МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

Інститут прикладного системного аналізу
(назва факультету, інституту)

Кафедра системного проектування
(назва кафедри)

До захисту допущено

Завідувач кафедри

_____ А.І. Петренко
(підпис) (ініціали, прізвище)

“___”_____200*_р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи) освітньо-кваліфікаційного рівня “ **спеціаліст** ”
(назва ОКР)

з напряму підготовки (спеціальності) _____
(код та назва напряму підготовки або спеціальності)

7.05010103 «Системне проектування».

на тему: «Реалізація технології розпізнавання облич при аутентифікації користувачів в мобільних пристроях»

Студент групи _____ _____ _____
(шифр групи) (прізвище, ім’я, по батькові) (підпис)

Керівник проекту доц. Капшук О.А. _____
(вчені ступінь та звання, прізвище, ініціали) (підпис)

Консультанти:

з технічних вимог ____ к.т.н., доц. Харченко К.В. _
(назва розділу ДП (ДР)) (вчені ступінь та звання, прізвище, ініціали) (підпис)

нормоконтроль _____ к.т.н., доц. Стіканов В.Ю. _____
(назва розділу ДП (ДР)) (вчені ступінь та звання, прізвище, ініціали) (підпис)

Київ – 2017

Національний технічний університет України
“Київський політехнічний інститут”

Факультет (інститут) **Інститут прикладного системного аналізу**.
(повна назва)

Кафедра **Системного проектування**.
(повна назва)

Напрям підготовки **050101, Комп’ютерні науки**.
(код, назва)

Спеціальність **7.05010103 «Системне проектування».**
(код, назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ А.І. Петренко .
(підпис) (ініціали, прізвище)

“___”_____ 2016 р.

ЗАВДАННЯ
на дипломний проект (роботу) освітньо-кваліфікаційного рівня
“спеціаліст” .
(назва рівня)

студенту Савчук Артем Юрійович
(прізвище, ім’я, по батькові)

1. **Тема проекту** (роботи) Реалізація технології розпізнавання облич при аутентифікації користувачів в мобільних пристроях
затверджена наказом по університету від «__»_____ 2016р. №_____

2. **Термін здачі** студентом закінченого проекту (роботи) “15” 01 2017р.

3. **Вихідні дані до проекту** (роботи)

Існуючі технології розпізнавання облич. Методи і алгоритми аутентифікації. Обмеження технічними можливостями мобільних пристроїв: 4 Android, фронтальна кмера 2mp, 200mb ОЗУ.

4. **Перелік питань, які мають бути розроблені**

- Авторизація користувачів мобільних пристроїв.
- Ідентифікація/аутентифікація за допомогою біометричних даних.
- Аналіз існуючих підходів до розпізнавання осіб.
- Розпізнавання осіб за допомогою бібліотеки OpenCV.
- Реалізація техгології розпізнавання обличчя в мобільних пристроях.

5. **Перелік графічного (ілюстративного) матеріалу**

Схема загального алгоритму розпізнавання обличчя (креслення)
UML-діаграма додатку (креслення)
Приклад роботи алгоритму Eigenfaces (1-й плакат)
Таблиця порівнянь методів розпізнавання облич(2-й плакат)
Порівняння методів EigenFaces і FisherFaces(3-й плакат)
Демонстрація роботи додатку(4-й плакат)

.....

6. **Консультанти**

з технічних вимог ____ к.т.н., доц. Харченко К.В. _____ _ _____
(назва розділу ДП (ДР)) (вчені ступінь та звання, прізвище, ініціали) (підпис)

7. **Дата видачі завдання** “ 07 ” 09 2016 р.

Керівник дипломного проекту (роботи) _____ __Капшук О.А.__
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ __Савчук А.Ю.__
(підпис) (ініціали, прізвище)

ЗАТВЕРДЖУЮ

Керівник
дипломного проекту (роботи)
_____ __Капшук О.А._
(підпис) (ініціали, прізвище)

“___”_____2016 р.

КАЛЕНДАРНИЙ ПЛАН-ГРАФІК

виконання дипломного проекту (роботи)

студентом _____Савчук А.Ю._____
(прізвище, ініціали)

№ з/п	Назва етапів роботи та питань, які повинні бути розроблені відповідно до завдання	Термін виконання	Позначки керівника про виконання завдань
1	Ознайомлення з технічною літературою і підготовка теоретичної частини роботи	10.09.2016 – 30.09.2016	
2	Аналіз вимог завдання, вибір методів і засобів розв’язання поставленої задачі	15.10.2016	
3	Огляд та аналіз існуючих рішень	15.11.2016	
4	Створення свого рішення та імплементація мобільного додатку	30.12.2016	
5	Підготовка графічного матеріалу, оформлення пояснювальної записки, підготовка до захисту	05.01.2017	
6	Проходження нормоконтролю, отримання відгуку, рецензії, передача роботи в ДЕК	10.01.2017	
7	Захист дипломної роботи	24.01.2017	

Студент _____
(підпис)

АНОТАЦІЯ

до дипломного проекту (роботи) освітньо-кваліфікаційного рівня “спеціаліст”
Савчука Артема Юрійовича

на тему: «Реалізація технології розпізнавання облич при аутентифікації користувачів в мобільних пристроях»

Дипломна робота присвячена дослідженню та аналізу методів аутентифікації користувачів, та дослідження використання технології розпізнавання обличчя, у якості одного з методів аутентифікації на мобільних пристроях.

Було розроблено систему для аутентифікації користувачів на мобільних пристроях завдяки розпізнаванню обличчяю. У процесі були використані насутпні середовища, інструменти та засоби: Microsoft Visual Studio, C++, OpenCV.

Загальний об’єм роботи 83 сторінки, 30 рисунків, 1 таблиця, 14 посилань

ABSTRACT

of a specialist degree work, which made by Savchuk Artem Yuriyovych

on theme: “Implementation of face recognition technology while user authentication on mobile devices”

This work is devoted to research and analyze user authentication methods, and research the use of technology for face recognition, as one of the authentication methods on mobile devices.

As result, developed an approach of system for user authentication on mobile devices by face recognition. The process was used such environment, instruments and tools: Microsoft Visual Studio, C++, OpenCV.

The total amount of work 83 pages, 30 figures, 1 table, 14 references

ЗМІСТ

Перелік умовних позначень, символів, скорочень і термінів

Скорочення:

- ПЗ – Програмне забезпечення;
- CV – Computer Vision;
- ГР – Гральний рушій;
- ц.р. – Цього року
- HDFS – Hadoop Distributed File System
- GFS – Google File System, Файлова система Google

Терміни:

- Ідентифікація - це процес розпізнавання системою або людиною (криміналістом, дослідником, операційною системою тощо) іншої системи або об'єкта (людини, користувача, предмету, процесу тощо);
- Аутентифікація - процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора.
- Біометрія - це методи автоматичної аутентифікації людини і підтвердження особистості людини, засновані на фізіологічних або поведінкових характеристик. Прикладами фізіологічних характеристик є відбитки пальців, форма руки, характеристика особи, райдужна оболонка ока. До поведінкових характеристик належать особливості характерні риси, або придбані або з'явилися з часом, тобто динаміка підпису, ідентифікація голосу, динаміка натискання на клавіші.
- Нативний інтерфейс – інтерфейс, який відповідає деяким звичаям та правилам оформлення конкретної платформи.

ВСТУП

В даний час активно розвиваються біометричні технології, спрямовані на отримання та використання біометричних даних людини з метою його ідентифікації. Системи, використовують такі технології, які можуть застосовуватися в різних галузях інформаційної безпеки: системи паспортного контролю в аеропортах та інших великих транспортних системах електронної торгівлі, системах спостереження для зниження терористичних загроз і розшуку людей. Істотною перевагою розпізнавання по обличчю перед іншими біометричними методами є можливість ідентифікації на відстані. Створення системи розпізнавання зображень, що характеризуються високою розмірністю простору ознак, є актуальною для вирішення завдань ідентифікації особистості та аналізу психофізичного стану людини. В даний час проблеми ідентифікації графічних образів присвячено безліч робіт (багато з яких базуються на нейромережевих методах), однак в цілому вона ще далека від вирішення.

Областю використання розпізнавання обличь у цій роботі стане аутентифікація користувача. Автоматична ідентифікація особистості людини завдяки його зображенню на фотографії або у відеопотоці має широке комерційне і наукове застосування. Дана тематика з'явилася на початку 80-х років, однак, її бурхливий розвиток почався в 90-х, після створення нових технологій у сфері обробки зображень і обчислювальних машин. Дана технологія має особливий інтерес у зв'язку з тим, що може відбуватися безконтактно.

З кожним зареєстрованим в комп'ютерній системі суб'єктом (користувачем або процесом, чинним від імені користувача) пов'язана деяка інформація, що однозначно ідентифікує його. Це може бути число або рядок символів, які називають даний суб'єкт. Цю інформацію називають ідентифікатором суб'єкта. Якщо користувач має ідентифікатор, зареєстрований в мережі, він вважається легальним (законним) користувачем; інші користувачі, які відносяться до нелегальних користувачам. Перш ніж отримати доступ до ресурсів комп'ютерної системи, користувач повинен пройти процес первинного

взаємодії з комп'ютерною системою, що включає ідентифікацію та аутентифікацію.

Мета дипломної роботи – дослідити існуючі методи розпізнавання обличчя, та досягти можливості використання одного з методів на мобільному пристрої, як спосіб аутентифікації користувача.

Для досягнення мети були поставлені наступні завдання:

- Зробити огляд існуючих методів аутентифікації;
- Розглянути існуючі методи розпізнавання обличь;
- Виділити методи розпізнавання обличь, базуючись на обмеженнях мобільних пристроїв.
- Реалізувати метод аутентифікації обличь, базуючись на проведеному аналізі.
- Розробити мобільний додаток із аутентифікацією користувача завдяки розпізнаванню його обличчя.

Об’єкт дослідження – дослідження методів аутентифікації та методів розпізнавання обличь.

Предмет дослідження – мобільний додаток із реалізованим прикладом роботи розпізнавання обличчя у якості методу аутентифікації.

Актуальність дипломної роботи – Задача розпізнавання осіб стає все більш актуальною. Є безліч місць, де доцільно застосувати системи розпізнавання осіб. Найбільш відомими областями застосування є безпека та криміналістика. Але існують і інші області застосування. Наприклад, у сфері соціальних мереж дану технологію можна застосувати автоматичного виділення і підписання людей на фотографіях. Дана технологія вкрай важлива і для робототехніки, і у військовій справі, оскільки дозволить поділяти людей на «свій» – «чужий» або поділяти на класи за рівнем доступу. Використання розпізнавання обличчя у якості способу аутентифікаці користувача є актуальною, так як обличчя є досить вагомим і унікальним критерієм аутентифікаціїї.

1 АВТОРИЗАЦІЯ КОРИСТУВАЧІВ МОБІЛЬНИХ ПРИСТРОЇВ

Ідентифікацію та аутентифікацію можна вважати основою програмно-технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів. Ідентифікація і аутентифікація - це перша лінія оборони, "прохідна" інформаційного простору організації.

Ідентифікація дозволяє суб'єкту (користувачу, процесу, чинним від імені визначеного користувача, чи іншого апаратно-програмного компоненту) назвати себе (повідомити своє ім'я). За допомогою аутентифікації друга сторона пересвідчується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова "аутентифікація" іноді використовують словосполучення "перевірка автентичності"[1].

Аутентифікація буває односторонньою (зазвичай клієнт доводить свою справжність сервера) і двосторонній (взаємний). Приклад односторонньої аутентифікації - процедура входу користувача в систему.В мережевому середовищі, коли сторони ідентифікації/аутентифікації територіально рознесені, у розглянутого сервісу є два основних аспекти:

- що служить аутентифікатором (тобто використовується для підтвердження достовірності суб'єкта);
- як організований (і захищений) обмін даними дентифікації/аутентифікації.
- Суб'єкт може підтвердити свою автентичність, пред'явивши принаймні одну з таких сутностей:
- що він знає пароль, особистий ідентифікаційний номер, криптографічний ключ тощо);
- щось, чим він володіє (особисту картку або інший пристрій аналогічного призначення);

щось, що є частиною його самого (голос, відбитки пальців тощо, тобто свої біометричні характеристики)[3].

У відкритій мережі між сторонами ідентифікації/аутентифікації не існує довіреної маршруту; це означає, що у загальному випадку дані, передані суб'єктом, можуть не співпадати з даними, одержаними та використаними для автентифікації. Необхідно забезпечити захист від пасивного й активного прослуховування мережі, тобто від перехоплення, зміни та/або відтворення даних. Передача паролів у відкритому вигляді, очевидно, незадовільна; не рятує становище і шифрування паролів, так як воно не захищає від відтворення. Потрібні більш складні протоколи аутентифікації.

Надійна ідентифікація і ускладнена не тільки з-за мережевих загроз, але і по цілому ряду причин. По-перше, майже всі аутентифікаційні сутності можна дізнатися, вкрасти або підробити. По-друге, є протиріччя між надійністю аутентифікації, з одного боку, і зручностями користувача та системного адміністратора з іншого. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно вводити аутентификационную інформацію (адже на його місце міг сісти інша людина), а це не тільки клопітно, але і підвищує ймовірність того, що хтось може підглянути за введенням даних. По-третє, чим надійніше засіб захисту, тим воно дорожче. Сучасні засоби ідентифікації/аутентифікації повинні підтримувати концепцію єдиного входу у мережу. Єдиний вхід в мережу - це, в першу чергу, вимога зручності для користувачів. Якщо в корпоративній мережі багато інформаційних сервісів, що допускають незалежне звернення, то багаторазова ідентифікація/аутентифікація стає занадто обтяжливою. На жаль, поки не можна сказати, що єдиний вхід в мережу став нормою, домінуючі рішення поки не сформувалися. Таким чином, необхідно шукати компроміс між надійністю, доступністю за ціною і зручністю використання і адміністрування засобів ідентифікації та автентифікації. Цікаво відзначити, що сервіс ідентифікації / аутентифікації може стати об'єктом атак на доступність. Якщо система налаштована так, що після певного числа невдалих спроб пристрій введення ідентифікаційної інформації (таке, наприклад, як термінал) блокується, то зловмисник може зупинити роботу легального користувача буквально декількома натисканнями клавіш[2].

1.1 Парольна аутентифікація

Головне достоїнство парольного аутентифікації - простота і звичність. Паролі давно вбудовані в операційні системи та інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Тим не менш, за сукупністю характеристик їх слід визнати самим слабким засобом перевірки автентичності.

Щоб пароль був незабутнім, його часто роблять простим (ім'я подруги, назва спортивної команди тощо). Однак простий пароль неважко вгадати, особливо якщо знати пристрасті даного користувача. Відома класична історія про радянського розвідника Ріхарда Зорге, об'єкт уваги якого через слово говорив "карамба"; зрозуміло, цим же словом відкривався надсекретний сейф[4].

Іноді паролі з самого початку не зберігаються в таємниці, так як мають стандартні значення, вказані в документації, і далеко не завжди після установки системи проводиться їх зміна.

