NEURAL NETWORKS FOR PERSONALIZATION THROUGH BIOMETRIC DATA

Borislav Toskov, University of Plovdiv "Paisii Hilendarski", btoskov@gmail.com
Asya Toskova, University of Plovdiv "Paisii Hilendarski", asy@mail.bg

Abstract: This publication explores the possibilities for biometrics identification in the cyber-physical space of the Faculty of Mathematics and Informatics at Plovdiv University. The proposed fingerprint customization system uses algorithms to process and normalize images. The approach described is focused on the development of a neural network-based matching detection method.

Key words: biometrics identification, fingerprint customization system, cyber-physical social space, IoT, neural networks.

НЕВРОННИ МРЕЖИ ЗА ПЕРСОНАЛИЗАЦИЯ ЧРЕЗ БИОМЕТРИЧНИ ДАННИ

Борислав Тосков, Пловдивски университет „Паисий Хилендарски", btoskov@gmail.com
Ася Тоскова, Пловдивски университет „Паисий Хилендарски", asy@mail.bg

Въведение

Във ФМИ на Пловдивския университет се развива интелигентно, персонализирано и адаптивно кибер-физическо социално пространство, което обслужва различни процеси, в това число обучението и управлението на образователни ресурси, обособени във виртуално образователно пространство (ВОП) [**9**,**11**,**12**,**13**]. Персонализацията в пространството може да се разглежда в две направления – първо, предоставяне на съобразена със знанията и желанията на съответния потребител информация и второ, идентификация на различните потребителите. В момента идентификацията се осъществява стандартно, чрез използването на потребителско име и парола. Въвеждането на биометрична идентификация и оторизация би подсигурило обмена на информация в системата.

От една страна ВОП се използва както за предоставяне на образователни ресурси, така и за контрол на знанията на студентите. От друга страна ВОП използва IoT технологията и интегрира адаптивно интелигентни софтуерни компоненти със специализирани сензорни елементи. Основната задача на тези интелигентни компоненти (гардове) е да се осигуряват нормалното протичане на процесите в системата, от гледна точка на външния, физически свят. Гардовете отчитат промените в околната среда, като обработват информацията, получена от съществуващите сензорни устройства и я предават към други (оперативни) агенти в подходящ вид.

Локалното осъществяване на контрола върху придобитите от студентите знания, както и възможността на виртуалното пространство да контактува с физическия свят, позволяват използването на биометрични системи за доказване на самоличност.

Един от най-ефективните начини за биометрична идентификация са пръстовите отпечатъци. Те са уникални, сравнително трудни за копиране и с малка промяна във времето, което ги прави удобни и дълготрайни маркери за доказване на идентичност.

Автоматизирането на метода за идентификация чрез пръстови отпечатъци по време на изпит може да бъде направено чрез използването на машинно учене с невронни мрежи.

Специфични характеристики на пръстовите отпечатъци

Методите за идентификация чрез пръстови отпечатъци се базират на факта, че епидермисът на пръстите не е гладък. Той представлява поредица от издигнати и вдлъбнати участъци, наречени съответно „хребети“ (friction ridges) и „долини“ (furrows). При разпознаването на пръстите се търсят характерни модели, образувани от епидермалните хребети. Тези модели съдържат специфични за всеки човек характеристики, които са най-общо два типа – глобални и локални.

Глобалните характеристики включват няколко фигури от хребети върху епидермиса, които се виждат с просто око. Различават се три основни фигури – арка (arch), бримка (loop) и обръч (whorl) (фиг.1).

Арка Бримка Обръч

Фиг. 1.

При арката хребетите влизат от едната страна на пръста, издигат се в центъра, образувайки дъга, и излизат от другата страна на пръста. При бримката хребетите влизат от едната страна на пръста, образуват крива и излизат от същата страна на пръста. В зависимост от страната, от която влизат и излизат хребетите, бримките могат да се разделят на лява и дясна. При обръча хребетите образуват кръгообразна форма около една или няколко централни точки.

