

Застосування нечіткої логіки для підвищення стійкості біометричної ідентифікації в системах прокторингу

Євгенія Шабала¹, Борис Корнійчук², Сергій Палій³

^{1,2} Київський національний університет будівництва і архітектури
пр-т Повітряних Сил, 31, м.Київ, Україна, 03037,

³ Київський національний університет імені Тараса Шевченка
вул. Володимирська, 60, м.Київ, 01033,

¹ shabala.ieie@knuba.edu.ua, <https://orcid.org/0000-0002-0428-9273>,

² korniichuk.bv@knuba.edu.ua, <https://orcid.org/0000-0003-3881-1581>,

³ sergiy.paliy@knu.ua, <https://orcid.org/0000-0001-9742-1116>

Received 03.11.2025; Accepted 15.12.2025

<https://doi.org/10.32347/st.2025.4.1203>

Анотація. У статті розглядається необхідність впровадження математичного апарату нечітких множин для підвищення надійності біометричної ідентифікації обличчя в системах автоматизованого прокторингу в умовах екзаменаційного центру. Звертається увага на те, що зовнішнє середовище є нестабільним (освітлення, тіні, відхилення ракурсу). Це призводить до деградації точності класичних бінарних алгоритмів і збільшення частоти помилкової відмови.

Пропонується поєднання нечіткої логіки для обробки невизначеності вхідних даних. Здійснюється перетворення об'єктивних метрик якості кадру на лінгвістичні змінні ("освітлення", "ракурс") із побудовою відповідних функцій приналежності. В результаті роботи нечіткої системи, сформованої на базі правил із застосуванням Мамдані-алгоритму, отримується коефіцієнт довіри ідентифікації (КДІ). Наводиться приклад застосування КДІ для динамічної корекції порогу верифікації. Це забезпечує гнучке прийняття рішень та підвищує надійність системи прокторингу.

Ключові слова: нечіткі множини, прокторинг, ідентифікація обличчя, коефіцієнт довіри ідентифікації, дефазифікація.

ВСТУП

Сучасний розвиток освіти та професійної сертифікації, включаючи масове тестування (наприклад, НМТ/ЗНО, ЄДКІ), вимагає впровадження високоточних та надійних механізмів контролю ідентичності здобувачів. Гарантування академічної доброчесності та валідності результатів

SMART TECHNOLOGIES:

Industrial and Civil Engineering, Issue 4(17), 2025, 23-31



Євгенія Шабала
доцент кафедри кібербезпеки
та комп'ютерної інженерії



Борис Корнійчук
доцент кафедри професійної
освіти



Сергій Палій
доцент кафедри інформаційних
систем та технологій

іспитів забезпечується системами прокторингу, ключовим елементом яких є біометрична верифікація особистості.

Метод розпізнавання обличчя (Face Recognition) є найбільш затребуваним для прокторингу, оскільки він забезпечує неперервний, неінвазивний моніторинг учасника іспиту. Проте, застосування цієї технології в реальних умовах екзаменаційних центрів стикається з низкою критичних викликів. На відміну від лабораторних умов, екзаменаційний центр характеризується нестабільністю вхідних даних, такими як динамічне освітлення та тіні, низька якість відео, зміна ракурсу та

рух (Рис. 1). Такі чинники суттєво підвищують ризик виникнення помилок у роботі автоматизованих систем, що робить процес верифікації даних значно складнішим порівняно з контрольованим середовищем.



Рис.1. Особливості екзаменаційного центру
Fig. 1. Features of the examination center

Класичні алгоритми ідентифікації працюють із "чіткими" даними, де рішення приймається за бінарним принципом (ідентифіковано/не ідентифіковано). Наявність перелічених вище на малюнку перешкод призводить до деградації точності, збільшуючи ймовірність помилкового відхилення справжнього користувача (FRR) або, що критичніше, помилкового прийняття іншої особи (FAR).

