ЗМІСТ

Перелік умовних позначень, символів, скорочень і термінів

БД – база даних.

Верифікація – порівняння один до одного з біометричним шаблоном (перевірка того, що людина та, за яку себе видає).

Ідентифікація – порівняння один до багатьох: після отримання біометричних даних йде з’єднання з біометричною базою даних шаблонів для визначення особистості.

Аутентифікація – процедура перевірки справжньості, наприклад: перевірка справжньості користувача шляхом порівняння введеного ним пароля з паролем, збереженим у базі даних користувачів.

Авторизація – надання певній особі чи групі осіб прав на виконання певних дій, а також процес перевірки (підтвердження) даних прав при спробі виконання цих дій.

Оклюзія – ситуація, в якій два об’єкти розташовані приблизно на одній лінії і один об’єкт, розташований ближче до віртуальної камери або вікна перегляду, частково або повністю закриває видимість іншого об'єкта.

Морфінг – спеціальний ефект в кіно та анімації, що змінює одне зображення або форму в інше через плавний перехід.

Аберація – дефект, похибка зображення в оптичних системах. Аберація оптичних систем проявляється в тому, що зображення втрачають чіткість і не точно відповідають зображуваним об’єктам.

Альбедо – фізична величина, що описує здатність поверхні чи космічного тіла відбивати та розсіювати випромінення (світло).

Рендеринг – в комп'ютерній графіці — це процес отримання зображення за моделлю з допомогою комп’ютерної програми. Тут модель — це опис тривимірних об’єктів (3D) на визначеній мові програмування і у вигляді структури даних. Такий опис може містити геометричні дані, положення точки спостерігача, інформацію про освітлення. А зображення — це цифрове растрове зображення.

Спуфінг – обман біометричних систем шляхом представлення біометричному сенсору копій, муляжів, фотографій, муляжів відбитків пальців, заздалегідь записаних звуків і т. і.

GUI – Graphical User Interface.

ВСТУП

Біометричні системи аутентифікації — системи аутентифікації, що використовують для розпізнавання людей їх біометричні дані. Біометричні дані можуть бути фізіологічними чи поведінковими. Фізіологічні відносяться до особливостей тіла — відбитки пальців, розпізнавання лиця, ДНК, долоня руки, сітчатка ока, запах, голос. Поведінкові — пов’язані з поведінкою людини (хода та мова).

Застосування біометричних технологій є різноманітним: доступ до робочих місць та мережевих ресурсів, захист інформації, забезпечення доступу до певних ресурсів та безпека в аеропортах. Ведення електронного бізнесу та електронних урядових справ можливе лише після дотримання певних процедур по ідентифікації особистості. Біометричні технології використовуються в області безпеки банківських звернень, інвестування та інших фінансових операцій, а також у роздрібній торгівлі, охороні правопорядку, питаннях охорони здоров’я, а також у сфері соціальних послуг. Біометричні технології у близькому майбутньому будуть відігравати головну роль у питаннях персональної ідентифікації у багатьох сферах.

Але вони вразливі до атак на різних стадіях обробки інформації. Ці атаки можливі на рівні сенсора, де сприймається зображення чи сигнал від індивідуума, атаки повтору (replay) на лініях комунікацій, атаки на базу даних, де зберігаються біометричні шаблони, атаки на модулі порівняння та прийняття рішень.

Необхідним кроком для застосування біометричних систем розпізнавання особистості є аналіз факторів, що впливають на надійність використання цих систем, та прийняття відповідних рішень щодо забезпечення максимальної надійності при використанні даних систем.

Темою даної магістерської дисертації є аналіз факторів, що впливають на надійність технологій розпізнавання облич (для дослідження взято конкретну тему розпізнавання облич, адже біометричні технології у цілому вимагають надзвичайно об’ємного дослідження), та надання конкретних рекомендацій щодо більш надійного застосування систем розпізавання облич. У практичній частині виконано розробку програми 2D розпізнавання облич, що має можливість проводити розпізнавання також у відеопотоці, і створене програмне забезпечення протестовано на можливість застосування фото-спуфінгу.

1 АНАЛІЗ ТЕХНОЛОГІЇ РОЗПІЗНАВАННЯ

Отже, оскільки дослідження звузилося до біометричних технологій розпізнавання облич, то і розглядатимуться конкретно ці технології та їх особливості. Для того, аби зрозуміти «слабкі» місця технології з точки зору безпеки, необхідно для початку зрозуміти саму суть технології.

Розпізнавання облич — завдання, з яким люди справляються надзвичайно легко та швидко. Ця очевидна простота виявилася небезпечно оманливою, адже завдання автоматичного розпізнавання облич виявилося проблемою, що досі є далекою від вирішення. Незважаючи на 20 років інтенсивних досліджень, велику кількість опублікованих статей в журналах та конференцій, що присвячені цій темі, досі неможливо заявити, що штучні системи можуть «позмагатися» з людськими показниками.

Автоматичне розпізнавання облич є «заплутаним» завданням в першу чергу через складні вимоги до зображень (освітлення та зміна позиції і повороту лиця під час руху людини), а також через інші різноманітні ефекти, такі як старіння, вираз обличчя, оклюзії та т. і. Дослідники по комп’ютерному баченню, аналізу зображень та їх обробки, розпізнаванню паттернів та іншим сферам працюють разом над вирішенням цього питання, змотивовані великою кількістю можливих практичних застосувань технології розпізнавання облич.

Розпізнавання облич стало одним з трьох методів ідентифікації, що використовуються у електронних паспортах, а також є вибором для багатьох інших програм для безпеки. З-поміж шести біометричних атрибутів (рис. 1.1) ознаки обличчя мають найкращу сумісність у системі машинозчитувальних проїзних документів (Machine Readable Travel Documents – MRTD), і це базується на оціночних факторах — реєстрації, оновленні, вимогах до машини, і суспільному сприйнятті [2].

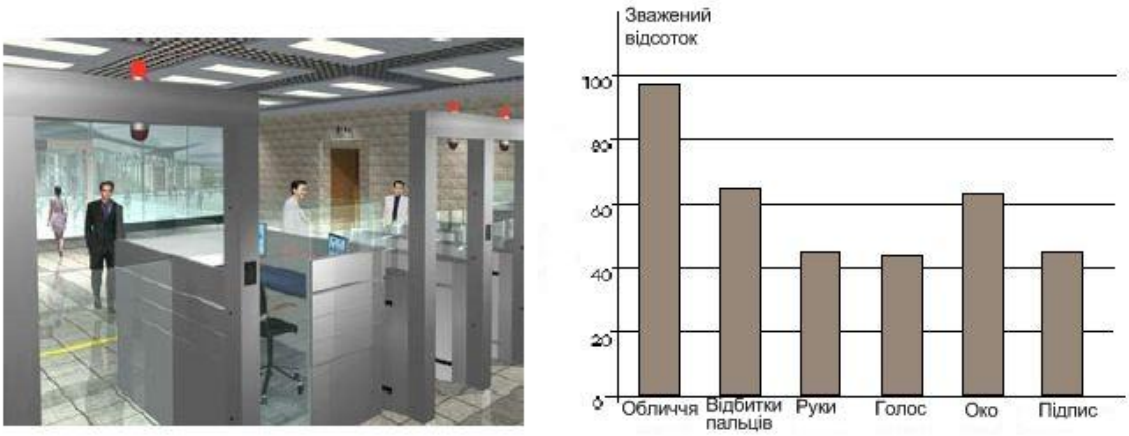


Рисунок 1.1 – Сценарій застосування MRTD-системи при паспортному контролі (зліва), і порівняння різних біометричних ознак щодо MRTD-сумісності (справа)

Системи розпізнавання облич повинні «знаходити» обличчя на зображеннях та відео автоматично. Вони можуть функціонувати у одному з двох режимів: (1) – верифікація обличчя (або аутентифікація), та (2) – ідентифікація обличчя (або розпізнавання). Верифікація обличчя включає в себе порівняння один до одного, тобто обличчя з зображення до шаблону обличчя тієї людини, яку верифікують. Ідентифікація обличчя включає в себе порівняння один до багатьох — обличчя з зображення до усіх шаблонів облич в базі даних для визначення особи, чиє лице є на зображенні. Інший сценарій розпізнавання облич включає в себе порівняння один до декількох — обличчя з зображення порівнюється до декількох шаблонів облич тих людей, що обрані користувачем (наприклад, полісмен обирає підозрюваних для визначення злочинця).

Продуктивність систем розпізнавання облич значно покращилась з того часу, як було розроблено першу автоматичну систему розпізнавання облич. Крім того, виявлення обличчя на зображенні, виділення ознак обличчя та розпізнавання можуть зараз бути виконані у «realtime» для тих зображень, що були отримані під бажаними (тобто, доволі суворими) вимогами.

1.1 Процес розпізнавання облич

Розпізнавання облич — це задача розпізнавання візуальних паттернів. Таким чином, обличчя являє собою тривимірний об’єкт, що може піддаватися різним рівням освітлення, змінювати позу, вираз і таке інше, тож ідентифікація обличчя базується на двовимірному зображенні (тривимірні зображення, що отримуються за допомогою лазерів, також використовуються). Система розпізнавання облич загалом складається з чотирьох модулів, як зображено на рис. 1.2: виявлення, оцінка положення, виділення ознак та зіставленння, де локалізація та нормалізація (виявлення обличчя та його положення) — це етапи попередньої обробки, що виконуються безпосередньо перед тим, як проводиться розпізнавання обличчя (виділення ознак обличчя та зіставлення його з шаблонами з бази даних).

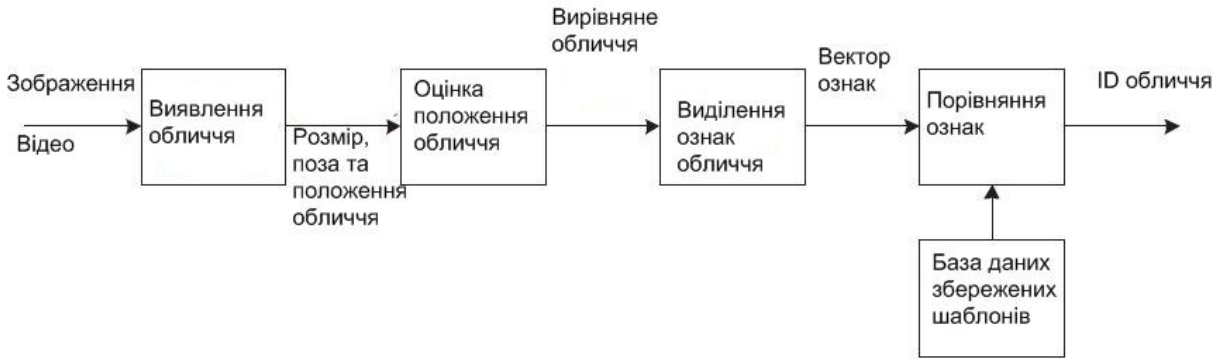


Рисунок 1.2 – Схема процесу розпізнавання облич

Виявлення обличчя відмежовує область обличчя від фону. У випадку відео для виявлення обличчя спеціальні компоненти трекінгу (відстеження) облич можуть бути застосовані. Оцінка положення обличчя має за мету досягнення більш точної локалізації та нормалізацію облич, в той час, як виявлення обличчя забезпечує лише грубу оцінку місця розташування і масштабу кожного виявленого обличчя. Виявляються компоненти обличчя, такі як ніс, очі, рот та контур обличчя; на основі точок місцезнаходження вхідне зображення обличчя нормалізується у відношенні до геометричних властивостей, таких як розмір та

поза, при цьому використовуються геометричні перетворення або морфінг. Обличчя зазвичай і далі нормалізується по відношенню до фотометричних властивостей, таких як освітлення та відтінки сірого.

Після того, як обличчя нормалізовано геометрично та фотометрично, проводиться виділення ознак обличчя для забезпечення ефективної інформації, що використовується для того, щоб відрізняти обличчя різних людей одне від одного, причому ця інформація повинна бути настільки точною, щоб відрізняти обличчя можна було навіть при різному наборі геометричних та фотометричних даних. Для зіставлення облич виділений вектор ознак вхідного обличчя порівнюється з векторами облич з бази даних; система виводить результат (розпізнавану особу) у тому випадку, якщо співпадіння виявлено при задовільному порозі точності, або ж виводить, що обличчя належить невідомій людині.

Результати розпізнавання облич сильно залежать від виділених ознак, що представляють шаблон обличчя, та методів класифікації, що використовуються для відрізнення облич одне від одного, в той час, як локалізація та нормалізація облич є базисом для виділення ефективних ознак. Ці проблеми можуть бути проаналізовані з точки зору підплощин чи колекторів (різноманіття).

1.2 Аналіз в підплощинах облич

Техніки аналізу підплощин для розпізнавання облич базуються на факті того, що клас шаблонів облич знаходиться у площині вхідного зображення. Наприклад, невелике зображення розміру 64 x 64 має 4096 пікселів і може створити велику кількість класів шаблонів, таких як дерева, будинки та обличчя. Однак з-поміж $256^{4096} > 10^{9864}$ можливих «конфігурацій» лише декілька відповідають обличчям. Саме тому першопочаткове представлення зображення є надлишковим, і вимірність цього представлення може бути значно зменшена саме тоді, коли потрібен лише шаблон обличчя.

З підходом eigenface (власне обличчя) чи аналізу принципового компоненту (principal component analysis – PCA) невелика кількість (наприклад, 40 чи навіть менше) компонентів eigenface (власних облич) отримується з набору навчальних зображень обличчя, при цьому використовується перетворення Кархунена-Лоева або PCA. Зображення обличчя продуктивно представлене як вектор ознак (або вектор ваги) низької вимірності. Ознаки у такому підпросторі надають більш помітну та багату інформацію для розпізнавання, аніж початкове зображення. Використання техніки моделювання підплощин значно просунуло вперед технологію розпізнавання облич.

Різноманіття або розподіл усіх облич складає варіації вигляду обличчя, тоді як різноманіття не-облич складає все інше. Якщо розлядати ці колектори (різноманіття) у площині зображення, то зрозуміло, що вони дуже нелінійні та неопуклі. Рис. 1.3 (а) ілюструє колектор облич проти колектору не-облич, (б) ілюструє колектор облич двох людей у цілому колеторі облич. Виявлення обличчя може розглядатись як задача виявлення відмінності між колекторами облич та не-облич у площині зображення, розпізнавання ж облич може бути трактовано як задача виявлення відмінності між обличчями у колекторі облич.

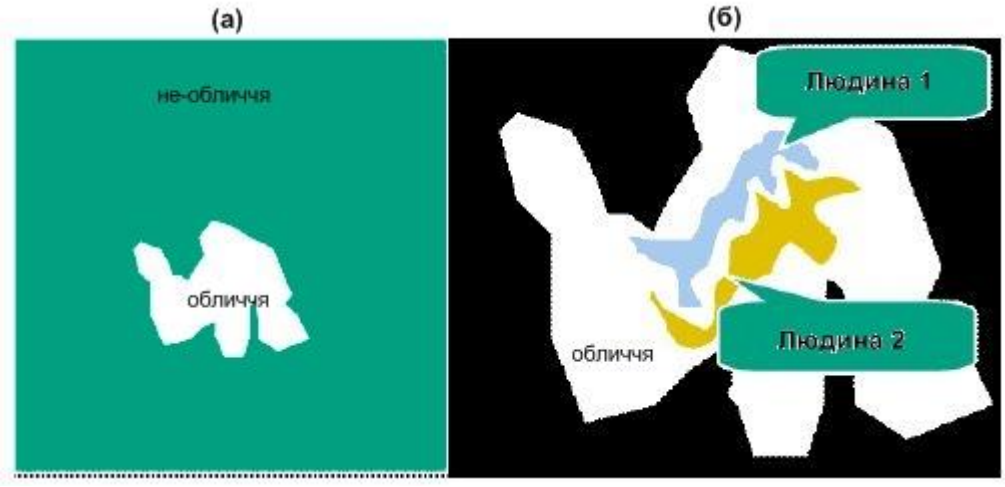


Рисунок 1.3 – (а) ілюструє колектор облич проти колектору не-облич, (б) ілюструє колектор облич двох персон у цілому колеторі облич

Рис. 1.4 детальніше ілюструє нелінійність та неопуклість колектору зображень у площині PCA, що використовує три принципових перших компонента, причому графіки побудовано з зображення реального обличчя. Кожен графік відображає колектори трьох людей (у трьох кольорах). Для кожної людини використовується 64 фронтальних зображення обличчя. Використовується певний тип перетворення на оригінальному зображенні обличчя з 11 поступово змінюваними параметрами, що створюють 11 трансформованих зображень обличчя; кожне трансформоване зображення «обрізане» таким чином, що містить лише область обличчя; 11 «обрізаних» зображень обличчя формують послідовність. Крива на цьому рисунку відображає таку послідовність у площині PCA, таким чином є 64 криві для кожної людини. Тривимірна PCA площина спроектована на двовимірну площину. Видно нелінійність траекторій.

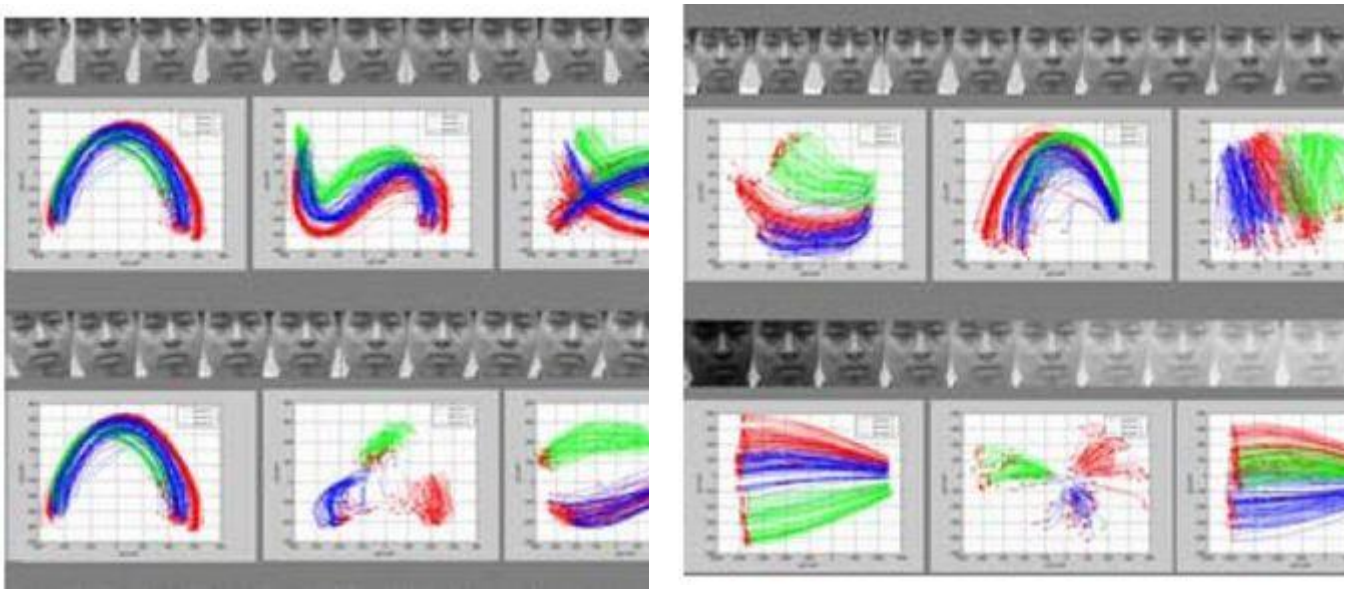


Рисунок 1.4 – Нелінійність та неопуклість колекторів облич під перетвореннями переміщення, повороту, масштабування та Гамма-перетворенням

Два важливих зауваження: по-перше, ці приклади продемонстровано у площині PCA, але більш складні (нелінійні та неопуклі) криві будуть на площині

оригінального зображення; по-друге, хоч ці приклади піддавались геометричним перетворенням у двовимірному просторі та точковому освітленню (Гамма-перетворення), більша складність буде у тривимірних геометричних перетвореннях (повороти поза площиною та зміна направленості освітлення).

1.3 Технічні складнощі

Як показано на рис. 1.3, класифікаційна проблема, пов’язана з виявленням обличчя, є дуже нелінійною та неопуклою, та навіть більше для зіставлення облич. Оціночні звіти по розпізнаванню облич та інші незалежні дослідження показують, що продуктивність багатьох сучасних методів розпізнавання облич погіршується зі змінами в освітленні, позі та інших факторах. Ключові технічні складнощі описано далі.

1.3.1 Велике різноманіття змін у зовнішності обличчя

У той час, як форма та відображення є внутрішніми властивостями обличчя, зовнішність (вигляд текстури) обличчя піддається декільком іншим факторам, включаючи позу обличчя (або, іншими словами, точку зйомки камери), освітлення, вираз обличчя. Рис. 1.5 показує приклад значної внутрішьопредметної варіації, що викликана цими факторами. У додаток до цього різні параметри зображення, такі як діафрагма, час експозиції, аберації об’єктиву і датчик спектральної характеристики, також збільшують внутрішьопредметну варіацію.

Ідентифікація персони по обличчю далі ускладнюється можливими невеликими внутрішьопредметними варіаціями (рис. 1.6). Усі ці фактори включені у інформацію зображення, тому «варіації між зображеннями одного і того самого обличчя через освітлення та напрямок споглядання майже завжди більші, аніж варіації між обличчями різних людей». Ця варіативність ускладнює отримання внутрішньої інформації об’єктів обличчя з їх відповідних зображень.