Пароль можна підглянути. Іноді для підглядання використовуються навіть оптичні прилади.

Паролі нерідко повідомляють колегам, щоб ті могли, наприклад, підмінити на деякий час власника пароля. Теоретично в подібних випадках більш правильно задіяти засоби управління доступом, але на практиці так ніхто не надходить; а таємниця, яку знають двоє, це вже не таємниця.

Пароль можна вгадати "методом грубої сили", використовуючи, скажімо, словник. Якщо файл паролів зашифрований, але доступний для читання, його можна завантажити собі на комп'ютер і спробувати підібрати пароль, запрограмувавши повний перебір (передбачається, що алгоритм шифрування відомий).

Тим не менш, такі заходи дозволяють значно підвищити надійність парольного захисту:

- накладення технічних обмежень (пароль повинен бути не занадто коротким, він повинен містити букви, цифри, знаки пунктуації тощо);

- управління строком дії паролів, їх періодична зміна;
- обмеження доступу до файлу паролів;
- обмеження числа невдалих спроб входу в систему (це ускладнить застосування "методу грубої сили");
- навчання користувачів;
- використання програмних генераторів паролів (така програма, ґрунтуючись на нескладних правил, може породжувати тільки милозвучні і, отже, запам'ятовуються паролі).

Перераховані заходи доцільно застосовувати завжди навіть якщо поряд з паролями використовуються інші методи аутентифікації.

1.1.1 Одноразові паролі

Розглянуті вище паролі можна назвати базовими; їх розкриття дозволяє зловмисникові діяти від імені легального користувача. Набагато більш сильним засобом, стійким до пасивного прослуховування мережі, є одноразові паролі.

Найбільш відомим програмним генератором одноразових паролів є система S/KEY компанії Bellcore. Ідея цієї системи полягає в наступному. Нехай є одностороння функція f (тобто функція, обчислити зворотну якої за прийнятний час не представляється можливим). Ця функція відома і користувачеві, і сервером аутентифікації. Нехай, далі, є секретний ключ K, відомий тільки користувачеві[4].

На етапі початкового адміністрування користувача функція f застосовується до ключа K n разів, після чого результат зберігається на сервері. Після цього процедура автентифікації користувача виглядає наступним чином:

- сервер надсилає на власну систему число (n-1);
- користувач застосовує функцію f до секретного ключа K (n-1) раз і відправляє результат по мережі на сервер аутентифікації;
- сервер застосовує функцію f до отриманого від користувача значенням і порівнює результат із раніше збереженої величиною. У разі збігу справжність користувача вважається встановленою, сервер запам'ятовує

нове значення (прислане користувачем) і зменшує на одиницю лічильник (n).

Насправді реалізація влаштована трохи складніше (крім лічильника, сервер посилає затравочное значення, яке використовується функцією f), але для нас зараз це не важливо. Оскільки функція f незворотна, перехоплення пароля, так само як і отримання доступу до сервера аутентифікації, не дозволяють дізнатися секретний ключ K і передбачити наступний одноразовий пароль.
Система S/KEY має статус Internet-стандарту (RFC 1938).

Інший підхід до надійної аутентифікації полягає в генерації нового пароля через невеликий проміжок часу (наприклад, кожні 60 секунд), для чого можуть використовуватися програми або спеціальні інтелектуальні карти (з практичної точки зору такі паролі можна вважати одноразовими). Сервера аутентифікації повинен бути відомий алгоритм генерації паролів та асоційовані з ним параметри; крім того, годинник клієнта і сервера повинні бути синхронізовані.

1.1.2 Сервер аутентифікації Kerberos

Kerberos - це програмний продукт, розроблений у середині 1980-х років в Массачусетському технологічному інституті і зазнав відтоді ряд принципових змін. Клієнтські компоненти Kerberos присутні в більшості сучасних операційних систем.

Kerberos призначений для вирішення наступного завдання. Є відкрита (незахищена) мережа, у вузлах якої зосереджені суб'єкти - користувачі, а також клієнтські і серверні програмні системи. Кожен суб'єкт володіє секретним ключем. Щоб суб'єкт C міг довести свою автентичність суб'єкту S (без цього S не стане обслуговувати C), він повинен не лише назвати себе, але і продемонструвати знання секретного ключа. C не може просто послати S свій секретний ключ, по-перше, тому, що мережа відкрита (доступна для пасивного й активного прослуховування), а, по-друге, тому, що S не знає (і не повинен

знати) секретний ключ C. Потрібно менш прямолінійний спосіб демонстрації знання секретного ключа.

Система Kerberos являє собою надійну третю сторону (тобто сторону, якій довіряють всі), що володіє секретними ключами обслуговуються суб'єктів і допомагає їм у попарної автентифікації.

Щоб з допомогою Kerberos отримати доступ до S (зазвичай це сервер), C (як правило - клієнт) посилає Kerberos запит, що містить інформацію про нього (клієнта) і про запитуваної послуги. У відповідь Kerberos повертає так званий квиток, зашифровані секретним ключем сервера, і копію інформації з квитка зашифровані секретним ключем клієнта. Клієнт повинен розшифрувати другу порцію даних та надіслати її разом з квитком сервера. Сервер, розшифрувавши квиток, може порівняти його вміст за додатковою інформацією, надісланою клієнтом. Збіг свідчить про те, що клієнт зміг розшифрувати призначені йому дані (адже вміст квитка нікому, крім сервера і Kerberos, недоступне), тобто продемонстрував знання секретного ключа. Отже, клієнт - саме той, за кого себе видає. Підкреслимо, що секретні ключі в процесі перевірки автентичності не передавалися по мережі (навіть у зашифрованому вигляді) - вони використовувалися тільки для шифрування. Як організований первинний обмін ключами між Kerberos і суб'єктами і як суб'єкти зберігають свої секретні ключі - питання окреме[3].

1.1.3 Ідентифікація/аутентифікація за допомогою біометричних даних

Біометрія (англ. Biometrics) — технологія ідентифікації особи, яка використовує фізіологічні параметри суб'єкта (відбитки пальців, райдужна оболонка ока тощо) (Вікіпедія)

Біометричні технології активно застосовуються в багатьох областях пов'язаних із забезпеченням безпеки доступу до інформації та матеріальним об'єктам. З метою цифрової ідентифікації особистості багато держави в найближчій перспективі планують ввести в обіг паспорти з біометричними даними. Наведемо лише деякі приклади, що свідчать про цих процесах.

В рамках безвізової програми США підписала з 27 країнами угоду, за якою громадяни цих держав зможуть в'їжджати на територію США строком до 90 днів без візи за наявності біометричних документів. Початок дії програми - 26 жовтня 2005.

Британський уряд має намір з 2008 року видавати візи з біометричними даними тим іноземцям, які мають намір в'їхати до Великобританії для роботи, навчання або проживання на строк більше шести місяців. Для цього по всьому світу будуть організовані 150 центрів для сканування біометричних даних.

Україна також не стоїть осторонь від застосування біометричних даних при вирішенні певних завдань.

Постановою Кабінету Міністрів України від 9 листопада 2004 року № 1500 на виконання Указу Президента України від 30 квітня 2004 року № 500 «Про створення Єдиного державного реєстру фізичних осіб» (в даний момент зазначені Постанова Кабінету Міністрів України та Указу Президента України недійсні) була затверджена Концепція створення Єдиного державного реєстру фізичних осіб, яка передбачала, як основи побудови інформаційного забезпечення цього Реєстру, використання даних біометричної ідентифікації і машиносчитывающей інформації[3].

Концепція створення Єдиного державного реєстру фізичних осіб дала визначення терміну «біометрична ідентифікація», як способу підтвердження особи, належності паспорта його власникові-шляхом розпізнавання і зіставлення, зафіксованих носіями біометричної інформації біометричних даних (кольору очей, малюнка сітківки ока, відбитків пальців, геометрії руки, а також малюнка особи).

23-го лютого 2007 року Верховна Рада України 233 голосами народних депутатів ухвалила Постанову Верховної Ради України «Про внесення змін у Постанову Верховної Ради України «Про затвердження положень про паспорт громадянина України та свідоцтва про народження», яким затверджується «Положення про паспорт громадянина України для виїзду за кордон».

Цим «Положенням про паспорт громадянина України для виїзду за кордон» передбачається внесення відомостей до сторінки даних паспорта шляхом лазерного гравірування та лазерної перфорації. Крім того, передбачається, що додаткова інформація (зокрема біометрична) про власника паспорта, зміст якої визначається чинним законодавством, може відображатися безконтактним електронним носієм, який вмонтований в паспорт.

Однак необхідно зауважити, що прийняте зазначена Постанова Верховної Ради України створює певну юридичну колізію – одночасно діє і Указ Президента України «Про внесення змін до Положення про паспорт громадянина України для виїзду за кордон та визнання такими, що втратили чинність, деяких указів Президента України» від 10 березня 2005 року № 457, положення якого не передбачають застосування при виготовленні закордонних паспортів ні лазерного гравіювання, ні лазерної перфорації, ні додаткової інформації (зокрема біометрична) про власника паспорта, крім як, на прохання громадянина України, даних про його місце проживання, номера телефону, а також групи крові і резус-факторі[5].

15 грудня 2006 року 255-ма голосами народних депутатів України Верховна Рада України прийняла в першому читанні проект Закону України «Про Національний демографічний регістр». У статті 9 «Інформація регістру» цього проекту Закону України передбачається, що у разі прийняття Верховною Радою України відповідних рішень, внесення в паспорт громадянина України для виїзду за кордон і біометричних даних особи, а також застосування біометричної інформації для ідентифікації особи на електронному носії (мікрочип), який передбачається вмонтувати в правий форзац документа. Також цей законопроект передбачає використання високотехнологічних методів виготовлення документів, у тому числі і лазерне гравіювання та лазерної перфорації.

Існуючі процедури біометричної ідентифікації особистості умовно можна розділити на два класу.

Перший клас - це статичні методи, побудовані на аналізі статичних образів; до них відносяться системи ідентифікації особистості по геометрії руки, папилярному малюнку пальця, по особливостям райдужної оболонки ока, з геометричним параметрам особи і т. д.

Другий клас - це динамічні методи ідентифікації особистості, побудовані на аналізі динаміки відтворення складних підсвідомих рухів; до них, наприклад, відносяться методи ідентифікації по голосу, підписи, особливостям клавіатурного почерку.

Існують промислові системи, що охоплюють обидва названих підходу, наприклад, пропонована компанією Motorola повнофункціональна цифрова система Omnitrak. У цій комплексній системі біометричної можуть зберігатися самі різні зображення: відбитки пальців і долонь, фотознімки осіб, зразки підписів, опису громадян, з яких знято відбитки пальців, а також різні документи: заяви про прийом на роботу, паспортні дані, дані кримінальних розслідувань і т. д.

1.1.3.1 Сучасні методи статичної біометричної ідентифікації

Статичні методи біометричної ідентифікації особистості ґрунтуються на невід'ємних фізіологічних характеристиках людини, даних йому від народження. До цих методів належать:

• Аналіз відбитків пальців. В основі цього методу лежить унікальність для кожної людини малюнка паппілярних візерунків на пальцях. Дана технологія є найбільш поширеною серед всіх біометричних методів.

Компанія NEC розробила сенсор для розпізнавання відбитків пальців, вірогідність помилки (false acceptance rate, FAR) якого – менше однієї десятимилионной, що на два порядки краще, ніж у поширених в даний час сенсорів.

Компанія Microsoft розпочала продаж USB-пристрою розпізнавання відбитку пальця "Fingerprint Reader". Новинка сумісна з усіма версіями операційної системи Windows XP, включаючи Media Center Edition і Tablet PC

Edition, її вартість $75. Пристрій "Fingerprint Reader дозволяє асоціювати відбиток пальця з паролями користувача і використовувати його для швидкого доступу, наприклад, до веб-сайтів, які вимагають введення пароля, або ж для швидкої зміни користувача, у разі якщо комп'ютером користуються кілька осіб і т. д[5].

Компанія APC також представила біометричний менеджер паролів (Biometric Password Manager) - персональний сканер відбитків пальців, полегшує користувачам комп'ютерів керування персональними паролями. Біометричний менеджер паролів запам'ятовує до двадцяти еталонів відбитків пальців, що дозволяє зберігати паролі двадцяти користувачів на одній комп'ютерній системі. Для ідентифікації користувачеві досить прикласти до пристрою палець. У комплект постачання включений кабель USB завдовжки 1,8 м і сумісний з операційними системами Windows (XP, ME, 2000 і 98) програмне забезпечення, що дозволяє зберігати необмежену кількість імен користувачів і паролів.

• Аналіз форми долоні. Даний метод, побудований на геометрію кисті руки. За допомогою спеціального пристрою будується тривимірний образ кисті руки, по якому формується згортка і розпізнається особистість. Наприклад, пристрій під назвою «Biometric Hand Reader» IR Recognition Systems одночасно аналізує більш 31,000 точок руки і виробляє більше 90 вимірювань руки, визначаючи відповідність людини і його ID. Така процедура займає менше секунди і здійснює ідентифікацію з високим ступенем точності.

• Аналіз форми особи. У даному методі ідентифікації будується тривимірний образ особи, виділяються контури брів, очей, носа, губ і т. д. Компанія Lenovo розпочала постачання індійським покупцям нових ноутбуків Y300 і Y500. Ноутбуки оснащені вбудованою системою біометричної ідентифікації Veriface. Зазначена система ідентифікує господаря ноутбука по його обличчю. Моментальне фото хазяїна перетворюється в цифрову карту" особи власника ноутбука, і вона перетворюється в "пароль" для доступу в Windows і прикладні програми. Таким чином, самі паролі власнику ноутбука ні

створювати, ні тим більше запам'ятовувати і постійно вводити не потрібно. Міністерство внутрішньої безпеки США (The U. S. Department of Homeland Security, DHS) схвалило стандарт по особовому розпізнавання, розроблений, щоб відповідати міжнародним біометричних стандартам, що використовується в таких додатках, як проїзні документи.

• Аналіз запаху. Не так давно хіміки з Лестерського університету розробили пристрій, здатний розпізнавати людей і місцевість по запаху. Електронний ніс зможе дізнатися марку парфумів або визначити "власника" дихання або запаху тіла менш ніж за хвилину, аналізуючи леткі органічні сполуки і порівнюючи їх з наявними в базі даних. Таким чином, до набору біометричних даних про людину додався ще один параметр - "відбиток запаху".

1.1.3.2 Динамічна ідентифікація – ідентифікація психологічна

Динамічні методи біометричної ідентифікації особистості ґрунтуються на поведінковій характеристиці людини, тобто побудовані на особливостях, характерних для підсвідомих рухів в процесі якої-небудь дії. Динамічні біометричні процедури ідентифікації особистості ґрунтуються на аналізі підписів, особливостей голосу, клавіатурного почерку, інших ознаках складних підсвідомо керованих рухів.

