not suitable for iris image with dark iris, because the iris area would be identified as a part of the black hole area.

1.2.2. Iris normalization

Iris may be captured in different size due to varying imaging distance and illumination variations. As a result, the radial size of the pupil may change accordingly, resulting in deformation of the iris texture and affection of the next processing stages. Therefore, the iris region needs to be normalized to compensate for these variations.

The homogeneous rubber sheet model algorithm remaps each pixel in the localized iris region from the Cartesian coordinates to polar coordinates. This method accounts for pupil dilation, imaging distance and non-concentric pupil displacement, but it does not compensate for the rotation variance.

1.2.3. Image enhancement

The normalized iris image has low contrast and non-uniform illumination caused by the light source position, thus there is the necessity to enhance the image to compensate for these factors. Local histogram analysis is applied to the normalized iris image to reduce the effect of non-uniform illumination and obtain well-distributed texture image. Reflections regions are characterized by high intensity values close to 255. A simple thresholding operation can be used to remove the reflection noise.

1.3. Feature extraction

In this stage, texture analysis methods are used to extract the significant features from the normalized iris image. The extracted features will be encoded to generate a biometric template. An explanation of four most commonly used feature extraction algorithms will be given below.

Wavelet transform decomposes the iris region into components with different resolutions. The features are localized in both space and frequency domains with varying window sizes. A bank of wavelet filters is applied to the normalized iris region. The output of the filters is encoded to generate a compact biometric template.

Laplacian of Gaussian filters are used to encode feature by decomposing the iris region and applying a cascade of Gaussian-like filters to the necessary image section. The filtered image is realized as a four-level Laplacian pyramid, which allows to generate a compact biometric template.

Key local variations are used to represent the characteristics of the iris by decomposing the normalized iris image into a set of 1D intensity signals and applying dyadic wavelet transformations to each signal. The local maximum and minimum points are encoded into a feature vector, which is later converted to a binary template with the same size as the normalized iris image.

During discrete cosine transform (DCT) the normalized image is divided into diagonal 8x12 patches, and DCT is applied along the patch’s length. The differences between the DCT coefficients of adjacent patches are obtained, and when there are zero crossings between the DCT coefficients (meaning that all corresponding coefficients are different), a binary template is generated from these coefficients. This coding method has low complexity, which makes it superior to other approaches in terms of both speed and accuracy.

1.4. Template matching

The generated template need a corresponding matching metric that compares the similarities between this template and the one stored in the database. An explanation of three most commonly used template matching algorithms will be given below.

Hamming distance is defined as the fractional measure of dissimilarity between two binary templates, where the value of zero would represent a perfect match. The two templates that are completely independent would give a Hamming distance near to 0.5. A threshold is set to decide the two templates are from the same person or different persons. The fractional hamming distance is sum of the exclusive-OR between two templates over the total number of bits. The advantage of Hamming distance is fast matching speed because the templates are in binary format. Hamming distance is suitable for comparisons of millions of template in large database.

For Weighted Euclidean distance the template is composed of integer values. Weighted Euclidean distance is defined as a measure of similarity between two templates and is calculated using Pythagorean Theorem to obtain the distance between the point of the template and corresponding point of the template in the database. The two templates are considered matched if the Weighted Euclidean Distance is a minimum.

Normalized correlation between two representations is defined as the normalized similarity of corresponding points in the iris region. The correlations are performed over small blocks of pixels in four different spatial frequency bands. However, normalized correlation method is not computationally effective because images are used for comparisons.

2. Advantages and disadvantages of iris recognition

Iris biometrics have several unique advantages when used for identification and authentication. These include:

1. Accuracy. The false acceptance rate and false rejection rate is very low in this modality, thus ensuring a higher rate of accuracy in its results.

2. Distance. Unlike retina scanning or fingerprint scanning, iris scanning can be done from a normal distance without interaction with anything, which also makes it more sanitary.

3. Stability. Iris patterns remains stable throughout an individual's life due to the protection against damage and wear by the cornea. This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labor or in some specific conditions (for example, wet, oily or dry fingers).

4. Security. The possibility of creating a complete copy of the iris is relatively low. Also, there are no similar parts of different irises (unlike for fingerprints, where similarities can be found), which makes the creation of so-called master copy that can be used to fake multiple identities impossible.

On the other hand, iris recognition has some major disadvantages:

1. Eye trauma is rarely present, but still possible. As a result, scanners will not be able to recognize the traumatized eye.