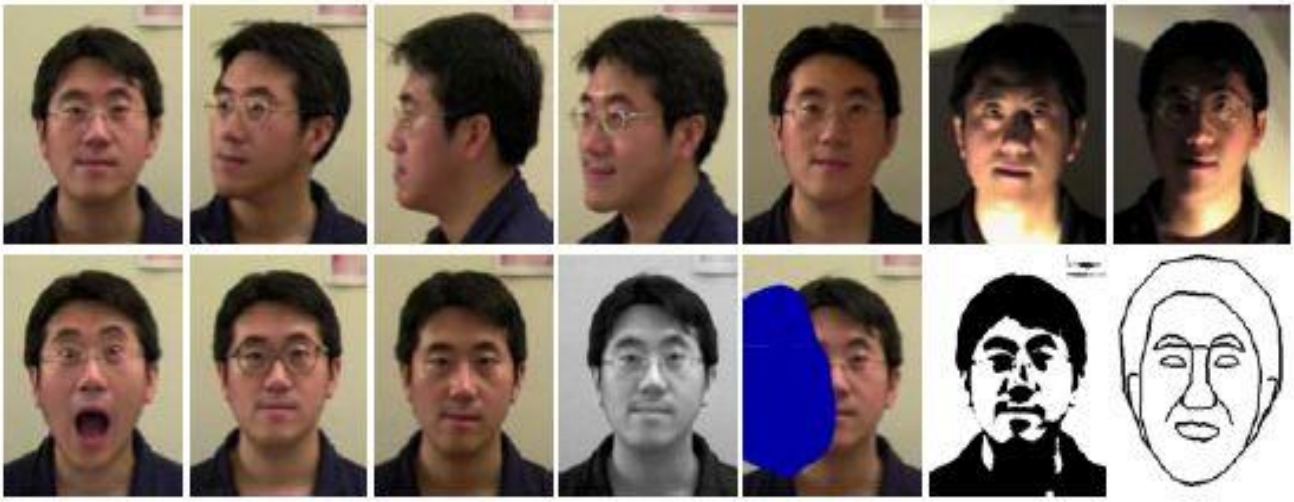


Рисунок 1.5 – Внутрішньопредметні варіації у позі, освітленні, виразі обличчя, оклюзії, аксесуарах (у цьому випадку, окулярах), кольорі та яскравості

Рисунок 1.6 – Схожість фронтального обличчя між (а) близнюками та (б) батьком та сином

1.3.2 Надзвичайно складні нелінійні колектори

Як показано вище, колектор цілого обличчя є дуже неопуклим, точно так само і колектори облич буль-якої людини з різними змінами. Лінійні методи, такі як PCA, аналіз незалежних компонентів (independent component analysis – ICA) та аналіз лінійного дискримінанту (linear discriminant analysis – LDA), проектують дані лінійно з багатовимірного простору (тобто простору зображення) у маловимірну підплощину. Саме тому вони не в змозі зберегти неопуклі варіації колекторів обличчя, що необхідні для того, щоб розрізняти між людьми. У лінійній підплощині Евклідова відстань та узагальнена відстань Махаланобіса, що зазвичай використовуються для зіставлення шаблонів, не є достатньо продуктивними для класифікації між колекторами облич та не-облич та між колекторами облич різних людей (рис. 1.7 (а)). Цей вирішальний факт обмежує потужність лінійних методів у досягененні високоточного розпізнавання та виявлення облич.

1.3.3 Висока розмірність та малий розмір вибірки

Наступна складність полягає у неможливості узагальнювати, як показано на рис. 1.7 (б). Канонічне зображення обличчя розміром 112 x 92 перебуває у просторі ознак з 10304 вимірами. Не дивлячись на це, кількість прикладів на людину (типово менше 10, навіть тільки один), доступних для вивчення колектору, зазвичай значно менша, ніж вимірність простору зображення; система, натренована на такій невеликій кількості прикладів, не може добре узагальнити невидимі зразки обличчя.

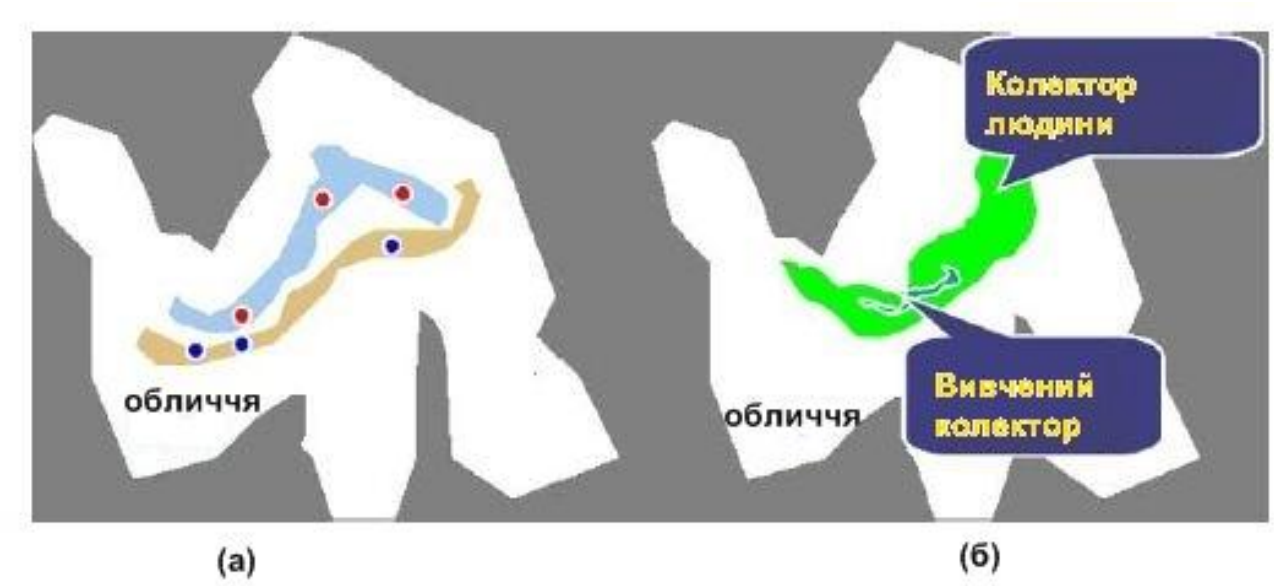


Рисунок 1.7 – Труднощі у ропізнаванні облич з точки зору підплощин. (а) – Евклідова відстань не може відрізнити людей: у термінах Евклідової відстані, міжособистісна відстань може бути меншою, ніж внутрішньоособистісна. (б) – вивчений колектор чи класифікатор не в змозі узагальнити невидимі зображення одного і того самого обличчя людини

1.4 Технічні рішення

Існує дві стратегії для того, щоб мати справу з вищеописаними труднощами: відокремлення ознак та класифікація шаблонів на основі відокремлених ознак. Перша стратегія існує для того, щоб сконструювати «гарний» простір ознак, у якому колектори облич стають «простішими», тобто менш нелінійними та неопуклими, аніж у інших просторах. Це включає в себе два рівня обробки: (1) геометрична та фотометрична нормалізації зображення обличчя, такі як морфінг та вирівнювання гістограми; та (2) відокремлення ознак у нормалізованих зображеннях, що є стійкими до варіацій.

Другою стратегією є конструювання класифікаційних інструментів, що можуть вирішувати складні нелінійні класифікаційні та регресійні задачі у просторі ознак, а також краще узагальнювати. Хоч гарна нормалізація та відокремлення ознак зменшують нелінійність та неопуклість, вони все ж таки не вирішують проблеми повністю, саме тому класифікаційні інструменти, що здатні мати справу з такими складнощами, є досі необхідними для досягнення високої продуктивності. Успішні алгоритми зазвичай поєднують обидві стратегії.

З геометричним підходом, що використовувався спочатку і який базується на ознаках, можна виявити ознаки обличчя такі як очі, ніс, рот та підборіддя. Властивості та зв'язки (наприклад, області, відстані та кути) між ознаками використовуються як дескриптори для розпізнавання обличчя. Переваги цього підходу включають в себе економію та ефективність при досягненні зменшення кількості даних та нечутливості до варіацій у освітленні та точці зйомки. Однак, виявлення ознак обличчя та оціночні техніки, розроблені на сьогоднішній день, є недостатньо надійними для геометричного розпізнавання, базованого на ознаках, і такі геометричні ознаки наодинці не підходять для розпізнавання облич, адже багаті на інформацію дані, що знаходяться у текстурі обличчя чи зовнішності, взагалі не враховуються. Саме через ці причини техніки, що використовувались на початку, не є ефективними сьогодні.

Статистичний підхід «вивчає» тренувальні дані (зображення зовнішності або ознаки, відокремлені з зовнішності), щоб відокремити хороші ознаки та сконструювати класифікаційні інструменти. Під час навчання і попередні знання про обличчя, і варіації, які видно на навчальному матеріалі, взяті до уваги.

1.5 Висновки

Як показано раніше, система розпізнавання облич складається з декількох компонентів, — виявлення обличчя, оцінка положення, виокремлення ознак та

зіставлення. То на якому етапі зараз технологія, чи здатна вона створити систему автоматичного розпізнавання облич? Щоб відповісти на це запитання, потрібно зробити припущення про деякі дані обмеження, а саме про те, якою є ситуація застосування технології та наскільки сильними ці обмеження мають бути у цій ситуації; тож обмеженнями є поза, освітлення, вираз обличчя, вік, оклюзія та волосся на обличчі. Задача виявлення обличчя у режимі реального часу у нормальному закритому середовищі вже досить добре розв’язана, в той час як для відкритого середовища ще треба вдосконалити алгоритм. Коли обличчя виявлені, може бути відразу зроблена оцінка їх положення, якщо припустити, що роздільча здатність зображення є достатньо високою для локалізації компонентів обличчя; розпізнавання облич надає досить точні результати для фронтальних зображень облич без надмірних емоцій та при освітленні без сильної тіні. Розпізнавання облич у невимушеному середовищі повсякденного життя без співпраці з користувачем, наприклад розпізнавання людей у аеропорті, ще досі є складною задачею. Багато років зусиль необхідні для того, щоб надати практичні рішення цих проблем.

2 ПОРІВНЯЛЬНИЙ АНАЛІЗ 2D ТА 3D ТЕХНОЛОГІЙ

Виживання індивідууму у соціально-складному світі сильно залежить від вміння інтерпретувати візуальну інформацію про вік, расу, особистість та емоційний стан іншої людини на основі обличчя цієї людини. Не дивлячись на різноманітні несприятливі умови (змінювані вирази обличчя та пози, зміни освітлення та зовнішності), люди можуть розпізнавати обличчя з високою точністю та без свідомих затрат зусиль.

Дослідження розпізнавання облич з використанням автоматичних та напівавтоматичних технологій розпочалося у 1960 році, та отримало максимальну увагу на протязі останніх двох десятиліть. Однією з основних причин цього зростаючого інтересу стала велика кількість можливих застосувань технології, іншою причиною стала наявність доступних апаратних засобів, таких як фото- та відеоапаратура, що зробили отримання високоякісних зображень набагато розповсюдженішим. Попри зростаючий інтерес, сучасні системи розпізнавання облич працюють добре у тому випадку, коли зображення отримані під постійними та контрольованими умовами. Тож розробка систем розпізнавання облич, що працюють надійно у неконтрольованих ситуаціях, є досі відкритою темою досліджень.

Хоч існує багато інших альтернативних біометричних технологій, що на сьогоднішній день надають хороші результати (наприклад, аналіз відбитків пальців та сканування радужної оболонки ока), ці методи потребують взаємодії з об’єктом розпізнавання та слідують достатньо чіткому протоколу отримання інформації. Розпізнавання облич є набагато більш гнучким, адже взаємодія з об’єктом розпізнавання не завжди потрібна, а інколи розпізнавана людина навіть не здогадується про те, що її сканують та ідентифікують. Це робить розпізнавання облич менш надокучливим та потенційно більш ефективним. І наостанок,

публічне сприйняття обличчя як біометричної модальності є кращим у порівнянні з іншими модальностями.

Обличчя — це тривимірний об’єкт. Його зовнішність визначається на основі форми та текстури обличчя. Загалом, складнощі, які розпізнавання облич повинно подолати, — це зміни у зовнішності через зміну освітлення, зміну точки/кута зйомки, вираз обличчя, оклюзію та зміну обличчя з часом (зморшки, наявність чи відсутність волосся на обличчі).

При використанні 2D зображень для розпізнавання облич, інтенсивність та колір пікселів представляють всю інформацію, що наявна, і саме тому буль-який алгоритм повинен точно співпрацювати з варіаціями через освітлення. Людський мозок також піддається впливу освітлення при виконанні розпізнавання облич. Це видно через складність у ідентифікації знайомих облич, якщо дивитися зверху або при різних напрямках. Також було показано, що обличчя, показані на фотонегативах, мали згубний вплив на ідентифікацію знайомих облич. Подальші дослідження показали, що ефект напрямку освітлення може бути вирішальним фактором негативних фотографічних ефектів. Як результат, обличчя, що при нормальних умовах освітлюються згори, може бути складніше розпізнати у негативі, частково через супроводжуючі зміни напрямку освітлення знизу. Одним з пояснень цього є те, що різка зміна освітлення та зміни у пігментації перетинаються з процесом конструювання репрезентації облич, базованим на побудові форми з тіней. Якщо мозок реконструює 3D форму з 2D зображень, залишається питання чому розпізнавання облич людьми є до певної міри залежним від точки зйомки/споглядання.

Однією з найбільших труднощів для розпізнавання облич є факт того, що різниця між двома зображеннями одного і того самого об’єкту, сфотографованого під різними кутами, більша, ніж різниця між двома зображеннями різних об’єктів, сфотографованих під одним кутом. Було доведено, що швидкість розпізнавання

невідомих облич значно зменшується, якщо у тренувального набору зображень та тестового набору різні точки зйомки (хоч недавно були суперчки щодо того, чи розпізнавання об'єктів є залежним від точки зйомки, чи незалежним). Мозок здатний до гарного узагальнення за умови, що зміна у кутах не є різкою. Наприклад, зіставлення зображення профілю обличчя до фронтального зображення є непростим, хоча зіставлення зображення, зробленого під кутом в 45°, до фронтального зображення вже не є таким складним. Були припущення, що для того, щоб вирішити проблему змінюваних точок споглядання, мозок зберігає абстракції прототипів обличчя, специфічних до кожної точки споглядання. Моделі, базовані на інтерполяції, наприклад, підтримують ідею того, що мозок ідентифікує обличчя при різних точках споглядання, інтерполюючи до найближчого зображення, яке було вже бачене.

Ще однією ключовою проблемою для розпізнавання облич є ефект виразу обличчя. Обличчя являє собою динамічну структуру, що змінює свою форму, адже м'язи деформують м'які тканини та рухають кістки. Нейрофізіологічні дослідження припускають, що розпізнавання виразів обличчя відбувається паралельно до ідентифікації облич. Деякі дослідження у цій області показують, що просопагностичні пацієнти (просопагнозія – це порушення сприйняття облич, при якому здатність впізнавати обличчя втрачена, але при цьому здатність впізнавати предмети у цілому збережена) здатні розпізнавати вирази обличчя навіть тоді, коли розпізнати актора взагалі неможливо. Точно так само пацієнти, що страждають від органічного мозкового синдрому, майже не здатні до аналізу виразів обличчя, але зовсім не мають проблем з розпізнаванням облич. Проте зовнішність обличчя також змінюється через старіння та різні стилі життя людей. Наприклад, шкіра стає менш еластичною та більш в'ялою, лінія губ та волосся часто змінюється, колір шкіри змінюється, люди набирають чи втрачають вагу,

відрощують бороди, змінюють зачіски та таке інше. Це може призвести до різких змін у зовнішності обличчя на зображеннях.

Остання проблема розпізнавання облич пов’язана з оклюзією. Такі оклюзії можуть траплятися через цілий набір причин, наприклад, частина обличчя закрита і її не видно, коли зображення отримуються при певних кутах, або коли людина відрощує бороду, носить окуляри чи капелюх.

2.1 Переваги та недоліки 3D та 2D технологій розпізнавання облич

2D розпізнавання облич є нагато «старшою» темою досліджень, аніж 3D розпізнавання облич, і якщо узагальнити, то вона також є більш продуктивною. Однак велика кількість інформації, що доступна у інформації з 3D шаблону, означає, що техніки 3D розпізнавання у ближчому майбутньому можуть «обійти» техніки 2D розпізнавання. Розглянемо основні відмінності між 2D та 3D технологіями розпізнавання облич.

Як вже було показано, розпізнавання облич, що використовує 2D зображення, є чутливим до змін освітлення. Світло, відбите від обличчя, являє собою функцію геометрії обличчя, альбедо обличчя, властивостей джерела світла та властивостей камери [2]. Враховуючи усе це, надзвичайно важко розробити моделі, які б враховували зміни усіх цих компонентів. З невеликим успіхом проходили розпізнавання 2D зображень при різному освітленні та нормалізації освітлення. У 3D зображеннях варіації освітлення впливають лише на текстуру обличчя, але форма обличчя залишається незмінною.

Іншим відмінним фактором між 2D та 3D технологіями розпізнавання облич є ефект варіацій поз. При 2D зображеннях багато зусиль йде на трансформацію зображення у канонічну позицію. Проте це залежить від точного розміщення орієнтиру і зовсім не виключає проблему оклюзії. Більш того, у 2D зображеннях

це практично неможливо через проективну природу 2D зображень. Для рішення цієї проблеми можливо зберігати зображення обличчя, отримані з різних точок зйомки. Однак це вимагає великої кількості 2D зображень та зусиль на їх отримання. Альтернативною методикою для рішення проблеми варіацій поз у 2D зображеннях є або статистичні моделі для інтерполяції точок зйомки, або використання генеративних моделей. Використовуючи 3D зображення, інтерполяція точок зйомки може бути вирішена просто за допомогою рендерингу інформації з 3D шаблону обличчя, після чого можна отримати зображення нової пози. Це дозволяє моделям, що піддаються морфінгу, оцінювати 3D форму непобаченого обличчя з нефронтальних вхідних 2D зображень та генерувати 2D фронтальні зображення реконструюваного обличчя, використовуючи ре-рендеринг. Іншою проблемою, пов'язаною з позами, є те, що фізичні виміри обличчя на 2D зображеннях невідомі. Розмір обличчя на 2D зображеннях звичайно є функцією відстані об'єкту від сенсору. Проте на 3D зображеннях фізичні виміри обличчя відомі та по суті закодовані у інформації.

На відміну від 2D зображень, 3D зображення краще відображають геометрію поверхні обличчя. Традиційне 2D розпізнавання облич фокусується на висококонтрастних областях обличчя, таких як очі, рот, ніс та контур обличчя, адже малоконтрастні області, такі як контур підборіддя та щоки, важко отримати з яскравих зображень. 3D зображення, з іншого боку, не відрізняються у високо- та малоконтрастних областях. І все ж таки 3D розпізнавання облич теж має свої недоліки. Наприклад, освітлення може і не бути проблемою під час обробки 3D даних, але воно все ще є проблемою під час фотографування. В залежності від використовуваної сенсорної технології, частини обличчя, що виділяють підшкірний жир, мають високий коефіцієнт відбиття і можуть створювати артефакти при певному освітленні поверхні. У цілому якість даних з 3D зображень, отриманих з ряду камер, мабуть не така висока, як дані з 2D

зображень, адже технології 3D-сенсорів ще не настільки розвинуті як технології 2D-сенсорів. Іншим недоліком технік 3D розпізнавання облич є вартість апаратного забезпечення. 3D-сенсори стають дешевшими та більш широко розповсюдженими, але їх вартість значно вища у порівнянні з високо-роздільчою цифровою камерою. Більш того, поточна обчислювальна вартість обробки 3D даних більша, ніж для 2D даних.

І наостанок, одним з найбільших недоліків 3D розпізнавання облич є факт того, що технологія 3D фотографування потребує взаємодії з об'єктом. Як згадувалось вище, лінзи чи лазерні сканери потребують, щоб об'єкт був на певній відстані від сенсору. Крім того, лазерні сканери потребують декілька секунд повної нерухомості, тоді як традиційні камери можуть знімати зображення з великої відстані не потребуючи взаємодії з об'єктом. На додачу, на даний момент є дуже небагато баз даних високоякісних 3D зображень облич, що доступні для тестувальних та оціночних цілей. Ці доступні бази даних невеликі за розміром у порівнянні до 2D баз даних.

3 АНАЛІЗ НАДІЙНОСТІ 2D ТА 3D ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧ

3.1 Вступ

Біометричні системи знаходять широке використання в системах інформаційної безпеки, електронної комерції, при розкритті та запобіганні злочинів, судовій експертизі, митному контролі та т. і. Але вони вразливі до атак на різних стадіях обробки інформації. Ці атаки можливі на рівні сенсора, де сприймається зображення чи сигнал від індивідуума, атаки повтору (replay) на лініях комунікацій, атаки на базу даних, де зберігаються біометричні шаблони, атаки на модулі порівняння та прийняття рішень. Основну потенційну загрозу на рівні сенсора представляють атаки спуфінгу (spoofing). Спуфінг — це обман біометричних систем шляхом представлення біометричному сенсору копій, муляжів, фотографій, муляжів відбитків пальців, заздалегідь записаних звуків і таке інше [3]. Ціль атаки спуфінгу при верифікації — представлення незаконного користувача у системі як законного, а при ідентифікації — добитися невиявлення індивідуума, що знаходиться у базі даних. Протидії атакам спуфінгу більш важкі, так як зловмисник безпосередньо має контакт з сенсором і неможливо використати криптографічні чи інші методи захисту.

В системах розпізнавання облич для спуфінг-атаки можна застосовувати фотографію обличчя, записане відео, 3D моделі обличчя з рухом губ, 3D моделі з різноманітними виразами обличчя і т. д. Значно більш стійкою до спуфінгу являється нова 3D-технологія 3D Hybrid Face Recognition, що враховує не тільки структуру людського обличчя, а і його форму.

Отже, враховуючи аналіз роботи технології, можна зробити висновок, що є сильна залежність надійності систем розпізнавання облич від наступних факторів:

- Актуальності фотографії, занесеної в базу даних: це стосується зміни зовнішності — зміни кольору шкіри, наявності чи відсутності бороди та вусів, зміни поверхності шкіри після чи під час хвороби, зміни міміки.
- Величини бази даних: для підвищення ефективності розпізнавання доцільно використовувати багато зображень однієї людини (наприклад, 10).
- Якості зображення: примітно знижується вірогідність безпомилкової роботи системи, якщо людина, яку ми намагаємося розпізнати, дивиться не прямо в камеру або сфотографована при поганому освітленні. На практиці при використанні систем розпізнавання облич у складі стандартних електронних охоронних систем передбачається, що людина, яку необхідно розпізнати, дивиться прямо в камеру. Таким чином, система працює з відносно простим двомірним зображенням, що значно спрощує алгоритми і знижує інтенсивність обчислень. Але навіть в цьому випадку задача розпізнавання все ж таки не є тривіальною, оскільки алгоритми повинні приймати до уваги можливість зміни рівня освітлення, зміну виразу обличчя, наявність чи відстутність макіяжу та окулярів.
- Апаратури, що використовується (камера): технології розпізнавання облич добре працюють із стандартними відеокамерами, що передають дані та керуються персональним

  комп’ютером, і потребують роздільчої здатності 320 х 240 пікселів на дюйм при швидкості відеопотоку, принаймні, 3 – 5 кадрів за секунду. Для порівняння – прийнятна якість для відеоконференції потребує швидкості відеопотоку вже 15 кадрів за секунду. Більш висока швидкість відеопотоку при більш високій роздільчій здатності веде до

покращення якості ідентифікації. При розпізнаванні облич з большої відстані існує сильна залежність між якістю відеокамери та результатом ідентифікації.