Таким чином, виникає потреба у розробці такого математичного апарату, який здатен ефективно обробляти невизначеність та нечіткість вхідної інформації. Теорія нечітких множин пропонує потужний інструментарій для кількісного представлення лінгвістичних змінних ("погане освітлення", "високий рівень шуму"). Інтеграція апарату нечіткої логіки дозволить створити робастну (стійку) модель прийняття рішень, яка трансформуватиме неточні дані про навколишнє середовище в надійний коефіцієнт довіри ідентифікації

ОСНОВНІ ПОЛОЖЕННЯ

За принципом дії біометричні методи ідентифікації поділяються на статичні (за ознаками, даними людині з народження), динамічні (за ознаками, що набуті в процесі існування) та комбіновані (поєднання двох перших). Фізіологічні (статичні) методи біометричної ідентифікації:

- сканування райдужної оболонки ока;
 - сканування сітківки ока;
 - сканування рисунку вен долоні;
 - геометрія кисті руки (відбитки пальців
 - дактилоскопія, розмір, довжина і ширина долонь);
 - розпізнавання рис обличчя (контур, форма; розташування очей і носа);
 - структура ДНК-сигнатури.
- Поведінкові (динамічні) методи;
- аналіз підпису (форма букв, манера письма, натиск);
 - аналіз тембру голосу;
 - аналіз клавіатурного почерку тощо [1, 2].

Саме до категорії статичних біометричних систем, що використовують вроджені фізичні характеристики, належить технологія Face Recognition (розпізнавання обличчя), яка використовує унікальну геометрію та текстуру обличчя для ідентифікації особи.

1. Виявлення обличчя. На цьому етапі система визначає, чи є обличчя на зображенні або у відеопотоці, і де саме воно розташоване. Для локалізації використовуються моделі YOLO (You only look once) або RetinaNet, для сканування зображення та ідентифікації областей, що, ймовірно, містять людське обличчя. Результатом є обмежуючий прямокутник.

Далі відбувається вирівнювання, де система знаходить ключові орієнтири (це близько 68-100 точок), такі як кути очей, кінчик носа та контури рота. На основі цих точок обличчя геометрично трансформується, щоб привести його до стандартного, фронтального положення, мінімізуючи вплив кута зйомки та нахилу голови.

Наприкінці цього етапу відбувається нормалізація, де зображення обличчя обрізається, масштабується до фіксованого розміру та коригується освітлення, щоб зменшити вплив тіней і різноманітності умов зйомки.

2. Виділення ознак. Це етап, де зображення обличчя перетворюється на його унікальне цифрове представлення — вектор ознак. Зазвичай використовуються CNN (згорткові нейронні мережі) глибокої

архітектури (ResNet або Inception) або спеціалізовані моделі FaceNet або ArcFace.

Нейронна мережа пропускає нормалізоване зображення через свої шари, вивчаючи та ієрархічно кодує геометричні та текстурні ознаки. Останній шар мережі генерує вектор ознак фіксованої довжини. Вектор ознак - це унікальний математичний шаблон обличчя. Він спроектований так, що вектори, згенеровані для однієї й тієї ж особи (навіть при різних виразах/освітленні), розташовані близько в багатовимірному просторі. Також можуть бути згенеровані вектори для різних осіб, розташовані далеко один від одного.

3. Зберігання та індексація. Згенерований вектор ознак обличчя (не саме зображення) зберігається в базі даних разом з ідентифікатором особи. Зберігається пара: IDособи та Vознак.

Для швидкого пошуку серед мільйонів векторів використовуються методи індексації, що дозволяють швидко знаходити "сусідні" вектори в багатовимірному просторі.

4. Порівняння та прийняття рішення. Отриманий вектор ознак обличчя-запиту $V_{\text{запит}}$ порівнюється з векторами в базі даних $V_{\text{база}}$.

Далі система обчислює метрику відстані або подібності між $V_{\text{запит}}$ та одним або кількома $V_{\text{база}}$. Найпоширенішою метрикою є косинусна подібність

$$\text{Подібність} = \frac{V_{\text{запит}} \cdot V_{\text{база}}}{\|V_{\text{запит}}\| \cdot \|V_{\text{база}}\|} \quad (1)$$

Чим ближче значення до 1, тим вища ймовірність, що це та сама особа. Прийняття рішення відбувається згідно умов, які подано в Табл. 1.

Порогове значення – це значення, яке налаштовується. Встановлення високого порогу зменшує кількість помилкових спрацьовувань, але може збільшити кількість хибних відмов і навпаки. Оскільки Face Recognition є потужним інструментом для ідентифікації та верифікації особи, тоді саме дана технологія відіграє критичну роль у сучасних системах прокторингу, забезпечуючи контроль за поведінкою

екзаменованих під час віддаленого тестування.