2. Out of all the biometric authentication methods, iris recognition is currently the most expensive to implement. The main reason is because it requires an infrared light source and sensor and cannot use a regular camera.

3. If hackers steal person's data, it will pose a life-long threat for the victim due to the impossibility of iris changing.

3. Real-life examples

1. In 1999 Bank United (Texas, USA) became the first bank in the world to deploy iris recognition ATMs. The technology was deployed at that time in multiple pilots with the premise that it would provide convenience and the use of a PIN code was not required, nor was an ATM card required.

2. In 2009 in Hashemite Kingdom of Jordan IrisGuard also deployed one of the world's first operational iris-enabled ATM at Cairo Amman Bank, where bank customers can seamlessly withdraw cash from ATMs without a bank card or PIN but simply by presenting their eye to the iris recognition camera on the ATM.

3. United Arab Emirates IrisGuard's Homeland Security Border Control has been operating a tracking system in the United Arab Emirates (UAE) since 2003, when the UAE launched a national border-crossing security initiative. Today, all of the UAE's land, air and sea ports of entry are equipped with systems. All foreign nationals who need a visit visa to enter the UAE are now processed through iris cameras installed at all primary and auxiliary immigration inspection points.

4. In 2009 the Government of India set up the Unique Identification Authority of India and enrolled 1.25 billion Indian citizens in three years in their ID card program, recording both iris and fingerprint data of each citizen.

5. Since at least 2011, Google uses iris scanners to control access to their data centers.

6. On May 28, 2015, Fujitsu released Arrows NX F-04G – the first smartphone with an iris scanner.

7. At the end of 2015, Microsoft launched two Lumia phones (Lumia 950 and Lumia 950 XL) featuring iris scanning as a way to authenticate the user.

Summary

This paper provides a review of researches on iris recognition. The algorithms used in iris recognition of provided iris image sample are categorized into three stages: image preprocessing, feature extraction and template matching.

There are increasing demands on iris recognition, because if the iris recognition algorithms are optimized for low-cost dedicated hardware, this authentication method can be employed in various applications due to its reliability and accuracy. It is currently widely used in transportation industries, defense, business and finance. With further development of this technology, iris recognition can be potentially used in all business spheres that require person authentication.

A key advantage of iris recognition is its stability of template; a single enrollment can last for a long time during life. In addition, iris recognition is currently the most precise out of all biometric authentication methods due to low false acceptance rate and false rejection rate. However, the iris recognition technology is far from perfection. The stability of template is also a major weakness in case of unauthorized access to samples database: hackers obtain permanent authentication keys while victims have life-long problems.

While the debates about the use of biometrics are still on, one thing is for certain: the technology is here to stay. The advantages of using biometrics still outweigh the disadvantages, so much so that companies are expected to continue adopting biometrics for authentication. And with further development of this technology and improvement of security in storing collected data, iris recognition will inevitably become an integral part of everyday life.

Summary translation

У цій роботі наведений огляд досліджень на тему автентифікації за райдужною оболонкою ока. Алгоритми обробки заданого зображення райдужної оболонки ока, що використовуються для цього виду автентифікації, розділяються на три стадії: попередня обробка зображення, виділення особливих ознак та порівняння із шаблоном.

Вимоги до використання технології автентифікації за райдужною оболонкою ока швидко зростають через те, що якщо алгоритми розпізнавання райдужної оболонки ока оптимізувати для недорогого спеціалізованого обладнання, то автентифікацію за райдужною оболонкою ока можна використовувати в різних програмних забезпеченнях завдяки її надійності та точності. У даний час цей метод автентифікації широко використовується у транспортних галузях, обороні, бізнесі та фінансах. З подальшим розвитком цієї технології, вона може бути потенційно використана у всіх сферах бізнесу, де потрібна автентифікація особи.

Ключовою перевагою автентифікації за райдужною оболонкою ока є стабільність шаблону; один зареєстрований шаблон може бут дійсним довгий час упродовж життя. Крім того, автентифікація за райдужною оболонкою ока на даний момент є найточнішим із усіх біометричних методів автентифікації через низькі коефіцієнти помилкового прийняття та хибного відхилення. Однак технологія розпізнавання райдужної оболонки ока далека від досконалості. Стабільність шаблону також є основною слабкістю у випадку несанкціонованого доступу до бази даних зразків: хакери отримують постійні ключі автентифікації, а жертви мають проблеми на все життя.