Основна проблема всіх технологій біометричної ідентифікації полягає в тому, що результати ідентифікації людини носять ймовірнісний характер і залежать від багатьох чинників, тому інколи можна сприйняти дії зловмисника за помилку алгоритму.

У біометрії параметри надійності алгоритмів (тобто саме помилок алгоритму) задаються помилкою FRR (False Reject Rate), коли система не впізнала «свою» людину, і помилкою FAR (False Accept Rate), коли система пропустила «чужу» людину [5].

Повні дані про FRR і FAR для 3D технологій розпізнавання облич на сайтах виробників зазвичай не наводяться. За даними, наведеними в [4], для кращих моделей фірми Bioscript (3D EnrolCam, 3D FastPass) при FAR = 0.0047% FRR складає 0.103%. Представляє особливий інтерес японська міні-система розпізнавання осіб, яка легко вмонтовується в зручному для користувача місці, підключається через USB порт або Ethernet вхід до будь-якого персонального комп'ютеру. Вірогідність помилки складає 0.00001%, а вартість — $1550 (станом на лютий 2010 року). Вважається, що статистична надійність 3D технологій розпізнавання облич дорівнює надійності методу ідентифікації по відбитках пальців.

Слід відмітити розробки компанії Identix, яка при реалізації 3D технології розпізнавання облич використовує не тільки геометричну 3D-модель, а також доповює її описом поверхні шкіри (текстури обличчя). При цьому фотографується ділянка шкіри обличчя, розбивається на декілька дрібніших блоків, де система виявляє особливі лінії, пори і інші текстурні елементи. За повідомленнями компанії Identix це дозволяє підвищити ефективність ідентифікації на 20-25%.

3.2 Надійність 2D технології розпізнавання

Технології 2D розпізнавання облич — одні з самих статистично неефективних методів біометрії. З'явилися ці методи досить давно, і в основному завдяки криміналістиці. У подальшому з'явились комп'ютерні інтерпретації цього напрямку, внаслідок чого він став більш надійним, але все ж таки програвав, і досі програє, іншим методам біометричної ідентифікації.

На теперішній момент цей напрямок є широко використовуваним, але у поєднанні з іншими методами ідентифікації, створюючи цим самим перехресну біометрію, або іншими словами, мультимодальні системи.

Щоб оцінити ймовірності FAR та FRR, можна оцінити, як часто будуть з'являтися помилкові ситуації, якщо встановити систему ідентифікації на вході організації з чисельністю персоналу N людей. Ймовірність помилкового співпадання отриманого сканером (фотоапаратом) зображення обличчя людини та зображення з бази даних, що містить N зображень, дорівнює FAR * N. І кожного дня через пункт контроля доступу проходить теж N людей. Отже, ймовірність помилки за час робочого дня дорівнює FAR * N * N. Звісно, в залежності від цілей системи ідентифікації ймовірність помилки за одиницю часу може сильно змінюватись, але якщо допустити, що одна помилка на день є прийнятною, то:

$$FAR * N^2 \approx 1 ==> N \approx \sqrt{\frac{1}{FAR}} \quad (1)$$

Тоді отримаємо, що стабільна робота системи ідентифікації при FAR = 0.1% = 0.001 можлива при чисельності персоналу N ≈ 30.

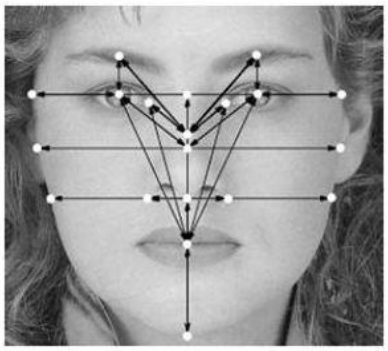


Рисунок 3.1 – 2D зображення обличчя та визначення важливих точок та відстаней на ньому

Отже, статистичні характеристики методу:

для FAR та FRR використовувались дані для алгоритмів VeriLook. Знову ж таки, як для сучасних алгоритмів вони мають досить звичайні характеристики. Інколи зустрічаються алгоритми з FRR = 0.1% при аналогічному значенні FAR, але бази даних, з яких ці дані були отримані, є досить сумнівними, тобто на зображеннях вирізано фон, один вираз обличчя, однакові зачіска, освітлення та таке інше — ці зображення є далекими від ситуацій реального життя.

Таблиця 3.1 – Статистичні дані технологій 2D розпізнавання облич

FAR	**FRR**
0.10%	2.50%
0.01%	5%
0.00%	6%
0.00%	9%

Характерне значення FAR – 0.1%.

З формули (1) отримуємо $N \approx 30$ — чисельність персоналу організації, при якій ідентифікація співробітників проходить досить стабільно.

Як видно, статистичні показники методу доволі скромні: це практично зводить нанівець той факт, що можна проводити приховану зйомку у людних місцях. За останній десяток років статистичні характеристики методу не покращились, а кількість проектів все ж таки виросла. Проте слід відмітити, що для стеження за людиною за допомогою великою кількості камер у натовпі цей метод є досить корисним та його можливостей вистачає.

Отже, переваги та недоліки методу.

Перевагою є те, що при 2D розпізнаванні не потрібна дорога апаратура. При наявній апаратурі є можливість розпізнавання на великій відстані від камери.

Недоліками методу є низька статистична достовірність. Також є вимоги щодо освітлення (наприклад, неможливо реєструвати обличчя людей, що заходять ззовні в сонячний день). Для більшості алгоритмів також є неприйнятність яких-небудь зовнішніх перешкод, як наприклад окуляри, борода, деякі елементи зачіски. Обов’язковим є фронтальне зображення обличчя, з дуже невеликими відхиленнями. Багато алгоритмів не беруть до уваги можливі зміни міміки обличчя, тобто вираз обличчя повинен бути нейтральним.

3.3 Надійність 3D технології розпізнавання

Реалізація даного методу являє собою досить складну задачу. Незважаючи на це в даний час існує безліч методів по 3D розпізнаванню облич. Методи неможливо порівняти один з одним, так як вони використовують різні сканери і бази даних. Далеко не всі з них видають нормальні значення FAR і FRR, адже використовуються абсолютно різні підходи.

Перехідним від 2D до 3D методом є метод, який реалізує накопичення інформації про особу. Цей метод має кращі характеристики, ніж 2D метод, але так само як і він використовує всього одну камеру. При занесенні суб'єкта в базу даних суб'єкт повертає голову і алгоритм з'єднує декілька зображень в одне ціле, створюючи 3D шаблон. При розпізнаванні використовується кілька кадрів відеопотоку. Цей метод більше відноситься до експериментальних методів, аніж часто використовуваних на практиці.

Найбільш класичним методом є метод проектування шаблону. Він полягає в тому, що на об'єкт (особу) проектується сітка. Далі камера робить знімки зі швидкістю десятків кадрів в секунду і отримані зображення обробляються спеціальною програмою. Промінь, падаючий на викривлену поверхню, згинається (чим більше кривизна поверхні, тим сильніше вигин променя). Спочатку при цьому застосовувалось джерело видимого світла, що подається через «жалюзі». Потім видиме світло було замінене на інфрачервоне світло, який має низку переваг. Зазвичай на першому етапі обробки відкидаються зображення, на якому обличчя не видно взагалі або присутні сторонні предмети, що заважають ідентифікації. За отриманими знімками відновлюється 3D модель особи, на якій виділяються і видаляються непотрібні перешкоди (зачіска, борода, вуса та окуляри). Потім проводиться аналіз моделі — виділяються антропометричні особливості, які в результаті і записуються в унікальний код, який заноситься в базу даних.

Так само набирає популярність метод 3D розпізнавання по зображенню, одержаному з декількох камер. Прикладом цього може бути фірма Vocord зі своїм 3D сканером. Цей метод дає точність позиціонування кращу за метод проектування шаблону.

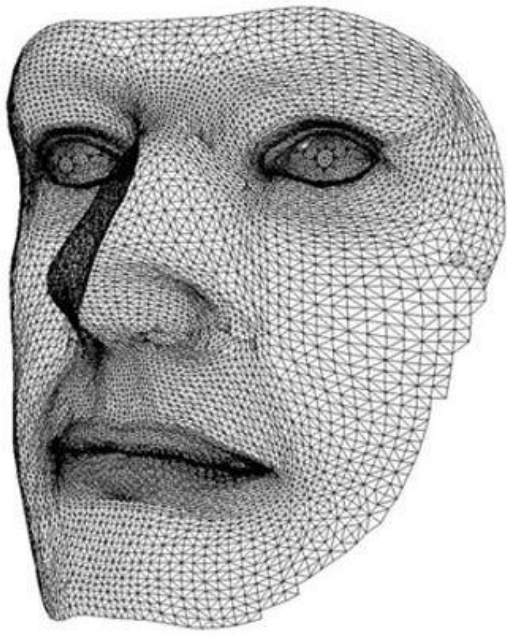


Рисунок 3.2 – 3D зображення обличчя

Отже, статистичні характеристики методу:

повні дані про FRR і FAR для алгоритмів цього класу на сайтах виробників відкрито не наведено. Але для кращих моделей фірми Bioscript (3D EnrolCam, 3D FastPass), що працюють за методом проектування шаблону при FAR = 0.0047% FRR становить 0.103%.

Вважається, що статистична надійність методу майже така ж, як надійність методу ідентифікації за відбитками пальців.

Переваги та недоліки методу.

Перевагою є те, що не потрібно контактувати зі скануючим пристроєм. Також низька чутливість до зовнішніх чинників, як на самій людині (поява окулярів, бороди, зміни зачіски), так і в його оточенні (освітленість, поворот голови). Високий рівень надійності.

Недоліками методу є дорожнеча обладнання. Наявні в продажі комплекси перевершували за ціною навіть сканери райдужної оболонки. Зміни міміки

обличчя і перешкоди на обличчі погіршують статистичну надійність методу. Метод ще недостатньо добре розроблений, особливо у порівнянні з давно застосовуваною дактилоскопією, що ускладнює його широке застосування.

3.4 Розпізнавання живучості

Мета виявлення живучості в біометричних системах полягає в тому, щоб переконатися, що для реєстрації, верифікації та ідентифікації використовуються тільки «справжні» біометричні характеристики. В принципі виявлення живучості ґрунтується на збігу одного або декількох ознак біометричного зразка з ознаками, пов’язаними з живим біометричним зразком [1].

Підходи по виявленню живучості можна розділити на виявлення живучості та виявлення неживучості. На практиці біометричні системи частіше розробляються на виявлення живучості, ніж неживучості.

У методах виявлення живучості в якості ознак життя використовується фізіологічна або поведінкова інформація або інформація, що міститься в біометричному зразку. В системах розпізнавання відбитків пальців для виявлення живучості використовуються вимір температури, пульсу, діелектричного опору, виявлення підшкірних ознак, порівняння послідовно прийнятих біометричних зразків і т. д.

Для інших біометричних характеристик методи виявлення живучості, як правило, основані на аналізі довільної і мимовільної поведінки. Системи розпізнавання обличчя можуть вимагати від користувача рухи голови, губ, очей або зміни виразу обличчя. Системи розпізнавання голосу можуть запитувати користувача вимовити випадково згенеровану фразу або буквенно-цифрову послідовність, щоб запобігти відтворення записаних звуків.

3.4.1 Методи виявлення живучості обличчя

У системах розпізнавання облич для спуфінг-атаки можна застосовувати фотографію особи, записане відео, 3D моделі особи з рухом губ, 3D моделі з різними виразами обличчя і т. д.

А. Джейн та ін. [6] використовують аналіз спектра частот одного зображення особи або послідовності зображень облич, визначають два дескриптори для вимірювання співвідношення високих частот і тимчасову дисперсію всіх частот. Їх метод заснований на поганій якості фотографії або зміні розташування живих осіб.

Деякі методи виявлення живучості обличчя засновані на вимірі інформації про 3D глибину. В роботі [7] будується карта глибин з відновленням 3D структури. Карту глибин можна використовувати для визначення вхідного зображення, отриманого від живої людини або фотографії. При русі фотографії сама карта глибин залишається незмінною, а живе обличчя дає змінні значення глибини.

В роботі [8] застосовується метод оптичного потоку для оцінки структури послідовності зображень. У методі оптичного потоку сегментується карта оптичного потоку і групуються пікселі, що належать окремим об’єктам. Після обчислення потоку кожного пікселя можна оцінити 3D координати точок поверхні.

Алгоритм, запропонований в роботі [9], оснований на аналізі руху очей в послідовності зображень. Загалом варіації у формі компонентів осіб у послідовності зображень дуже незначні, але варіації у формі ока можуть бути великими, адже наше миготіння і рух зіниці ока завжди є мимовільними.

В роботі [10] для виявлення живучості розроблений метод стеження за особами в реальному часі. Ознаки особи витягуються за допомогою фільтрів Габора та класифікуються SVM-експертами. Для продуктивності в реальному часі обрані точки були використані для формування регіональних моделей особи.

Д. Денг та ін. повідомляють про розробку методу виявлення живучості особи на основі SVM (Support Vector Machine) з використанням моделі руху очей. Модель руху очей навчається з використанням численних зразків позиції очей. У цьому методі для виявлення живучості користувач повинен кліпати очима, щоб пройти тест. Фальшиві зображення особи, які не вміють блимати, не надходять у стадію розпізнавання та зупиняються.

Фірма Identix для виявлення живучості пропонує систему запит-відповідь, так зване множинне фрейм/відео-тестування [11]. Система дає вказівку користувачеві посміхнутися або моргнути, щоб переконатися за короткий період часу, що зображення обличчя належить даній людині, обидва рухи не можна здійснити одночасно. Ця технологія виявлення живучості потребує зазвичай 2 - 3 с і не вимагає спеціального обладнання.

В роботі [12] пропонується метод виявлення живучості для системи аутентифікації «Особа-голос» на основі двох ознак. Ці ознаки засновані на латентному семантичному аналізі (ЛСА) і канонічному кореляційному аналізі (ККА). Метод збільшує стійкість систем аутентифікації до атак відтворення відео. Експерименти з базами даних «мова – особа» при злитті векторів ознак «особа – голос» дали на 42% менше помилок з ЛСА-ознаками і на 61% менше помилок з ознаками ККА.

3.5 Алгоритм розпізнавання живучості для захисту від спуфінгу

Як було сказано вище, основну потенційну загрозу на рівні сенсору представляють атаки спуфінгу. Протидії атакам спуфінгу є більш складними, адже зловмисник безпосередньо має контакт з сенсором, таким чином неможливо використати криптографічні чи інші методи захисту.

Наприклад, зловмисник може представити фотографію іншої людини для системи розпізнавання облич, і система «не зрозуміє», що насправді їй представили фото, тобто що перед сканером (камерою) системи не жива людина, а всього навсього зображення.

У зв’язку з вразливістю систем розпізнавання облич великою є актуальність завдання по протидії зловмисникам. Одним із способів вирішення цього завдання є додатковий аналіз ознак живучості сканованих об’єктів. Живучість — життєва сила, якщо говорити відносно біометричних систем, то це означає навність життєвих ознак об’єкта перед сканером (камерою). Аналіз живучості дозволяє подолати частину атак спуфінгу на біометричні системи розпізнавання, в яких пред’являються підроблені зразки, що не володіють властивостями, характерними для живих об’єктів.

Задача виявлення живучості розглядалася як додаток до задачі розпізнавання. При такому підході в першу чергу необхідно визначити місце модуля аналізу живучості в структурі системи розпізнавання.

У алгоритмічну частину будь-якої системи розпізнавання облич входять три модулі: обчислення, аналіз інформативних ознак і прийняття рішень про результати розпізнавання. Для захисту від атак спуфінгу крім алгоритмічних модулів в систему розпізнавання можуть входити й інші модулі, наприклад алгоритм виявлення атак на біометричну систему (зокрема, алгоритм аналізу ознак живучості).

У апаратну частину системи розпізнавання, як правило, входять наступні функціональні блоки: біометричний сканер, база даних і ЕОМ.

Розглянемо основні етапи роботи алгоритму виявлення живучості. На першому етапі відбувається обробка даних, отриманих з біометричного сканеру. Апріорне поняття живого об’єкта включає в себе безліч різних характеристик, що

відрізняють його від штучно сформованого. Тому в процесі обробки даних обчислюється кілька незалежних кількісних оцінок ознак живучості.

На другому етапі виконується порівняння розрахованих значень з еталонними значеннями відповідних ознак живого і штучного об’єктів. База таких еталонних значень векторів ознак є аналогом бази даних системи розпізнавання. У результаті формується вектор, кожен елемент якого характеризує вірогідність того, що спостережуваний об’єкт є справжнім біологічним об’єктом з точки зору тієї чи іншої характеристики.

З точки зору вбудовування алгоритму виявлення живучості в алгоритмічну частину системи розпізнавання облич важливим є питання про взаємозв’язок інформативних ознак розпізнавання і ознак живучості. Для типової системи розпізнавання багато біометричних особливостей людини є перешкодою, що заважає коректному розпізнаванню. До таких особливостей можна віднести залежність параметрів відбитого сигналу від спектру падаючого випромінювання, вплив ракурсу реєстрації на результат розпізнавання у зв’язку з наявністю тривимірного рельєфу, мінливість цього рельєфу, обумовлена мімікою, мовою, морганням, емоціями та ін.

Для вирішення задачі виявлення живучості ці фактори являються не перешкодами, а навпаки ознаками, що дозволяють відрізнити справжні біометричні об’єкти від підробки. Крім перерахованих вище особливостей людини, ознаками живучості можуть бути специфічні властивості шкіри або тканин ока, наявність пульсацій в судинах і капілярах, мимовільний рух очей, аккомодація, наявність природної реакції на певний вплив.

Таким чином, набір ознак живучості принципово відрізняється від словника ознак розпізнавання. В цілому алгоритм виявлення живучості не залежить від бази даних розшуку, від обраних структури біометричного шаблону і методів порівняння отриманих образів з образами з бази даних. Тому можна ставити

задачу розробки таких алгоритмів як задачу розробки незалежних модулів, які можуть функціонувати разом з будь-якою системою розпізнавання.

Існують обмеження на використання різних алгоритмів виявлення живучості в системах розпізнавання. Одним з таких обмежень є належність ознак розпізнавання і ознак живучості до одного біометричного об’єкту. Наприклад, у системі розпізнавання людини по райдужній оболонці ока доцільно використовувати ознаки живучості в області ока, а в системі розпізнавання за відбитками пальців — ознаки живучості пальців людини. Тому найбільш економічним варіантом є використання в системі виявлення живучості біометричного сканера системи розпізнавання. В цьому випадку додаткові кошти на апаратуру реєстрації не потрібні. З точки зору економічності для розрахунків доцільно використовувати обчислювальні засоби системи розпізнавання. Дана вимога накладає певні обмеження на обчислювальнускладність алгоритму виявлення живучості.

Залежно від способу взаємодії з реєстрованою людиною системи розпізнавання підрозділяють на:

• кооперативні — людина, що бажає пройти процедуру розпізнавання, вживає для цього спеціальні дії, наприклад повертає обличчя до камери, наближається оком до окуляра або проводить пальцем по сканеру;

• некооперативні — розпізнавання відбувається без спеціальної участі людини.

В модулі аналізу живучості доцільно застосовувати відповідний спосіб взаємодії з реєстрованою людиною. При найбільш економічному виконанні система виявлення живучості включатиме в себе тільки програмні модулі. Однак для забезпечення досить високої надійності виявлення підробки можливостей звичайного біометричного сканера може бути недостатньо. При розробці

біометричного сканера з функцією виявлення живучості необхідно знайти компроміс між надійністю і економічністю.

Загальний алгоритм роботи системи розпізнавання з функцією виявлення живучості можна представити у вигляді певної послідовності процедур.

1. Отримання інформації, що реєструється біометричним сканером.

2. Виділення з отриманої інформації ознак розпізнавання і ознак живучості.

3. Порівняння отриманих ознак живучості з еталонними.

4. Прийняття рішення про приналежність біометричних характеристик штучному об’єкту чи живій людині.

5. Порівняння отриманих інформативних ознак об’єкта з ознаками, що містяться в базі даних системи розпізнавання.

6. Прийняття рішення про те, чи відноситься розпізнаваний об’єкт до одного з класів бази даних.

В даний час в біометрії переважають три технології ідентифікації особи: розпізнавання по зображенню особи, по відбитках пальців і по райдужній оболонці очей. Питома вага трьох зазначених технологій становить за різними підрахунками від 85 до 95%. Особливий інтерес представляють біометричні системи, що базуються на розпізнаванні особи, так як на відміну від інших вони можуть працювати у некооперативному режимі. З одного боку, це є перевагою таких систем, оскільки значно збільшує пропускну спроможність постів контролю, але, з іншого боку, досить легко організувати атаку спуфінгу на систему.

Проведений аналіз методів виявлення живучості особи показав, що одним із підходів, що забезпечують стійкість системи розпізнавання до атак спуфінгу з використанням більшості існуючих підробок, є аналіз спектральних характеристик відображення шкіри людини. Даний підхід був взятий за основу при реалізації алгоритму виявлення живучості [18].

Відомо, що залежність спектрального коефіцієнта відбиття шкіри людини від довжини хвилі падаючого випромінювання має досить складний вид. Графіки спектральних коефіцієнтів відбиття шкіри людей різних етнічних груп наведені на рис. 3.3. Присутні локальні мінімуми і максимуми обумовлені наявністю гемоглобіну у внутрішньому шарі шкіри. Спектральні характеристики відображення більшості штучних матеріалів, використовуваних для виготовлення підробок, не мають локальних мінімумів або максимумів. Для виготовлення муляжів пальців або масок обличчя особи зазвичай застосовується силікон. Також для маскування особи може використовуватися грим.