Арката се среща при 5% от пръстовите отпечатъци, а обръчът – при 25-35%. Най-разпространената фигура е бримката, която присъства в 60-70% от отпечатъците.

Основните фигури могат да се разделят на множество подкласове за повишаване бързодействието на търсене.

Локалните характеристики за описание на отпечатъка, са т.нар. минютини или особени точки (minutiae features). Според American National Standards Institute (ANSI) те биват четири основни вида - край (termination), разклонение (bifurcation), кръстосване (trifurcation) и неспецифичност (undetermined). Най-често използваните обаче са само два - край и разклонение (фиг. 2), а останалите са комбинация от тях.

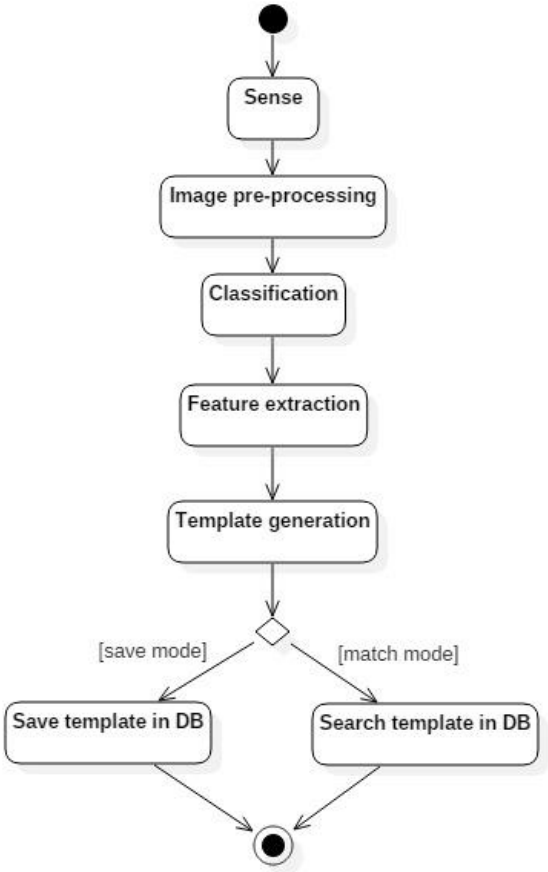
Анализът на пръстовите отпечатъци при търсене на съвпадение изисква откриването на модела и сравняването на уникалните характеристики за дадения индивид в него.

Край Разклонение

Фиг. 2.

Идентификация на пръстов отпечатък

Методът за идентификация на пръстови отпечатъци има два основни сценария: запис и търсене на съвпадение (фиг. 3).



Фиг. 3.

И в двата сценария сензорът сканира пръста (sense), при което се получава изображение с пръстов отпечатък. Изображението се обработва (pre-processing, classification, feature extraction) и се генерира темплейт (template generation), който или се записва в база данни (save mode) или се сравнява с вече записан такъв (match mode).

Методите за обработка включват лимитиране на цветовете до сиво, сегментация, филтрация и др. Обработката спомага да се подобри качеството на изображението и да се отделят съществените елементи, като се премахне шума. Причини за поява на шум обикновено са начинът, по който хората слагат пръстите си върху сензора за сканиране, както и процесите на дискретизация и квантуване в самия сензор.

Изображението се обработва в зависимост от алгоритъма за съвпадение, който ще се използва, след което се генерира темплейт.

В базата данни не се съхраняват сурови изображения, тъй като те заемат твърде много памет (приблизително 250 KB за сурово изображение срещу 500 B за обработено), и защото търсенето на съвпадение ще отнеме много време.

Според стандарта ANSI/NIST-ITL (American National Standards Institute/National Institute of Standards and Technology) съхраняваните темплейти могат да бъдат с ниска (250 ppi) или висока резолюция (550 ppi), до 8 бита в сивата гама или 1 бит в черно-бял цвят и компресия, използваща Wavelet Scalar Quantization или JPEG2000, в зависимост от резолюцията [**1**].