Таблиця 1

Режим	Мета	Процес	Умова успіху
Верифікація (1:1)	Підтвердити, що $V_{\text{запит}}$ відповідає заявленому $V_{\text{база}}$.	Порівняння $V_{\text{запит}}$ з одним $V_{\text{база}}$.	Подібність $> = \text{Поріг}$
Ідентифікація (1:N)	Знайти, хто є особа $V_{\text{запит}}$ серед усіх у базі.	Порівняння $V_{\text{запит}}$ з усіма $V_{\text{база}}$.	Подібність $_{\text{макс}} > = \text{Поріг}$

Системи прокторингу дозволяють застосувати ефективніший контроль за роботою користувача з електронними ресурсами, особливо в процесах перевірки знань. Прокторінг — це процедура контролю онлайн-екзамену чи процесу тестування у різних галузях та відповідно різної складності, де за всім процесом слідкує людина, яку називають проктор.

Зі свого боку, процес прокторингу виключає будь-яку зацікавленість навчального закладу в результатах екзаменів, позаяк проктор — це не екзаменатор, а незалежна особа. Виділяють три типи прокторингу:

- синхронний прокторінг -тобто, прокторінг у реальному часі;
- асинхронний прокторінг;
- автоматичний прокторінг [3].

На сьогодні існує низка готових рішень в контексті прокторингу, які широко використовуються і надають можливість інтеграції з існуючими системами оцінювання та контролю знань, такими як Moodle, Stepik та StartExam [4].

Ідентифікації обличчя - це складова автоматизованих систем прокторингу. Екзаменаційний центр, який є віддаленим середовищем кандидата, створює значний набір зовнішніх перешкод, що прямо

ускладнюють функціонування систем Face Recognition. Основні зовнішні перешкоди включають нестабільне освітлення (зміна природного чи штучного), появу динамічних тіней на обличчі, а також поструральні зміни та рух голови кандидата. Крім того, на точність впливає часткове перекриття обличчя через окуляри чи випадковий рух рук, що порушує цілісність вхідних даних для біометричного аналізу. Ці неконтрольовані атмосферні та поведінкові фактори вимагають від алгоритмів прокторингу високої надійності та ефективної нормалізації зображення для збереження якості біометричного вектора.

Ці перешкоди впливають на ключові метрики продуктивності. Нестабільне освітлення, тіні та перекриття призводять до значного збільшення FRR (частота помилкової відмови). Це відбувається тому, що спотворення зображення змінює вектор ознак кандидата настільки, що система помилково відмовляє у верифікації законному користувачеві, генеруючи хибні попередження або перериваючи тест. Хоча вплив на FAR (частота помилкового допуску) менш виражений, пріоритетом для надійності прокторингу є мінімізація саме FRR, що вимагає вдосконалення алгоритмів для компенсації цих непередбачуваних зовнішніх факторів.

Проблеми, які наведені вище призводять до невизначеності у даних біометричних систем. Ця невизначеність потребує застосування спеціалізованого математичного апарату, наприклад теорії нечітких множин, для прийняття надійних рішень у прокторингу та біометричній безпеці загалом.

Нечітка логіка є особливо цінною в біометрії та прокторингу і це пов'язано з тим, що рішення про ідентифікацію рідко бувають абсолютно бінарними (ідентичний або неідентичний).

Замість встановлення жорсткого порогу подібності, нечітка логіка може оцінювати результат порівняння як: "Ймовірно це та сама особа" ($\mu=0.95$), "Потрібне додаткове підтвердження" ($\mu=0.6$), або "Низька ймовірність збігу" ($\mu=0.1$). Завдяки цьому

система може гнучкіше реагувати на варіативність, викликану перешкодами.

Теорія нечітких множин дозволяє ефективно моделювати вплив зовнішніх перешкод екзаменаційного середовища на біометричну систему Face Recognition та кількісно оцінювати достовірність ідентифікації в умовах невизначеності. Основним кроком є перетворення об'єктивних метрик якості кадру (чисельні значення) на суб'єктивні лінгвістичні змінні, які можуть бути оброблені нечіткою логікою.

Вхідні лінгвістичні змінні — це вимірювані характеристики зовнішніх перешкод, що впливають на якість Face Recognition. Вони означають якісні оцінки числових показників, отриманих із відеопотоку.