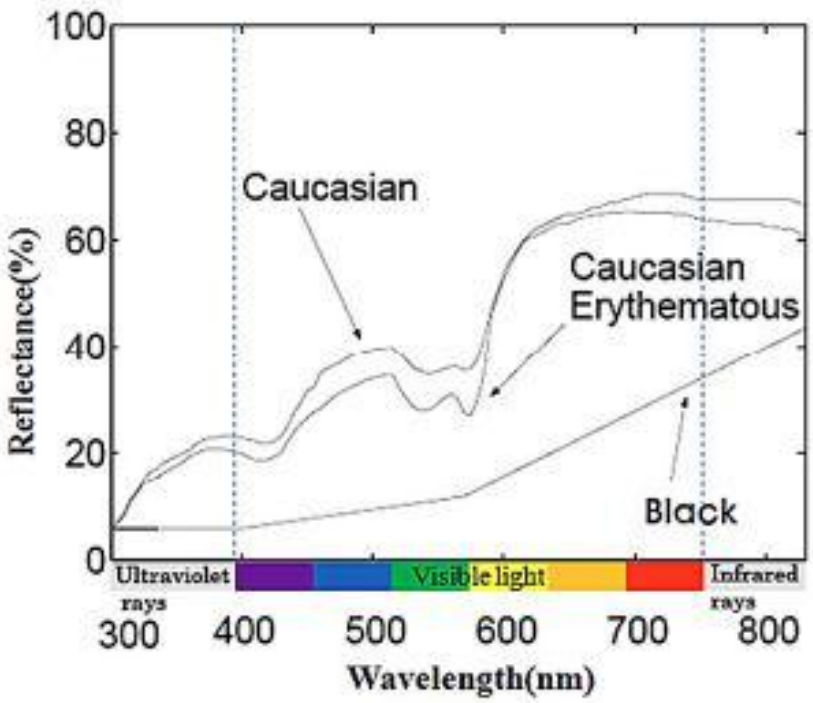


Рисунок 3.3 – Графіки спектральних коефіцієнтів відбиття шкіри людей різноманітних етнічних груп

В алгоритмі визначення ознак живучості, вимірювання коефіцієнта відбиття шкіри проводиться тільки в двох точках. Таким чином, при виготовленні підробки може бути підібрана така фарба, графік спектрального коефіцієнту відображення якої є монотонним і проходить через дві зазначені точки. Для обману такої

системи виявлення живучості достатньо при виготовленні маски витримати визначене співвідношення червоної і зеленої складових фарби.

Пропонується для виявлення характерних локальних мінімумів проводити вимірювання коефіцієнта відбиття не менш ніж на трьох довжинах хвиль. Відповідно до екстремумів спектрального коефіцієнту відбиття шкіри рекомендується використовувати наступні довжини хвиль: 500, 549 і 633 нм. При цьому кольорові телевізійні камери в системах розпізнавання також мають три спектральних канала, однак ширина смуги пропускання кожного каналу занадто велика для проведення точної спектральної селекції. Отже, необхідне додаткове обладнання, що дозволить більш точно вимірювати коефіцієнти відображення на запропонованих довжинах хвиль.

Для проведення експериментальних досліджень було розроблено макетний зразок експериментальної установки, до складу якої входять система реєстрації, система освітлення та обчислювальна техніка для обробки зареєстрованих зображень. Система освітлення містить спеціально підібрані компактні люмінісцентні лампи, смуги випромінювання яких збігаються з вікнами пропускання фільтрів. До складу системи реєстрації (рис. 3.4) окрім основної кольорової камери системи розпізнавання входять три додаткові камери, оснащені інтерференційними фільтрами з максимальним пропусканням на зазначених довжинах хвиль (500, 549 і 633 нм). Ширина смуги пропускання кожного фільтра 15 нм.

Рисунок 3.4 – Система реєстрації

Для аналізу ознак живучості по чотирьох зареєстрованих зображеннях розроблений наступний алгоритм. На кольоровому зображенні за допомогою алгоритму виявлення (детекції) обирається область обличчя — так звана область інтересу. На інших трьох зображеннях область інтересу визначається з використанням відомого перетворення між камерами: вважається, що всі зображення отримані практично одночасно. Параметри такого перетворення визначаються в результаті геометричного калібрування системи реєстрації з використанням алгоритму «Огляд методів виявлення кольору шкіри на основі пікселів» (Survey on Pixel-Based Skin Color Detection Techniques) при застосуванні калібрацйних інструментів пакету Matlab (Camera Calibration Toolbox for Matlab). Результат виконання процедури виділення області інтересу представлений на рис. 3.5.

Рисунок 3.5 – Виділення області інтересу на зображеннях, отриманих з різних каналів

На наступному кроці в межах області інтересу виконується процедура селекції пікселів, що представляють основний колір обличчя. Метою даної процедури є виділення областей, що представляють відкриті ділянки людської шкіри, придатні для вимірювання спектральних характеристик відбиття. Така селекція проводиться з використанням кольорового зображення; маска переноситься на зображення, отримані в інших спектральних каналах. Основою алгоритму селекції цих відкритих підходящих ділянок є аналіз колірних характеристик зображення в просторі HSV з використанням критеріїв, схожих з описаними в роботі «Принциповий Аналіз Компонент» (Principal Component Analysis), а також аналіз градієнта зображення з метою вибору найбільш рівномірних ділянок. Визначення характеристик відбиття шкіри по таких ділянках, а також усереднення по площі роблять визначення характеристик відбиття шкіри стійким до погрішностей поєднання зображень в окремих каналах.

На рис. 3.6 наведено результат селекції. Для компактності представлення зображення у відтінках сірого кольору для трьох спектральних каналів накладені один на одного (а) аналогічно тому, як це зроблено для зображення, отриманого з кольорової камери (б).

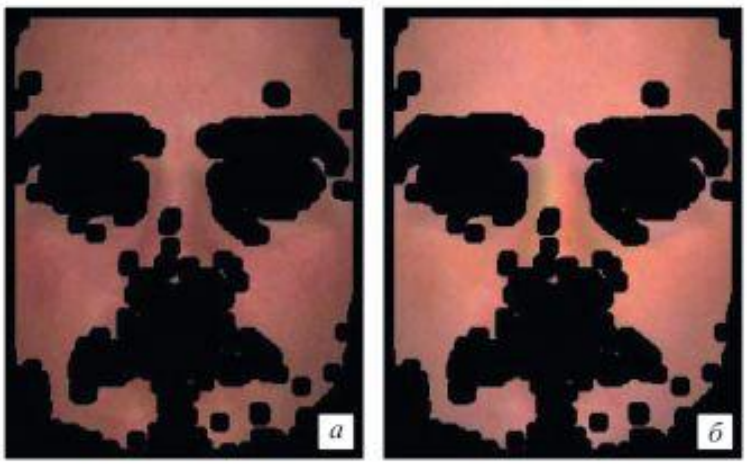


Рисунок 3.6 – Результат селекції областей, що використовуються для аналізу спектральних характеристик шкіри

Після остаточного виділення аналізованих ділянок кожен піксель представляється вектором $v = (r, g, b, x, y, z)^T$, координатами якого є значення даного пікселя на кольоровому зображенні (r, g, b) і його значення, отримані з кожного з трьох спектральних каналів, (x, y, z). Для того щоб результат аналізу залежав тільки від колірних характеристик і не залежав від загальної освітленості, використовуються нормовані координати:

$$r_n = \frac{r}{r+g+b} \qquad g_n = \frac{g}{r+g+b} \qquad b_n = \frac{b}{r+g+b} \tag{2}$$

$$x_n = \frac{x}{x+y+z} \qquad y_n = \frac{y}{x+y+z} \qquad z_n = \frac{z}{x+y+z} \tag{3}$$

Для аналізу спектральних характеристик відбиття відбираються по дві будь-які кольорові координати з кожної трійки, а отриманий вектор ознак $v_n = (r_n, g_n, x_n, y_n)^T$ усереднюється по виділеній області аналізу. Внаслідок лінійного спектру джерела випромінювання, що використовувся для підсвічування, елементи такого вектора сильно корельовані, тому для виділення незалежних ознак використовується метод головних компонент. За результатами досліджень навчальної вибірки (рис. 3.7), в якій представлені зображення восьми осіб, двох масок (mask1, mask2) і однієї роздрукованої на кольоровому принтері фотографії (photo), було виявлено, що для надійного виділення справжніх осіб достатньо використовувати дві головні компоненти простору векторів v_n.

На рис. 3.7 (а) наведено розподіл значень вектора ознак $v_c = (c_1, c_2)^T$ для об’єктів навчальної вибірки в просторі двох виділених головних компонент для різних об’єктів (осіб, масок і фотографії), хрестиками відзначені результати окремих вимірювань, колечками — середній результат для кожного об’єкта по серії зображень, отриманих під різними ракурсами. В якості критерію близькості об’єкта по спектральних характеристиках можна використовувати апостеріорний розподіл ймовірності відповідності об’єкта живій людині, розрахований за тестовою вибіркою

$$P(v_c|v_c^0, \sum c) = \frac{1}{2\pi\sqrt{|\sum c|}} \exp\left(-\frac{1}{2}(v_c - v_c^0)^T \sum_c^{-1} (v_c - v_c^0)\right), \quad (4)$$

де v_c^0 — середнє значення вектору ознак для групи людей; $\sum c$ — матриця коваріації.

Значенню виразу (4), помноженому на деяку константу, відповідають лінії рівного рівня на рис. 3.7 (а). З аналізу даних випливає, що шкіра людей утворює досить компактний кластер, маски (крайній праворуч і крайній ліворуч об’єкти) та фотографію (крайній зверху об’єкт) вдається надійно виділити за допомогою пропонованого двовимірного критерію. Використання аналогічного одновимірного критерію — з аналізом тільки однієї головної компоненти (результат роботи такого критерію на тій же самій тестовій вибірці наведено на рис. 3.7 (б)) або тільки трьох спектральних каналів без урахування зображення, отриманого з кольорової камери (результат роботи двовимірного критерію без урахування кольорового зображення приведено на рис. 3.7 (в)), дозволяє практично з тією ж надійністю виділяти маски, але не фотографії.

Слід зазначити, що виділений вектор ознак залежить не тільки від коефіцієнта відбиття об’єкта, але також від числа, розміщення і спектральних характеристик джерел випромінювання, характеристик чутливості і параметрів конфігурації використовуваних камер та інших факторів.

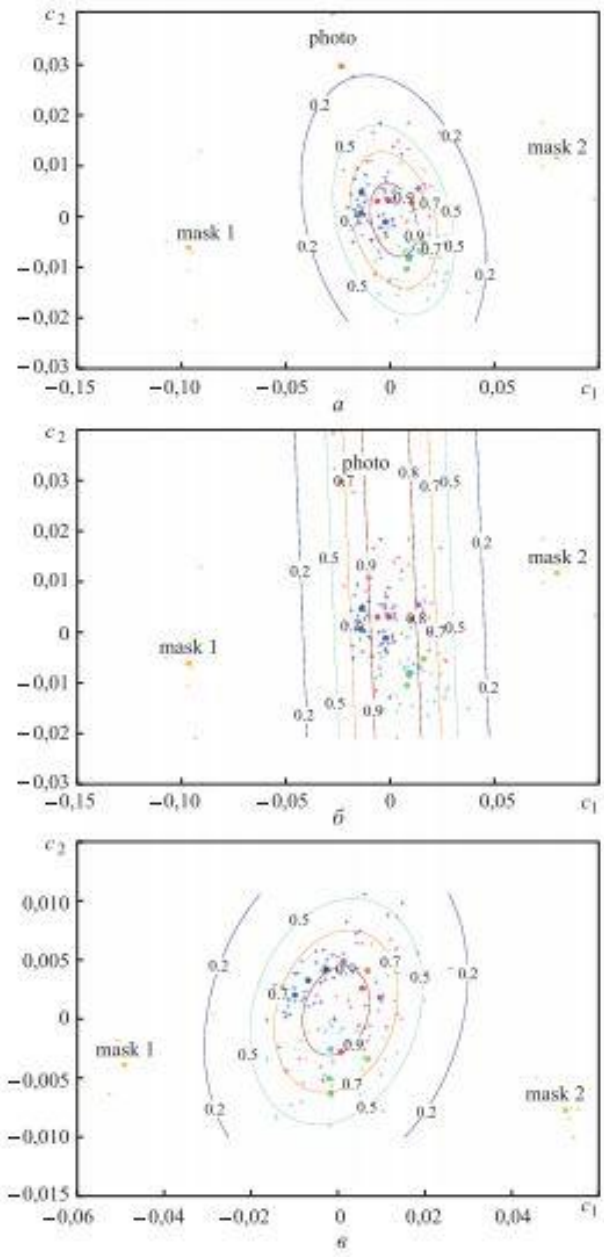


Рисунок 3.7 – Розподіл значень тестової вибірки в двовимірному просторі ознак: а – лінії рівня показані для двовимірного розподілу ймовірності; б – для одновимірного розподілу ймовірності; в – з використанням даних тільки трьох спектральних каналів

Для забезпечення стійкості виділених ознак до змін зовнішнього середовища і параметрів пристроїв реєстрування необхідно проводити калібрування системи

по об’єкту з відомою спектральною характеристикою коефіцієнта відбиття. В якості такого об’єкта можна обрати білий аркуш паперу, який пред’являється системі перед початком роботи. Оскільки коефіцієнти відображення калібровочного об’єкту на різних довжинах хвиль відомі, можна визначити нормувальні коефіцієнти для кожного з каналів і використовувати їх при обробці зображень на стадії обчислення v_n.

За результатами дослідження наявної навчальної вибірки вибрано значення критерію FAR = FRR = 0. Це значення відповідає лінії рівня 0.2 на рис. 3.5.5 (а). В результаті випробувань на тестовій вибірці, що включає двадцять чоловік, три маски і три фотографії особи, при обраному значенні критерію отримані наступні значення ймовірностей: FAR = 0.05, FRR = 0.09.

Таким чином, отримані результати підтверджують високу ступінь ефективності модуля аналізу живучості для захисту системи розпізнавання людини по зображенню особи від атак спуфінгу.

3.6 Інші методи захисту від спуфінгу

Біометрична громадськість відповіла атакам спуфінгу введенням низки механізмів протидії. Заходи антиспуфінгу в біометричних системах включають такі методи:

• Рандомізація даних верифікації.

Система може рандомізувати відбитки пальців або вирази облич, запитуваних для верифікації. Це зменшує ймовірність представлення фальшивих біометричних зразків для верифікації.

• Використання декількох біометричних зразків.

У процесі реєстрації в системі на кожного користувача реєструється, наприклад, кілька відбитків пальців (в ідеалі всі 10). Після цього в процесі аутентифікації у користувача запитуються для перевірки кілька пальців в

довільній послідовності, що значно ускладнює вхід в систему по фальшивих пальцях.

• Мультимодальна аутентифікація.

Для виявлення живучості можна використовувати кілька біометричних характеристик одночасно, наприклад, відбиток пальця і зображення обличчя особи або райдужну оболонку ока і т. д. Це створює для зловмисника труднощі, адже треба сфальсифікувати кілька біометричних характеристик одночасно.

• Мультифакторна аутентифікація.

Мультифакторна аутентифікація використовує поряд з біометрією смарт-карти, токени або паролі, і таким чином може зменшити ймовірність обману біометричних систем. У цьому випадку для обману системи зловмисникові разом з фальшивими біометричними даними потрібні додаткові ідентифікатори. Але мультифакторна аутентифікація також цим самим зменшує основну перевагу біометричних систем — зручність використання.

• Контроль над процесом верифікації (ідентифікації).

Контроль над операціями біометричних систем може підвищити рівень безпеки системи. Очевидно, що зробити атаку спуфінгу проти контрольованої біометричної системи в цьому випадку важче. Супервізор допоможе користувачам правильно представити свої біометричні характеристики і мінімізувати помилки.

• Запит-відповідь.

У методі запит-відповідь користувача просять подивитися на щось, прослухати якесь аудіо або щось відчути, а потім щось зробити у відповідь. Наприклад, запит, що вимагає одну відповідь з декількох можливих, може затруднити просте програвання сигналів, заздалегідь записаних зловмисником. Як приклад можна привести зміну виразу обличчя (посміхнутися або хмуритися) або відтворення безлічі випадково генерованих фраз (використовується в системі VeriVoice). Цей метод застосовують зазвичай проти атак відтворення, але його

можна використовувати і як метод виявлення живучості. Може використовуватися і мимовільний запит-відповідь. Сюди відносяться рефлекс на удари, зміна розміру зіниці ока залежно від інтенсивності світла, рефлекс м'язів на електричне подразнення. Ясно, що методи, в яких використовуються удари, не схвалюються користувачами. Важливий аспект полягає в тому, що запит-відповідь показує тільки присутність людини, але вона може бути і неавторизованим користувачем.

3.7 Висновки

Як і будь-який метод аутентифікації, біометричні технології повністю не захищені від атак спуфінгу. Методи виявлення живучості є найбільш часто обговорюваним заходом протидії спуфінгу. Виявлення живучості є однією з важливих процедур у процесах реєстрації, верифікації та ідентифікації. Отже, його необхідно розглядати як складову компоненту біометричної системи. Звичайно, виявлення живучості впливає на відсоток помилкового прийняття або помилкової відмови, на відсоток відмови від реєстрації та на інші індикатори продуктивності. При реалізації методів виявлення живучості повинні прийматися до уваги такі аспекти оцінки біометричних систем, як зручність використання, універсальність і т. д.

Деякі технології виявлення живучості вже використовуються на практиці, але оцінка їх продуктивності та оцінка їх впливу на підсумкову продуктивність біометричної системи вимагають незалежного тестування. Більшість вендорів не розкривають власні методи виявлення живучості, «щоб забезпечити конкурентну перевагу». Ці методи зазвичай захищаються як комерційні таємниці і не обговорюються в суспільному середовищі. Отже, їх продуктивність неможливо оцінити, тому заяви про успіхи виявлення живучості можуть бути завищеними і оманливими.

Методи виявлення живучості можуть зменшити ризик атаки фальшивими біометричними характеристиками, але неможливо забезпечити абсолютной захист системи від атак спуфінгу. Це негативно впливає на використання біометричних технологій в якості засобів аутентифікації в додатках, де пред'являються високі вимоги до безпеки. Вразливість до атак спуфінгу і помилки біометричного збігу доводять, що не можна розглядати рішення біометричної системи як вирішальний вердикт верифікації та ідентифікації. До остаточних результатів ідентифікації особистості повинні бути підключені також і інші фактори. Наприклад, в деяких правоохоронних та громадянських додатках біометричний пошук для прийняття остаточного рішення про збіг і розбіжності передбачає участь людини-оператора. Автоматизовані біометричні системи створюються не для заміни процесу прийняття рішень людиною, а для надання йому допомоги.

4 РОЗРОБКА ПРОГРАМИ 2D РОЗПІЗНАВАННЯ ОБЛИЧ ДЛЯ ТЕСТУВАННЯ НАДІЙНОСТІ

4.1 Обрані засоби

Для написання програми 2D розпізнавання облич було обрано наступні засоби: програму було написання на мові C++ з використанням бібліотеки OpenCV у середовищі Microsoft Visual Studio 2012.

Microsoft Visual Studio — серія продуктів фірми Microsoft, які включають інтегроване середовище розробки програмного забезпечення та ряд інших інструментальних засобів [19]. Ці продукти дозволяють розробляти як консольні програми, так і програми з графічним інтерфейсом, в тому числі з підтримкою технології Windows Forms, а також веб-сайти, веб-додатки, веб-служби як в рідному, так і в керованому кодах для всіх платформ, що підтримуються Microsoft Windows, Windows Mobile, Windows Phone, Windows CE, .NET Framework, .NET Compact Framework та Microsoft Silverlight.

Вибір мови реалізації був здійснений на підставі таких переваг:

- підтримується більшістю платформ (Windows, Linux, iOS, Android);
- одна із лідерів серед мов програмування, які застосовуються для створення програмного забезпечення;
- легка взаємодія з бібліотекою OpenCV, адже цю бібліотеку теж написано на C++;
- можливість створення графічного інтерфейсу у Microsoft Visual Studio.

Бібліотека OpenCV — (Open Source Computer Vision Library, бібліотека комп’ютерного зору з відкритим вихідним кодом) бібліотека функцій та алгоритмів комп’ютерного зору, обробки зображень і чисельних алгоритмів загального призначення з відкритим кодом [20]. Бібліотека розроблена компанією Intel і нині підтримується Willow Garage та Itseez. Реалізована на C/C++, також

розробляється для Python, Java, Ruby, Matlab, Lua та інших мов. Може вільно використовуватися в академічних та комерційних цілях — поширюється на умовах ліцензії BSD.

Бібліотека містить понад 2500 оптимізованих алгоритмів, серед яких повний набір як класичних так і практичних алгоритмів машинного навчання і комп'ютерного зору. Алгоритми OpenCV застосовують у таких сферах:

- Аналіз та обробка зображень;
- **Системи з розпізнавання облич**;
- Ідентифікації об'єктів;
- Розпізнавання жестів у відео;
- Відстежування переміщення камери;
- Побудова 3D моделей об'єктів;
- Створення 3D хмар точок з стерео камер;
- Склеювання зображень між собою, для створення зображень всієї сцени з високою роздільною здатністю;
- Система взаємодії людини з комп'ютером;
- Пошуку схожих зображень із бази даних;
- Усування ефекту червоних очей при фотозйомці із спалахом;
- Стеження за рухом очей;
- Аналіз руху;
- Ідентифікація об'єктів;
- Сегментація зображень;
- Трекінг відео;
- Розпізнавання елементів сцени і додавання маркерів для створення доповненої реальності.

OpenCV написана на C++ і її основний інтерфейс також реалізовано на C++, але бібліотека і досі представляє старіший C інтерфейс. На даний момент

реалізовано інтерфейс на мовах Python, Java і MATLAB/OCTAVE (починаючи з версії 2.5). API для цих інтерфейсів можна знайти в онлайн документації. Оболонки для інших мов, таких як C#, CH, Ruby були розроблені з метою охоплення ширшої аудиторії.

Всі нові розробки та алгоритми OpenCV у даний момент розробляються у C++ інтерфейсі.

OpenCV підтримує наступні платформи та інструменти:

- Бібліотеки:

  Microsoft Windows: компілятори Microsoft Visual C + + (6.0,. NET 2003), Intel Compiler, Borland C ++, Mingw (GCC 3.x).

  Linux: GCC (2.9x, 3.x), Intel Compiler: «./configure-make-make install», RPM

  Mac OS X: GCC (3.x, 4.x)

  Android

  iOS — неофіційно.

- Засоби GUI, захоплення відео:

  Microsoft Windows: DirectShow, VfW, MIL, CMU1394

  Linux: V4L2, DC1394, FFMPEG

  Mac OS X: QuickTime.