Привабливою рисою систем динамічної ідентифікації є те, що вони здатні паралельно з ідентифікацією оцінювати поточний психічний стан особистості. Динаміка підпису і динаміка відтворення голосом ключової фрази істотно змінюється, наприклад, при сп'янінні або при попаданні особистості в стресовий стан. З цієї причини динамічні методи розглядається як психологічні. Розглянемо деякі з цих методів:

• Аналіз почерку. Як правило, для цього виду ідентифікації людини використовується його підпис. Аналізується як сама підпис (ступінь схожості накреслень), так і динамічних характеристик написання. Наприклад, вчені з Римського університету, які проводили роботи під керівництвом Джузеппе Ширрипа Спаньоло, розробили тривимірну технологію аналізу рукописних

написів, що дозволяє з дуже високою точністю ідентифікувати автора документа або підпису. Система виявляється мікроскопічні поглиблення, залишені ручкою на папері, і "ямки", що утворюються в місцях перетину ліній. У результаті може бути складений своєрідний "портрет" підпису. Далі, порівнюючи досліджуваний зразок напису " з оригіналом, можна без зусиль виявити підробку. Зокрема, точність розпізнавання в ході експериментів досягла 90 відсотків в загальному випадку і 100%, коли мова йшла про написи, зробленої кульковою ручкою на папері.

• Аналіз клавіатурного почерку. Основною характеристикою, за якою будується згортка для ідентифікації – динаміка набору кодового слова;

• Аналіз голоси. При цьому аналізуються різні поєднання частотних і статистичних характеристик голосу.

• Аналіз енцефалограми. В процесі електроенцефалографічного дослідження визначається область і інтенсивність електричних імпульсів тривалістю в кілька мілісекунд в мозку пацієнта. Система здійснює моніторинг електричної активності мозку і відсилає інформацію по бездротовому зв'язку на комп'ютер. Далі формується своєрідний цифровий портрет користувача. При подальшій ідентифікації знімається электроэнцефалограмма порівнюється з раніше записаної, і комп'ютер робить висновок про особистість людини.

• Інші методи, в яких застосовується, наприклад, тривимірне моделювання руху. У банку данського містечка Альсгарде під час грабежу один з двох злочинців вбив відвідувача. Система охоронного телебачення DigiEye зареєструвала подія. Однак, незважаючи на реєстрацію зображень, поліція не змогла відразу ідентифікувати грабіжників, які були в капюшонах. Була використана нова технологія, яка поєднує зображення, отримані з допомогою видеоохранной системи і фотограмметрическое програмне забезпечення PhotoModeler. Методика фотограмметричних вимірювань генерує точні 3D моделі і точні вимірювання пропорцій тіла з зображень охоронного телебачення. Анімація реберних моделей людей, дає можливість з'ясувати, чи є пропорції тіла і руху підозрюваного ідентичними пропорціям тіла і руху

зловмисника. Доказ, забезпечене фотограмметрическими зображеннями PhotoModeler дозволило знайти і покарати злочинців.

1.3.3.3 Області застосування

Можна назвати деякі з великого списку областей застосування методів біометричної ідентифікації:

• Паспорти, перевірка громадян, що в'їжджають в країну. Наприклад, США розширюють застосування програми оцінки автоматизованих процедур біометричної перевірки від'їжджаючих «US-VISIT» відносно іноземних громадян.

Іноземці, які відбувають із США, повинні пройти реєстрацію в якості виїжджають у спеціальних реєстраційних кабінках. Як і при проходженні процедури реєстрації при в'їзді, при проходженні процедури перевірки в'їжджають буде проводитися контроль їх проїзних документів, електронне сканування двох відбитків вказівних пальців в реєстраційній кабінці та виготовлення цифрового фотографічного знімка, після цього в'їжджають отримають друковану квитанцію про проходження реєстрації. Міністерство внутрішньої безпеки США повідомило, що сформована в рамках програми US-VISIT база відбитків пальців претендентів американських віз включає відомості про 70 млн. чоловік[5].

• Корпоративні системи ідентифікації співробітників. Близько 1300 співробітників Пентагону користуються системою ідентифікації за відбитками пальців U. are.U Pro компанії DigitalPersona Inc. в рамках пілотного проекту, який був ініційований відділом інформаційних технологій Міністерства Безпеки США. Зареєстровані користувачі входять допомогою одного відбитка пальця у вісім різних захищених програм, наприклад, у програму бухгалтерського обліку. Також біометрична система компанії DigitalPersona використовується для надання доступу користувачам Common Access Cards для підпису електронних документів і роботи з електронною поштою. Заявки в службу забезпечення з приводу проблем з паролями знизилися на 90%, у той

час як відсоток звернень у службу з приводу біометричної ідентифікації, склав лише 0,05%. Компанія Ingersoll Rand Security Technologies оголосила про чергове впровадженні розробленої нею біометричної системи обліку робочого часу. Російський біометричний портал Biometrics.ru з посиланням на прес-реліз Ingersoll Rand Security Technologies повідомляє, що згадана система функціонує в офісі ізраїльської фірми DBtell, яка спеціалізується у сфері телемаркетингу та надає замовникам послуги колл-центру.

• Охоронні системи. Компанія bioMETRX приступила до виконання замовлень на нові біометричні термінали контролю доступу в гаражі. Для ідентифікації користувачів терміналу використовуються відомості про відбитки їх пальців. Вже в першому кварталі 2007 р. bioMETRX планує відвантажити споживачам, дистриб'юторам і рітейлерам до 30 тисяч біометричних терміналів. Великий замовлення отримано від найбільшої мережі Home Depot, серйозний інтерес до новинки проявляють три провідних виробників гаражних воріт. Обсяг продажів біометричних терміналів на 2007 рік в цілому оцінюється в 150 тисяч штук. Південнокорейські виробники стільникових телефонів останнім часом охоче оснащують свої апарати системою розпізнавання відбитків пальців. Система задумана таким чином, що відбитки пальців є ключиком для доступу до телефону. Оскільки відбитки пальців унікальні для кожної людини, то вважається, що така система безпеки телефону дуже надійна. Однак, насправді ж будь-хто, хто володіє паролем, зможе отримати доступ до телефону (Російський біометричний портал).

• Платіжні системи. Компанія Brown Investments оголосила про випуск нового платіжного кіоску серії Pinnacle, однією з ключових функцій якого є ідентифікація користувача за відбитками пальців. Крім відбитків пальців, кіоск може дізнаватися клієнтів і за іншими ідентифікаторами, приймати чеки, встановлювати їх справжність і навіть за невелику комісію випускати платіжну дебетову карту, рахунок якої буде дорівнює сумі чека.

• Медичні системи. Незабаром працівники локомотивних та поїзних бригад РЖД, обслуговуючих поїзні рейси, будуть відправлятися в дорогу,

маючи на руках персоніфіковані флеш-карти, що містять повну інформацію про стан здоров'я та результати передрейсових медичних оглядів. Медична інформація на флеш-карті структуровано за такими розділами: інформація для екстрених ситуацій (група крові і резус-фактор, алергічні реакції, телефони лікарів, номер страхового поліса, оперативні втручання, поточні призначення тощо); основна інформація (поліклінічний і стаціонарний епікризи на момент останніх відвідувань медичних закладів) про стан пацієнта з можливістю швидкого переходу до первинних результатами обстежень (рентгенівським знімкам, ЕКГ тощо); повна медична карта пацієнта; для локомотивних бригад у картці містяться дані передрейсових обстежень.

• Освіта. Британське управління кваліфікаційних випробувань та навчальних планів розповсюдило доповідь на тему "Цифрові технології і шахрайства на іспитах і тестах". Доповідь було підготовлено групою експертів університету Nottingham Trent і в якості ключових рекомендацій містить висновки про необхідність розширити застосування технологій біометричної ідентифікації та нанотехнологій. Голова групи експертів Джин Ундервуд зазначає, що поряд з інтернет-плагіатом і активним використанням засобів мобільного зв'язку на іспитах ще одним видом шахрайства під час різних випробувань стає имперсонализация - участь в тестах одних людей замість інших. Як вважає Ундервуд, єдиним способом підтвердити ідентичність того, хто повинен проходити тест, і того, хто справді з'явився на тестування, служить біометрична ідентифікація.

• Гральний бізнес. Іллінойс стане першим американським штатом, де запроваджується обов'язкова ідентифікація особистості клієнтів казино при вході. Ця процедура повинна захистити гральні будинки від відвідувань патологічних гравців. Сканування штрих-кодів на документах дозволяє звірити дані клієнта з базою даних про небажані гравців і громадян. Таким чином, автоматично відбувається відсів малолітніх бажаючих зіграти у «дорослі» ігри - тих, хто молодше двадцяти одного року.

1.2 Висновки

Біометричні технології використовуються вже понад 20 років. Проте учасники ринку безпеки продовжують уважно стежити за їх розвитком, а також прогнозувати: як інновації в області біометрії можуть вплинути на вигляд індустрії протягом найближчих 10 років.

З часів перших дактилоскопічних зчитувачів (які досі асоціюються з ідентифікацією злочинців, а також зі скепсисом користувачів про те, що зчитувач неважко "обдурити") з'явився цілий ряд технологій на базі різних ідентифікаторів (райдужна оболонка ока, малюнок вен, обличчя, голос). Сьогодні у керівників є з чого вибирати (за співвідношенням достовірність якість надійність швидкодія, вартість) з урахуванням особливостей вирішуваних завдань.

У той час як дактилоскопічні зчитувачі традиційно знаходяться на нижньому щаблі цінової шкали біометричних технологій, вони забезпечують і менш точний результат, тому призначені для використання на об'єктах з невисоким ризиком небезпеки і в системах з великою кількістю користувачів.

Системи на базі технології розпізнавання особи - на другому місці за часткою ринку. Їх вартість вище, але і рівень точності роботи системи краще. Перевагами рішень на основі цього ідентифікатора є лояльне ставлення до них з боку користувачів і відносна простота інтеграції з іншими системами, наприклад відеоспостереженням. Перед розробниками стоїть завдання забезпечити можливість коригувати шаблони біометричної характеристики з плином часу, щоб відобразити, зокрема, вікові зміни людини.

Тому у виконанні даної роботи задачею є реалізація методу розпізнавання обличчя.

2 ЗАСТОСУВАННЯ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ В СИСТЕМАХ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

2.1 Передмова

Розпізнавання обличь — практичне застосування теорії розпізнавання образів, в завдання якого входить автоматична локалізація особи на фотографії і, у разі необхідності, ідентифікація особи по обличчю. Функцію ідентифікації людей на фотографіях вже активно використовують у програмному забезпеченні для керування фотоальбомами (Picasa, iPhoto і ін).

Завдання ідентифікації і розпізнавання осіб – це одна з перших практичних завдань, яка стимулювала становлення і розвиток теорії розпізнавання та ідентифікації об'єктів. Існує дев'ять категорій об'єктів, які відповідають гностичним областях і викликають зорові образи:

- об'єкти, якими можна маніпулювати (чашка, ключі, годинники тощо);
- об'єкти, якими можна частково маніпулювати (автомобілі, матеріали тощо);
- об'єкти не керовані (дерева, будівлі і т. д.);
- особи;
- вирази осіб;
- живі істоти (тварини, фігура людини);
- друковані знаки (літери, символи, знаки);
- рукописні зображення;
- характеристики та розташування джерел світла (місяць, сонце).

Інтерес до процедур, що лежить в основі процесу впізнавання, розпізнавання осіб, завжди був значним, особливо у зв'язку із зростаючими практичними потребами: охоронні системи, верифікація, криміналістична експертиза, телеконференції і т. д. Незважаючи на ясність того життєвого факту, що людина добре ідентифікує обличьчя людей, зовсім не очевидно, як навчити ЕОМ проводити цю процедуру, в тому числі як декодувати і зберігати цифрові зображення осіб. Ще менш ясними є оцінки схожості осіб, включаючи

їх комплексну обробку. Можна виділити кілька напрямків досліджень проблеми розпізнавання осіб:

- нейропсихологические моделі;
- нейрофізіологічні моделі;
- інформаційно – процесуальні моделі;
- комп'ютерні моделі розпізнавання.

Проблема розпізнавання осіб розглядалася ще на ранніх стадіях комп'ютерного зору. Ряд компаній протягом більше 40 років активно розробляють автоматизовані, а зараз автоматичні системи розпізнавання людських обличь: Smith & Wesson (система ASID – Automated Suspect Identification System); ImageWare (система FaceID); Imagis, Epic Solutions, Spillman, Miros (система Trueface); Vissage Technology (система Vissage Gallery); Visionics (система FaceIt)[6].

Технології розпізнавання осіб дозволяють проводити автоматичний пошук і розпізнавання осіб в графічних файлах і відеопотоці.

Основні характеристики:

- можливість пошуку і розпізнавання декількох осіб;
- стійкість до змін в зачісці, наявності/відсутності вусів і бороди, очками (крім сонцезахисних), віковим змінам (крім дітей), поворотів (до 30 градусів)
- практично лінійна масштабованість продуктивності при установці на багатопроцесорні, багатоядерні системи та комп'ютерні кластери;
- можливість прив'язки до зображень ключових слів (наприклад, «політик», «бізнесмен» і т. д.) і короткого опису для подальшої автоматичної класифікації оброблюваного контенту;
- можливість багатокадрового аналізу відеопотоку, що забезпечує підвищення точності розпізнавання;

- виведення результатів розпізнавання у вигляді простого тексту, або XML-документа, що включає інформацію про стан і розмірі знайдених осіб, результати розпізнавання і тимчасових мітках;
- слабка залежність швидкості роботи від розміру використовуваної галереї осіб. Наприклад, при збільшенні галереї зі 100 до 1000 осіб, швидкість роботи зменшується менш ніж на 10%;
- робота з відео в режимі реального часу.

2.2 Історія розвитку розпізнавання образів

Розглянемо коротко математичний формалізм розпізнавання образів. Об'єкт в розпізнаванні образів описується сукупністю основних характеристик (ознак, властивостей). Основні характеристики можуть мати різну природу: вони можуть братися з упорядкованого безлічі типу речовій прямий, або з дискретного безлічі (яке, втім, так само може бути наділене структурою). Таке розуміння об'єкта узгоджується як потребою практичних додатків розпізнавання образів, так і з нашим розумінням механізму сприйняття об'єкта людиною. Дійсно, ми вважаємо, що при спостереженні (вимірі) об'єкта людиною, відомості про нього надходять з кінцевого числа сенсорів (аналізованих каналів) у мозок, і кожному сенсору можна зіставити відповідну характеристику об'єкта. Крім ознак, відповідних наших вимірів об'єкта, існує виділений ознака або група ознак, які ми називаємо класифікуючими ознаками, і в з'ясуванні їх значень при заданому векторі X і складається задача, яку виконують природні і штучні системи розпізнавання[7].

Зрозуміло, що для того, щоб встановити значення цих ознак, необхідно мати інформацію про те, як пов'язані відомі ознаки з класифікуючими. Інформація про цій зв'язку задається у формі прецедентів, тобто безлічі описів об'єктів з відомими значеннями класифікують ознак. І з цієї прецедентної інформації і потрібно побудувати вирішальне правило, яке буде ставити безпідставного опису об'єкта значення його класифікують ознак.