Таблиця 2

Вхідна лінгвістична змінна	Призначення	Базовий простір
Освітлення	Відображає рівень яскравості та рівномірності освітлення обличчя.	Діапазон значень середньої яскравості пікселів (від 0 до 255 або нормалізований діапазон).
Якість кадру	Відображає ступінь різкості та відсутність шуму/розмиття на зображенні обличчя.	Діапазон значень метрик різкості (наприклад варіація Лапласіана).
Ступінь відхилення ракурсу	Відображає кутову різницю між поточним положенням обличчя та фронтальним (еталонним) ракурсом.	Діапазон кутів повороту, зазвичай вимірюється в градусах.

Вхідні лінгвістичні змінні — це вимірювані характеристики зовнішніх перешкод, що впливають на якість Face Recognition. Вони означають якісні оцінки

числових показників, отриманих із відеопотоку.

Побудова функцій приналежності μ для вхідних змінних

Функції приналежності (MF) μ визначають, наскільки числове значення x належить до певного лінгвістичного терму (наприклад "низьке" чи "високе"). Найчастіше використовуються трикутні, трапецієподібні або Гауссові MF.

Приклад для змінної "освітлення":

"Низьке": $\mu \in [0, 1]$, якщо середня яскравість менше певного порогу, $\mu \approx 1$.

"Середнє": $\mu \in [0, 1]$, якщо яскравість у межах оптимального діапазону.

"Високе": $\mu \in [0, 1]$, якщо освітлення занадто інтенсивне або викликає пересвічування.

Результатом роботи нечіткої системи є вихідна змінна, яка кількісно оцінює довіру до біометричного результату.

Після фазифікації вхідних змінних, таких як освітлення, результатом роботи нечіткої системи є вихідна змінна – коефіцієнт довіри ідентифікації (КДІ), який кількісно відображає ступінь надійності біометричної верифікації з урахуванням виявлених зовнішніх перешкод. Коефіцієнт довіри залежить від ймовірності, за якою можна стверджувати, що гранична похибка буде гарантована в заданих межах [5]. КДІ є множником, який може бути застосований до основного показника подібності або використовуватися для порівняння з динамічним порогом. КДІ зазвичай визначається в інтервалі $[0, 1]$, де 1 - максимальна довіра, а 0 — відсутність довіри.

Для вихідної змінної КДІ також визначаються лінгвістичні терми та відповідні функції приналежності.

- "Низька довіра": КДІ $\mu \approx 1$ у нижньому діапазоні (наприклад $[0, 0.4]$).
- "Прийнятна довіра": КДІ $\mu \approx 1$ у середньому діапазоні (наприклад $[0.3, 0.7]$).
- "Висока довіра": КДІ $\mu \approx 1$ у верхньому діапазоні (наприклад $[0.6, 1]$).

Після визначення цих лінгвістичних термів для КДІ, на наступному етапі формулюється база правил нечіткого виведення, де ці терми використовуються для зв'язування вхідних перешкод із прогнозованим рівнем довіри. Правила моделюють, як поєднання несприятливих умов знижує довіру до ідентифікації:

IF (Освітлення є Низьке) AND (Ракурс є Високе відхилення) THEN (КДІ є Низька довіра)

IF (Якість кадру є Висока) AND (Освітлення є Середнє) THEN (КДІ є Висока довіра)

IF (Ракурс є Низьке відхилення) OR (Якість кадру є Висока) THEN (КДІ є Прийнятна довіра)

Зазвичай використовується метод Mamdani або Sugeno. На цьому етапі визначаються ступені виконання кожного правила шляхом застосування операторів $\min$ для AND або $\max$ для OR до ступенів належності вхідних змінних.

Після виконання всіх правил отримується нечітка вихідна множина (сукупність активованих термів КДІ). Для прийняття чіткого рішення цю нечітку множину необхідно перетворити на єдине числове значення. Цей від лінгвістичної оцінки до числового результату реалізується за допомогою процесу дефазифікації.

Дефазифікація є процедурою розрахунку звичайного значення вихідної змінної на основі узагальненого нечіткого числа, отриманого на етапі акумуляції для відповідної вихідної лінгвістичної змінної [6].

Метод центру тяжіння - найпоширеніший і найточніший метод, що дозволяє здійснити приведення до чіткості вихідної змінної без попереднього акумулювання актуалізованих висновків окремих правил [7]. Він обчислює центр площі під об'єднаною нечіткою вихідною множиною. Отримане значення є чітким числовим коефіцієнтом довіри ідентифікації.