4.2 Опис бібліотеки OpenCV

OpenCV складається з декількох модулів [21]:

1) CXCORE — ядро, що містить:

- Базові структури;
- Матричну алгебру;
- Алгоритми роботи з пам’яттю;
- Алгоритми перетворення типів;

- Алгоритми для обробки помилок;

- Функції для запису/читання XML файлів;

- Функції для роботи з 2D графіками.

2) CV — модуль обробки зображень, робота з комп'ютерним зором, що містить:

- Функції для роботи із зображеннями (перетворення, фільтрація і т. д.);

- Функції для аналізу зображень (пошук контурів, гістограми і т. д.);

- Алгоритми аналізу рухів, спостереження за об'єктами;

- Алгоритми розпізнання об'єктів (осіб, предметів);

- Алгоритми для калібрування камер.

3) ML — модуль машинного навчання:

- Функції для класифікації та аналізу даних.

4) HighGUI — модуль для створення інтерфейсу користувача, відповідає за:

- Створення вікон;

- Вивід зображень на екран;

- Захоплення відео з файлів і камер;

- Читання/запис зображень.

5) CVCAM — захоплення відео з цифрових камер.

6) CVAUX — застарілі функції:

- Просторовий зір;

- Знаходження і опис ознак та рис обличчя;

- Пошук стерео відповідностей;

- Опис текстур.

Відкрита ліцензія для OpenCV була складена таким чином, щоб було можливо створювати комерційні додатки, використовуючи будь-які можливості OpenCV. Частково саме через такі ліберальні умови і існує велика спільнота користувачів, що включає в себе такі великі компанії як IBM, Microsoft, Intel,

Sony, Siemens, Google, і це далеко не повний список, а також науково-дослідні центри, такі як Стенфорд, Массачусетський технологічний інститут, CMU, Кембридж, і INRIA. OpenCV популярна у всьому світі, причому великі спільноти користувачів можна знайти в Китаї, Японії, Росії, Європі та Ізраїлі.

З моменту свого альфа-релізу в січні 1999 року, OpenCV була використана в багатьох додатках і науково-дослідних роботах, у тому числі: накладення звичайних карт і фотографій з супутника, вирівнювання документів при скануванні, видалення шуму з медичних зображень, аналіз об'єктів, системи безпеки, автоматичне спостереження, системи контролю за якістю на виробництві, калібрування камер, а також безпілотні літальні, наземні і підводні апарати. Вона навіть була використана для розпізнавання звуку та музики, де методи розпізнавання образів були застосовані до зображень спектрограм звуку. Бібліотека стала ключовою частиною системи зору робота «Stanley» зі Стенфорда, який виграв 2.000.000$ на Великих Пустельних перегонах роботів DARPA.

4.3 Каскади Хаара

Каскади Хаара — це один з найпростіших способів розпізнавання класів об'єктів з великою швидкістю роботи. До них відносяться обличчя і руки людей, номери автомобілів, пішоходи і т. і. Детектором Хаара просто знаходити тварин в кадрі. До того ж, готові реалізації OpenCV є під більшість існуючих систем. Все це робить каскади Хаара одним з найбільш зручних методів, що дозволяють вирішувати завдання відеостеження навіть людям, які ніколи не працювали з обробкою відео [22].

Ознаки Хаара — ознаки цифрового зображення, що використовуються в розпізнаванні образів. Своєю назвою вони зобов'язані інтуїтивною схожістю з вейвлетами Хаара. Ознаки Хаара використовувалися в першому детекторі осіб, що працював в режимі реального часу.

Історично склалося так, що алгоритми, що працюють тільки з інтенсивністю зображення (наприклад, значення RGB в кожному пікселі), мають велику обчислювальну складність. Віола і Джонс адаптували ідею використання вейвлетів Хаара і розробили те, що було названо ознаками Хаара. Ознака Хаара складаються з суміжних прямокутних областей. Вони позиціонуються на зображенні, далі сумуються інтенсивності пікселів в областях, після чого обчислюється різниця між сумами. Ця різниця і буде значенням певної ознаки, певного розміру, певним чином позиційованого на зображенні.

Для прикладу розглянемо базу даних з людськими обличчями. Спільним для всіх зображень є те, що область в районі очей темніше, ніж область в районі щік. Отже загальною ознакою Хаара для осіб є 2 суміжних прямокутних регіону, що лежать на очах і щоках.

На етапі виявлення в методі Віоли-Джонса вікно встановленого розміру рухається по зображенню, і для кожної області зображення, над якою проходить вікно, розраховується ознака Хаара. Наявність або відсутність предмета у вікні визначається різницею між значенням ознаки і навченим порогом. Оскільки ознаки Хаара мало підходять для навчання або класифікації (якість трохи вища, ніж у випадковій нормально розподіленій величині), для опису об’єкта з достатньою точністю необхідно більше число ознак. Тому в методі Віоли-Джонса ознаки Хаара організовані в каскадний класифікатор [23].

Найпростішу прямокутну ознака Хаара можна визначити як різницю сум пікселів двох суміжний областей усередині прямокутника, який може займати різні положення і масштаби на зображенні. Такий вид ознак називається 2-прямокутним. Віола і Джонс так само визначили 3-прямокутні і 4-прямокутні ознаки. Кожна ознака може показати наявність (або відсутність) будь-якої конкретної характеристики зображення, такої як кордони або зміна текстур.

Наприклад, 2-прямокутний ознака може показати, де знаходиться межа між темним і світлим регіонами.

Ключовою особливістю ознак Хаара є найбільша, в порівнянні з іншими ознаками, швидкість. При використанні інтегрального представлення зображення, ознаки Хаара можуть обчислюватися за постійний час (приблизно 60 процесорних інструкцій на ознаку з двох областей).

4.4 Метод Віоли-Джонса

У методі Віоли-Джонса основу складають примітиви Хаара, що представляють собою розбивку заданої прямокутної області на набори різнотипних прямокутних підобластей:

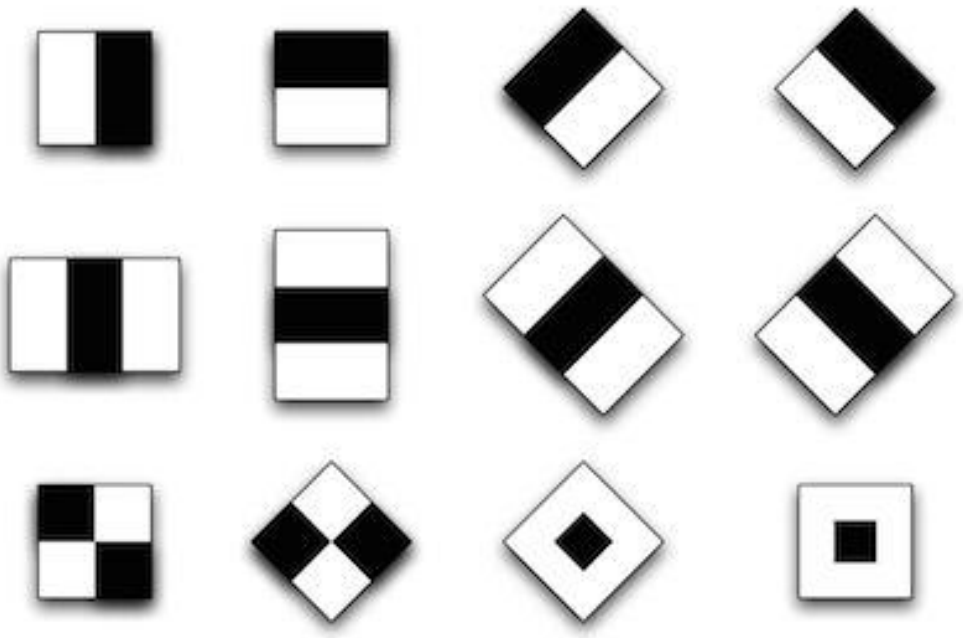


Рисунок 4.1 – Набори різнотипних прямокутних областей

В оригінальній версії алгоритму Віоли-Джонса використовувалися тільки примітиви без поворотів, а для обчислення значення ознаки сума яскравостей пікселів однієї підобласті віднімалася із суми яскравостей інших підобластей.

Пізніше були запропоновані примітиви з нахилом на 45 градусів і несиметричних конфігурацій. Також замість обчислення звичайної різниці, було запропоновано приписувати кожній підобласті певну вагу і значення ознаки обчислювати як зважену суму пікселів різнотипних областей:

$$feature = \sum_{i \in I=1,\dots,N} w_i * RectSum(r_i) \quad (5)$$

Чому в основу методу лягли примітиви Хаара? Основною причиною була спроба відійти від піксельного уявлення із збереженням швидкості обчислення ознаки [24]. З значень пари пікселів складно винести якусь осмислену інформацію для класифікації, в той час як з двох ознак Хаара будується, наприклад, перший каскад системи з розпізнавання осіб, який має цілком осмислену інтерпретацію:

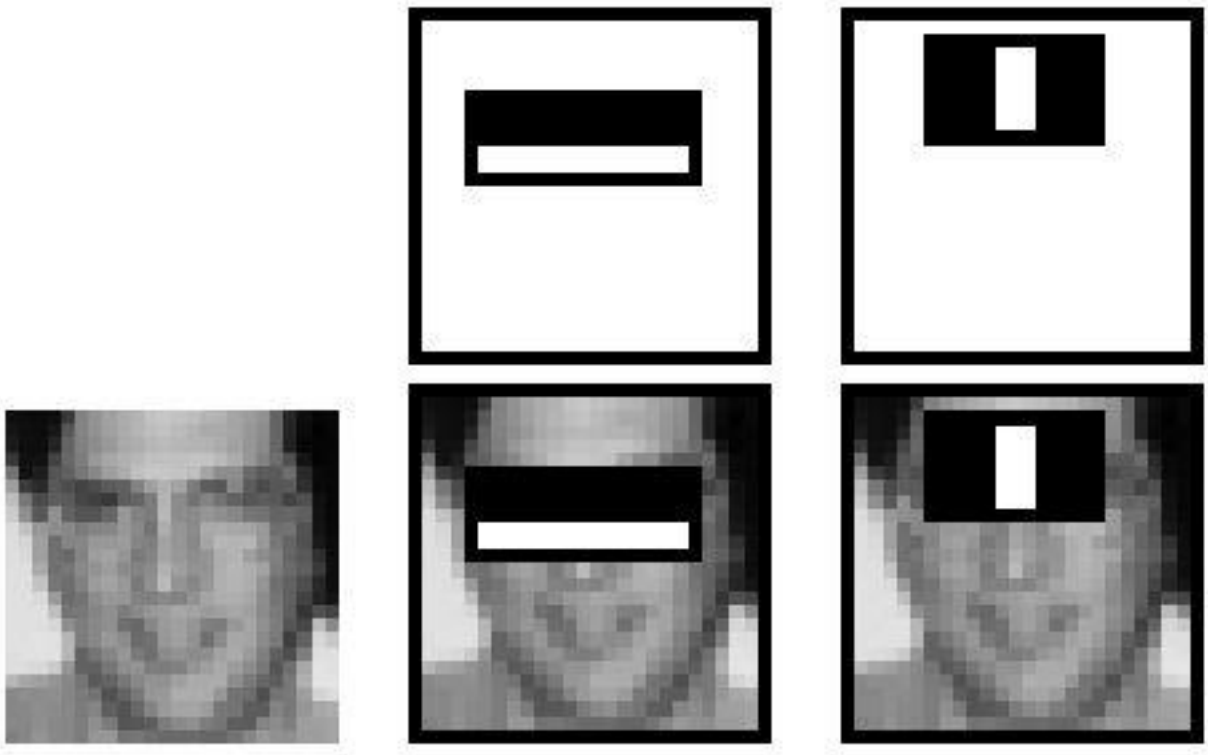


Рисунок 4.4.2 – Ознаки Хаара на зображенні обличчя

Для визначення приналежності до класу в кожному каскаді знаходиться сума значень слабких класифікаторів цього каскаду. Кожен слабкий класифікатор видає два значення залежно від того, чи значення ознаки є більшим чи меншим за заданий поріг, що належить цьому класифікатору. Наприкінці сума значень слабких класифікаторів порівнюється з порогом каскаду і виноситься рішення про те, чи знайдено об’єкт даним каскадом.

Основні принципи, на яких заснований метод, такі:

- використовуються зображення в інтегральному уявленні, що дозволяє обчислювати швидко необхідні об’єкти;
- використовуються ознаки Хаара, за допомогою яких відбувається пошук потрібного об’єкта (у даному контексті, обличчя та його рис);
- використовується бустінг (від англ. boost — поліпшення, посилення) для вибору найбільш підходящих ознак для шуканого об’єкта на даній частині зображення;
- всі ознаки надходять на вхід класифікатора, який дає результат «вірно» або «невірно»;
- використовуються каскади ознак для швидкого відкидання вікон, де не знайдено обличчя.

Навчання класифікаторів йде дуже повільно, але результати пошуку особи дуже швидкі, саме тому був обраний даний метод розпізнавання осіб на зображенні. Метод Віоли-Джонса є одним з кращих по співвідношенню показників ефективність розпізнавання/швидкість роботи. Також цей детектор має вкрай низьку ймовірність помилкового виявлення особи. Алгоритм навіть добре працює і розпізнає риси обличчя під невеликим кутом, приблизно до 30 градусів. При куті нахилу більше 30 градусів відсоток виявлень різко падає. І це не дозволяє в стандартній реалізації виявляти повернене обличчя людини під довільним кутом, що значною мірою ускладнює або унеможливлює використання алгоритму в сучасних виробничих системах з урахуванням їх зростаючих потреб.

Даний метод в загальному вигляді шукає особи і риси обличчя за загальним принципом скануючого вікна. У загальному вигляді, завдання виявлення особи та рис обличчя людини на цифровому зображенні виглядає саме так: є зображення, на якому є шукані об’єкти. Воно представлено двовимірною матрицею пікселів розміром w * h, в якій кожен піксель має значення:

- від 0 до 255, якщо це чорно-біле зображення;
- від 0 до 2553, якщо це кольорове зображення (компоненти R, G, B).

В результаті своєї роботи, алгоритм повинен визначити особи та їх риси та позначити їх — пошук здійснюється в активній області зображення прямокутними ознаками, за допомогою яких і описується знайдена особа та її риси:

$$rectangle_i = \{x, y, w, h, a\}, \quad (6)$$

де x та y — координати центру i-го прямокутника, w — ширина, h — висота, a — кут нахилу прямокутника до вертикальної осі зображення.

Алгоритм сканування вікна з ознаками виглядає так: є досліджуване зображення, обрано вікно сканування, обрані використовувані ознаки;

- далі вікно сканування починає послідовно рухатися по зображенню з кроком в 1 клітинку вікна (припустимо, розмір самого вікна є 24 * 24 комірки);
- при скануванні зображення в кожному вікні обчислюється приблизно 200 тисяч варіантів розташування ознак, за рахунок зміни масштабу ознак та їх положення у вікні сканування;
- сканування проводиться послідовно для різних масштабів;
- масштабується не саме зображення, а скануюче вікно (змінюється розмір комірки);
- всі знайдені ознаки потрапляють до класифікатора, який «виносить вердикт».

Іншими словами, стосовно до малюнків і фотографій використовується підхід на основі скануючого вікна (scanning window): сканується зображення вікном пошуку (так зване, вікно сканування), а потім застосовується класифікатор

до кожного положення [25]. Система навчання і вибору найбільш значущих ознак повністю автоматизована і не вимагає втручання людини, тому даний підхід працює швидко.

Завдання пошуку і знаходження осіб на зображенні за допомогою даного принципу часто буває черговим кроком на шляху до розпізнавання характерних рис, наприклад, верифікації людини по розпізнаваній особі або розпізнавання міміки обличчя.

Результати навчання каскадів у вигляді класифікаторів Хаара знаходяться в XML-форматі.

Для кожного класифікатора, вираженого як сутність з підлеглими атрибутами треба створити окреме XML-сховище DOM (Document Object Model) — об’єктна модель документа такого класифікатора в загальному вигляді представлена нижче.

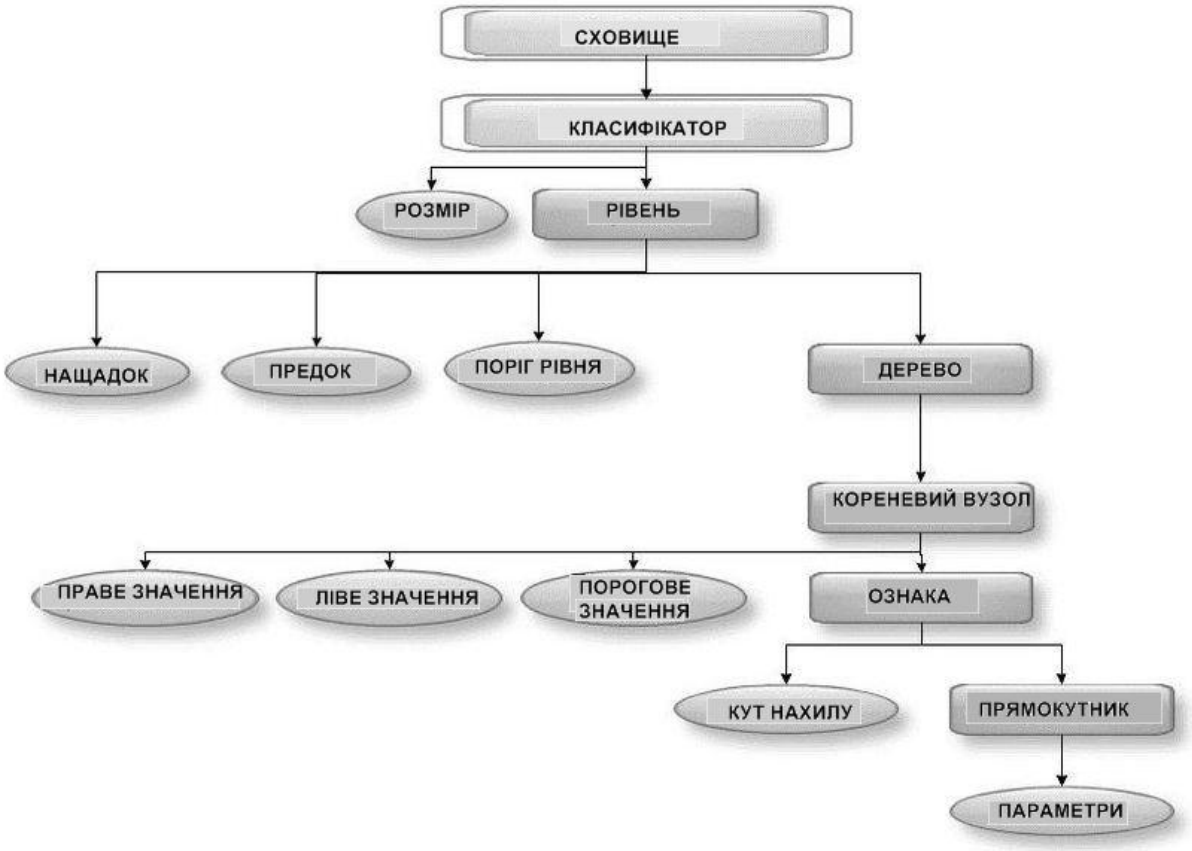


Рисунок 4.2 – Об’єктна модель документа класифікатора

Нижче наведено класифікатор, що використовується у програмі:

```
<opencv_storage>
<haarcascade_eye_tree type_id="opencv-haar-classifier">
  <size>
    20 20</size>
  <stages>
    <_>
      <!-- stage 0 -->
      <trees>
        <_>
          <!-- tree 0 -->
          <_>
            <!-- root node -->
            <feature>
              <rects>
                <_>
                  8 7 12 1 -1.</_>
                <_>
                  8 7 6 1 2.</_></rects>
              <tilted>1</tilted></feature>
            <threshold>-0.0269871093332767</threshold>
            <left_node>2</left_node>
            <right_node>1</right_node></_>
          <_>
            <!-- node 1 -->
            <feature>
              <rects>
                <_>
                  4 7 8 6 -1.</_>
                <_>
                  6 7 4 6 2.</_></rects>
              <tilted>0</tilted></feature>
            <threshold>0.0506705306470394</threshold>
            <left_val>-0.8039547204971314</left_val>
            <right_val>0.6049140095710754</right_val></_>
          <_>
```

Тут haarcascade_eye_tree type_id — набір слабких класифікаторів, на основі яких виноситься рішення про те, чи знаходиться об’єкт на зображенні чи ні, left_val і right_val - це параметри конкретного слабкого класифікатора.

На даному прикладі видно, яка інформація зберігається у використовуваних XML. Це інформація про класифікатор (haarcascade) і його розміри (size), про використані рівні (stage), попередника, або предка даного рівня (parent), наступного рівня, або нащадка (next), вибудовується дерево (tree) і його кореневий вузол (root node) з параметрами (threshold, left, right). Далі вибудовується інформація про самі ознаки (features) у вузлах цього дерева, які задаються прямокутниками з параметрами (rects) з певним кутом нахилу (tilted).

У роботі використовувались готові натреновані класифікатори haarcascade_mcs_nose.xml, haarcascade_mcs_mouth.xml, haarcascade_mcs_eyepair_small.xml, haarcascade_mcs_eyepair_big.xml, haarcascade_frontalface_alt.xml, haarcascade_eye_tree_eyeglasses.xml.

4.5 Розробка програмного забезпечення

Є кілька варіантів отримання зображень облич людей:

1) Власноруч отримати фотографії з фотоапарату (або використовуючи веб-камеру);

2) Використовувати готову базу, якщо вона є в інтернеті. Для осіб, номерів, очей, емоцій, людей і т. д. таких баз доволі багато;

3) Включити відеокамеру і зробити набір знімків з відеопотоку;

4) Використовувати програмне забезпечення і згенерувати нові вибірки з наявних 2-3 зображень.

Для варіантів 1-3 є кілька програм, що спрощують життя. У першу чергу це програми, що дозволяють розмітити фотографії. У статтях англійською використовується самописна програма «imageclipper». Але вона не досить

коректно працює з великими фотографіями. У нашому випадку використовується веб-камера, якою оснащений майже кожен сучасний ноутбук, а у випадку якщо програму буде використано десь на персональному комп'ютері, можна придбати веб-камеру.