Хоча дебати щодо використання біометричних показників все ще тривають, одне можна сказати напевно: ця технологія залишиться. Переваги використання біометричних даних все ще переважають над недоліками, тому очікується, що компанії продовжуватимуть використання біометричних даних для автентифікації. І з подальшим розвитком цієї технології та підвищенням безпеки при зберіганні зібраних даних, автентифікація за райдужною оболонкою ока неминуче стане невід’ємною частиною повсякденного життя.

References

1. Biometric Authentication: Good, Bad, & Ugly [Електронний ресурс] — Режим доступу до ресурсу: https://www.onelogin.com/learn/biometric-authentication

2. Biometric Authentication: A Review [Електронний ресурс] / D.Bhattacharyya, R. Ranjan, F. Alisherov, C. Minkyu — Режим доступу до ресурсу: https://www.researchgate.net/publication/46189709_Biometric_Authentication_A_Review

3. Faundez-Zanuy M. Biometric security technology [Електронний ресурс] / Marcos Faundez-Zanuy — Режим доступу до ресурсу: https://www.researchgate.net/publication/3278329_Biometric_security_technology

4. Kanu P. Iris Recognition: A Biometric Authentication Approach [Електронний ресурс] / P. Kanu, A. Khan, A. Kumari — Режим доступу до ресурсу: https://www.researchgate.net/publication/329921008_Iris_Recognition_A_Biometric_Authentication_Approach

5. Pujari V. Research Paper on Biometrics Security [Електронний ресурс] / V. Pujari, R. Patil, S. Sutar — Режим доступу до ресурсу: https://www.researchgate.net/publication/352508064_Research_Paper_on_Biometrics_Security

6. Tay Y. A review of iris recognition algorithms [Електронний ресурс] / Yong Haur Tay – Режим доступу до ресурсу: https://www.researchgate.net/publication/4376330_A_review_of_iris_recognition_algorithms

Glossary

1. Advantage (noun) — a condition or circumstance that puts one in a favorable or superior position.
2. An automated teller machine (ATM) (noun) — an electronic banking outlet that allows customers to complete basic transactions without the aid of a branch representative or teller.
3. Algorithm (noun) — a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.
4. Aperture (noun) — in terms of camera: opening of a lens's diaphragm through which light passes.
5. Authentication (noun) — the process of verifying the identity of a user or proving something to be true, genuine, or valid.
6. Binary (adjective) — relating to, being, or belonging to a system of numbers having 2 as its base (a number system based only on the numerals 0 and 1).
7. Biometric (adjective) — referring to detailed information about someone's body that can be used to prove who that person is.
8. Biometrics (noun) — body measurements and calculations related to human characteristics.
9. Bit (noun) — in terms of programming, a binary digit, the smallest increment of data on a computer.
10. Bisection (noun, math term) — the division of something into two equal or congruent parts, usually by a line.
11. Camera (noun) — a device for recording visual images in the form of photographs, film or video signals.
12. Cartesian coordinates (phrase, math term) — the system in which the location of a point is given by coordinates that represent its distances from perpendicular lines that intersect at a point called the origin. A Cartesian coordinate system in a plane has two perpendicular lines (the x-axis and y-axis); in three-dimensional space, it has three (the x-axis, y-axis, and z-axis).
13. Coefficient (noun, math term) — a numerical or constant quantity placed before and multiplying the variable in an algebraic expression.
14. Concentric (adjective) — describing circles or other shapes which share the same center, the larger often completely surrounding the smaller.
15. Convolve (verb, math term) — the combination of one function or series of functions with another by forming their convolution.
16. Cornea (noun) — the transparent layer forming the front of the eye and protecting iris from outer damage.
17. Database (noun) — a structured set of data held in a computer, especially one that is accessible in various ways.
18. Data center (noun) — the department in an enterprise that houses and maintains back-end IT systems and data stores — its mainframes, servers and databases.
19. Decompose (noun, math term) — expression of a number or function as a combination of simpler components.

