Автентифікація за клавіатурним почерком на основі нейромережевого підходу

Кондратенко Н.Р.[1], Мельник Л.С.[2]

1 Доцент, к.т.н., викладач кафедри ЗІ, Вінницький національний технічний університет, Хмельницьке шосе, 95, Вінниця, 21021, Україна, тел.: (0432) 59-83-79, e-mail: kondrn@yandex.ru
2 Студентка кафедри захисту інформації , Вінницький національний технічний університет
вул. Хмельницьке шосе 95, м. Вінниця, Україна, Ludmula91@gmail.com

***Анотація* — Обґрунтовано використання нейронних мереж для розпізнавання користувачів за клавіатурним почерком. Запропоновано використання поєднання двох архітектур нейромеж. Визначаються обмеження які пов'язані із сферою застосування даного підходу. Виділяються найбільш критичні параметри за рахунок налаштування яких можна підвищувати ефективність даного методу. Визначено напрямки та прикладні задачі ефективного застосування даного методу.**

Ключові слова: нейонні мережі, ймовірнісні нейронні мережі, нейронна мережа Кохонена.

Authentication keyboard writing by neural network approach

Kondratenko N.R., Melnuk L. S.[1]

[1] Associate Prof., Ph. D., lecturer WITH, Vinnytsia national technical University, Khmel'nyts'ke shose, 95, Vinnytsia, 21021, Ukraine, tel: (0432) 59-83-79, e-mail: kondrn@yandex.ru
[1]Student Information Protection Department, Vinnytsia National Technical University st. Khmelnytsky Highway 95, m. Vinnitsa, Ukraine, Ludmula91@gmail.com

***Abstract* — The application of neural networks to detect users on keyboard handwriting. The use of a combination of two neural network architectures. Identify constraints related to the scope of this approach. There are the most critical parameters by setting that can improve the efficiency of this method. Directions and applied problems of effective application of this method.**

Keywords: neural networks, probabilistic neural networks, Kohonen neural network.

I. Вступ

За останні декілька років в розвитку комп'ютерних мереж виявляються дві важливі тенденції. Перша тенденція полягає у підвищенні значення комп'ютерних мереж для практично всіх сфер діяльності людського суспільства, а друга тенденція пов'язана із зростанням і ускладненням їх архітектури, програмно-апаратного забезпечення та сервісних функцій. Разом вказані тенденції викликають посилення вимог до забезпечення надійності та ефективності функціонування комп'ютерних мереж. Одним із основних шляхів забезпечення вказаних вимог є вдосконалення існуючих методів діагностики технічного стану програмно-апаратного забезпечення в процесі експлуатації за рахунок впровадження сучасних математичних теорій, в тому числі і теорії штучних нейронних мереж (НМ), яка вже довела свою ефективність для розв'язання подібних задач[1].

Упродовж останніх 10–15 років прогрес галузі захисту інформації в комп'ютерних системах та мережах безпосередньо пов'язаний з використанням різноманітних теорій штучного інтелекту, серед яких особливе місце займає теорія штучних нейронних мереж (НМ)[2].

Вирішення задачі захисту з використанням біометричних характеристик є актуальною задачею, що стає популярнішою щодня, це є цілком виправдано враховуючи преваги які надають дані методи захисту.

II. Основи біометричного захисту

Системи біометричного захисту використовують унікальні для кожної людини вимірювані фізіологічні характеристики для перевірки особи індивіда. Цей процес називається електронною автентифікацією. Його суть — визначити, чи справді індивід є тією особою, якою він або вона себе називає.

Біометричні системи забезпечують найбільш точну автентифікацію, оскільки перевіряють параметри, які дуже важко або неможливо змінити чи підробити. Їхні переваги очевидні, оскільки традиційні системи захисту не здатні з'ясувати, наприклад, хто саме вводить код або вставляє смарт-картку.

На сьогоднішній день біометричні системи доступу є найнадійнішими. Ситуацію, що склалася

сьогодні на ринку інформаційної безпеки, можна сміливо назвати передднем буму біометричних технологій. Часто з'являються нові сканери, які набагато надійніше попередніх. Ще одним дуже важливим чинником збільшення популярності біометричного захисту є спрощення її експлуатації.

Слід зазначити, що біометричні технології мають один суттєвий недолік. Вони спрацьовують завдяки тому, що системі відомі унікальні, конфіденційні характеристики кожної конкретної людини. Однак прибічники біометрії стверджують, що насправді вона забезпечує вищий рівень секретності, оскільки під час аутентифікації не залучається інформація про адресу людини, домашній телефон, банківський рахунок тощо.