Таке розуміння задачі розпізнавання образів затвердилося в науці починаючи з 50-х років минулого століття. І тоді ж було помічено що така постановка зовсім не є новою. З подібним формулюванням стикалися і вже існували цілком не погано зарекомендували себе методи статистичного аналізу даних, які активно використовувалися для багатьох практичних завдань, таких як, наприклад, технічна діагностика. Тому перші кроки розпізнавання образів пройшли під знаком статистичного підходу, який і диктував основну проблематику.

Статистичний підхід ґрунтується на ідеї, що початкове простір об'єктів являє собою ймовірнісний простір, а ознаки (характеристики) об'єктів являють собою випадкові величини задані на ньому. Тоді завдання дослідника даних полягала в тому, щоб з деяких міркувань висунути статистичну гіпотезу про розподіл ознак, а точніше про класифікують залежно ознак від решти. Статистична гіпотеза, як правило, представляла собою параметрично задану безліч функцій розподілу ознак. Типовою і класичної статистичної гіпотезою є гіпотеза про нормальність цього розподілу (різновидів таких гіпотез статистики придумали безліч). Після формулювання гіпотези залишалося перевірити цю гіпотезу на прецедентних даних. Це перевірка полягала у виборі деякого розподілу із початково заданого безлічі розподілів (параметра гіпотези про розподіл) та оцінки надійності(довірчого інтервалу) цього вибору. Власне ця функція розподілу і була відповіддю до задачі, тільки об'єкт класифікувався вже не однозначно, але з певними ймовірностями приналежності до класів. Статистиками було розроблено так само і ассимптотическое обґрунтування таких методів. Такі обґрунтування робилися за наступною схемою: встановлювався деякий функціонал якості вибору розподілу (довірчий інтервал) і показувалося, що при збільшенні числа прецедентів, наш вибір з імовірністю прагне до 1 ставав вірним у сенсі цього функціоналу (довірчий інтервал прагнув до 0). Забігаючи вперед скажемо, що статистичний погляд на проблему розпізнавання виявився досить плідним не тільки в сенсі розроблених алгоритмів (в число яких входять методи кластерного, дискримінантного

аналізів, непараметрична регресія тощо), але і привів згодом Вапника до створення глибокої статистичної теорії розпізнавання.

Тим не менше існує серйозна аргументація на користь того, що задачі розпізнавання образів не зводяться до статистики. Будь-яку таку задачу, в принципі, можна розглядати зі статистичної точки зору і результати її рішення можуть інтерпретуватися статистично. Для цього необхідно лише припустити, що простір об'єктів задачі є ймовірнісним. Але з точки зору інструменталізму, критерієм вдалості статистичної інтерпретації деякого методу розпізнавання може слугувати лише наявність обоснавания цього методу на мові статистики як розділу математики. Під обоснаванием тут розуміється вироблення основних вимог до задачі які забезпечують успіх у застосуванні цього методу. Однак на даний момент для більшої частини методів розпізнавання, в тому числі і для тих, які безпосередньо виникли в рамках статистичного підходу, подібних задовільних обґрунтувань не знайдено. Крім цього, найбільш часто вживані на даний момент статистичні алгоритми, типу лінійного дискримінанта Фішера, парзеновского вікна, ЕМ-алгоритм, метод найближчих сусідів, не кажучи вже про байєсівських мережах довіри, мають сильно виражений евристичний характер і можуть мати інтерпретації відмінні від статистичних. І нарешті, до всього вищесказаного варто додати, що крім асимптотичної поведінки методів розпізнавання, яке і є основним питанням статистики, практика розпізнавання ставить питання обчислювальної і структурної складності методів, які виводять далеко за межі однієї лише теорії ймовірностей.

Отже, всупереч прагненням статистиків розглядати розпізнавання образів як розділ статистики, у практику та ідеологію розпізнавання входили зовсім інші ідеї. Одна з них була викликана дослідженнями в області розпізнавання зорових образів і базується на такій аналогії.

Як вже зазначалося, в повсякденному житті люди постійно вирішують (часто несвідомо) проблеми розпізнавання різних ситуацій, слухових і зорових образів. Подібна здатність для ЕОМ являє собою в кращому випадку справа майбутнього. Звідси деякими піонерами розпізнавання образів був зроблений

висновок, що вирішення цих проблем на ЕОМ має в загальних рисах моделювати процеси людського мислення. Найбільш відомою спробою підійти до проблеми з цього боку було знамените дослідження Ф. Розенблатта за перцептронам.

До середини 50-х років здавалося, що нейрофізіологами були зрозумілі фізичні принципи роботи мозку (у книзі "Новий Розум Короля" знаменитий британський фізик-теоретик Р. Пенроуз цікаво ставить під сумнів нейромережеву модель мозку, обґрунтовуючи істотну роль у його функціонуванні квантовомеханических ефектів; хоча, втім, ця модель піддавалася сумніву з самого початку. Відштовхуючись від цих відкриттів Ф. Розенблатт розробив модель навчання розпізнаванню зорових образів, названу ним персептроном. Персептрон Розенблатта являє собою таку функцію (рис.2.2.1):

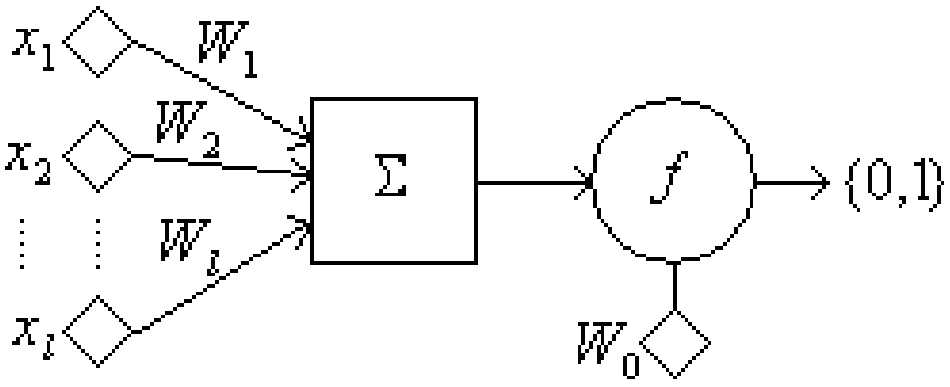


Рис – 2.2.1 Схема Персептрона

На вході персептрон отримує вектор об'єкта, який в роботах Розенблатта представляв собою бінарний вектор, який показував який з пікселів екрана зачернен зображенням а який ні. Далі кожен з ознак подається на вхід нейрона, дія якого являє собою просте множення на деякий вага нейрона. Результати подаються на останній нейрон, який їх і складає загальну суму порівнює з деяким порогом. Залежно від результатів порівняння вхідний об'єкт X визнається належним чином, або ні. Тоді завдання навчання розпізнаванню образів полягала в такому виборі ваг нейронів і значення порога, щоб

персептрон давав на прецедентних зорових образах правильні відповіді. Розенблатт вважав, що отримана функція буде непогано розпізнавати потрібний зоровий образ навіть якщо вхідного об'єкта і не було серед прецедентів. З біонічних міркувань їм так само був придуманий і метод підбору ваг і порога, на якому зупинятися ми не будемо. Скажемо лише, що його підхід виявився успішним у ряді задач розпізнавання і породив собою цілий напрям досліджень алгоритмів навчання, заснованих на нейронних мережах, окремим випадком яких є персептрон.

Далі були придумані різні узагальнення персептрона, функція нейронів була ускладнена: нейрони тепер могли не тільки множити вхідні числа або складати їх і порівнювати результат з порогами, але застосовувати по відношенню до них більш складні функції. На рисунку 1.2.2 зображено одне з подібних ускладнень нейрона:

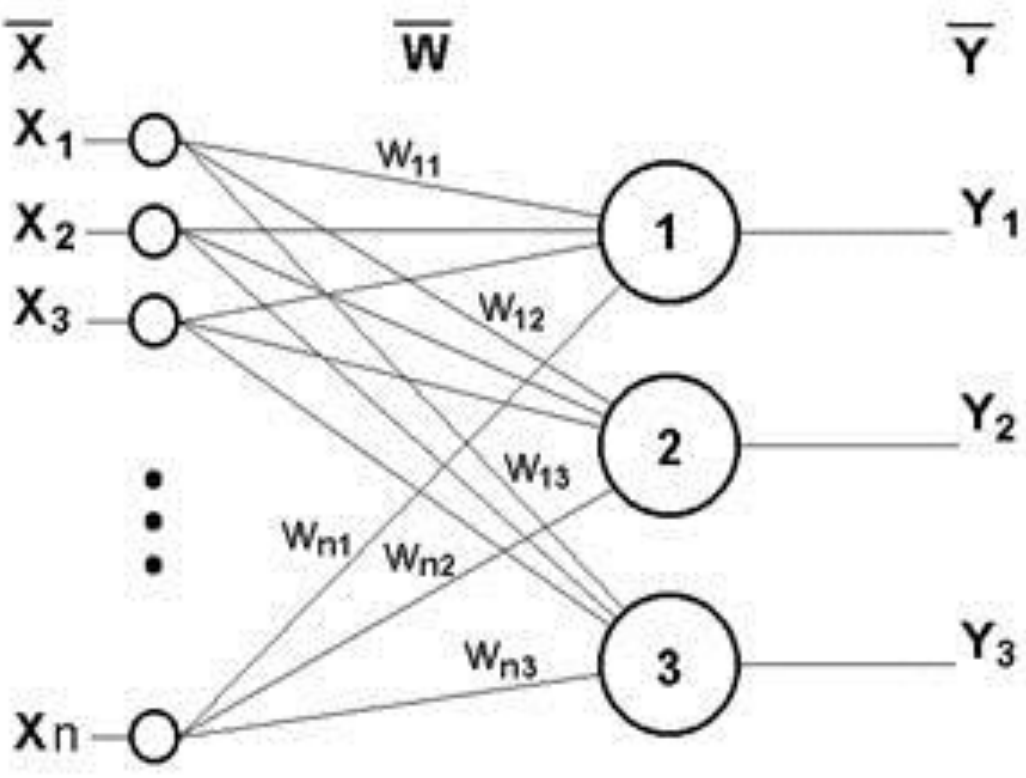


Рис – 2.2.2 Схема нейронної мережі.

Ускладнення приводили до збільшення числа параметрів при навчанні, але при цьому збільшували можливість налаштовуватися на дуже складні закономірності. Дослідження в цій області зараз йдуть за двома тісно

пов'язаним напрямками - вивчаються і різні топології мереж і різні методи налаштувань[8].

Нейронні мережі на даний момент є не тільки інструментом вирішення задач розпізнавання образів, але отримали застосування в дослідженнях по асоціативної пам'яті, стиску зображень. Хоча цей напрям досліджень і сильно перетинається з проблематикою розпізнавання образів, але являє собою окремий розділ кібернетики. Для розпізнавання на даний момент, нейронні мережі не більше ніж дуже специфічно певне, параметрично задана множина відображень, яке в цьому сенсі не має яких-небудь істотних переваг над багатьма іншими подібними моделями навчання які далі будуть коротко перераховані.

У зв'язку з даною оцінкою ролі нейронних мереж для розпізнавання (тобто не для біоніки, для якої вони мають першорядне значення вже зараз) хотілося б відзначити наступне: нейронні мережі, будучи надзвичайно складним об'єктом для математичного аналізу, при грамотному їх використанні, дозволяють знаходити досить нетривіальні закони даних. Їх складність для аналізу, в загальному випадку, пояснюється їх складною структурою і як наслідок, практично невичерпними можливостями для узагальнення різних закономірностей. Але ці достоїнства, як це часто і буває, є джерелом потенційних помилок, можливості перенавчання. Як буде розказано далі, такий двоякий погляд на перспективи будь-якої моделі навчання є одним з принципів машинного навчання.

Ще одним популярним напрямком в розпізнаванні є логічні правила і дерева рішень. У порівнянні з вищезгаданими методами розпізнавання ці методи найбільш активно використовують ідею вираження наших знань про предметну область у вигляді, ймовірно самих природних (на свідомому рівні) структур - логічних правил. Під елементарним логічним правилом мається на увазі висловлювання типу «якщо неклассифицируемые ознаки знаходяться в співвідношенні X то класифікуються знаходяться в співвідношенні Y». Прикладом такого правила в медичній діагностиці служить наступне: якщо вік

пацієнта вище 60 років і раніше він переніс інфаркт, то операцію не робити - ризик негативного результату великий.

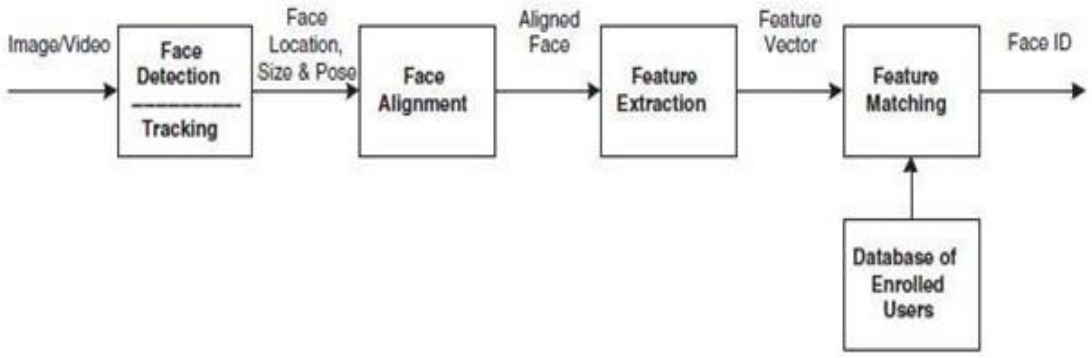
Для пошуку логічних правил в даних необхідні 2 речі: визначити міру «інформативності» правила і простір правил. І задача пошуку правил після цього перетворюється в задачу повного або часткового перебору в просторі правил з метою знаходження найбільш інформативних з них. Визначення інформативності може бути введено різними способами і ми не будемо зупинятися на цьому, вважаючи що це теж певний параметр моделі. Простір же пошуку визначається стандартно.

Після знаходження досить інформативних правил настає фаза «складання» правил кінцевий класифікатор. Не обговорюючи глибоко проблеми, які тут виникають, а їх виникає чимала кількість) перерахуємо 2 основних способи «складання». Перший тип - лінійний список. Другий тип – зважене голосування, коли кожному правилом ставиться у відповідність деякий вагу, і об'єкт відноситься класифікатором до того класу за який проголосувала найбільша кількість правил.

Насправді, етап побудови правил і етап «складання» виконуються спільно і, при побудові зваженого голосування або списку, пошук правил на частинах прецедентних даних викликається знову і знову, щоб забезпечити найкраще узгодження даних і моделі[9].

2.3 Аналіз існуючих підходів до розпізнавання осіб

Незважаючи на велику різноманітність представлених алгоритмів, можна виділити загальну структуру процесу розпізнавання осіб (рис 2.3)



Face recognition processing flow.