Международният стандарт ISO/IEC 19794-2 описва обмена на данни, отнасящи се до специфичните характеристики на отпечатъците, между системите за сканиране, съхранение и съвпадение [**3**].

Алгоритмите за съвпадение се използват за сравняване на новогенерирани темплейти на пръстови отпечатъци с предварително съхранени в базата. Откриването на съвпадение е процес, изискващ време, пропорционално на големината на базата. Бързината на алгоритъма зависи и от това дали се търси съвпадение с един отпечатък (1:1) или с много отпечатъци на един и същ индивид (1:M). Някои от алгоритмите работят и в двата варианта.

Съществуват няколко техники за търсене на съвпадение - сравнение на базата на минютините (minutiae-based matching), сравнение на базата на корелация (correlation-based matching) и сравнение на базата на хребетите (ridge feature-based matching).

Най-популярният алгоритъм за съвпадение е алгоритъмът на базата на минютините. За да извлече особеностите (feature extraction), алгоритъмът извършва нормализация на изображението (binarization) и изтъняване на хребетите до 1 пиксел (skeletonization) [**5**]. Моделът, създаден посредством този алгоритъм, е ефективен и точен, което се дължи на неговата простота и на факта, че хората имат до 80 характерни особености на всеки отпечатък.

Биометрични софтуерни разработки чрез невронни мрежи

Има голямо разнообразие от гледна точка на реализацията на алгоритми за разпознаване на отпечатъци. Реализацията се различава по начина на изпълнение на определена фаза, по етапите, които използва и по методите за машинно обучение, които използва. За сегментацията на изображението, за класифициране на фигурата на отпечатъка, за екстракцията на минютините и за търсенето на съвпадение често се използват невронни мрежи, които са мощно средство за автоматизация на процеси, работещи с големи обеми данни.

В биометричния софтуер NBIS (NIST Biometric Image Software) [**6**], който се използва във FBI и CIA, класификацията на фигури на отпечатъци се извършва от модула PCASYS. Модулът категоризира изображението в шест класа - arch, tented arch, left or right loop, scar, whorl, като използва вероятностна невронна мрежа и многослоен персептрон. Времето за отговор на заявка на NBIS е около 30 минути, защото в базата се пазят повече от 70 млн десет-пръстови отпечатъка.

В [**4**] са имплементирани два модула, базирани на многослойни прави мрежи. Първият модул класифицира отпечатъците в пет класа - arch, tented arch, left or right loop, whorl. Вторият модул отделя минютините и формира вектора на особеностите.

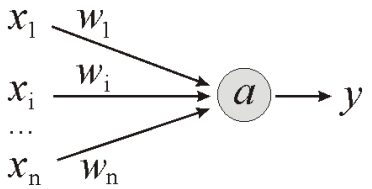
За разпознаването на вида на минютините в [**2**] е използван двуслоен персептрон и е приложен обучаващ алгритъм с обратно разпространение на грешката.

За подобряване на процеса на реконструкция на отпечатъци, в [**7**] прилагат конволюционна невронна мрежа (CNN).

Основни параметри на невронните мрежи

Невронната мрежа (НМ) е опростен изчислителен модел на човешкия мозък, който анализира, запомня и възпроизвежда информация. НМ работи с разпределени многомерни данни, прави паралелни изчисления, има способност за обучение и обобщение, адаптивна е към промени и е толерантна към грешки. Въпреки всички предимства, НМ има склонност към преобучение и ако архитектурата й е по-сложна - тя е сравнително бавна.

В своята същност НМ представлява граф, чиито възли се наричат неврони, а ребрата между тях - синапси. Базовите елементи на невронната мрежа са показани на фиг. 4. Основни параметри на мрежата са активността на неврона *a* и теглото на синаптичната връзка *w*. Активността на неврона се променя по т.нар. обновяващо правило, а теглото на връзката – по т.нар. обучаващо правило [**10**]. Положителното тегло възбужда неврона, а отрицателното го подтиска.