Отже, для того, щоб підключити веб-камеру, потрібно створити подію, яка б розпочиналася при натисненні на кнопку «Ввімкнути камеру»:

```
//Подія, що викликається при натисненні клавішею миші на кнопку
«Ввімкнути камеру»
private: System::Void button1_Click(System::Object^  sender, System::EventArgs^
e) {

//Вказуємо роздільчу здатність камери
double width = 640;
double height= 480;
int counter = 0;

//Створюємо камеру
CvCapture* Camera= cvCreateCameraCapture(0);

        //Задаємо width і height
      cvSetCaptureProperty(Camera, CV_CAP_PROP_FRAME_WIDTH, width);
      cvSetCaptureProperty(Camera, CV_CAP_PROP_FRAME_HEIGHT, height);

//Створюємо вікно для обробки клавіш
   cvNamedWindow("Веб-камера", 1);//1 = авто розмір
while (true){
            //Отримуємо кадр
            CamShot = cvQueryFrame(Camera);
```

Після того, як отримано зображення з веб-камери, дані зображення записуються до бази даних. Наразі база даних являє собою звичайний текстовий файл, що збергігає інформацію про користувачів системи. Зберігається не зображення саме по собі, а значення відстаней між очами, між очами та ротом, між

ротом та носом і т. і. Ці відстані обраховуються відразу при отриманні зображення. Зразок запису даних про користувача з бази даних:

```
Olga
#
275
218
338
213
#
302
261
#
299
292
#
```

Приклад виявлення області, на якій знаходиться рот людини:

```
        //Функція виявлення області рота
vector<Rect> detectmouth(IplImage* frame1)
{
    //Завантажуємо класифікатор каскадів для рота
  CascadeClassifier face("haarcascade_mcs_mouth.xml");
    //Присвоюємо поточне зображення з камери
    Mat frame = frame1;

    //Перетворюємо у відтінки сірого
  Mat frame_gray;
  cvtColor(frame,frame_gray,CV_BGR2GRAY);

  vector<Rect> faces;
```

```
	vector<Rect> faces1;

	//System::Windows::Forms::MessageBox::Show(eye1[0].x.ToString());
	//System::Windows::Forms::MessageBox::Show(eye1[1].x.ToString());
	//Виявляємо правий та лівий ока
	int t1,t2;
	if(eye[0].x>eye[1].x)
	{
		t1=eye[1].x;
		t2=eye[0].x;
	}
	else
	{
		t1=eye[0].x;
		t2=eye[1].x;
	}
	//r1=sqrtf((eye[i].x-nose[j].x)*(eye[i].x-nose[j].x)+(eye[i].y-
nose[j].y)*(eye[i].y-nose[j].y));
	//Знаходимо координати ротів
  face.detectMultiScale(frame_gray, faces, 1.1, 1,0|CV_HAAR_SCALE_IMAGE );
  //Тепер відсіюємо непотрібне
	for ( int i=0; i<faces.size(); i++ )
	{
		//По-перше, рот повинен розміщуватись між правим та лівим оком (адже виявляється ротів набагато більше, ніж їх відображено)
		if(faces[i].x>t1 && faces[i].x<t2)
			//По-друге, відстань від ока до рота не повинна бути надто великою чи надто маленькою
			if(faces[i].width>=eye[0].width*0.8)
				//Ну і рот звісно не повинен бути нижче за очі
			if(faces[i].y>eye[0].y)


//І лежати в діапазоні більше 1.1 відстані між очами та менше 1.5
				if(sqrtf((eye[0].x-faces[i].x)*(eye[0].x-faces[i].x)+(eye[0].y-
faces[i].y)*(eye[0].y-faces[i].y))>sqrtf((eye[0].x-eye[1].x)*(eye[0].x-
eye[1].x)+(eye[0].y-eye[1].y)*(eye[0].y-eye[1].y))*1.1)
```

```
                        if(sqrtf((eye[0].x-faces[i].x)*(eye[0].x-faces[i].x)+(eye[0].y-
faces[i].y)*(eye[0].y-faces[i].y))<sqrtf((eye[0].x-eye[1].x)*(eye[0].x-
eye[1].x)+(eye[0].y-eye[1].y)*(eye[0].y-eye[1].y))*1.5)
                                faces1.push_back(faces[i]);
        }

        //Виявляємо те, що залишилось
        for ( int i=0; i<faces1.size(); i++ )
        {
                rectangle( frame, faces1[i], Scalar( 0, 255, 255 ), 2 );
        }
return faces1;
}
```

Коли отримуємо зображення з камери, застосовуємо функції для виявлення носа, рота, очей та контура обличчя:

```
//Дія на клік клавішею миші по кнопці «Зробити знімок»
private: System::Void button2_Click(System::Object^  sender, System::EventArgs^
e) {

        IplImage* CamS = 0;
        //Отримуємо поточне зображення
CamS=cvCloneImage(CamShot);
                //      detect(CamS);
                //      detecteye(CamS);
                //      detectnose(CamS);
                //      detectmouth(CamS);
        //Поміщаємо його в Picturebox1
                        pictureBox1->Image=(gcnew
System::Drawing::Bitmap(CamS->width,CamS->height,CamS->widthStep,
System::Drawing::Imaging::PixelFormat::Format24bppRgb,(System::IntPtr)CamS-
>imageData));
        //      cvShowImage("Изображение с WEB CAM", CamShot);

//detect(CamS);
//Виявляємо параметри обличчя
eye=detecteye(CamS);
//Якщо виявлено невірну кількість очей, треба переробити знімок
if(eye.size()!=1)
```

```
{
nose=detectnose(CamS);
mouth=detectmouth(CamS);
```

Щоб ідентифікувати людину, потрібно порівняти отримані значення відстаней із значеннями всіх записів з бази даних:

```
//Дія на клік миші по кнопці «Порівняти з базою»
private: System::Void button3_Click(System::Object^  sender, System::EventArgs^ e) {


IplImage* CamS = 0;
//Беремо поточне зображення з камери
            CamS=cvCloneImage(CamShot);
            //Виводимо його у picturebox1
            pictureBox1->Image=(gcnew System::Drawing::Bitmap(CamS->width,CamS->height,CamS->widthStep,
System::Drawing::Imaging::PixelFormat::Format24bppRgb,(System::IntPtr)CamS->imageData));


// detect(CamS);
//Виявляємо очі
eye=detecteye(CamS);
//Перевіряємо вірність виявлення очей
if(eye.size()!=1)
{
//Визначаємо інші параметри
nose=detectnose(CamS);
mouth=detectmouth(CamS);


inf.eye=eye;
inf.nose=nose;
inf.mouth=mouth;

eye2=eye;
nose2=nose;
mouth2=mouth;
int min=1000;
```

```
int m=-1;
                    int k=0;
                    int k1=0;
                    int fl=0;
                    //info.[w]
        //Порівнюємо усі можливі варіації відстаней між параметрами з варіантами, що є у базі даних
        for(int w=0;w<info.size();w++)
        {
        for(int i=0;i<info[w].eye.size();i++)
        {
                for(int j=0;j<info[w].nose.size();j++)
                {
                        for(int c=0;c<info[w].mouth.size();c++)
                        {

        for(int i1=0;i1<eye2.size();i1++)
        {
                for(int j1=0;j1<nose2.size();j1++)
                {
                        for(int c1=0;c1<mouth2.size();c1++)
                        {

double r1,r2,r3,r4;

r1=sqrtf((info[w].eye[i].x-info[w].nose[j].x)*(info[w].eye[i].x-
info[w].nose[j].x)+(info[w].eye[i].y-info[w].nose[j].y)*(info[w].eye[i].y-
info[w].nose[j].y));
r2=sqrtf((info[w].eye[i].x-info[w].mouth[c].x)*(info[w].eye[i].x-
info[w].mouth[c].x)+(info[w].eye[i].y-info[w].mouth[c].y)*(info[w].eye[i].y-
info[w].mouth[c].y));

r3=sqrtf((eye2[i1].x-nose2[j1].x)*(eye2[i1].x-nose2[j1].x)+(eye2[i1].y-
nose2[j1].y)*(eye2[i1].y-nose2[j1].y));
r4=sqrtf((eye2[i1].x-mouth2[c1].x)*(eye2[i1].x-mouth2[c1].x)+(eye2[i1].y-
mouth2[c1].y)*(eye2[i1].y-mouth2[c1].y));

if(abs(abs(r1/r3)-abs(r2/r4))<=0.02) //0.02 – точність співпадіння
{
```

```
		if(abs(abs(r1/r3)-abs(r2/r4))<min)
		{
			min=abs(abs(r1/r3)-abs(r2/r4));
			m=w;

		}

		//System::Windows::Forms::MessageBox::Show(abs(r1/r3).ToString());
		//System::Windows::Forms::MessageBox::Show(abs(r2/r4).ToString());

		//Якщо є співпадіння з заданою точністю, то проводимо відрізки між параметрами, що співпали
		cvLine(CamS, cvPoint(eye2[i1].x,eye2[i1].y), cvPoint(nose2[j1].x,nose2[j1].y),CV_RGB(250,0,0),1,8);
		cvLine(CamS, cvPoint(eye2[i1].x,eye2[i1].y), cvPoint(mouth2[c1].x,mouth2[c1].y),CV_RGB(250,0,0),1,8);

fl=1;
k++;
}
k1++;

				}
			}
		}

				}
			}
		}

		}
if(m!=-1) //Якщо хоча б один параметр співпав, виводимо ім'я
{
		label3->Text=gcnew System::String(info[m].name.c_str());
}
else
		label3->Text=gcnew System::String("никто");
		//System::Windows::Forms::MessageBox::Show(gcnew System::String(info[m].name.c_str()));
}
```

Отже, з боку користувача робота з програмою виглядає наступним чином:

1. Головне вікно програми:

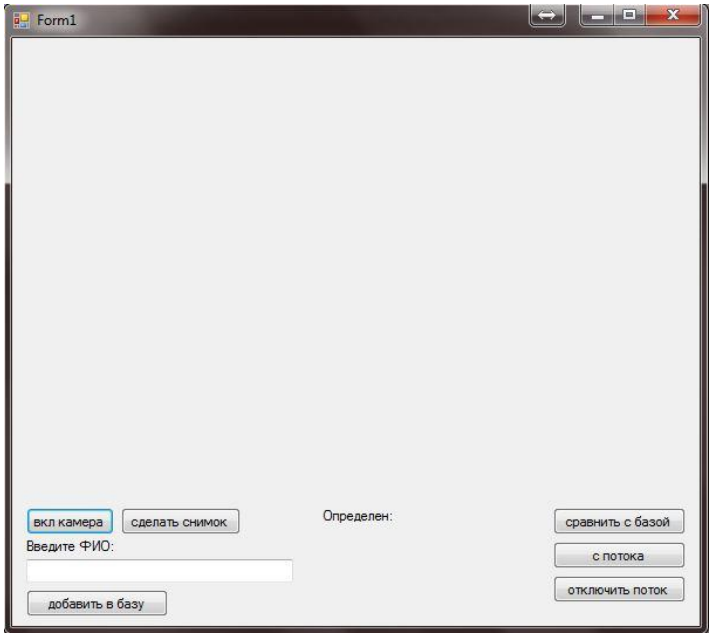


Рисунок 4.3 – Головне вікно програми

2. Натискаємо на кнопку «вкл камера» і бачимо, що відкривається нове діалогове вікно, яке показує зображення з веб-камери:

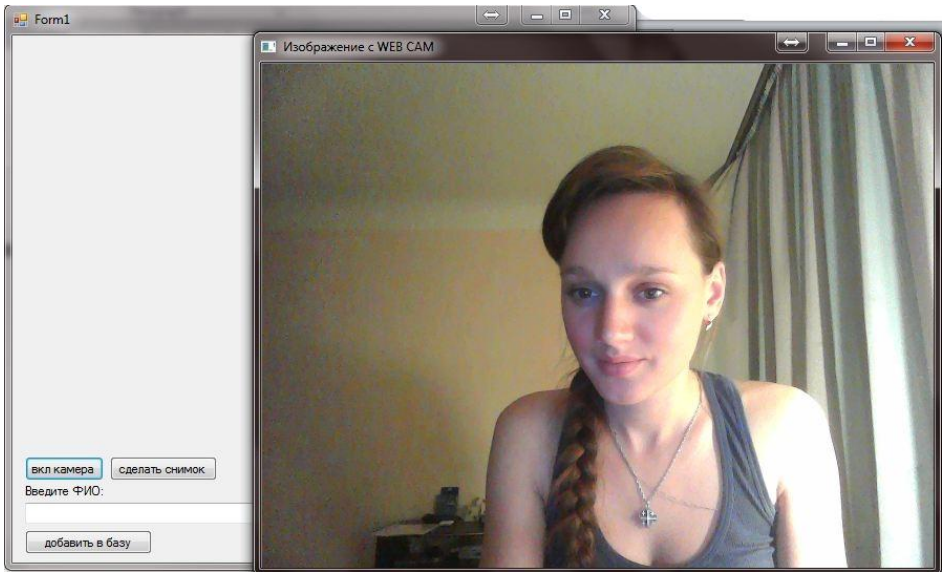


Рисунок 4.4 – Діалогове вікно веб-камери

3. Робимо знімок і зберігаємо його у базу даних (клавіші «сделать снимок» і «добавить в базу» відповідно), при цьому вказуємо ім’я користувача:

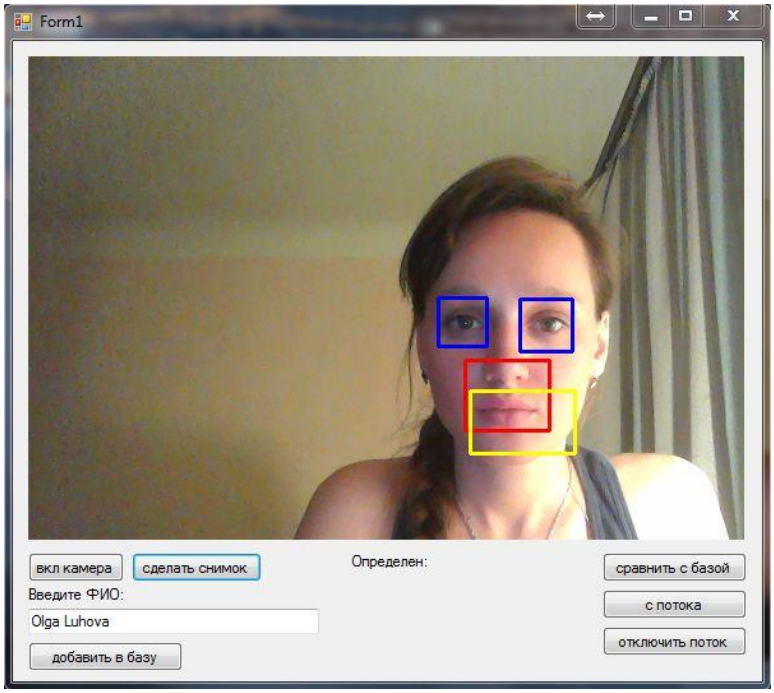


Рисунок 4.5 – Виявлені області очей, носу та рота

Як видно на зображенні, програма виявила області очей, носу та рота. При записі до бази даних програма видає MessageBox:

Рисунок 4.6 – MessageBox з ім’ям, що внесене до бази даних

4. Тепер коли дані внесені до бази даних, можна перевірити, чи програма здатна ідентифікувати. Натискаємо на клавішу «сравнить с базой» та перевіряємо, який результат було повернуто:

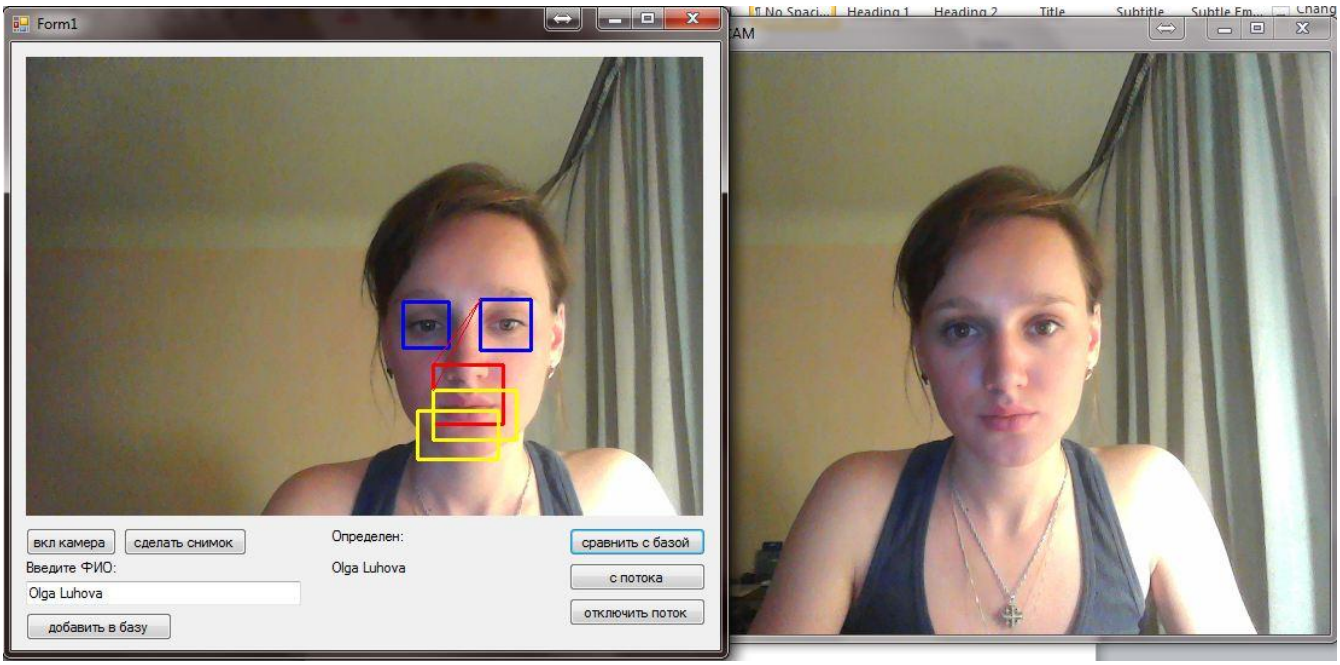


Рисунок 4.7 – Результат ідентифікації

Як видно на зображенні, програма повернула вірний результат.

5. Також є можливість проводити розпізнавання облич у відеопотоці. Для цього треба натиснути клавішу «с потока», але процес буде таким же, як і з фотографіями – програма буде робити фото і порівнювати дані відстаней з даними з бази даних. Варто відмітити, що процес розпізнавання є ресурсозатратним. На тестовому комп'ютері з процесором Intel core i7 та 8Гб RAM найвищий показник зайнятості процесора досягав 60% при розпізнаванні у відеопотоці.

4.6 Аналіз надійності розробленого програмного забезпечення

Щоб проаналізувати, наскільки легко обманути створену систему розпізнавання облич, будемо підносити до веб-камери справжнє обличчя, та фотографію, адже це один з найпростіших методів спуфінгу (фото-спуфінг).

Зазвичай, програма видає 90% успішних результатів – при розпізнаванні обличчя з веб-камери (10% невдач обумовлені поворотом голови та нерівномірним освітленням).

Отже, для фото-спуфінгу використаємо 10 фотографій. Деякі з них були зроблені 5 і більше років тому, тобто є різниця в зовнішності (зачіска). Також використаємо фото схожих людей, аби перевірити, чи відрізнить система цих людей, хоча тут перевіряється не сама система, а реалізований алгоритм (FAR та FRR), хоча слід мати на увазі, що ефективність алгоритму також безпосередньо впливає на рівень надійності системи розпізнавання облич.

Отже, отримані результати:

1) 2 фотографії інших людей були розпізнані, як «Оля» - тобто тут маємо помилку як самого алгоритму Віоли-Джонса, так і системи розпізнавання облич, адже вона не виявила різниці між реальною людиною та фотографією.

2) 4 фотографії, зроблені у різний час, були розпізнані вірно – маємо помилку системи розпізнавання, адже вона не виявила різниці між реальною людиною та зображенням, а це означає, що фото-спуфінг тут спрацював.

3) 4 фотографії розпізнано не було (результат програми «ніхто»), але це можна пояснити наявністю емоційного забарвлення обличчя, а також не фронтальним його зображенням.

Зображення та результати програми наведені у Додатку А.

Отже, загалом маємо, що при піднесенні до веб-камери фотографій – 40% (4 з 10 фотографій) результатів видали вірну інформацію того, чиє обличчя зображене на фотографії, 20% видали помилку розпізнавання взагалі, адже на фотографіях були зображені інші люди, тобто це означає, що система не є надійною, а отже достатньо легко піддається фото-спуфінгу. Залишок в 40% не означає, що система має певну міру надійності. Насправді, 40% результату «ніхто» знову ж таки обумовлені освітленням та тим, що не всі зображення демонструють

фронтальне зображення обличчя. Насправді ж система не має перевірки того, чи використовується фотографія, чи реальне зображення з веб-камери, тобто система не захищена від фото-спуфінгу та буде пропускати зловмисника, який використає фотографію.

При таких результатах без сумніву можна заявити, що принаймні для 2D технологій обов'язковим є введення мультимодальної аутентифікації або додаткового розпізнавання інших ознак людини (наприклад, голосу). Інакше систему дуже просто «обманути» – достатньо мати фронтальне зображення необхідної людини в гарній якості.

З 3D технологією дещо легше, адже вона базується на формі голови, текстурі шкіри та інших ознаках, що недоступні 2D технології. 3D технологію протестовано не було через відсутність необхідних сканерів.

4.7 Висновки

Розроблено програмне забезпечення, що проводить 2D розпізнавання облич як зі звичайних зображень, так і у відеопотоці. Програмне забезпечення розроблене на мові C++ у середовиці Microsoft Visual Studio 2012 з використанням бібліотеки OpenCV.

Використано метод Віоли-Джонса, що базується на примітивах Хаара. При цьому при написанні програмного забезпечення використовувались стандартні класифікатори (xml файли) бібліотеки OpenCV для ідентифікації областей рота, носа та очей. Ці класифікатори вже достатньо натреновані та майже не потребують додаткового тренування.

Дане програмне забезпечення можна використовувати для обмеження доступу до комп'ютерного обладнання небажаних користувачів. У подальшому планується створення повноцінної бази даних, що вже не буде текстовим файлом, а матиме повноцінну структуру (реляційної бази даних) та розміщуватиметься на

сервері. Там же і можна буде зберігати повний список користувачів з їх даними. Також доцільним у майбутньому є додання функціїї отримання зображень не лише з веб-камери, а й з інших носіїв (для того, щоб взаємодія з об’єктами розпізнавання була мінімальною).