Для методу Центру тяжіння чітке значення коефіцієнта довіри ідентифікації $\text{КДІ}_{\text{чітке}}$ обчислюється за формулою:

$$КДІ_{\text{чітке}} = \frac{\sum_{i=1}^n x_i \cdot \mu_{\text{вихід}}(x_i)}{\sum_{i=1}^n \mu_{\text{вихід}}(x_i)} \quad (2)$$

де:

x_i - дискретне значення вихідного універсуму (можливі значення КДІ від 0 до 1).

$\mu_{\text{вихід}}(x_i)$ - агрегована функція належності вихідної нечіткої множини у точці x_i (об'єднання результатів усіх активованих правил).

n — кількість точок дискретизації.

Отримане чітке значення КДІ використовується для корекції біометричного рішення, пов'язаного з коригуванням порогу. Фактичний показник біометричної подібності множиться на $КДІ_{\text{чітке}}$, або ж поріг для прийняття рішення динамічно підвищується, якщо КДІ низький, змушуючи систему вимагати вищу біометричну відповідність в умовах поганої якості кадру.

Якщо $КДІ_{\text{чітке}}$ падає нижче критичного порогу, то система генерує попередження або автоматично призупиняє тестування, вимагаючи від кандидата покращити якість середовища (наприклад, виправити освітлення).

На Рис. 2 зображений Fuzzy Logic Designer для проектування нечіткої системи, яка здатна оцінювати якість середовища тестування на основі таких вхідних параметрів, як "Освітлення" та "Ракурс". Ця нечітка система, що використовує Мамдані-алгоритм і обчислює кінцевий показник "КДІ".

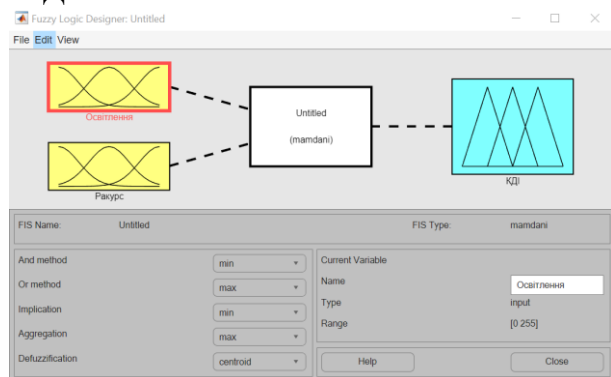


Рис. 2. Введення вхідних і вихідних змінних
Fig. 2. Entering input and output variables

Далі необхідно визначити функції приналежності для кожної змінної. На Рис. 3 продемонстровано Membership Functions для вихідної змінної КДІ, яка є результатом роботи нечіткої логічної системи в автоматизованому прокторингу.

Для цієї змінної визначено три лінгвістичні терми: «Низька_довіра», «Прийнятна_довіра» та «Висока_довіра», що описуються трикутними та Z-подібними функціями приналежності. Такий розподіл дозволяє системі диференціювати якість біометричного аналізу, де терм «Прийнятна_довіра» досягає свого максимуму при значенні 0.6. Це означає достатній рівень стабільності даних навіть за наявності незначних перешкод.

КДІ кількісно оцінює надійність біометричної верифікації обличчя в умовах зовнішніх перешкод екзаменаційного центру і перебуває в діапазоні [0, 1].

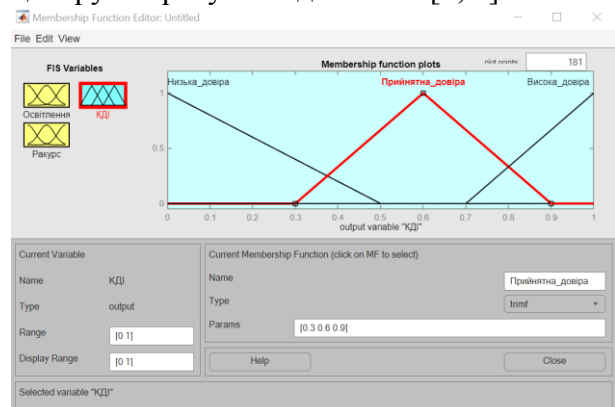


Рис. 3. Membership Functions для КДІ
Fig. 3. Membership Functions for ICF

Далі наведено створення бази правил нечіткого виведення. Наприклад, Правило 1 ("If (Освітлення is Низьке) and (Ракурс is Високе_відхилення) then (КДІ is Низька_довіра)") відображає логіку, згідно з якою наявність двох несприятливих факторів одночасно призводить до найнижчого рівня довіри до процесу ідентифікації.