Рис – 2.3 Загальний процес обробки зображення особи при розпізнаванні

На першому етапі проводиться виявлення і локалізація особи на зображенні. На етапі розпізнавання проводиться вирівнювання зображення особи (геометричне та яркістне), обчислення ознак і безпосередньо розпізнавання – порівняння обчислених ознак із закладеними в базу даних еталонами. Основною відмінністю всіх представлених алгоритмів буде обчислення ознак і порівняння їх сукупностей між собою.

2.3.1 Метод гнучкого порівняння на графах

Суть методу зводиться до еластичному зіставлення графів, що описують зображення осіб. Особи представлені у вигляді графів зі зваженими вершинами та ребрами. На етапі розпізнавання один з графів – еталонний – залишається незмінним, в той час як інший деформується з метою найкращої підгонки до першого. У подібних системах розпізнавання графи можуть являти собою як прямокутну сітку, так і структуру, утворену характерними (антропометричними) точками особи.

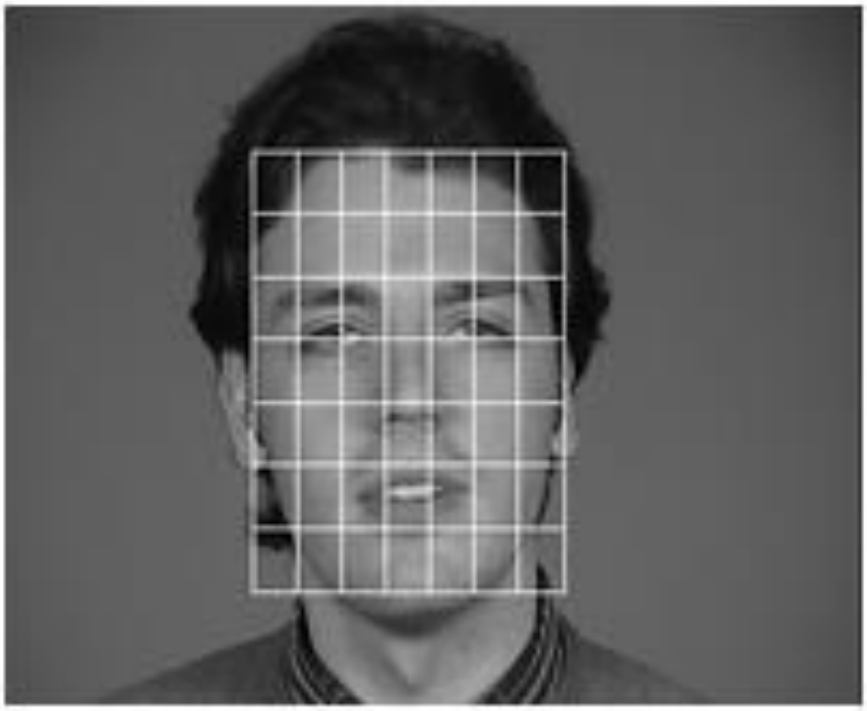


Рис – 2.3.1.1 Регулярна решітка

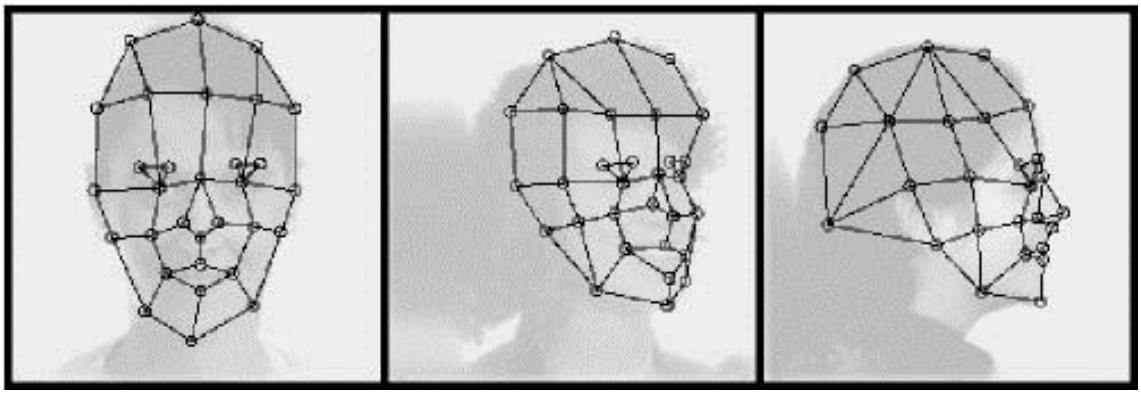


Рис – 2.3.1.2 граф на основі антропометричних точок обличчя.

У вершинах графа обчислюються значення ознак, найчастіше використовують комплексні значення фільтрів Габора або їх впорядкованих наборів – Габоровских вейвлет (строї Габора), які обчислюються у деякої локальної області вершини графа локально шляхом згортки значень яскравості пікселів з фільтрами Габора (Рис 1.3.1.3).

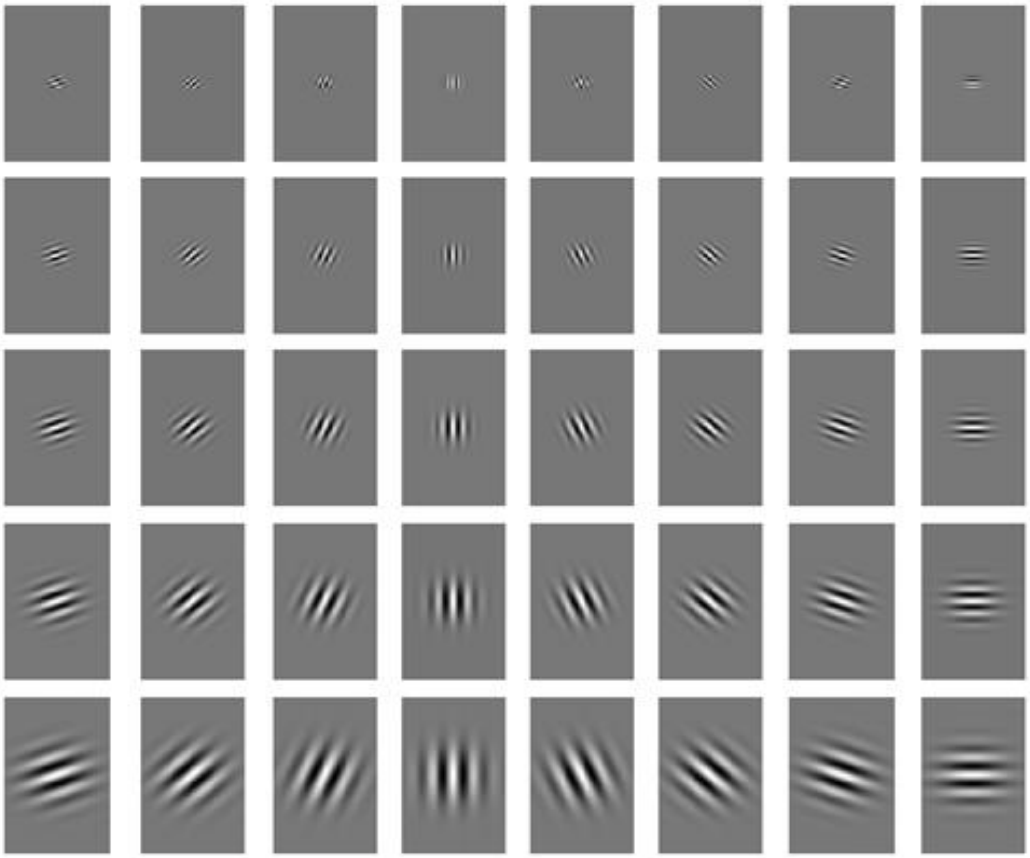


Рис - 2.3.1.3 Набір фільтрів Габора

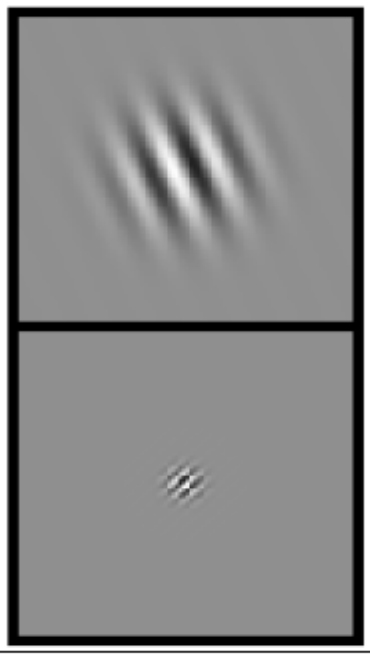
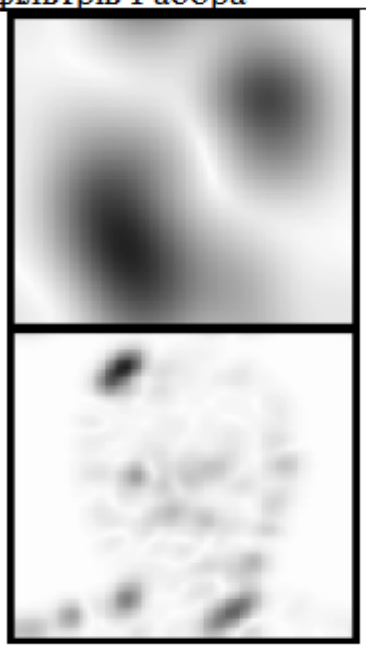
Вхідне зображення	Приклад двох фільтрів Габора	Результат згортки вхідного зображення і фільтрів Габора
		

Рис - 2.3.1.4 Приклад згортки зображення особи з двома фільтрами Габора

Ребра графа визначаються відстанями між суміжними вершинами. Різниця (відстань, дискримінаційна характеристика) між двома графами обчислюється за допомогою деякої функції цінової деформації, що враховує як розходження між значеннями ознак, обчисленими в вершинах, так і ступінь деформації ребер графа.

Деформація графа відбувається шляхом зміщення кожної з його вершин на деяку відстань в певних напрямках щодо її початкового місця розташування і вибору такої позиції, при якій різниця між значеннями ознак (відгуків фільтрів Габора) у вершині деформуємого графа і відповідної їй вершині еталонного графа буде мінімальною. Дана операція виконується по черзі для всіх вершин графа до тих пір, поки не буде досягнуто найменша сумарна різниця між ознаками деформуємого і еталонного графів. Значення цінової функції деформації при такому положенні деформуємого графа і буде мірою відмінності між вхідним зображенням обличчя і еталонним графом. Дана «релаксаційна» процедура деформації повинна виконуватися для всіх еталонних осіб, закладених в базу даних системи. Результат розпізнавання системи – еталон з найкращим значенням цінової функції деформації.

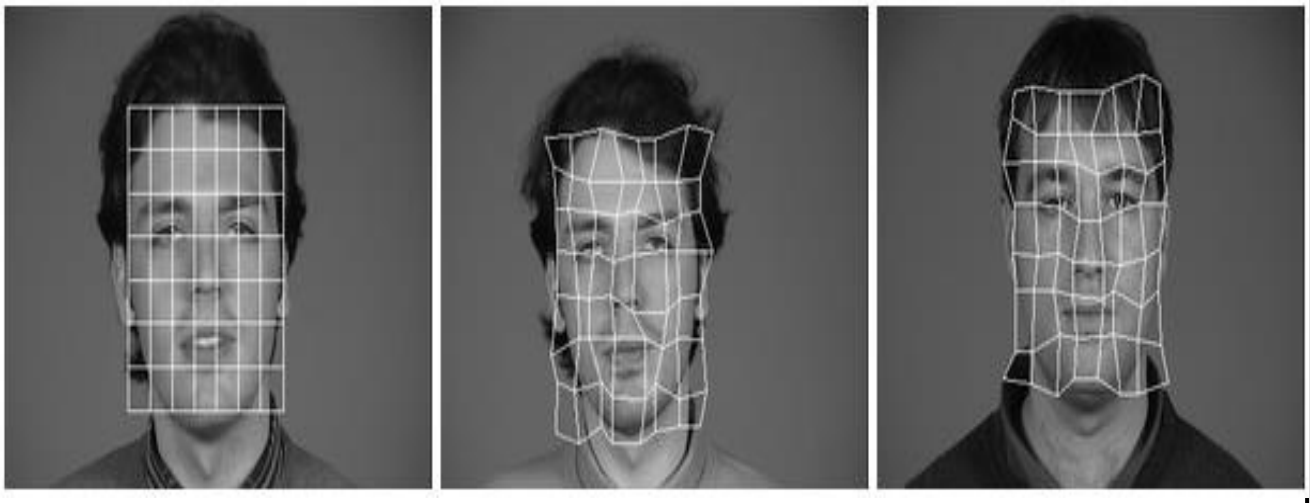


Рис – 2.3.1.5 Приклад деформації графа у вигляді регулярної решітки

В окремих публікаціях вказується 95-97%-ая ефективність розпізнавання навіть при наявності різних емоційних виразів і зміну ракурсу особи до 15 градусів. Однак розробники систем еластичного порівняння на графах

посилаються на високу обчислювальну вартість даного підходу. Наприклад, для порівняння вхідного зображення особи з 87 еталонними витрачалося приблизно 25 секунд при роботі на ЕОМ паралельної з 23 транспьютерами (Примітка: публікація датований 1993 роком). В інших публікаціях з даної тематики час або не вказується, або кажуть, що воно велике.

Недоліки: висока обчислювальна складність процедури розпізнавання. Низька технологічність при запам'ятовуванні нових еталонів. Лінійна залежність часу роботи від розміру бази даних осіб.

2.3.2 Нейронні мережі

В даний час існує близько десятка різновиди нейронних мереж (НМ). Одним з найбільш широко використовуваних варіантів бути мережа, побудована на багатошаровому перцептроне, яка дозволяє класифікувати подана на вхід зображення/сигнал у відповідності з попередньою настройкою/навчанням мережі.

Навчаються нейронні мережі на наборі навчальних прикладів. Сутність навчання зводиться до налаштування ваг міжнейронних зв'язків у процесі розв'язання оптимізаційної задачі методом градієнтного спуску. У процесі навчання НС відбувається автоматичний витяг ключових ознак, визначення їх важливості і побудова взаємозв'язків між ними. Передбачається, що навчена НС зможе застосувати досвід, отриманий у процесі навчання, на невідомі образи за рахунок узагальнюючих здібностей.

Найкращі результати в області розпізнавання осіб (за результатами аналізу публікацій) показала Convolutional Neural Network або сверточная нейронна мережа (далі – СНР), яка є логічним розвитком ідей таких архітектур НС як когнитрона і неокогнітрона. Успіх обумовлений можливістю обліку двовимірної топології зображення, на відміну від багатошарового перцептрона.

Відмітними особливостями СНР є локальні рецепторні поля (забезпечують локальну двовимірну зв'язність нейронів), загальні ваги (забезпечують детектування деяких рис у будь-якому місці зображення) та

ієрархічна організація з просторовими сэмплингом (spatial subsampling). Завдяки цим нововведенням CHP забезпечує часткову стійкість до змін масштабу, зміщень, повороту, зміні ракурсу та іншим спотворень.