Аналіз надійності розробленого програмного забезпечення показав, що принаймні для 2D технологій обов’язковим є введення мультимодальної аутентифікації або додаткового розпізнавання інших ознак людини (наприклад, голосу). Інакше систему дуже просто «обманути» – достатньо мати фронтальне зображення необхідної людини в гарній якості.

З 3D технологією дещо легше, адже вона базується на формі голови, текстурі шкіри та інших ознаках, що недоступні 2D технології.

5 ОХОРОНА ПРАЦІ

5.1 Вступ

У даному розділі проводиться аналіз середовища, в якому проводилося дослідження магістерської дисертації на основі санітарних норм України.

В даній роботі було створено програмне забезпечення, що проводить розпізнавання облич, використовуючи комп'ютерні ресурси та базу даних облич. Саме тому ця робота безпосередньо пов'язана з роботою на комп'ютері.

На робочому місці користувача ПК виникають небезпечні та шкідливі фактори: підвищений рівень шуму, несприятливі мікрокліматичні умови, недостатній рівень освітленості, шкідливі речовини, підвищений рівень електромагнітних випромінювань радіочастот, висока напруга електричної мережі, статична електрика та інші. Робота з ПК супроводжується також підвищеним ступенем напруженості трудового процесу. До хімічно небезпечних факторів, що постійно діють на користувача ПК, відноситься виникнення активних часток у результаті іонізації повітря при роботі комп'ютера. Біологічні шкідливі виробничі фактори в даному приміщенні відсутні.

Отже, треба визначити ряд шкідливих факторів, що можуть впливати на якість виконання роботи, а також на здоров'я користувача.

Шкідливі фактори, які можуть впливати на роботу програміста, можна поділити на дві категорії:

- Фізичні;
- Психофізіологічні.

Обидві ці групи можуть спричиняти дискомфорт при роботі, або ж навіть призвести до захворювань. Дотримання правил роботи з комп'ютером, а також санітарних норм, забезпечить безпеку користувача ПК.

Визначаючи основні загрози при роботі, розподілимо їх на дві категорії:

До фізичних віднесемо:

- Підвищений рівень освітленості;
- Нерівномірність розподілу яскравості в полі зору;
- Підвищену яскравість світлового зображення;
- Підвищене значення напруги в електричному ланцюзі;
- Підвищений рівень статичної електрики.

До психофізіологічних віднесемо:

- Напругу зору;
- Напругу уваги;
- Інтелектуальні навантаження;
- Великий обсяг інформації, що обробляється в одиницю часу;
- Нераціональну організацію робочого місця.

Неправильна організація робочого місця сприяє загальній і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, скривленню хребта й розвитку остеохондрозу.

5.2 Характеристика приміщення

Приміщення, в якому розроблялося програмне забезпечення, розташоване на одинадцятому поверсі 13-поверхового будинку. Робоче місце обладнане робочим столом площею 1.2$м^2$, стільцем та персональним комп'ютером, що складається з 24-дюймового монітору, системного блоку, що має у складі Intel Core i7 мікропроцесор, клавіатури, веб-камери та миші. Слід відзначити, що площа робочого місця не повинна бути меншою за 6$м^2$ [13].

Приміщення має однобічне природне освітлення та загальне штучне освітлення. Вікно орієнтовано на південь, площа засклення 30%. Стіни і стеля пофарбовані фарбою світлого кольору, підлога вкрита світлим лінолеумом. У

приміщенні відсутні сильні вібрації та шкідливі речовин, а також склад повітря в нормі.

Приміщення загальною площею 12$м^2$, ширина якого складає 3м, довжина – 4м, висота стелі – 3м.

Виходячи з того, що в приміщенні працює одна людина, отримаємо наступні дані, наведені в таблиці 5.1:

Таблиця 5.1 – Фактичні та нормативні значення параметрів приміщення

Параметр приміщення	**Нормативний**	**Фактичний**
Площа, $м^2$	6 і більше	12.0
Об’єм, $м^3$	15 і більше	36.0

Виходячи з даних, наведених в таблиці 5.1, робимо висновок, що розміри приміщення задовольняють існуючим вимогам.

На рис. 5.1 наведено схему кімнати:

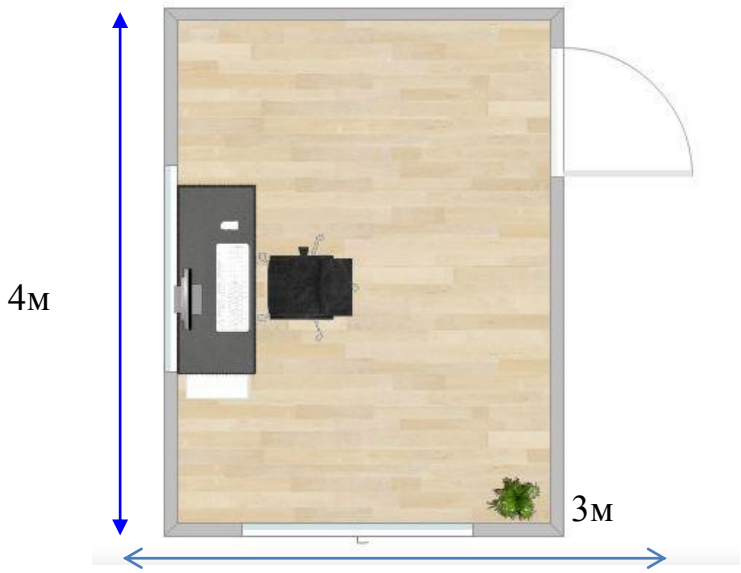


Рисунок 5.1 – Схема кімнати

5.3 Оцінка небезпечних і шкідливих виробничих

5.3.1 Мікроклімат робочої зони користувача ПК

Для постійних робочих місць, якими є робочі місця операторів ПК, встановлені оптимальні параметри мікроклімату, а при неможливості їх дотримання використовують допустимі параметри. Приміщення належить до Іа категорії (виконуються легкі фізичні роботи), тому повинні дотримуватися наступні вимоги:

Таблиця 5.2 – Параметри мікроклімату для приміщень з ПК

Період року	**Параметр мікроклімату**	**Величина**
Холодний	Температура повітря в приміщенні	22...24 °С
	Відносна вологість	40... 60%
	Швидкість руху повітря	0.1 м/с
Теплий	Температура повітря в приміщенні	23...25 °С
	Відносна вологість	40... 60%
	Швидкість руху повітря	0.1 м/с

Для створення й автоматичної підтримки в приміщенні оптимальних значень температури, вологості, чистоти і швидкості руху повітря незалежно від зовнішніх умов, у холодний час року використовується водяне опалення, у теплий час року застосовується кондиціонування повітря. Кондиціонер являє собою вентиляційну установку, яка за допомогою приладів автоматичного регулювання

підтримує в приміщенні задані параметри повітряного середовища. Користувачем ПК виділяється до 120 Ккал теплової енергії за годину.

Всі показники задовольняють вимогам, зазначеним в [14] для робіт категорії легка Іа, і є задовільними для здоров'я людини.

Таблиця 5.3 – Норми подачі свіжого повітря в приміщення з ПК

Характеристика приміщення	**Об'ємна витрата свіжого повітря, що подається в приміщення, на одну людину в годину**
Об'єм до 20$м^3$ на людину	Не менше 30
20... 40 $м^3$ на людину	Не менше 20
Більше 40$м^3$ на людину	Може бути використана природна вентиляція

5.3.2 Освітлення робочого місця

Згідно [15] ця робота відноситься до V_a розряду зорових робіт. Передбачається використання природного, штучного і змішаного освітлення.

Робота, що виконується з використанням обчислювальної техніки, має наступні недоліки: ймовірність появи прямого блиску, погіршена контрастність між зображенням і фоном, відбивання світла від екрану. Необхідно обмежувати нерівномірність розподілу яскравості в полі зору особи, яка працює з відеотерміналом, при цьому відношення значень яскравості робочих поверхонь не повинно перевищувати 3:1, а робочих поверхонь і навколишніх предметів (стіни, обладнання) – 5:1.

Необхідно використовувати систему вимикачів, що дозволяє регулювати інтенсивність штучного освітлення залежно від інтенсивності природного, а також дозволяє освітлювати тільки потрібні для роботи зони приміщення.

Природне світло повинно проникати через вікна, зорієнтовані на південь та схід, і забезпечувати коефіцієнт природної освітленості (КПО) не нижче 1.5%.

Вікна приміщень повинні мати регулювальні пристрої для відкривання, а також жалюзі.

Світильники з люмінесцентними лампами в приміщеннях для роботи рекомендують установлювати в декілька рядів.

Пропонується встановити два світильники в один ряд. Застосовуємо світильники ЛДР з лампами 2 х 40 Вт із загальним потоком 5700 лм.

5.3.3 Вплив шуму та вібрації на користувача ПК

Як було вказано вище, в приміщенні знаходиться одне робоче місце, що обладнане монітором, системним блоком, що має вінчестер та достатньо потужний вентилятор системи охолодження (кулер в блоці живлення складає 25 дБ, кулер процесора – 30 дБ, загальний, – 34 дБ), та клавіатурою. Таким чином, у приміщенні мають місце шуми механічного і аеродинамічного походження. Шум, що створюється роботою ПК у класах, умовно можна віднести до постійного. Сумарний рівень шумового забруднення приміщення трохи перевищує максимально допустимий рівень коригованої звукової потужності і складає більше 50 дБ.

При роботі з персональним комп’ютером в робочому приміщенні значення характеристик вібрації на робочих місцях не повинна перевищувати допустимих значень.

5.3.4 Електробезпека. Статична електрика

Приміщення по небезпеці ураження електричним струмом можна віднести до 1 класу, тобто це приміщення без підвищеної небезпеки (сухе, не пильне, з

нормальною температурою повітря, ізольованими підлогами і малою кількістю заземлених приладів).

На робочому місці користувача ПК з усього наявного устаткування металевим є лише корпус системного блоку комп'ютера, але тут використовуються системні блоки, що відповідають стандарту фірми IBM, у яких крім робочої ізоляції передбачений елемент для заземлення і провід з жилою, що заземлює, для приєднання до джерела живлення.

Електробезпечність у приміщенні лабораторії забезпечується технічними способами і засобами захисту, і так само організаційними і технічними заходами.

Основні причини ураження користувача ПК електричним струмом:

- заборонене використання електричних приладів, таких як електричні плити, чайники, обігрівачі;

- дотик до металевих не струмоведучих частин системного блоку ПЕОМ, які можуть працювати під напругою в результаті ушкодження ізоляції.

Усі струмоведучі частини ЕОМ ізольовані, тому випадковий дотик до струмоведучих частин виключено. Для забезпечення захисту від ураження електричним струмом при дотику до металевих не струмоведучих частин, що можуть виявитися під напругою в результаті ушкодження ізоляції, рекомендовано застосовувати захисне заземлення. Заземлення корпуса ЕОМ забезпечено підведенням жили, що заземлює, до живильних розеток.

Основним організаційним заходом щодо забезпечення електробезпеки є інструктаж і навчання безпечним методам праці, а також перевірка знань правил безпеки й інструкцій.

При проведенні незапланованого і планового ремонту обчислювальної техніки виконуються наступні дії: відключення комп'ютера від мережі та перевірка відсутності напруги. Після виконання цих дій проводиться ремонт несправного устаткування. Якщо ремонт проводиться на струмоведучих частинах,

що знаходяться під напругою, то виконання роботи проводиться не менш ніж двома особами з застосуванням електрозахисних засобів.

5.3.5 Випромінювання

У приміщенні відсутні інфрачервоні, ультрафіолетові та електромагнітні випромінювання, адже усі монітори ПК вироблені на основі рідко-кристалічної матриці, підсвітка якої здійснюється неоновою лампою, що не має сильного електромагнітного випромінювання, і є сертифікованими в Україні.

5.3.6 Шкідливі речовини в повітрі робочої зони

У внутрішньому оздобленні інтер'єру приміщень з ПЕОМ забороняється використання полімерних матеріалів, що не дозволені для застосування органами і установами Державного санітарно епідеміологічного нагляду.

Для захисту від впливу шкідливих речовин в повітрі робочої зони слід використовувати кондиціювання повітря робочого приміщення.

Для нормалізації повітря робочої зони необхідно**:**

- Проводити систематичне провітрювання з використанням кондиціонеру, або вікна, якщо рівень забруднення повітря за вікном не перевищує допустимої норми;
- Проводити вологе прибирання робочої кімнати не рідше двох разів на тиждень, або використовувати зволожувачі повітря;
- Слідкувати за температурою повітря.

5.3.7 Пожежна безпека

Приміщення, яке розглядається, належить до категорії В, так як в даному приміщенні є горючі та важкогорючі матеріали (документація, меблі тощо). Клас

приміщення з пожежонебезпеки — П-IIа, бо в приміщенні є тверді горючі речовини і матеріали [17].

Приміщення обладнане первинними засобами пожежогасіння: вуглекислотний вогнегасник типу ВВ-2 (ємність 2 л), та забезпечено інструкціями щодо його застосування. Кожен вогнегасник має паспорт.

Пристрої ПЕОМ встановлені на достатній відстані від опалювальних і нагрівальних приладів (відстань не менше 1 м і в місцях, де не затруднена їх вентиляція).

5.4 Ергономіка робочого місця користувача ПК

Робоче місце користувача ПК повинне займати площу не меншу за за $6м^2$, висота приміщення повинна бути не менше 3 м. У зв'язку з цим запропоновано організувати робоче місце користувача ПК наступним чином. Висота над рівнем підлоги робочої поверхні, на якій працює користувач, повинна складати 720 мм. Бажано, щоб робочий стіл при необхідності можна було регулювати по висоті в межах 680-780 мм. Оптимальні розміри поверхні столу 1600 х 1000 кв. мм. Під столом повинен бути простір для ніг з розмірами по глибині 650 мм.

Розміщення клавіатури повинно бути у межах 300 мм від краю столу і не більше цього, що забезпечить операторові зручну опору для передпліч.

Відстань між очима користувача й екраном відеодисплея повинна складати 40 - 80 см. Для очей також періодично виконується комплекс вправ для очей. До таких вправ можна віднести наступний комплекс:

1. Часто-часто моргати очима одну-дві хвилини.

2. Прикласти долоні до чола і зробити кілька рухів вниз до підборіддя. Проробити цю вправу 10 разів. Закінчивши її, не поспішати відкривати очі. Сидячи з закритими очима, зосередити свій внутрішній погляд на очних яблуках, на живильних їх судинах. Відкривати очі повільно.

3. Гарненько розігріти долоні, потерши їх одна об одну, скласти їх човниками і потримати напроти очей, не торкаючись до повік, наче прогріваючи очі теплом долонь.

4. При зімкнутих повіках обертати очима за годинниковою стрілкою 20 разів, стільки ж - проти годинникової; потім — 20 разів по горизонталі і стільки ж по вертикалі.

5. Повторити попередню вправу, але вже з відкритими очима.

6. Сфокусувати погляд на кінчику носа, а потім перевести його на який-небудь об’єкт, що знаходиться в двох-трьох метрах від вас, потім — на дальній об’єкт десь у лінії горизонту. Повторити 20 разів.

7. Подушечками трьох пальців — вказівного, середнього та безіменного — дуже-дуже легко натискати на закриті повіки 8-10 разів. Виконувати відразу двома руками.

Вимоги до робочого стільця користувача наступні: стілець повинен бути обладнаний підйомно-поворотним механізмом, висота сидіння повинна регулюватися в межах 400 - 500 мм, а глибина сидіння повинна складати не менш 380 мм, ширина – не менш 400 мм. Висота опорної поверхні спинки не менше 300 мм, ширина – не менше 380 мм.

5.5 Правила роботи з ПК

Перед початком роботи користувач повинен:

- Оглянути робоче місце та за необхідністю привести його в порядок;
- Відрегулювати освітленість робочого місця, усунути недостаток освітленості та блики на екрані, переконатися у відсутності зустрічного світлового потоку;
- Перевірити правильність підключення обладнання в електромережу;

- Протерти спеціальною серветкою поверхню екрана і захисного фільтра;
- Перевірити правильність установки столу, стільця, підставки для ніг, перевірити положення обладнання, кут нахилу екрану, положення клавіатури і, при необхідності, провести регулювання робочого столу і крісла, а також розташування елементів комп'ютера відповідно до вимог ергономіки та з метою уникнення незручних поз і тривалих напруг тіла.

При включенні комп'ютера користувач зобов'язаний дотримуватися наступної послідовності включення обладнання:

- Включити блок живлення;
- Включити периферійні пристрої (якщо вони є);
- Включити системний блок.

Користувачу забороняється приступати до роботи при:

- Відсутності інформації про результати атестації умов праці на даному робочому місці або при наявності інформації про невідповідність параметрів даного обладнання вимогам санітарних норм;
- Виявленні несправності обладнання;
- Відсутності захисного заземлення пристроїв ПЕОМ і ВДТ;
- Відсутності вуглекислотного або порошкового вогнегасника та аптечки першої допомоги;
- Порушення гігієнічних норм розміщення ВДТ (при однорядному розташуванні менше 1 м від стін, при розташуванні робочих місць в

колону на відстані менше 1.5 м, при розміщенні на площі менше 6 кв. м на одне робоче місце, при розміщенні дисплеїв екранами один до одного).

5.6 Висновки

Розглянуті можливі небезпеки та шкідливі чинники, які можуть виникнути під час роботи над розробкою підсистеми.

Виявлено, що приміщення відповідає санітарним нормам [13], – мінімальна площа та об’єм з розрахунку на одну людину повністю задовольняють нормативним значенням, пожежні умови також вимагають вимогам.

Рівні шуму, вібрації та загазованості не перевищують нормативних обмежень.

Для підтримання параметрів мікроклімату в приміщенні розташовано кондиціонер та систему водяного опалення для холодної пори року.

Умови праці відповідають вимогам, але рівень шуму наближається до граничного значення. Для зменшення шумового навантаження рекомендується встановити шумоізолюючі вікна та корпуси персональних комп’ютерів.

ВИСНОВКИ

Проаналізовано технології розпізнавання облич з точки зору надійності та використовуваних компонентів, і виявлені слабкі місця систем розпізнавання облич, а саме: база даних зображень та даних, адже вона піддається злому; також актуальності фотографії, яку занесено до бази даних, адже люди змінюють зовнішність (зачіска, окуляри, вік, наявність волосся на обличчі) і ці фактори впливають на розпізнавання облич, а отже зловмисники можуть використовувати ці фактори для проникнення до системи; якість зображення має немаленьку роль – якісне зображення представляє більше деталей системі розпізнавання; кількості зображень у базі даних – більше зображень з різних ракурсів дає системі чітке уявлення про обличчя людини, і всі зображення разом підробити не так і просто; та апаратури, що використовується – технології розпізнавання облич добре працюють із стандартними відеокамерами, що передають дані та керуються персональним комп'ютером, і потребують роздільчої здатності 320 x 240 пікселів на дюйм при швидкості відеопотоку, принаймні, 3 – 5 кадрів за секунду (більш висока швидкість відеопотоку при більш високій роздільчій здатності веде до покращення якості ідентифікації).

Враховуючи вищенаведені фактори, що впливають на розпізнавання облич, виділено наступні більш надійні методи захисту від спуфінгу, що використовуються на даний момент:

1. Можна використовувати методи на основі виявлення емоцій, моргання та руху очей, адже вони дають змогу захиститись від фото-спуфінгу, хоч вони і не ефективні проти відео-спуфінгу з використанням відео файлів, які містять в собі варіації емоцій, а також рух очей. Методи для визначення емоцій мають значно підвищену складність алгоритмів розпізнавання.

2. Актуальним є метод на основі мультимодальної аутентифікації (наприклад, відбитки пальців та сканування обличчя водночас), що забезпечує

більш ефективний захист, ніж методи для визначення емоцій та моргання. Водночас метод не є складним в реалізації.

3. Мультифакторна аутентифікація, що може не тільки сканувати обличчя людини, а й запросити слово-пароль, наприклад. В такому випадку зловмисникам доведеться не тільки мати зображення для спуфінгу, а й знати паролі, токени та таке інше.

4. Одним з найефективніших методів для визначення «живучості» є метод на основі аналізу спектральних характеристик відображення шкіри. Метод забезпечує надзвичайну точність у визначенні живучості і здатний розрізнити навіть близнюків.

Розроблено програмне забезпечення – 2D система розпізнавання облич. На основі розробленого продукту протестовано надійність, та встановлено, що система не є надійною, адже при представленні фотографій системі 60% результатів система видавала вірних – тобто ідентифікувала людину на фотографії, не «розуміючи» при цьому, що це всього лише фотографія, а не реальна людина.

Отже, розроблена система розпізнавання облич повинна використовуватись разом з іншими технологіями, інакше надійність її невисока.

Враховуючи зручність технологій розпізнавання облич, можна виділити наступні області застосування цих технологій:

1. Ідентифікація облич – системи розпізнавання облич перевіряють присутність самої людини, адже перевірити це неможливо в системах, що перевіряють PIN-коди чи паролі.

2. Контроль доступу (access control) – в системах, де не дуже багато користувачів та при умові якісної фронтальної фотозйомки облич цих користувачів, системи розпізнавання облич можуть досягнути досить непоганого рівня точності та не потребують взаємодії з користувачами. А в поєднанні з

іншими факторами ідентифікації (райдужка ока чи голос) взагалі можна досягнути високого рівня надійності.

3. Безпека – надзвичайно актуальна тема, особливо для аеропортів (пасажирів та персоналу). Такі системи виявляють в натовпі відомих злочинців чи терористів, хоч в таких умовах (великий натовп людей та неможливість контролювання освітлення та повороту голови) провести розпізнавання дуже складно.

4. Спостереження – такі системи отримують зображення облич людей та порівнюють з базою даних шуканих людей (злочинці та правопорушники), в разі виявлення співпадінь персонал системи отримує сигнал. Такі системи мають тукі самі складнощі, як і системи безпеки в аеропортах – неможливо контролювати освітлення, емоції, кут повороту голови.

Вже сьогодні можемо спостерігати надзвичайно високу точність розпізнавання. Наприклад, дослідники Китайської академії наук розробили систему розпізнавання облич, що здатна у натовпі виявити необхідну людину з точністю до 99,8%. Система пізнає людину з 91 різного ракурсу. Попередній рекорд точності у розпізнаванні облич знаходився на рівні 97,6% і належав американській системі.