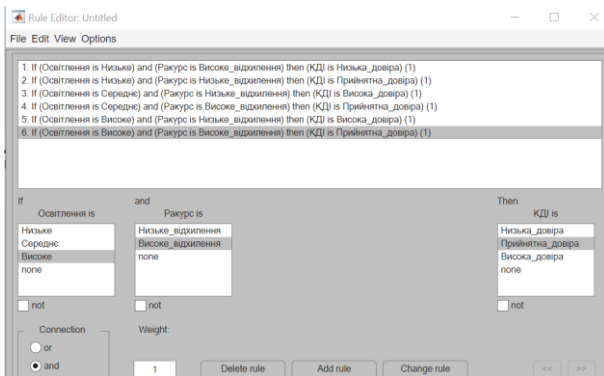


Рис. 4. База правил нечіткого виведення

Fig. 4. Fuzzy inference rule base

На Рис. 5 наведено результат виведення роботи правил. Оскільки обидва фактори, що погіршують якість (низьке освітлення та високе відхилення ракурсу), присутні, то нечітка система робить висновок, що довіра до результату біометричної ідентифікації низька. Ці умови зйомки суттєво ускладнюють процес ідентифікації у зв'язку з недостатньою кількістю деталей обличчя та викривлення і це призвело до того, що система видала низький коефіцієнт довіри ідентифікації 0.377.

У реальній системі прокторингу такий низький КДІ є привідом згенерувати попередження для користувача типу "покараще освітлення, поверніть обличчя" і т.п.

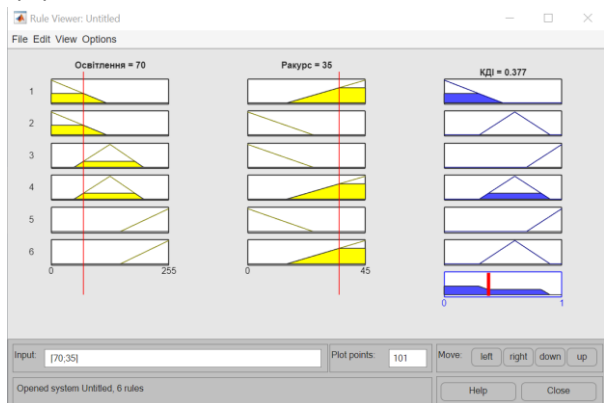


Рис. 5. Результат виведення роботи правил

Fig. 5. The output of the rules operation

Щоб завершити перевірку, було введено значення для сценарію високої довіри, коли освітлення = 150, а ракурс = 5 (Рис 6). При таких параметри означають хороші умови зйомки та мінімальний рух голови і система видає високий коефіцієнт довіри ідентифікації ≈ 0.9 .



Рис. 6. Результат виведення роботи правил при сприятливих умовах

Fig. 6. The result of deriving the rules under favorable conditions

На Рис. 7 показано вісь X визначає Освітлення в діапазоні від 0 до 255. Це є яскравістю середовища. Вісь Y – ракурс в діапазоні від 0 до 45 і визначає кутове відхилення голови (0° - фронтально). Вісь Z – це КДІ від 0 до 1 - числове значення довіри, де 1 - максимальна довіра.

Максимальна довіра. Пік знаходиться де освітлення $\sim 150-250$ (середнє або високе), а ракурс $\sim 0-10$ (при низькому відхиленні і обличчя фронтально). При оптимальних або просто хороших умовах зйомки та мінімальному русі голови (задовільняє умови правил №3 і №5), довіра до ідентифікації найвища.

Мінімальна довіра. Провал знаходиться там, де низьке освітлення $\sim 0-50$, а ракурс має високе відхилення $\sim 40-45$. Це підтверджує правило №1 - коли поєднуються два несприятливих фактора (темнота та значний поворот голови), то це призводить до різкого падіння КДІ і в такому випадку необхідне негайне втручання системи прокторингу. Якщо освітлення поступово падає з 150 до 50, то КДІ знижується плавно, а не стрибком, як це відбулося б у класичній системі з жорстким бінарним порогом. Ця плавність робить систему стійкішою до невеликих, але постійних коливань зовнішнього середовища.