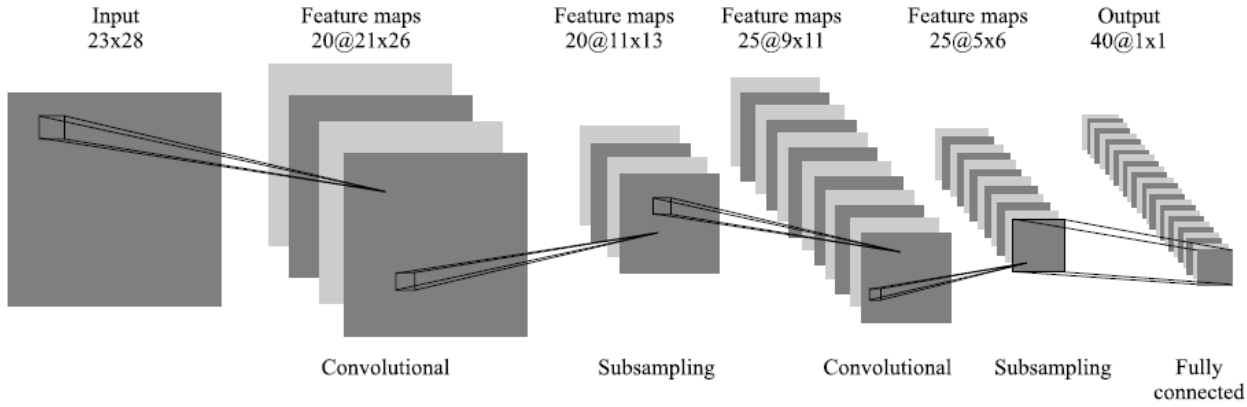


Рис - 2.3.2.1 Схематичне зображення архітектури згорнутої нейронної мережі

Тестування CHP на базі даних ORL, що містить зображення осіб з невеликими змінами освітлення, масштабу, просторових поворотів, положення і різними емоціями, показало 96% точність розпізнавання.

Свій розвиток CHP отримали в розробці DeepFace, яку придбав

Facebook для розпізнавання осіб користувачів своєї соцмережі. Всі особливості архітектури носять закритий характер.

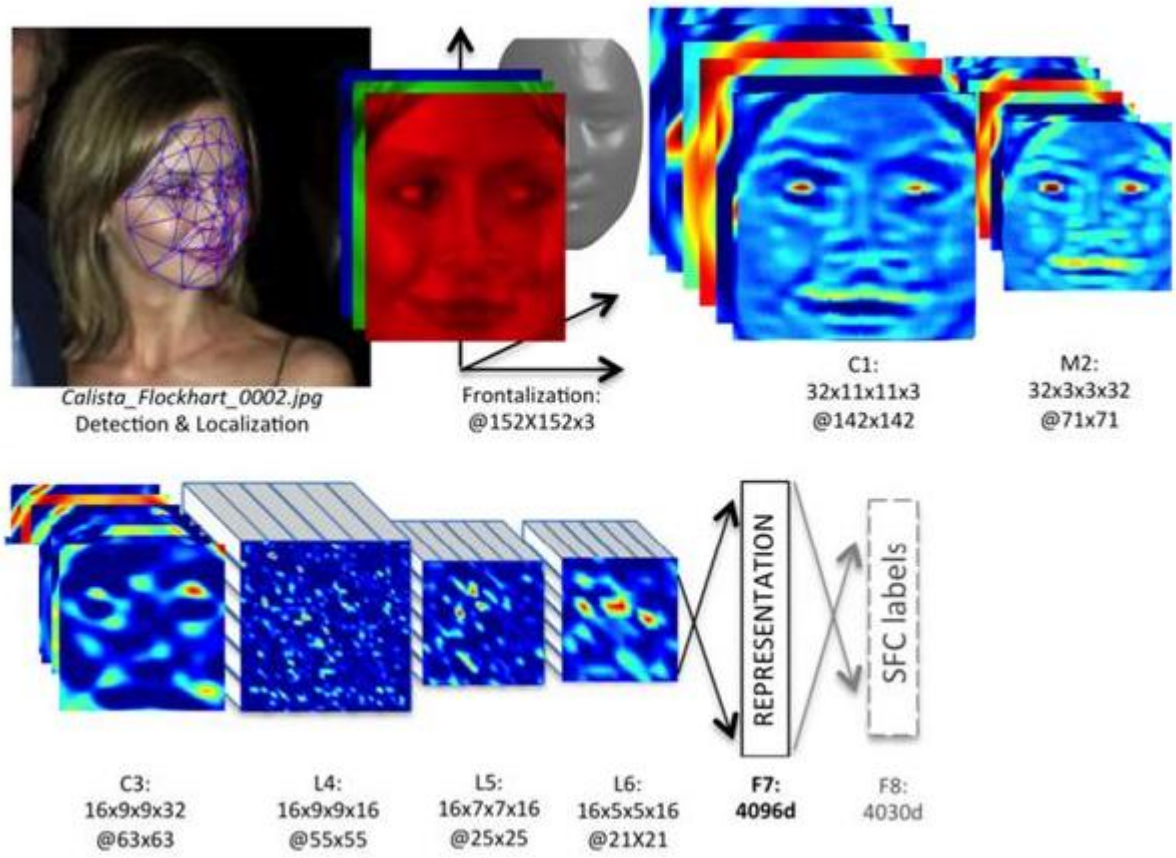


Рис 2.3.2.2 - Принцип роботи DeepFace

Недоліки нейронних мереж: додавання нового еталонного особи в базу даних вимагає повного перенавчання мережі на всьому наявному наборі (досить тривала процедура, в залежності від розміру вибірки від 1 години до декількох днів). Проблеми математичного характеру, пов'язані з навчанням: попадання в локальний оптимум, вибір оптимального кроку оптимізації, перенавчання і т. д. Важко формалізований етап вибору архітектури мережі (кількість нейронів, верств, характер зв'язків). Узагальнюючи все вищесказане, можна зробити висновок, що НС – «чорний ящик» з важко інтерпретуються результатами роботи.

2.3.3 Приховані Марківські моделі (СММ, НММ)

Одним із статистичних методів розпізнавання осіб є приховані Марківські моделі (СММ) з дискретним часом. СММ використовують статистичні властивості сигналів і враховують безпосередньо їх просторові характеристики. Елементами моделі є: безліч прихованих станів, безліч спостережуваних станів,

матриця перехідних ймовірностей, початкова ймовірність станів. Кожному відповідає своя Марковська модель. При розпізнаванні об'єкта перевіряються згенеровані для заданої бази об'єктів Марківські моделі і шукається максимальне з спостережуваних ймовірність того, що послідовність спостережень для даного об'єкта згенерована відповідною моделлю.

На сьогоднішній день не вдалося знайти прикладу комерційного застосування СММ для розпізнавання осіб[10].

Недоліки:

- необхідно підбирати параметри моделі для кожної бази даних;
- СММ не має различающей здатністю, тобто алгоритм навчання тільки максимізує відгук кожного зображення на свою модель, але не мінімізує відгук на інші моделі.

2.3.4 Метод головних компонент або головних компонент (PCA)

Одним з найбільш відомих і опрацьованих є метод головних компонент (principal component analysis, PCA), заснований на перетворення Карунена-Лоєва.

Спочатку метод головних компонент почав застосовуватися в статистиці для зниження простору ознак без суттєвої втрати інформації. У задачі розпізнавання осіб його застосовують головним чином для подання зображення особи вектором малої розмірності (головних компонент), який потім порівнюється з еталонними векторами, закладеними в базу даних.

Головною метою методу головних компонент є значне зменшення розмірності простору ознак таким чином, щоб воно якомога краще описувало «типові» образи, що належать безлічі осіб. Використовуючи цей метод можна виявити різні мінливості в навчальній вибірці зображень осіб і описати цю мінливість у базисі декількох ортогональних векторів, які називаються власними (eigenface).

Отриманий один раз на навчальній вибірці зображень осіб набір власних векторів використовується для кодування всіх інших зображень осіб, які

представляються зваженою комбінацією цих власних векторів. Використовуючи обмежену кількість власних векторів можна отримати стислу апроксимацію вхідному зображенню особи, яку потім можна зберігати в базі даних у вигляді вектора коефіцієнтів, службовця одночасно ключем пошуку в базі даних осіб.

Суть методу головних компонент зводиться до наступного. Спочатку весь навчальний набір осіб перетворюється в одну загальну матрицю даних, де кожна лінія являє собою один примірник зображення особи, розкладеного у рядок. Всі особи навчального набору повинні бути приведені до одного розміром і з нормованими гістограмами.

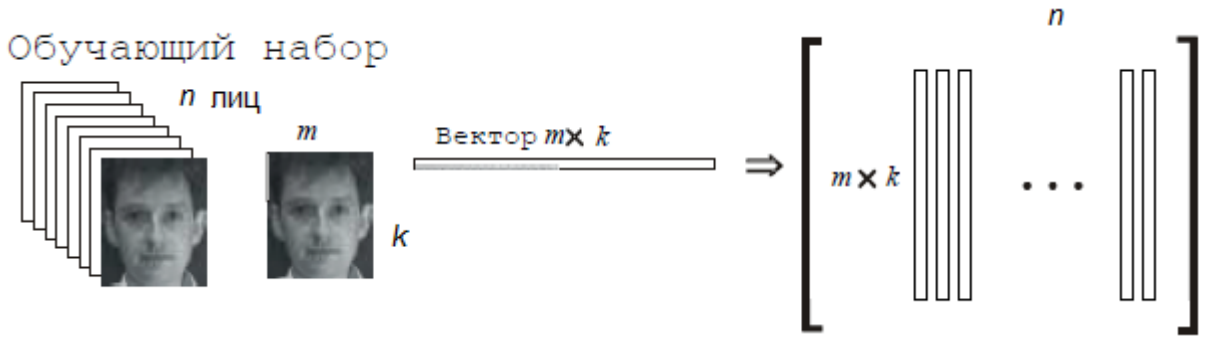


Рис. 2.3.4.1 - Перетворення навчального набору осіб в одну загальну матрицю X

Потім проводиться нормування даних та приведення рядків до 0-го середньому і 1-й дисперсії, обчислюється матриця коваріації. Для отриманої матриці коваріації вирішується задача визначення власних значень і відповідних їм власних векторів (власні особи). Далі виробляється сортування власних векторів в порядку убування власних значень і залишають тільки перші k векторів за правилом:

$$\frac{\sum_{i=1}^{k} \lambda_i}{\sum_{i=1}^{n} \lambda_i} > \text{Threshold (0.9 or 0.95)}$$

Principal Component Analysis

Covariance Algorithm

1. Zero mean: $x_{ij} = x_{ij} - \mu_i$ $\quad \mu_i = \frac{1}{n}\sum_{j=1}^{n} x_{ij}$
2. Unit variance: $x_{ij} = \frac{x_{ij}}{\sigma_j}$ $\quad \sigma_i = \frac{1}{n-1}\sum_{j=1}^{n}(x_{ij} - \mu_i)^2$
3. Covariance matrix: $\Sigma = \mathbf{X}\mathbf{X}^{\mathrm{T}}$
4. Compute eigenvectors of $\sum$: W^T
5. Project X onto the k principal components

k < d

Рис. 2.3.4.2 Правило сортування

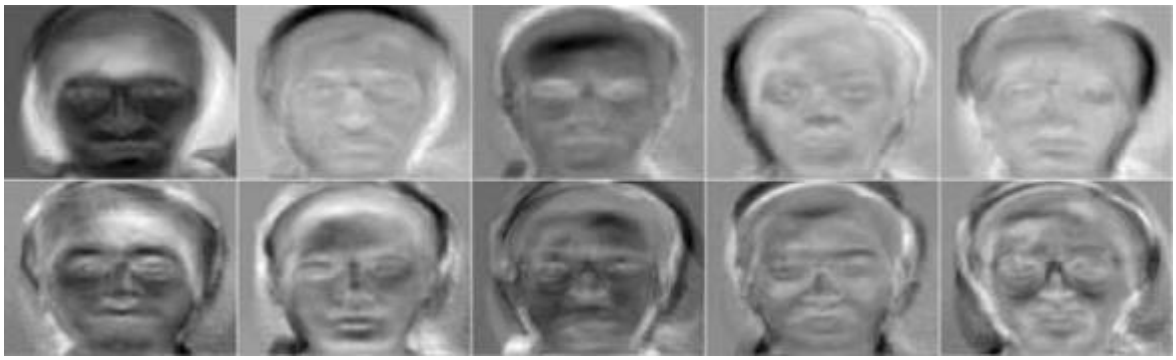


Рис – 2.3.4.1 Візуалізація алгоритму PCA

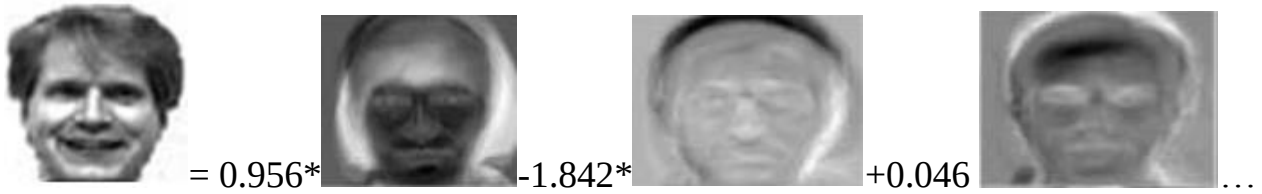


Рис – 2.3.4.2 Приклад побудови (синтезу) людського обличчя за допомогою комбінації власних осіб та головних компонент

Нещодавно з'явилася свіжа версія AIR, в якій є можливість розробки під IOS, Android і BlackBerry PlayBook. Нова версія принесла більше стабільності і продуктивності. Хоча серед демонстрації можливостей рушія були вказані

лише звичайні програми (не ігри). Також поки відсутня можливість використання нативних бібліотек. А сам API теж вельми бідний на можливості.

Метод головних компонент добре зарекомендував себе в практичних додатках. Однак, у тих випадках, коли на зображенні особи присутні значні зміни в освітленості або виразі обличчя, ефективність методу значно падає. Вся справа в тому, що PCA вибирає підпростір з такою метою, щоб максимально апроксимувати вхідний набір даних, а не виконати дискримінацію між класами осіб[12].

Було запропоновано вирішення цієї проблеми з використанням лінійного дискримінанта Фішера (у літературі зустрічається назва "Eigen-Fisher", "Fisherface", LDA). LDA вибирає лінійне підпростір, яке максимізує відношення:

$$\frac{|\mathbf{\Phi}^T \mathbf{S_b} \mathbf{\Phi}|}{|\mathbf{\Phi}^T \mathbf{S_w} \mathbf{\Phi}|}$$

$$\mathbf{S_b} = \sum_{i=1}^{m} N_i (\bar{\mathbf{x}}_i - \bar{\mathbf{x}})(\bar{\mathbf{x}}_i - \bar{\mathbf{x}})^T$$

де - матриця міжкласові розкиду,

$$\mathbf{S_w} = \sum_{i=1}^{m} \sum_{\mathbf{x} \in \mathbf{X}_i} (\mathbf{x} - \bar{\mathbf{x}}_i)(\mathbf{x} - \bar{\mathbf{x}}_i)^T$$

I - Матриця внутриклассового розкиду

m – число класів в базі данних.