III. НЕЙРОННІ МЕРЕЖІ

Оскільки однією з вимог до захисту інформації сучасних систем є адаптивність, тому доцільно в якості методу захисту використовувати нейронну мережу (НМ). Відомий ряд архітектур, що вже стали класичними, крім того, розроблена значна кількість специфічних. При цьому для кожного класу прикладних задач використовується своя архітектура НМ[3].

Як правило, НМ використовується тоді, коли невідомий точний вид зв'язків між входами і виходами, - якби він був відомий, то зв'язок можна було б моделювати безпосередньо, тому залежність знаходиться в процесі навчання мережі. Технічно навчання полягає в знаходженні коефіцієнтів зв'язків між нейронами. У процесі навчання мережа крім виявлення складних залежностей здатна також виконувати узагальнення. Це означає, що у разі успішного навчання вона зможе повернути вірний результат на підставі даних, які були відсутні в навчальній вибірці, а також неповних та/або «зашумлених», частково перекручених даних.

Одна з привабливих сторін ШНМ покладена в їх здатності адаптуватися до зовнішніх умов шляхом зміни зв'язків або структури.

Один з найпривабливіших аспектів використання НМ полягає у тому, що хоча елементи такої мережі мають дуже обмежені обчислювальні можливості, вся мережа в цілому, об'єднуючи велику кількість таких елементів, виявляється здатною виконувати досить складні задачі.

Вивчення клавіатурного почерку має давню історію. Сучасні дослідження показують, що клавіатурний почерк користувача має деяку стабільність, що дозволяє досить однозначно ідентифікувати користувача, який працює з клавіатурою. Для цього, застосовуються статистичні методи обробки вихідних даних і формування вихідного вектора, що є ідентифікатором даного користувача. В принципі, надійне розпізнавання користувача по клавіатурного почерку можливо тільки при багатопальцевого відпрацьованому методі друкування. Якщо користувач тільки почав працювати з клавіатурою і друкує одним пальцем, то ідентифікувати введення інформації дуже складно.

Враховуючи переваги нейронних мереж такі як швидке навчання, точність та оперативність відповіді використання їх в задачах автентифікації зводиться до вирішення задачі класифікації.

Для вирішення завдання за допомогою нейронної мережі, необхідно зібрати дані для навчання. НМ можуть працювати з різними типами даних проте в залежносі від задачі потребують мпевного масшатабування в підхоядщийдля мережі діапазон, а пропущені значення можна замінити на середнє значення (або на іншу статистику) цієї змінної по всіх наявних навчальних прикладах.

Як вже раніше наголошувалось в даному випадку використовується поєднання двох нейромереж. Перша - самоорганізована нейронна мережа, названа шаром Кохонена. Структура дуже проста і являє собою один шар адаптивних лінійних суматорів, що працюють за принципом WTA - Winner Takes All, або «Переможець забирає все». Іншими словами, нейрон, що має найбільший сигнал на вхідному векторі, ідентифікує клас, до якого нейронна мережа відносить цей вхідний вектор. Основне завдання, яке вирішується за її допомогою, - це завдання кластеризації.

Після навчання нейрони шару Кохонена мають ваги, максимально наближені до векторів кластерів, які вони визначають. Можна сказати, ваги вихідного кластера складають вектор-центр, ядро кластера (асоціація з методом кластеризації «динамічних ядер»). Це робить роботу мережі «прозорою», зрозумілою для користувача.

Вихідні дані дані даної мережі стають вхідними для наступної нейромережі - імовірнісної (PNN - мережі). Завдання якої – класифікація. В даній мережі щільність ймовірності приналежності класам оцінюється за допомогою ядерної апроксимації. Дані мережі мають шарувату структуру. Є три шари - вхідний, радіальний і вихідний. Кожному навчальному прикладу відповідає один елемент радіального шару. Кожному класу відповідає один вихідний елемент, який з'єднаний тільки з радіальними елементами, що відносяться до його класу. Вихідний елемент підсумовує сигнали всіх радіальних елементів, що належать до його класу. Нормовані значення вихідних сигналів дозволяють оцінити ймовірності приналежності класам.

Для мережі PNN не потрібно навчання в звичному розумінні, тому що всі параметри мережі PNN, такі як число елементів та значення ваг, визначаються безпосередньо навчальними даними [4]. Імовірнісна нейронна мережа має єдиний керуючий параметр навчання, значення якого вибирається користувачем, - ступінь згладжування (або відхилення гауссової функції). Як і у випадку RBF - мереж, цей параметр вибирається з тих міркувань, щоб шапки "певне число раз перекривалися": вибір занадто маленьких відхилень призведе до " гострих результатів"

апроксимуючої функції і нездатності мережі до узагальнення, а при дуже великих відхиленнях будуть губитися деталі. Необхідне значення нескладно знайти дослідним шляхом, підбираючи його так, щоб контрольна помилка була якомога менше. На щастя, PNN - мережі не дуже чутливі до вибору параметра згладжування.