Все це доводить, що майбутнє за біометричними технологіями є, і при поєднанні з іншими методами аутентифікації можна досягти надзвичайної точності розпізнавання.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методы обнаружения живучести в биометрических системах.: [Електронний ресурс]. – Режим доступу : http://masters.dgtu.donetsk.ua/2013/fknt/fomenko/library/biometric_security.pdf. – Дата доступу : 15.05.2015.

2. Handbook of face recognition.: [Електронний ресурс]. – Режим доступу : http://read.pudn.com/downloads142/ebook/618315/Handbook%20Of%20Face%20Recognition.pdf. – Дата доступу : 15.03.2015.

3. Биометрические методы защиты информации.: [Електронний ресурс]. – Режим доступу : http://stud24.ru/information/biometricheskie-metody-zashhity-informacii/18940-51253-page1.html. – Дата доступу : 10.04.2015.

4. Современные биометрические методы идентификации.: [Електронний ресурс]. – Режим доступу : http://habrahabr.ru/post/126144. – Дата доступу : 05.05.2015.

5. False Acceptance Rate (FAR) & False Recognition Rate (FRR).: [Електронний ресурс]. – Режим доступу : http://www.bayometric.com/blog/false-acceptance-rate-far-false-recognition-rate-frr/. – Дата доступу : 07.05.2015.

6. Live Face Detection Based on the Analysis of Fourier Spectra.: [Електронний ресурс]. – Режим доступу : http://www.nws-sa.com/biometrics/facial/SPIE2004.pdf. – Дата доступу : 15.05.2015.

7. Multimodal Person Recognition using Unconstrained Audio and Video.: [Електронний ресурс]. – Режим доступу : http://www.cs.columbia.edu/~jebara/papers/TR-472.pdf. – Дата доступу : 15.05.2015.

8. On the Computation of Motion from Sequences of Image.: [Електронний ресурс]. – Режим доступу : http://www.dtic.mil/dtic/tr/fulltext/u2/a211479.pdf. – Дата доступу : 15.05.2015.

9. Liveness Detection for Face Recognition System.: [Електронний ресурс]. – Режим доступу : http://ciitresearch.org/dl/index.php/bb/article/view/BB062011002. – Дата доступу : 15.05.2015.

10. Detecting cognitive impairment by eye movement analysis using automatic classification algorithms.: [Електронний ресурс]. – Режим доступу : http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3403832. – Дата доступу : 15.05.2015.

11. Identix Inc. .: [Електронний ресурс]. – Режим доступу : http://www.identix.com. – Дата доступу : 15.05.2015.

12. Liveness detection using cross-modal correlations in face-voice person authentication.: [Електронний ресурс]. – Режим доступу : http://staff.estem-uc.edu.au/html/MWagner/Papers/2005/IS052290.pdf. – Дата доступу : 15.05.2015.

13. ДСанПіН 3.3.2.007-98 Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. – К.: Постанова Головного державного санітарного лікаря України від 10.12.1998 р. №7.

14. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень. – К., 2000.- 16 с.

15. ДБН В.2.5-28:2006 Природнє і штучне освітлення. – К. : Міністерство будівництва, архітектури та житлово-комунального господарства України, 2006. – 68 с.

16. НПАОП 0.00-1.28-10 Правила охорони праці під час експлуатації ЕОМ. – Держгірпромнагляд, № 65 від 26 березня 2010 р.

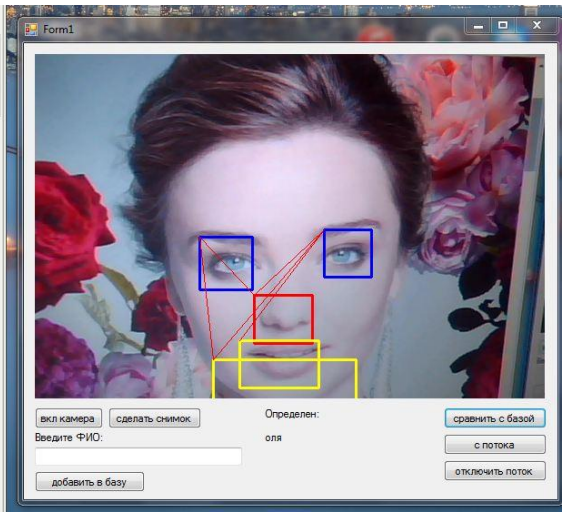
17. НАПБ Б.03.002-2007 Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою.

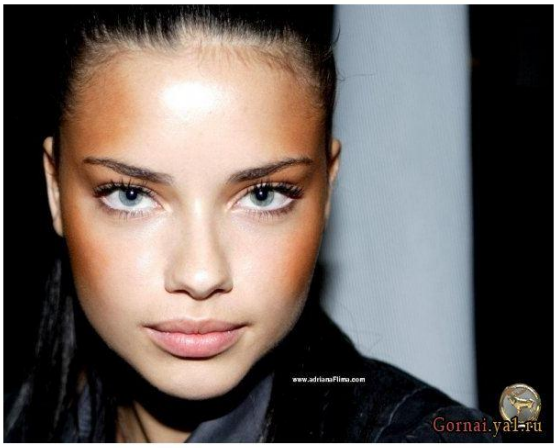
18. Модуль обнаружения витальности лица по спектральным характеристикам отражения кожи человека.: [Електронний ресурс]. – Режим доступу : http://engjournal.ru/articles/925/925.pdf. – Дата доступу : 25.05.2015.

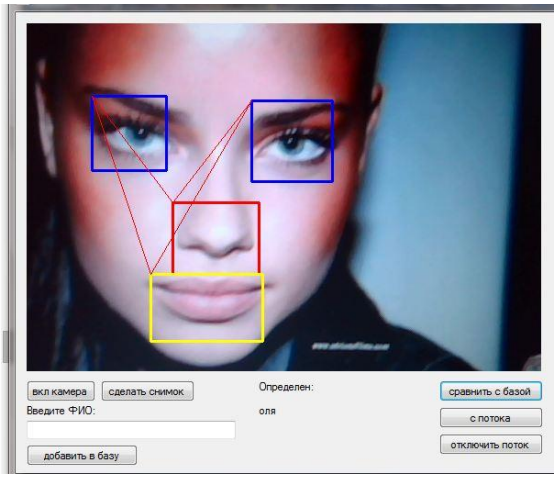
19. Microsoft Visual Studio.: [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/Microsoft_Visual_Studio. – Дата доступу : 01.03.2015.
20. OpenCV.: [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/OpenCV. – Дата доступу : 01.03.2015.
21. OpenCV – описание библиотеки компъютерного зрения.: [Електронний ресурс]. – Режим доступу : http://prog-master.com/opencv-opisanie/. – Дата доступу : 01.03.2015.
22. Признаки Хаара.: [Електронний ресурс]. – Режим доступу : https://ru.wikipedia.org/wiki/Признаки_Хаара. – Дата доступу : 01.03.2015.
23. Метод Виолы-Джонса (Viola-Jones) как основа для распознавания лиц.: [Електронний ресурс]. – Режим доступу : http://habrahabr.ru/post/133826/. – Дата доступу : 10.03.2015.
24. Работа каскада Хаара в OpenCV в картинках: теория и практика.: [Електронний ресурс]. – Режим доступу : http://habrahabr.ru/company/recognitor/blog/228195/. – Дата доступу : 10.03.2015.
25. Viola Jones на собственной шкуре.: [Електронний ресурс]. – Режим доступу : http://habrahabr.ru/post/134857/. – Дата доступу : 10.03.2015.

Додаток А

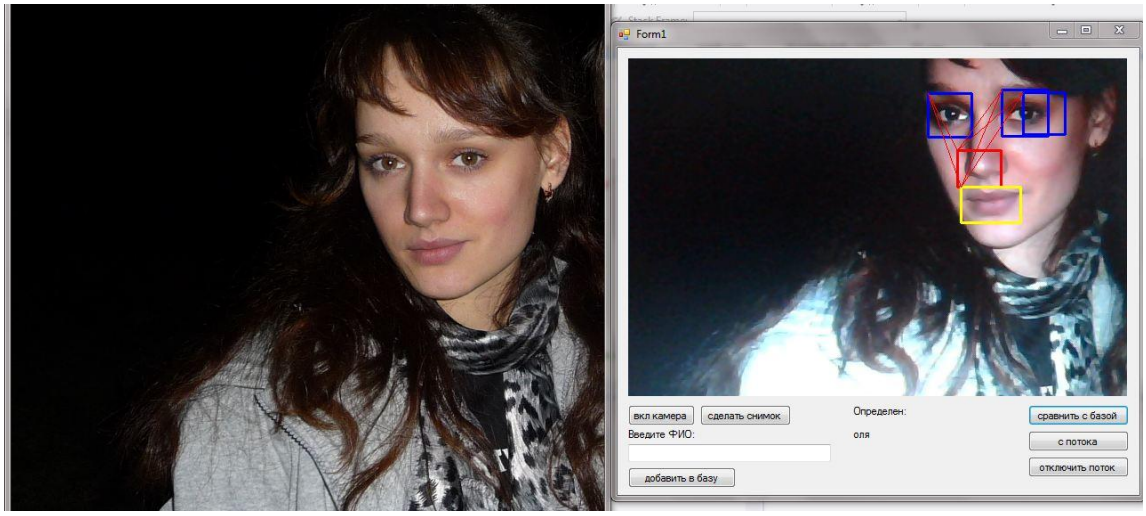
1. Фотографії інших людей, що розпізнані невірно:

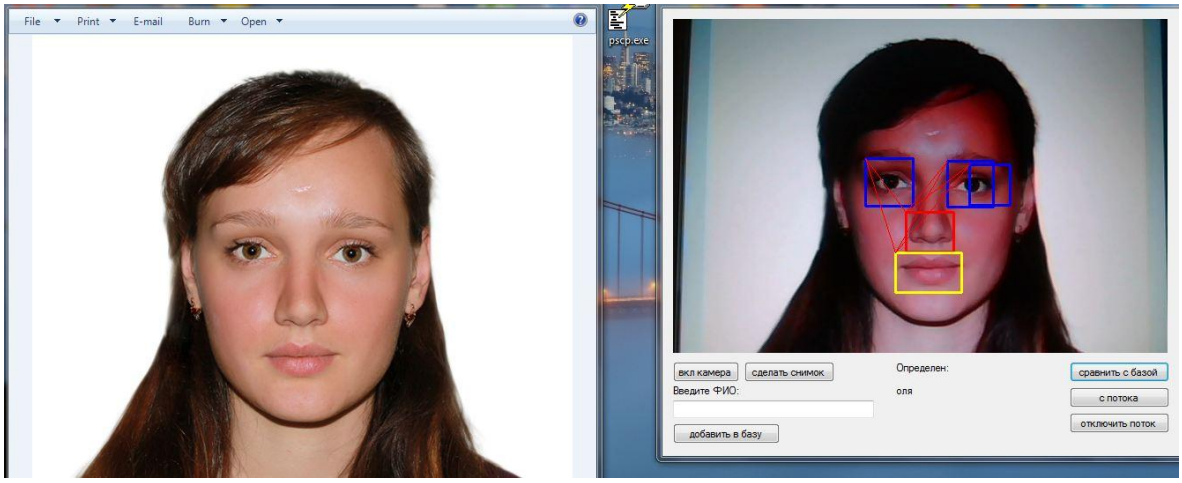




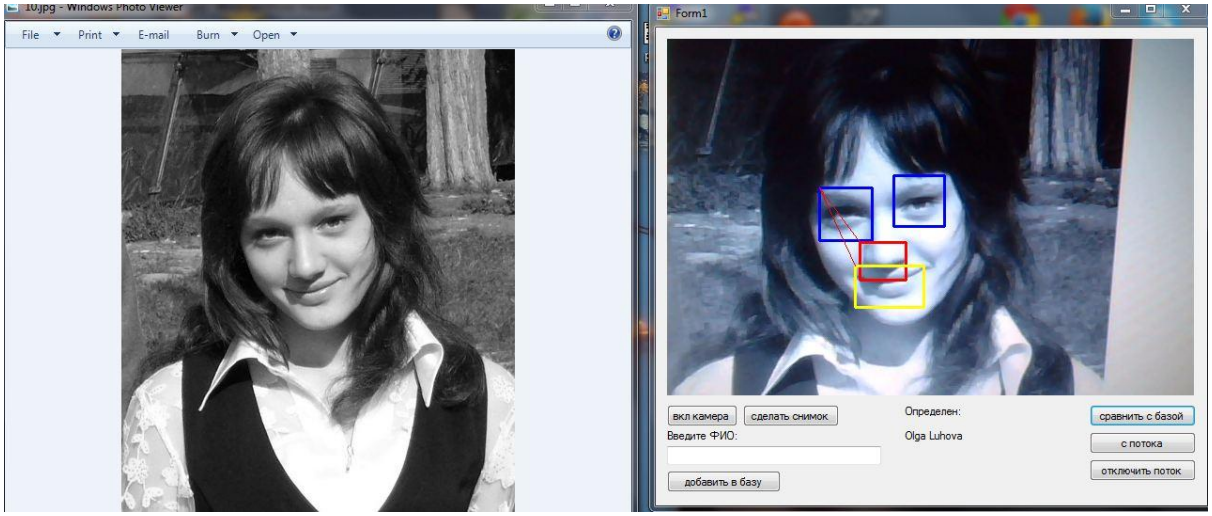


2. Фотографії, що розпізнані вірно, - фото-спуфінг спрацював:

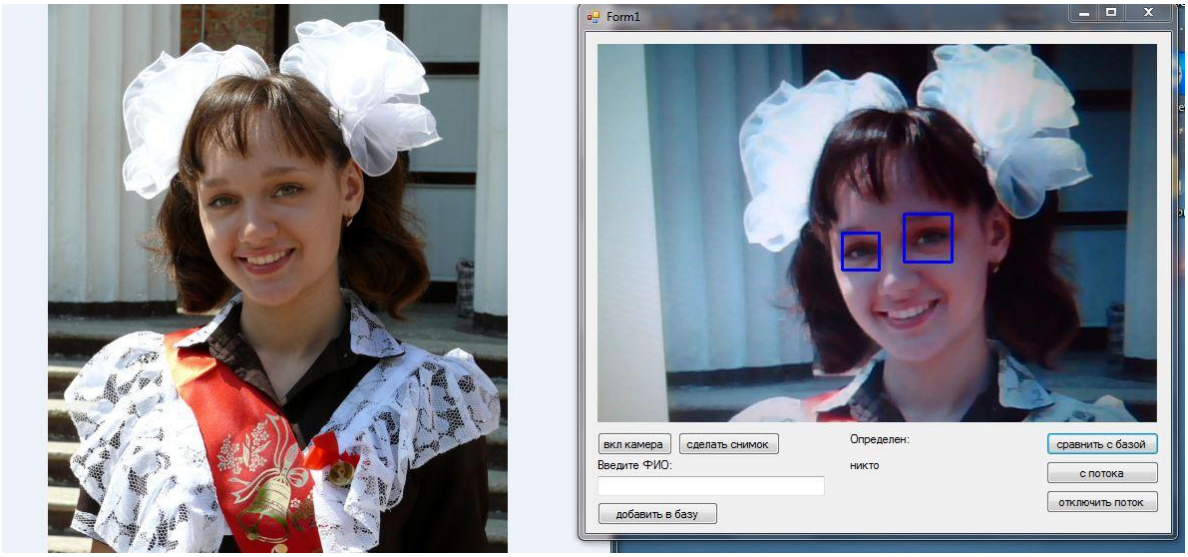


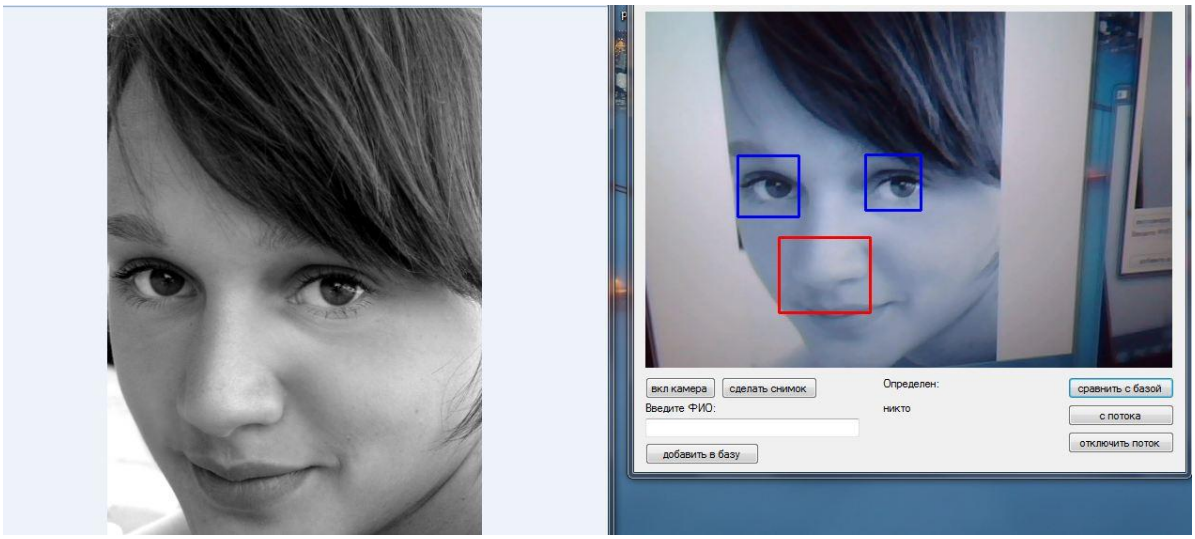


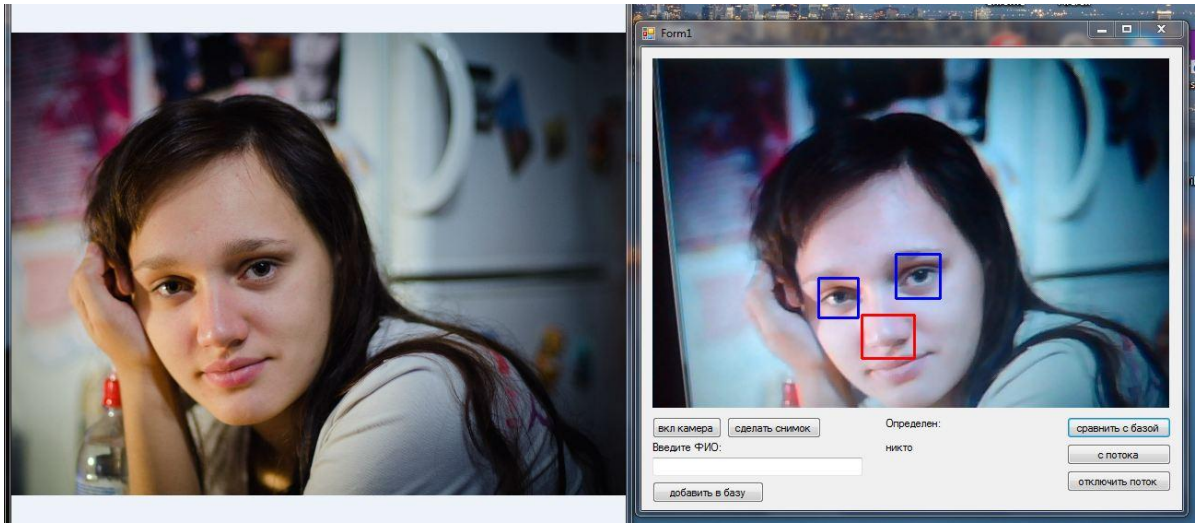

вкл камера
сделать снимок
Введите ФИО:
добавить в базу
Определен:
Olga Luhova
сравнить с базой
с потока
отключить поток

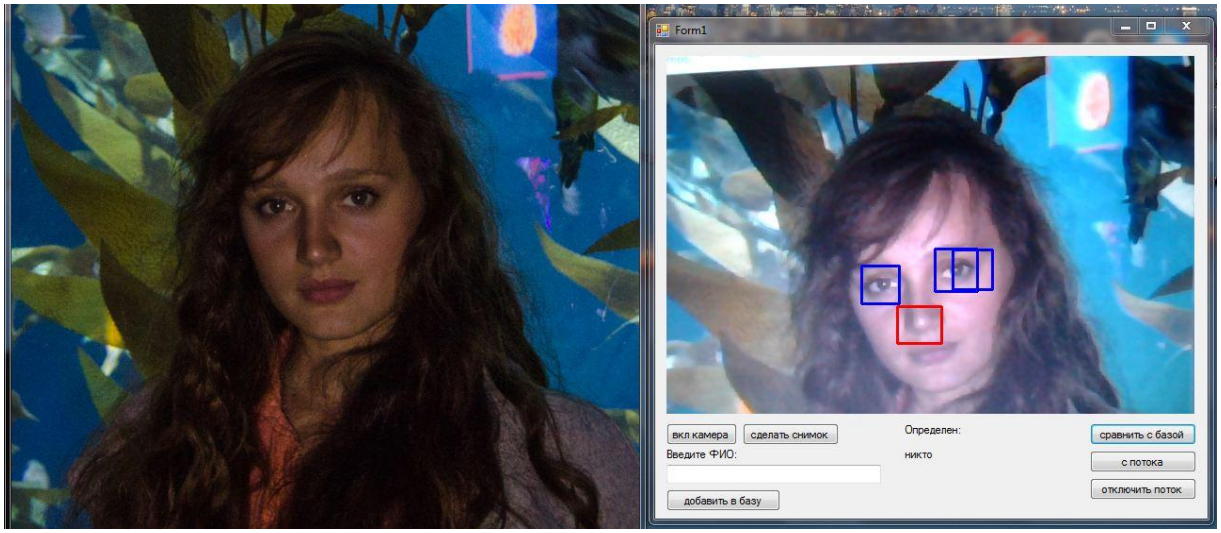

10.jpg - Windows Photo Viewer
File
Print
E-mail
Burn
Open
Form1
вкл камера
сделать снимок
Введите ФИО:
добавить в базу
Определен:
Olga Luhova
сравнить с базой
с потока
отключить поток

3. Фотографії, що розпізнано не було (через наявність емоційного забарвлення обличчя, поворот голови та освітлення):






Form1
вкл камера
сделать снимок
Введите ФИО:
добавить в базу
Определен:
никто
сравнить с базой
с потока
отключить поток


Form1
вкл камера
сделать снимок
Введите ФИО:
добавить в базу
Определен:
никто
сравнить с базой
с потока
отключить поток