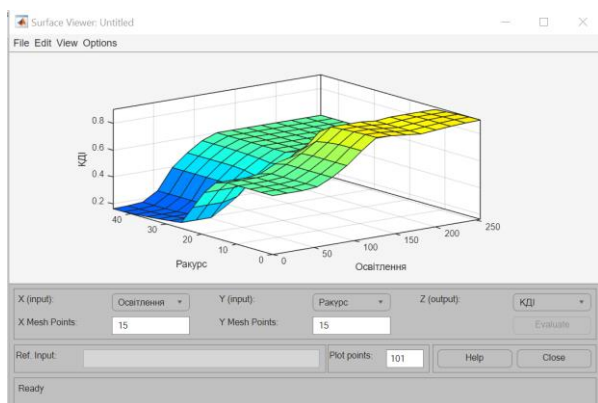


Рис. 7. 3D-модель залежності КДІ від освітлення та ракурсу

Fig. 7. 3D model of the dependence of ICF on lighting and angle

Для розуміння переваги застосування нечіткої логіки необхідно виконати візуалізацію за допомогою графіку. Для цього необхідно змінити функції приналежності на Гауссові (gaussmf) для освітлення та ракурсу у MFE (Рис.8).

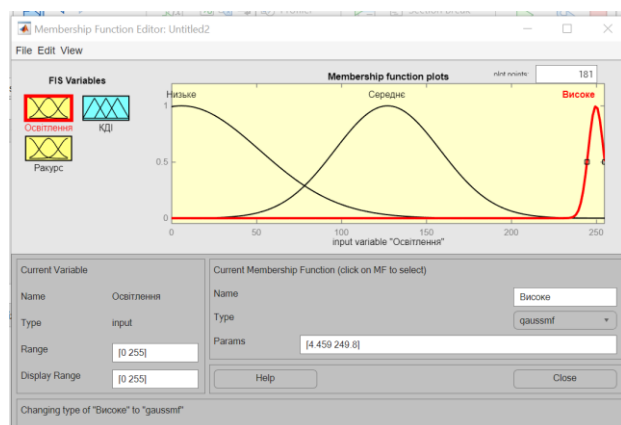


Рис. 8. Зміна функції приналежності на gaussmf

Fig. 8. Changing the membership function to gaussmf

На Рис. 9 зображено графік "Вплив освітлення на рішення про ідентифікацію", де порівнюється класична та нечітка системи.

На цьому графіку відображено дві криві, які демонструють різницю у реакції системи на зміну вхідного параметра освітлення.

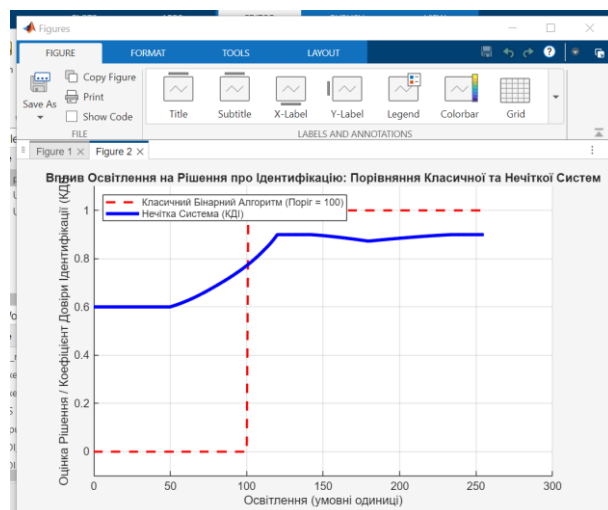


Рис. 9. Порівняння класичної та нечіткої систем

Fig. 9. Comparison of classical and fuzzy systems

Червоною пунктирною лінією позначається крива класичного бінарного алгоритму. Класичний бінарний алгоритм - метод прийняття рішення, який описує різкий, ступінчастий перехід від одного стану до протилежного, коли вхідний параметр досягає певного жорстко встановленого порогового значення. Крива має форму ступінчастої функції, тобто жорсткий перехід. До освітлення ≤ 100 одиниць КДІ дорівнює 0, тобто це буде відмова або мінімальна довіра. Оразу після Освітлення > 100 одиниць, КДІ миттєво стрибає до 1. Це означає допуск або повну довіру.

Коли є незначне коливання освітлення навколо порогового значення 100, то ця ситуація призводить до різкої зміни рішення з "допуск" на "відмова". Це призводить до високої частоти помилкової відмови (FRR) у реальних умовах.

Синя суцільна лінія позначає криву нечіткої системи. Крива показує плавний S-подібний перехід у діапазоні освітлення від 50 до 100. В такому графіку рішення змінюється поступово: коли освітлення, менше за 50, КДІ тримається близько 0.6 і це базовий рівень довіри системи при ракурсі 5° , а потім плавно зростає і досягає 0.9 після 100 одиниць освітлення.