Фиг. 4.

Обновяващото правило е уравнение на разделящата хиперповърхнина и представлява сума на входните сигнали на неврона, ограничени чрез някаква функция на активация f_{act}:

$$y = f_{act}\left(\sum_{i=1}^{n} x_i w_i\right).$$

Функцията на активация може да бъде линейна, униполярна или биполярна прагова, сигмоид, хиперболичен тангенс, радиално-базисна и др.
Обучаващото правило променя теглата на НМ с цел получаване на правилен изход за определен вход. Съществуват множество обучаващи алгоритми, но всички те са различни разширения на правилото на Хеб, според което връзката между два едновременно активни неврона a_1 и a_2 трябва да се усилва:

$$\Delta w = \eta a_1 a_2.$$

Тук Δw е промяната на синаптичното тегло, а η е коефицент на пропорционалност, наречен „скорост на обучение“.
НМ, използвани в алгоритмите за идентификация, могат да използват методите за обучение с учител и без учител.
При класификацията (учене с учител) мярка за качество на мрежата е функцията на грешката. Функцията на грешката показва разликата между очакваната (идеална) и получената (реална) стойност на изхода на НМ.
Ако използваме квадратично представяне на грешката E, то

$$E = (d - o)^2 = \left(d - f_{act}\left(\sum_{i} x_i w_i\right)\right)^2,$$

където d е очакваната желана стойност на изхода, а o е реално получената изходна стойност.
Обучението на НМ се състои в промяната на синаптичните тегла така, че да минимизират грешката. Най-простият метод за търсене на минимум на непрекъсната и диференцируема функция, каквато е функцията на грешката, е методът на градиентното спускане. Грешката на дадена връзка зависи единствено от синаптичното тегло на връзката, затова минимумът на градиента се определя чрез частната производна на E и w и формира следното обучаващо правило:

$$\Delta w = -\eta \frac{\partial E}{\partial w}.$$

Клъстеризацията (учене без учител) разделя множеството данни на непресичащи се клъстери, като изчислява вътреклъстерни и междуклъстерни разстояния. За изчислението на тези разстояния се използват метрики за близост между вектори, като най-разпространените са:

- Мярка за близост на Минковски (за вектори с реални компоненти)

$$\sqrt[n]{\sum_{i} (A_i - B_i)^n}$$

- Мярка за близост на Хеминг (за вектори с дискретни компоненти)

$$\sum_i \mathrm{XOR}(A_i, B_i).$$

Невронните мрежи дават изключително добри резултати при класификация и клъстеризация. Архитектурата и хиперпараметрите на НМ влияят на бързодействието, точността и възможността за откриване на решение и обуславят голямото разнообразие от модели. Съществени характеристики за всеки модел са: посоката на разпростанение на сигнала, броят слоеве, броят неврони във всеки слой, видът на функцията на активация, избраното обучаващо правило, скоростта на обучение и др.

Модел на алгоритъма за съвпадение

При голямото разнообразие от НМ е трудно да се определи кой точно модел ще даде най-добри резултати при търсене на съвпадение.

Мрежата трябва да сравнява два темплейта – запазеният в базата $T_B = (m_1, m_{2,} \dots, m_b)$ и сканираният от сензора $T_S = (m_1, m_{2,} \dots, m_s)$. Всеки темплейт може да се представи като матрица от вектори, като всеки вектор m_i описва една особеност.

Всяка особеност се характеризира с четири параметра:

$$m_i = (x_i, y_i, \alpha_i, t_i)$$

където x и y са координатите на особената точка, α е ъгълът на отклонение на прилежащия хребет спрямо Х-ординатата и t е типът й (прекъсване или разклонение).