Найбільш важливі переваги PNN - мереж полягають у тому, що вихідне значення має імовірнісний сенс (і тому його легше інтерпретувати), і в тому, що мережа швидко навчається. При навчання такої мережі час витрачається практично тільки на те, щоб подавати їй на вхід навчальні спостереження, і мережа працює настільки швидко, наскільки це взагалі можливо.

Істотним недоліком таких мереж є їх обсяг. PNN - мережа фактично вміщує в себе всі навчальні дані, тому вона вимагає багато пам'яті і може повільно працювати .

Нейрони шару аналізатора образів зв’язуються з нейронами сумуючого шару не випадково , а в залежності від того до якого класу відноситься образ. Вихідний шар представляє собою селектор який вибирає нейрон сумуючого шару з максимальним значенням вихідного сигналу і відносить його до відповідного класу.

Коли мережа побудована невідомий екземпляр подається на вхід мережі і в результаті прямого проходу через мережу вихідний шар вкаже клас до якого ймовірнішого усього належить зразок[3].

Були проведені дослідження які показують, що можливості нейромережевих біометричних технологій значно розширюються, якщо використовувати декілька нейромереж, які працюють поступово розвязуючи поставлену задачу.

Була зроблена структура нейромережі, що складається з двох компонент. В першій компоненті з вхідними даними працює мережа Кохонена результати роботи даної мережі використовуються як вхідні дані для ймовірнісної мережі. Структурна схема нейромережі наведена на рис.1.

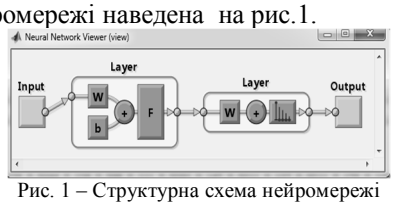

Рис. 1 – Структурна схема нейромережі

В якості вхідних даних використовуються тимчасові інтервали між натисканнями клавіш на клавіатурі і час їхнього утримання. При цьому тимчасові інтервали між натисканням клавіш характеризують темп роботи, а час утримання клавіш характеризує стиль роботи з клавіатурою – різкий удар чи плавне натискання.

Мережі PNN дуже зручно використовувати для класифікації. Вони дуже швидко навчаються, допускають наявність помилкових даних та забезпечують хороші результати навіть на малих наборах навчальних даних, тому цей вид нейронних мереж і був вибраний для вирішення поставленої задачі.

IV. Висновки

Розроблений метод антентифікації будується на основів конфігурації мереж Кохонена та ймовірнісної мережі. Мережа Кохонена дозволяє розпізнавати образи які надходять на її вхід, та функціонувати в умовах перешкод, що не заважає налаштуванню ваг, для наступного шару нейромережі. Швидке навчання мережі та ймовірнісне вихідне значення, дозволяють вирішувати задачу автентифікації та отримувати хороші результати.

Проведені експериментальні дослідження показали, що побудована нейромережева структура забезпечує необхідні вимоги до надійності автентифікаці та є перспективними оскільки володіють численними перевагами.

Головним недоліком даного підходу є затрати часу для накопичення навчальних даних та їх опрацювання, а також підвищення вимог до техніки що використовуватиметься. Ці недоліки є основними проблемами при застосуванні даного підходу для вирішення задачі автентифікації користувачів комп’ютерних систем, саме тому можна стверджувати, що вирішення цих проблем – це одна із задач, які необхідно вирішити в майбутньому.

[1] Терейковський І.А. Оптимізація архітектури нейронної мережі призначеної для діагностики стану комп’ютерної мережі- Вісник "Комп'ютерні системи та мережі" № 717 “2011”- 211 с.

[2] Терейковський І.А. Критерії вибору архітектури нейронної мережі для розв’язання задач з захисту інформації - Збірник наукових праць “Управління розвитком складних систем” Київського національного університету будівництва і архітектури №-6 “2011”- с.155-158.

[3] Терейковський І.А. Перспективи практичного використання нейронних мереж в задачах захисту програмного забезпеченя - Науково-технічний журнал "Захист інформації " №-1 “2008”- с.12-22.

[4] Каллан Р. Основные концепции нейронных сетей. - М.: Вильямс, 2001., - 291 с.

[5] Висоцкая Е. А., Давиденко А. Н. Исследование ефективности применения вероятносних нейронних сетей для решения задачи ацутентификации пользователя компютерних систем - Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні"№-9 “2004”- с.103-110.