УДК 004.056

Б. П. Книш
Д. О. Немировська

Біометричні системи захисту інформації

Вінницький національний технічний університет

Анотація

У роботі розглянуто біометричні системи захисту інформації, які базуються на різноманітних фізичних явищах та процесах, а саме оптичні, механічні, електромагнітні та акустичні. Наведено фізичні впливи, які можуть впливати на точність біометричного захисту інформації.

Ключові слова: біометричний захист, оптика, механіка, електромагнетизм, акустика, похибка

Abstract

Biometric information protection systems based on various physical phenomena and processes, namely optical, mechanical, electromagnetic and acoustic, are considered in this work. Physical influences that can affect the accuracy of biometric information protection are presented

Keywords: biometric protection, optics, mechanics, electromagnetism, acoustics, error

Вступ

На сьогодні інформація є важливим елементом нашого життя, який вимагає постійного та якісного захисту. Для цього розроблено різноманітні методи, зокрема біометричний, криптографічний, мережевий захист, шифрування, контроль доступу, антивірусне програмне забезпечення та фізична безпека. Серед них біометричний захист виділяється використанням біометричних даних для ідентифікації користувача. Це дозволяє забезпечити більш високий рівень захисту, оскільки ці дані є унікальними для кожної людини і їх важко підробити. Цей метод може використовуватися для різних цілей, наприклад, для захисту доступу до комп'ютерних систем, мобільних пристроїв, банківських рахунків, документів та інших конфіденційних даних. І з кожним днем він все частіше застосовується в поєднанні з іншими системами захисту. При цьому різноманітні фізичні явища та процеси відіграють надважливу роль у розробці нових методів біометричного захисту інформації та застосуванні відповідних систем. Також варто мати на увазі, що яким би якісним не був такий захист, інколи системи можуть давати збій і часто причиною цього є саме вплив фізичних явищ та процесів, на яких вони базуються. Тому **метою** дослідження є оцінювання всіх ризиків і факторів, які можуть впливати на точність біометричного захисту інформації.

Результати дослідження

Біометричні системи захисту інформації, які базуються на фізичних явищах та процесах, дуже різноманітні. Серед найбільш поширених є оптичні, механічні, електромагнітні та акустичні.

Оптичні біометричні системи

Оптичні біометричні системи використовуються для розпізнавання ока спеціальними камерами, що фіксують детальні зображення райдужної оболонки або сітківки, які потім аналізуються для створення унікального біометричного шаблону. Такі системи чутливі до таких фізичних впливів, як відбиття та заломлення, умови освітлення, фізичні перешкоди, старіння, систематичні зміщення.

Відбиття та заломлення світла може спричинити спотворення зображень, отриманих камерами, які використовуються в системах розпізнавання райдужної оболонки та сітківки ока. Наприклад, якщо камеру розташовано під кутом або якщо об’єкт зйомки в окулярах, то тоді можуть виникнути спотворення отриманих зображень, що призведе до неточностей у біометричному шаблоні.

Умови освітлення навколишнього середовища також можуть впливати на точність систем розпізнавання райдужної оболонки та сітківки ока. Яскраве або тьмяне освітлення може спричинити відблиски або тіні, що ускладнює отримання чітких зображень. Крім того, певні умови освітлення,

наприклад пряме сонячне світло, можуть спричинити звуження зіниць, що ускладнює отримання якісних зображень райдужної оболонки або сітківки.

Фізичні перешкоди, такі як вії або контактні лінзи, також можуть знижувати точність оптичних біометричних систем.

З часом текстура та колір райдужної оболонки або сітківки можуть змінюватися, що ускладнює зіставлення біометричного шаблону зі збереженими даними. Це може призвести до хибних спрацьовувань або помилкових виявлень, що знижує точність системи.

Деякі оптичні біометричні системи мають систематичні зміщення, наприклад, краще розпізнають певні кольори або форми очей, ніж інші. Це може призвести до неточностей у біометричному шаблоні та зробити систему менш надійною в цілому.

Механічні біометричні системи

Механічні біометричні системи використовуються для розпізнавання ходьби спеціальними датчиками для збору даних про модель ходьби людини, включно з довжиною кроку та швидкістю. Ці дані потім аналізуються для створення унікального біометричного шаблону. Такі системи чутливі до таких фізичних впливів, як сила інерції, збурення навколишнього середовища, варіабельність рухів, навчальні дані, систематичні зміщення.

Системи розпізнавання ходьби покладаються на датчики, які вимірюють прискорення та кутову швидкість тіла об’єкта. Сили інерції, спричинені ходьбою або бігом, можуть спричинити помилки у вимірюванні цих параметрів, що призведе до неточностей у біометричному шаблоні.

Вібрація та інші збурення навколишнього середовища також можуть спричинити помилки у вимірюванні таких параметрів, як прискорення та кутова швидкість. Це може бути спричинено нерівними поверхнями, вітром або іншими факторами, що призводять до неточностей у біометричному шаблоні.

Рухи людини дуже різноманітні та індивідуальні, що може спричинити труднощі в точному захопленні та зіставленні біометричного шаблону. Наприклад, такі фактори, як вік, вага та фізичний стан, можуть впливати на моделі ходьби, що призводить до хибно негативних або хибно позитивних результатів при розпізнаванні.