Двойка минютини се счита за еднаква ако разликите в позицията и в направлението са по-малки от предварително зададени стойности. За сравнение на векторите може да се използва Евклидова мярка за близост или обобщената мярка на Минковски.

Броят на входните неврони в една НМ се определя от размерността на входния вектор. При отпечатъци с добро качество могат да се отделят около 80 особени точки. При отпечатъци с лошо качество, броят на тези точки спада до около 20. Според криминалистите, когато два пръстови отпечатъка имат минимум 12 еднакви особени точки, те се считат за идентични [**8**].

Ако приемем минимума от 20 особени точки при недобър отпечатък, то размерността на входа на нашата НМ ще бъде 4 x 20 = 80.

Изходният слой на НМ ще съдържа един неврон с бинарна кодировка.

Скритият слой ще реализира нелинейно делене. Броят на невроните в него ще се определи итеративно.

Експериментът може да започне с двуслоен персептрон по Румелхарт, който предполага използването на алгоритъм с обратно разпространение на грешката, нелинейна функция на активация за скрития слой и прагова функция за класификация в изходния слой. Ако тази невронна мрежа не отговори на очакванията и не даде достатъчно добри резултати, в последствие ще бъде усложнена.

Благодарност

Изследването е частично финансирано по проект No. MU17-FMI-001 EXPERT[1] (Experimental Personal Robot That Learn), 2017-2018.

References

[1] ANSI/NIST. (2015) ANSI/NIST-ITL Standard. <https://www.nist.gov/programs-projects/ansinist-itl-standard>

[2] Gour, Bhuprsh , T. K. Bandopadhyaya и Sudhir Sharma, "Fingerprint Feature Extraction Using Midpoint Ridge Contour Method and Neural Network", IJCSNS International Journal of Computer Science and Network Security, vol. 8, no. 7, pp. 99-102, July 2008.
[3] International Organization for Standardization. (2011) ISO/IEC 19794-2. <https://www.iso.org/standard/50864.html>
[4] Marak, Pavol и Alexander Hambalik, "Fingerprint Recognition System Using Artificial Neural Network as Feature Extractor: Design and Performance Evaluation", Tatra Mountains Mathematical Publications, vol. 67, no. 1, pp. 117–134, 2016.
[5] National Institute of Justice, The Fingerprint Sourcebook, Alan McRoberts, Ed.
[6] National Institute of Standards and Technology. NIST Biometric Image Software (NBIS). <https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis>
[7] Svoboda, Jan , Federico Monti и Michael M. Bronstein. (2017, May) arXiv. <https://arxiv.org/abs/1705.01707>
[8] WIĘCŁAW, Łukasz , "A MINUTIAE-BASED MATCHING ALGORITHMS IN FINGERPRINT", JOURNAL OF MEDICAL INFORMATICS & TECHNOLOGIES , vol. 13, 2009.
[9] Дойчев, Е. , "Среда за електронни образователни услуги", Пловдивски университет "Паисий Хилендарски", Пловдив, България, Докторска дисертация 2013.
[10] Кирова, Теодора , Невронни мрежи - основни архитектури и обучаващи алгоритми. София, България: СОФТЕХ, 1995.
[11] Орозова, Д. , С. Стоянов и И. Попчев, "Виртуално образователно пространство" в Научна конференция с международно участие „Знанието – източник на иновации“ БСУ, 14-15 юни 2013, ISBN 978-954-9370-99-7 , Бургас, 2013, pp. 153-159.
[12] Стоянов, С. , "Формален модел на виртуално образователно пространство" в International Conference FROM DELC TO VELSPACE, Пловдив, 2014, Пловдив, 2014.
[13] Тоскова, Ася Тодорова, Емил Христов Дойчев и Борислав Петров Тосков, "Идея за разширение на Виртуалното образователно пространство за учене през целия живот" в Юбилейна научна конференция с международно участие - 2016, БСУ, Бургас, 2017, pp. 433-437.