У критичній зоні навколо 100 рішення не стрибає. Замість того, щоб переходити від 0 до 1, КДІ плавно змінюється. Це дозволяє системі коригувати фінальний поріг і мінімізувати помилкові спрацювання, які

пов'язані з вхідними даними, які містять шуми.

ВИСНОВКИ

Розроблена нечітка система виведення на основі правил Mamdani, яка трансформує поєднання несприятливих вхідних факторів у єдине чітке числове значення КДІ за допомогою методу центру тяжіння. Результати 3D-моделювання підтверджують, що в оптимальних умовах КДІ сягає максимальних значень, тоді як поєднання двох несприятливих факторів призводить до різкого падіння КДІ. Це дозволяє системі прокторингу не лише прийняти рішення про ідентифікацію, але й динамічно коригувати поріг верифікації. При ситуації, коли критично низький КДІ, система має автоматично генерувати попередження або призупиняти тестування. Застосування нечіткої логіки забезпечує розробку надійніших та справедливіших систем контролю академічної доброчесності в умовах нестабільного екзаменаційного середовища.

REFERENCES

1. Tsaryov R. Yu., Lemyekha T. M. (2016). Biometrychni tekhnolohiyi: navchal'nyy posibnyk. Odesa, ONAZ im. O. S. Popova Publ., 140.
2. Koval L. H., Zlepko S. M., Novitskyi H. M., Krekotenі Ye. H. (2019). Metody i tekhnolohiyi biometrychnoyi identyfikatsiyi za rezul'tatamy literaturnykh dzherel. Vcheni zapysky TNU imeni V. I. Vernads'koho. Seriya: tekhnichni nauky, 30(69), 1 (2), 104–112.
3. Denesyak O. I., Palamarchuk Ye. A. (2021). Kompleksna systema proktorynhu v informatsiynykh tekhnolohiyakh analizu kontekstu v systemakh otsynuyannya znan'. Visnyk Vinnyts'koho politekhnichnoho instytutu, 6, 93–99.
4. Filipova L. L., Hrusheva A. A. (2015). Metodyka vykladannya navchal'noyi dystsypliny «Shtuchnyy intelekt». Profesiyna osvita: metodolohiya, teoriya ta tekhnolohiyi, 1, 181–191.
5. Kalashnikova Kh. I., Bratash M. A., Ostrohlyad O. H. (2023). Osnovy naukovykh doslidzhen': konspekt lektsiy dlya здобувачів першого (bakalavrs'koho) рівня вищої освіти всіх форм навчання зі спеціальності 073 – Menedzhment. Kharkiv, KhNUMH im. O. M. Beketova Publ., 195.
6. Shushura O. M. (2023). Nechitke modelyuvannya ta upravlinnya. Laboratornyy praktykum. Kyiv, KPI im. Ihoria Sikorskoho Publ., 42.
7. Harmash E. V., Kollarov O. Yu. (2020). Vybir alhorytmiv rehulyatora nechitkoho typu dlya vitroenerhetychnykh ustanovoko. Naukovi pratsi DonNTU. Seriya: «Elektrotekhnika i enerhetyka», 1(22), 62–65.

Applying fuzzy logic to increase the stability of biometric identification in proctoring systems

*Yevheniia Shabala, Borys Korniiuchuk,
Sergiy Paliy*

*Kyiv National University of Construction and
Architecture,*

Taras Shevchenko National University of Kyiv

Abstract. The article considers the need to implement the mathematical apparatus of fuzzy sets to increase the reliability of biometric facial identification in automated proctoring systems in examination center conditions. Attention is drawn to the fact that the external environment is unstable (fluctuations in lighting, shadows, deviations in perspective). This leads to a degradation of the accuracy of classical binary algorithms and an increase in the frequency of false failures. A combination of fuzzy logic is proposed to handle input data uncertainty. Objective frame quality metrics are transformed into linguistic variables ("lighting", "angle") with the construction of corresponding membership functions. As a result of the operation of a fuzzy system formed on the basis of rules using the Mamdani algorithm, an identification confidence coefficient (CCI) is obtained. An example of using CCI for dynamic correction of the verification threshold is given. This provides flexible decision-making and increases the reliability of the proctoring system.

Keywords: fuzzy sets, proctoring, face identification, identification confidence factor, defuzzification.