LDA шукає проекцію даних, при якій класи є максимально лінійно сепарабельны (див. малюнок нижче). Для порівняння PCA шукає таку проекцію даних, при якій буде максимизирован розкид по всій базі даних осіб (без урахування класів). За результатами експериментів в умовах сильного бакового і нижнього затінення зображень осіб Fisherface показав 95% ефективність, порівняно з 53% Eigenface.

2.3.5 Active Appearance Models (AAM) и Active Shape Models (ASM)

Активні моделі зовнішнього вигляду (Active Appearance Models, AAM) — це статистичні моделі зображень, які шляхом різного роду деформацій можуть бути підігнані під реальне зображення. Даний тип моделей у двовимірному

варіанті була запропонована Тімом Кутсом і Крісом Тейлором у 1998 році. Спочатку активні моделі зовнішнього вигляду застосовувалися для оцінки параметрів зображень осіб.

Активна модель зовнішнього вигляду містить два типи параметрів: параметри, пов'язані з формою (параметри форми), і параметри, пов'язані зі статистичною моделлю пікселів зображення або текстурою (параметри зовнішнього вигляду). Перед використанням модель повинна бути навчена безлічі заздалегідь розмічених зображень. Розмітка зображень проводиться вручну. Кожна мітка має свій номер і визначає характерну точку, яку повинна буде знаходити модель під час адаптації до нового зображення.

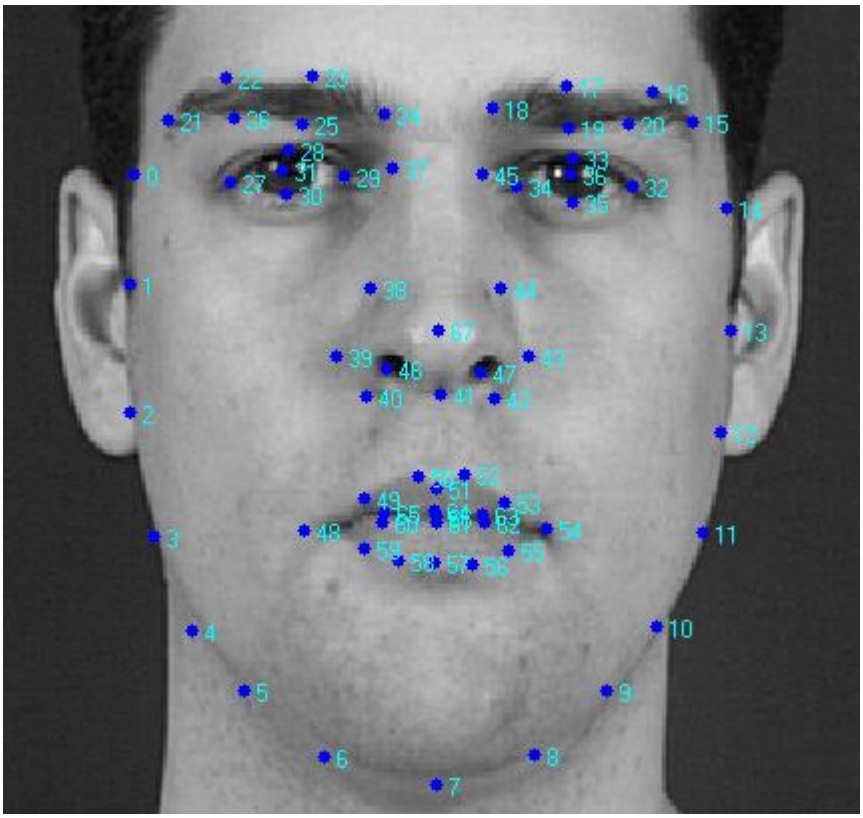


Рис - 2.3.5.1 Приклад розмітки зображення особи з 68 точок, що утворюють форму AAM.

Процедура навчання AAM починається з нормалізації форм, розмічених зображеннях з метою компенсації різниці в масштабі, нахилі і зсуві. Для цього використовується так званий узагальнений Прокрустов аналіз.

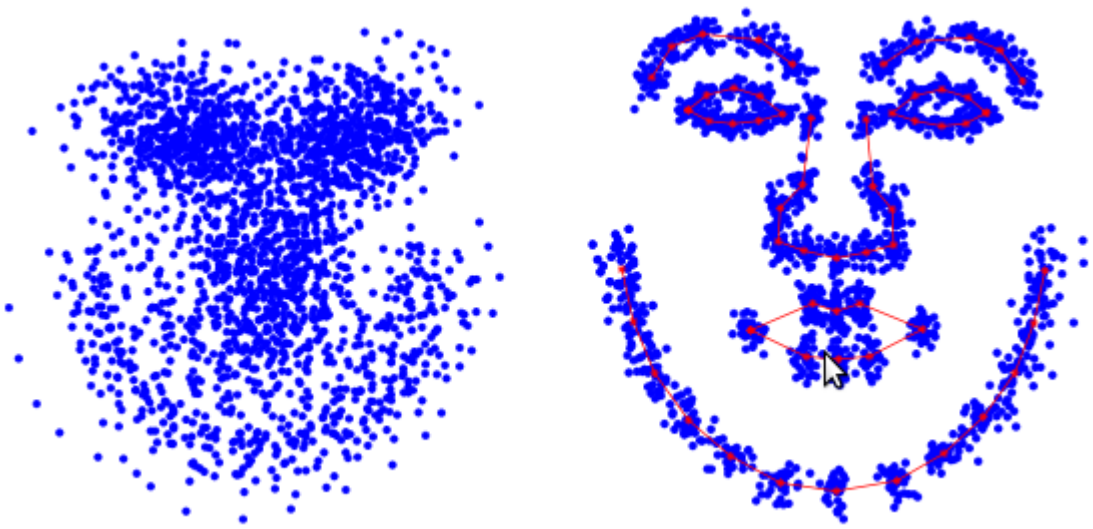


Рис - 2.3.5.2 Координати точок форми особи до і після нормалізації

З усієї множини нормованих точок потім виділяються головні компоненти з використанням методу PCA.

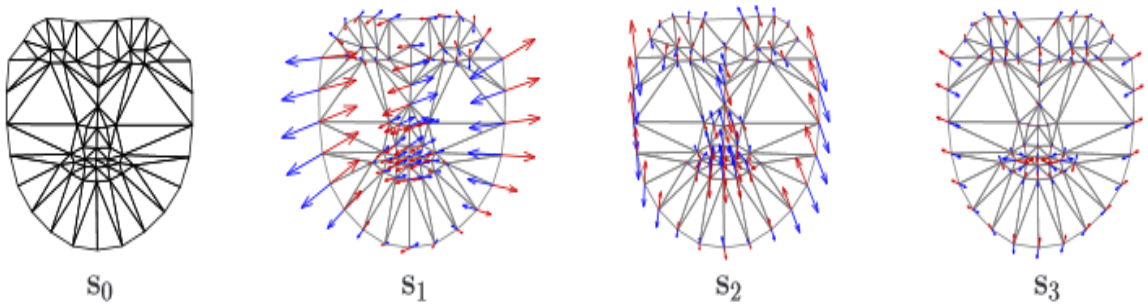


Рис - 2.3.5.3 Модель форми AAM складається з триангуляційної решітки s0 і лінійної комбінації зміщень si щодо s0

Далі з пікселів всередині трикутників, утворених точками форми, формується матриця, така що, кожен стовпець містить значення пікселів відповідної текстури. Варто відзначити, що використовуються для навчання текстури можуть бути одноканальними (градації сірого), так і багатоканальними (наприклад, простір кольорів RGB або інше). У разі багатоканальних текстур вектори пікселів формуються окремо по кожному з каналів, а потім виконується їх конкатенація. Після знаходження головних компонент матриці текстур модель AAM вважається навченою.

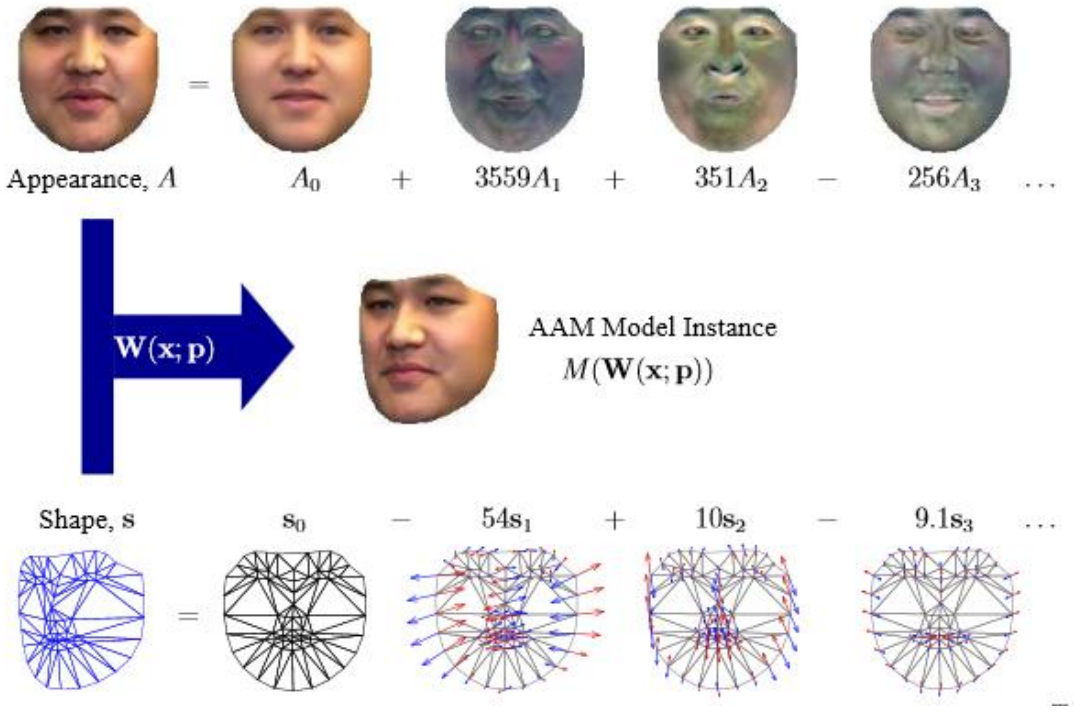


Рис – 2.3.5.4 Приклад конкретизації AAM. Вектор параметрів форми

p=(p_1,p_2,⟦...,p⟧_m)^T=(-54,10,-9.1,...)^T використовується для синтезу моделі форми s, а вектор параметрів λ=(λ_1,λ_2,⟦...,λ⟧_m)^T=(3559,351,-256,...)^Tдля синтезу зовнішнього вигляду моделі. Підсумкова модель особи ⟦M(W(x;p))⟧^ виходить як комбінація двох моделей – форми і зовнішнього вигляду.

Підгонка моделі під конкретне зображення особи виконується в процесі вирішення оптимізаційної задачі, суть якої зводиться до мінімізації функціоналу $p = (p_1, p_2, \dots, p_m)^T = (-54, 10, -9.1, \dots)^T$

Методом градієнтного спуску. Знайдені при цьому параметри моделі і будуть відображати положення моделі на конкретному зображенні.

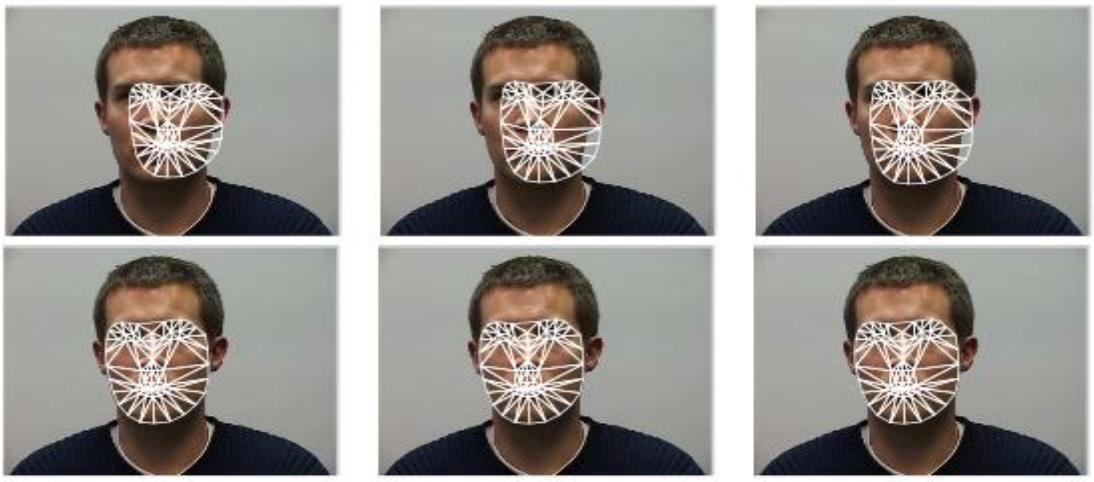


Рис - 2.3.5.5 Приклад підгонки моделі на конкретне зображення за 20 ітерацій процедури градієнтного спуску.

З допомогою AAM можна моделювати зображення об'єктів, схильних як твердої, так і нежорсткої деформації. AAM складається з набору параметрів, частину яких представляють форму обличчя, інші ставлять його текстуру. Під деформації зазвичай розуміють геометричне перетворення у вигляді композиції переносу, повороту і масштабування. При вирішенні задачі локалізації особи на зображенні виконується пошук параметрів (розташування, форма, текстура) AAM, які представляють синтезируемое зображення, найбільш близьке до спостережуваного. За ступенем близькості AAM подгоняемому зображенню приймається рішення – є особа чи ні[11].

Суть методу ASM полягає в обліку статистичних зв'язків між розташуванням антропометричних точок. На наявною вибірці зображень осіб, знятих в анфас. На зображенні експерт розмічає розташування антропометричних точок. На кожному зображенні точки пронумеровані в однаковому порядку.