Механічні системи біометричного захисту обробляють великі набори навчальних даних для точного розпізнавання біометричного шаблону та відповідати йому. Однак якість і кількість навчальних даних може вплинути на точність системи. Дані про навчання, які не відображають повний діапазон варіабельності рухів людини, можуть призвести до неточностей у біометричному шаблоні.

Механічні системи біометричного захисту можуть мати систематичні зміщення, наприклад, краще розпізнавати певні моделі рухів, ніж інші. Це може призвести до неточностей у біометричному шаблоні та зробити систему менш надійною в цілому.

Електромагнітні біометричні системи

Електромагнітні біометричні системи використовуються для розпізнавання відбитків пальців чи обличчя спеціальними датчики, які виявляють унікальний візерунок виступів і западин на кінчиках пальців людини чи особливості її обличчя, базуючись на особливостях електричних та магнітних полів, створюваних шкірою. Такі системи чутливі до таких фізичних впливів, як електричні перешкоди, фактори навколишнього середовища, фізичні пошкодження, систематичні зміщення.

Електричні перешкоди можуть спричинити проблеми з датчиками, які використовуються в системах розпізнавання відбитків пальців або обличчя. Наприклад, якщо датчики знаходяться надто близько до джерела електричного шуму, це може заважати сигналу та спричиняти неточності в біометричному шаблоні.

Такі фактори навколишнього середовища, як температура, вологість і якість повітря, можуть впливати на точність систем розпізнавання відбитків пальців або обличчя. Наприклад, зміна температури або вологості може спричинити розширення чи стискання шкіри, що призводить до різниці у розмірі чи формі відбитка пальця. Так само зміни якості повітря можуть вплинути на чіткість зображень обличчя, що призведе до неточностей у біометричному шаблоні.

Фізичне пошкодження датчиків може вплинути на точність системи. Наприклад, подряпини або порізи пальця можуть ускладнити точне захоплення візерунка відбитка пальця.

Електромагнітні біометричні системи можуть мати систематичні зміщення. Наприклад, краще розпізнавати певні типи відбитків пальців або риси обличчя, ніж інші. Це може призвести до неточностей у біометричному шаблоні та зробити систему менш надійною в цілому.

Акустичні біометричні системи

Акустичні біометричні системи використовуються для розпізнавання голосу за допомогою мікрофону для запису голосу, який потім аналізується для створення унікального біометричного шаблону на основі унікальних характеристик голосу людини. Загалом ці системи базуються на комбінації фізичних принципів і технологій захоплення, обробки та аналізу біологічних характеристик. Такі системи чутливі до таких фізичних впливів, як фоновий шум, відстань від мікрофона, варіабельність мовлення, систематичні зміщення.

Фоновий шум може спричинити проблеми в системах розпізнавання голосу. Наприклад, якщо в навколишньому середовищі є сильний фоновий шум, він може заважати сигналу та спричиняти неточності в біометричному шаблоні.

Відстань між динаміком і мікрофоном також може впливати на точність системи. Якщо динамік знаходиться надто далеко від мікрофона, сигнал може бути занадто слабким, щоб точно зафіксувати біометричні характеристики.

Людське мовлення дуже варіабельне, тому індивідуальні відмінності в моделях мовлення можуть спричинити труднощі з точним записом і відповідністю біометричного шаблону. Наприклад, такі фактори, як вік, стать і акцент, можуть впливати на моделі мовлення, що призводить до хибно негативних або хибно позитивних результатів у розпізнаванні.

Акустичні біометричні системи можуть мати систематичні зміщення. Наприклад, краще розпізнавати певні шаблони мовлення або акценти, ніж інші. Це може призвести до неточностей у біометричному шаблоні та зробити систему менш надійною в цілому.

Висновок

Системи біометричного захисту інформації не є абсолютно надійними. Проблеми можуть виникати через різні фактори, зокрема через фізичні явища. Тим не менш, прогрес у розвитку сенсорних технологій, алгоритмів аналізу даних і машинного навчання може допомогти подолати ці проблеми та зробити системи біометричного захисту більш точними та надійними. Таким чином, системи біометричного захисту будуть постійно вдосконалюватися, оскільки, незважаючи на обмеження та помилки, наприклад, хибні спрацьовування, вони залишаються ефективним засобом посилення заходів безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Біометричні технології захисту URL: https://sites.google.com/site/zahistlokalnoiemerezi/zahist/biometricnij-zahist-informaciie
2. «The Role of Physics in Advancing National Security Technologies» URL: https://nap.nationalacademies.org/read/10118/chapter/11
3. Гаврилова К., Коваль О. (2019). «Роль фізики в біометрії.»
4. Li, H., & Li, J. (2016). Physics-based Biometrics: A Comprehensive Survey. IEEE Transactions on Information Forensics and Security, 11(11), 2447-2471. doi: 10.1109/TIFS.2016.2581939

Книш Богдан Петрович – канд. техн. наук, доцент кафедри загальної фізики, Вінницький національний технічний університет, Вінниця, e-mail: tutmos-3@i.ua.

Немировська Дар'я Олександрівна – студентка групи 1БКС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця.

Knysh Bogdan P. — Cand. Sc. (Eng), Assistant Professor of Department of General Physics, Vinnytsia National Technical University, Vinnytsia, e-mail: tutmos-3@i.ua.

Daria Oleksandrivna Nemyrovska - is a student of group 1BKS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.