20. Derivative (noun, math term) — the rate of change of a function with respect to a variable.
21. Disadvantage (noun) — an unfavorable circumstance or condition that reduces the chances of success or effectiveness.
22. Discrete cosine transformation (DCT) (noun, math term) — a transformation that expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies.
23. Dyadic (adjective) — consisting of a dyad; being a group of two.
24. Enhancement (noun) — an increase or improvement in quality, value, or extent.
25. Exclusive-OR (noun) — a Boolean operator working on two variables that has the value one if one but not both of the variables is one.
26. Eyelid (noun) — each of the upper and lower folds of skin which cover the eye when closed
27. False acceptance rate (phrase) — the percentage of identification instances in which unauthorized persons are incorrectly accepted.
28. False rejection rate (phrase) — the percentage of identification instances in which authorized persons are incorrectly declined.
29. Feature (noun) — a distinctive attribute or aspect of something.
30. Filter (noun) — something that has the effect of holding back elements or modifying the appearance of something.
31. Frequency (noun, math term) — the rate per second of a vibration constituting a wave, either in a material (as in sound waves), or in an electromagnetic field (as in radio waves and light).
32. Gaussian filter (phrase) — a filter whose impulse response is a Gaussian function, used to ‘blur’ images and remove detail and noise.
33. Hacker (noun) — a person who uses computers to gain unauthorized access to data.
34. Hamming distance (phrase, math term) — the number of positions at which the corresponding symbols are different in two strings of equal length.
35. ID card (noun) — an official document or card with person’s name, date of birth, photograph or other information on it that proves who that person is.
36. Identification (noun) — the action or process of identifying someone or something or the fact of being identified.
37. Implement (verb) — to put a plan or system into operation.
38. Information technology (noun) — the study or use of systems (especially computers and telecommunications) for creating, processing, storing, retrieving and exchanging all kinds of electronic data and information.
39. Integer (noun) — a number which is not a fraction; a whole number.
40. Interloper (noun) — a person who becomes involved in a place or situation where they are not wanted or are considered not to belong.
41. Iris (noun) — a flat, colored, ring-shaped membrane behind the cornea of the eye, with an adjustable circular opening (pupil) in the center.

42. Iris recognition (phrase) — an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes.
43. Kernel (noun, math term) — a collection of all elements that are sent to zero by the transformation.
44. Localization (noun) — the process of making something local in character or restricting it to a particular place.
45. Master copy (phrase) — an original creation (for example, film or document) from which copies can be made.
46. Measure (noun) — a device for measuring distance, such as a graduated scale.
47. Non-uniform illumination (phrase) — low frequency intensity variations in the image caused by the sources of noise induced by the sensor being used to record the image.
48. Normalization (noun) — the process of bringing or returning something to a normal condition or state.
49. Operator (noun, math term) — a mapping or function that acts on elements of a space to produce elements of another space.
50. Passphrase (noun) — sequence of words or other text used to control access. Similar to password, but a passphrase is generally longer for added security.
51. Password, or passcode (noun) — a secret word or phrase that must be used to gain admission.
52. Patch (noun) — a part of something marked out from the rest by a particular characteristic.
53. Perpendicular lines (phrase) — such lines that intersect at a right (90 degrees) angle.
54. Polar coordinates (phrase, math term) — a pair of coordinates locating the position of a point in a plane, the first being the length of the straight line connecting the point to the origin, and the second the angle made by this line with a fixed line.
55. Pilot (noun) — a test example made before introducing the product more widely.
56. Pixel (noun) — the smallest controllable element of a picture represented on the screen.
57. Preprocessing (noun) — preliminary processing of data in order to prepare it for the primary processing or for further analysis.
58. Pupil (noun) — the black circle in the center of the iris.
59. Pythagorean theorem (phrase, math term) – the well-known geometric theorem that the sum of the squares on the legs of a right triangle is equal to the square on the hypotenuse (the side opposite the right angle).
60. Radius (noun) — a straight line from the center to the circumference of a circle or sphere.
61. Recognition (noun) — identification of someone or something from previous encounters or knowledge.
62. Re-issue (verb) — to issue (to cause to become available) again.

63. Retina (noun) — a layer at the back of the eyeball that contains cells sensitive to light, which trigger nerve impulses that pass via the optic nerve to the brain, where a visual image is formed.
64. Scanner (noun) — a device for examining, reading or monitoring something.
65. Security (noun) — the state of being free from danger or threat.
66. Template (noun) — something that is used as a pattern for producing other similar things.
67. Threshold (noun) — the point or level at which something begins or changes.
68. Visa (noun) — an endorsement on a passport indicating that the holder is allowed to enter, leave, or stay for a specified period of time in a country.
69. Wavelet (noun, math term) — a wave-like oscillation with an amplitude that begins at zero, increases or decreases, and then returns to zero one or more times (similar to a wave).
70. Wristband (noun) — a strip of material worn around the wrist, especially for identification or as an accessory.