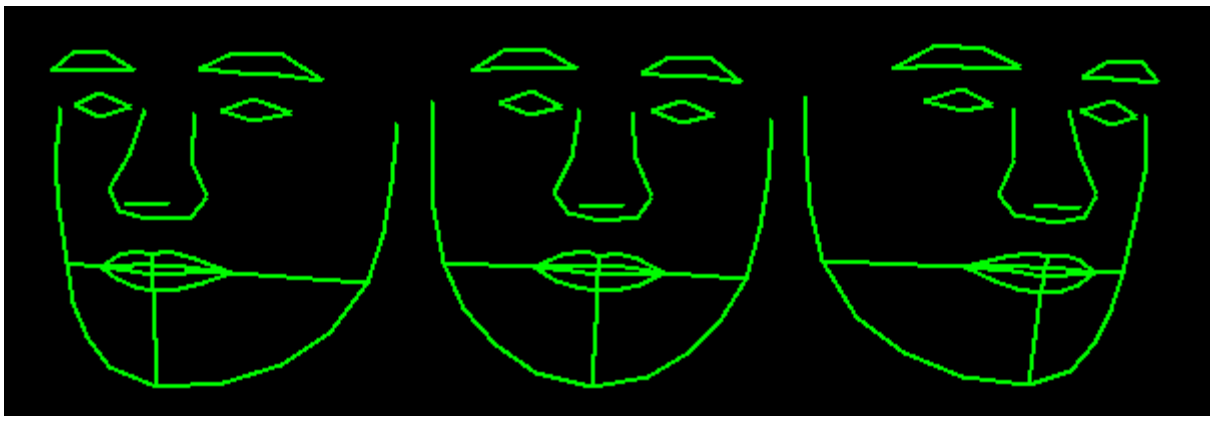


Рис – 2.3.5.6 Приклад подання форми обличчя з використанням 68 точок

Для того щоб привести координати на всіх зображеннях до єдиної системи зазвичай виконується т. н. узагальнений прокрустов аналіз, в результаті якого всі точки приводяться до одного масштабом і центруються. Далі для всього набору образів обчислюється середня форма і матриця коваріації. На основі матриці коваріації обчислюються власні вектори, які потім сортуються в порядку зменшення відповідних їм власних значень. Модель ASM визначається матрицею Ф і вектором середньої форми s .

Тоді будь-яка форма може бути описана за допомогою моделі та параметрів:

$$b_i = \Phi^T \bar{s}_i = \Phi^T (s_i - \bar{s})$$

Локалізації ASM моделі на новому, не входить у навчальну вибірку зображенні здійснюється в процесі рішення оптимізаційної задачі.

Рис – 2.3.5.7 Ілюстрація процесу локалізації моделі ASM на конкретному зображенні: а) початкове положення б) після 5 ітерацій в) після 10 ітерацій г) модель зійшлася

Однак все ж головною метою AAM і ASM є не розпізнавання осіб, а точна локалізація особи та антропометричних точок на зображенні для подальшої обробки.

Практично у всіх алгоритмах обов'язковим етапом, що передують класифікацію, є вирівнювання, під яким розуміється вирівнювання зображення особи під фронтальне положення щодо камери або приведення сукупності осіб (наприклад, навчальної вибірки для навчання класифікатора) до єдиної системи координат. Для реалізації цього етапу необхідна локалізація на зображенні характерних для всіх осіб антропометричних точок – найчастіше це центри зіниць або куточки очей. Різні дослідники виділяють різні групи таких точок. В цілях скорочення обчислювальних витрат для систем реального часу розробники виділяють не більше 10 таких точок .

Моделі AAM і ASM якраз і призначені для того, щоб точно локалізувати ці антропометричні точки на зображенні особи.

2.4 Розпізнавання осіб за допомогою бібліотеки OpenCV

OpenCV – de facto найпопулярніша бібліотека комп'ютерного зору. Вона написана на C/C++, її вихідний код відкрито. бібліотека містить більше 1000 функцій і алгоритмів. Вона розробляється з 1998 р., спочатку в компанії Інтел, тепер у Itseez при активній участі співтовариства. Про високої популярності бібліотеки свідчить кількість завантажень, їх більш 6000000 завантажень (без урахування svn/git трафіку).

Існують бібліотеки, більш просунуті функції, наприклад, Halcon. Є більш спеціалізовані бібліотеки, що роблять акцент на будь-якої конкретної задачі, наприклад, libmv. OpenCV – найбільша бібліотека за широтою тематики.

Бібліотека поширюється за ліцензією BSD, що означає, що її можна вільно і безкоштовно використовувати як у відкритих проектах з відкритим кодом, так і в закритих, комерційних проектах. Бібліотеку не обов'язково копіювати цілком у свій проект, можна використовувати шматки коду. Єдина вимога ліцензії – наявність у супроводжуючих матеріалах копії ліцензії OpenCV.

Через ліберальної ліцензії бібліотека використовується багатьма компаніями, організаціями, університетами, наприклад, NVidia, Willow Garage, Intel, Google, Stanford University. Компанії NVidia і WillowGarage частково спонсорують її розробку.

Є підстава думати, що не усі компанії, що використовують OpenCV, афішують це. Наведемо невеликий перелік відомих авторам проектів, в яких використовується OpenCV:

Система зору робота PR2, розробленого компанією WillowGarage (www.willowgarage.com). Проект PR2 націлений на рішення складної задачі – створення платформи для персональної робототехніки.

- Аудіо-візуальна інсталяція в Музеї Сучасного Мистецтва (Сан-Франциско).
- Контроль якості монет, виготовлених Центробанком Китаю.
- Курси комп'ютерного зору в Стенфорді.
- Панорами вулиць в картах Google.

Багатовимірна архітектура проекту представлена на рис. 4.1. Бібліотека складається з 16 модулів. Реалізовано близько 1000 алгоритмів. Функціональність доступна на різних мовах: C, C++, Python, CUDA, Java. Підтримуються основні операційні системи: MS Windows, Linux, Mac, Android, iOS. Є можливість використання сторонніх бібліотек, наприклад, для роботи з пристроєм Kinect (OpenNI), розробки паралельних програм (TBB) та ін.

Проект використовує систему безперервної інтеграції. Кожну ніч останні робочі версії OpenCV викачуються з репозиторію і компілюються на 50 різних конфігураціях (різні операційні системи, різні платформи, різні параметри і т. д.), після чого запускаються регресійні тести. Наприклад, проводиться реальне тестування на Android-планшетах.

Основні модулі бібліотеки можна віднести до 4 групи (розділами):

- Модулі core, highgui, що реалізують базову функціональність (базові структури, математичні функції, генератори випадкових

чисел, лінійна алгебра, швидке перетворення Фур'є, ввід/вивід зображень і відео, ввід/вивід в форматах XML, YAML та ін).

- Модулі imgproc, features2d для обробки зображень (фільтрація, геометричні перетворення, перетворення колірних просторів, сегментація, виявлення особливих точок і ребер, контурний аналіз та ін).
- Модулі video, objdetect, calib3d (калібрування камери, аналіз руху та відстеження об'єктів, обчислення положення в просторі, побудова карти глибини, детектування об'єктів, оптичний потік).
- Модуль ml, що реалізує алгоритми машинного навчання (метод найближчих сусідів, наївний байєсовський класифікатор, дерева рішень, бустинг, градієнтний бустинг дерев рішень, випадковий ліс, машина опорних векторів, нейронні мережі та ін).

Звернемо увагу на підтримку роботи з xml-файлами. Результати проміжних обчислень можна зберігати в xml-файлах, а потім їх прочитати, наприклад, в іншій програмі, що полегшує розробку алгоритму по частинах, роботу над алгоритмом цілою командою.

Зауважимо, що бібліотека OpenCV реалізує, як правило, тільки базові операції, що використовуються в комп'ютерному зорі. Таким чином, її можна розглядати як у цілому низькорівневу бібліотеку комп'ютерного зору. Для вирішення серйозних завдань необхідно на основі наданих бібліотекою цеглинок створювати складні додатки.

Все починається з захоплення зображень (модуль highgui). Ви читаєте зображення з файлу або читаєте відео з мережевої камери через мережевий протокол.

Далі здійснюється попередня обробка (модуль imgproc), така, як усунення шуму, вирівнювання яскравості, контрасту, виділення і видалення відблисків, тіней. Наприклад, один і той же об'єкт при різному освітленні виглядає по-різному. В яскравому світлі червона машина, рух якої, необхідно відстежувати, буде яскраво-помаранчевою. У похмуру погоду та ж машина буде виглядати

червоно-рожевої. У цьому випадку на зображенні необхідно виконати вирівнювання кольорів. Передобробка може бути простий, але може містити в собі цілу складну технологію.

Наступний етап – виділення особливостей (модулі imgproc, features2d). Наприклад, в задачі стеження за об'єктом це може бути пошук спеціальних точок на об'єкті, за якими легко спостерігати; завдання для детектування (тобто виявлення на зображенні) особи – обчислення опису кожного пікселя.

Далі відбувається детектування цікавлять нас об'єктів, виділення значущих частин, сегментація зображення (модулі imgproc, objdetect). Якщо, наприклад, камера нерухома, а зображення рухливе, можна використовувати алгоритми віднімання фону.

Після цього ви вирішуєте основну задачу, таку, як обчислення розташування об'єкта в 3d, реконструкцію 3d структури, аналіз структури, реєстрацію і т. п. (модулі calib3d, contrib, video, stitching, videostab, ml). Наприклад, у завданні склейки панорам зображень – це зіставлення різних частин кадрів, визначення потрібного перетворення. У задачі відеоспостереження це відновлення траєкторій об'єктів і т. д.

В кінці відбувається розпізнавання та прийняття конкретних рішень (модуль ml). Наприклад, у системі відеоспостереження: з'явився небажаний об'єкт в кадрі чи ні. У задачі детектування тексту – детектирован текст, що саме за текст і т. д.

Розпізнавання осіб являє собою окремий випадок задачі розпізнавання образів. Для вирішення задачі розпізнавання осіб існує безліч інструментів, з яких найбільш поширеним є бібліотека з відкритими вихідними кодами OpenCV, а саме – клас FaceRecognition, який займається конкретно розпізнаванням осіб.

OpenCV (Open Source Computer Vision, комп'ютерне зір з відкритими вихідними кодами) це популярна бібліотека комп'ютерного зору, розроблена компанією Intel у 1999 році. Крос-платформна бібліотека націлена на обробку зображень в режимі реального часу, і включає в себе вільну реалізацію новітніх

алгоритмів комп'ютерного зору. Бібліотека OpenCV зараз доступна для багатьох мов програмування і платформ, включаючи C, C++, Python і Android.

Версії OpenCV 2.4.1 і вище включають в себе навчені каскадні класифікатори для розпізнавання осіб, а також для розпізнавання очей, носа, і т. д. в бібліотеку включено два типи класифікаторів:

• Каскади Хаара.

• LBP-каскади.

Для розпізнавання осіб використовуються LBP-каскади, а каскади Хаара використовуються для розпізнавання очей. Деякі автори, серед яких Шервін Емамі, стверджують, що використання LBP-каскадів для розпізнавання осіб в кілька разів швидше, ніж за Хаару.

У OpenCV використовуються три алгоритму розпізнавання осіб:

• Eigenfaces.

• Fisherfaces.

• LBPH (local binary patterns histograms, гістограма двійкових локальних особливостей).

Кожен з цих алгоритмів підтримує навчання на основі заданого масиву зображень, передбачення знайденого особи, а також завантаження і збереження стану моделі у форматі XML або YAML. Алгоритм LBPH також підтримує оновлення моделі, інакше кажучи, ви можете оновити наявну модель новими зображеннями.

Реалізація алгоритму надає можливість установки чутливості розпізнавання. За замовчуванням значення чутливості встановлено на високий рівень, що означає, що процес розпізнавання завжди буде видавати вам результат з вашого набору даних. І навпаки, якщо рівень чутливості встановлений низьким, в результаті розпізнавання ви з більш високою будете отримувати невизначений результат. Таким чином, необхідно знайти оптимальне значення чутливості, яка може бути обчислена після кількох початкових тестів, і яка може сильно залежати від обраного алгоритму розпізнавання.

2.4.1 Алгоритм Eigenface

Робота алгоритму заснована на методі головних компонент. Припустимо, що є база даних осіб, де зображення розміром N x N пікселів. Кожне зображення з бази даних являють точкою в просторі розмірністю N x N. Основна ідея алгоритму полягає в тому, щоб знайти такий базис меншої розмірності, після проекції в який максимально зберігається інформація по осях з великою дисперсією і втрачається інформацію по осях з малою дисперсією. Це потрібно для того, щоб залишити тільки ту інформацію, яка б характеризувала відмінності осіб і видалити непотрібну інформацію, яка може перешкодити правильно ідентифікувати людину. Процедура ідентифікації виконується в новому базисі з використанням Евклідової метрики.

Основними недоліками алгоритму EigenFaces є відсутність стійкості до зміни умов освітленості і відсутність інваріантності до афінних перетворень.

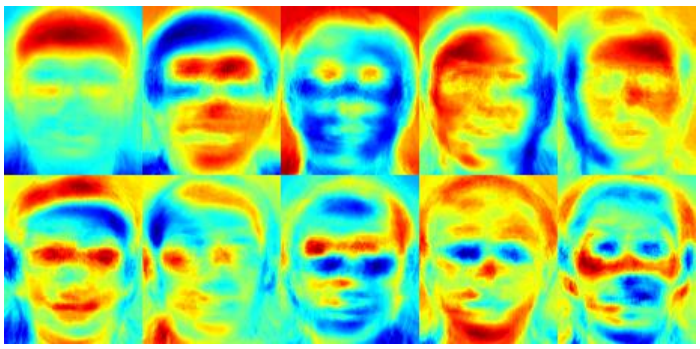


Рис – 2.4.1.1 Приклад роботи коду Eigenfaces

2.4.2 Алгоритм FisherFaces

Алгоритм передбачає наявність безлічі фотографій при різних умовах освітленості у кожної персони в базі даних. В алгоритмі, як і в EigenFaces, передбачається пошук базису, але такого, який дозволив би максимізувати дисперсію між множинами зображень осіб і одночасно мінімізувати дисперсію всередині кожного безлічі.

За рахунок безлічі фотографій кожної персони алгоритм виходить стійким до змін умов освітленості, але зберігає недолік алгоритму EigenFaces у відсутності інваріантності до афінних перетворень.

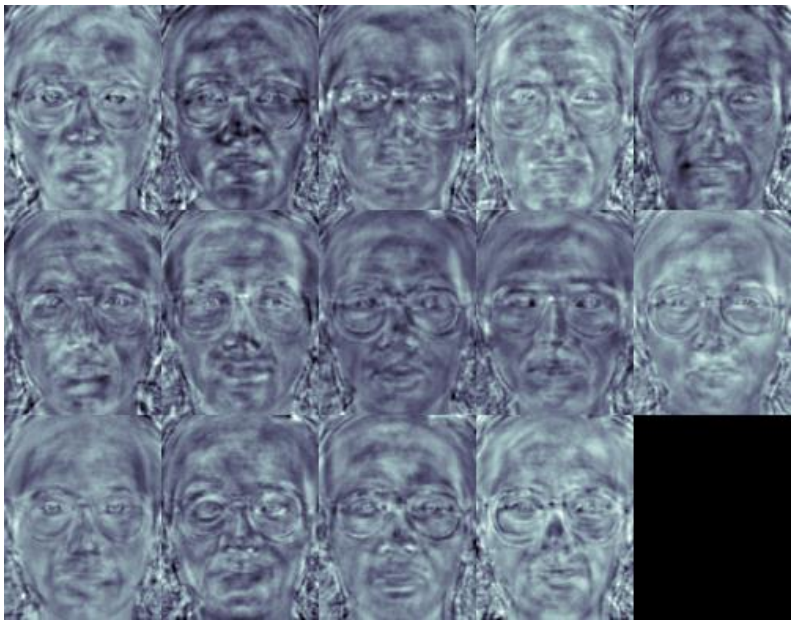


Рис – 2.4.2.1 приклад результату роботи коду FisherFaces

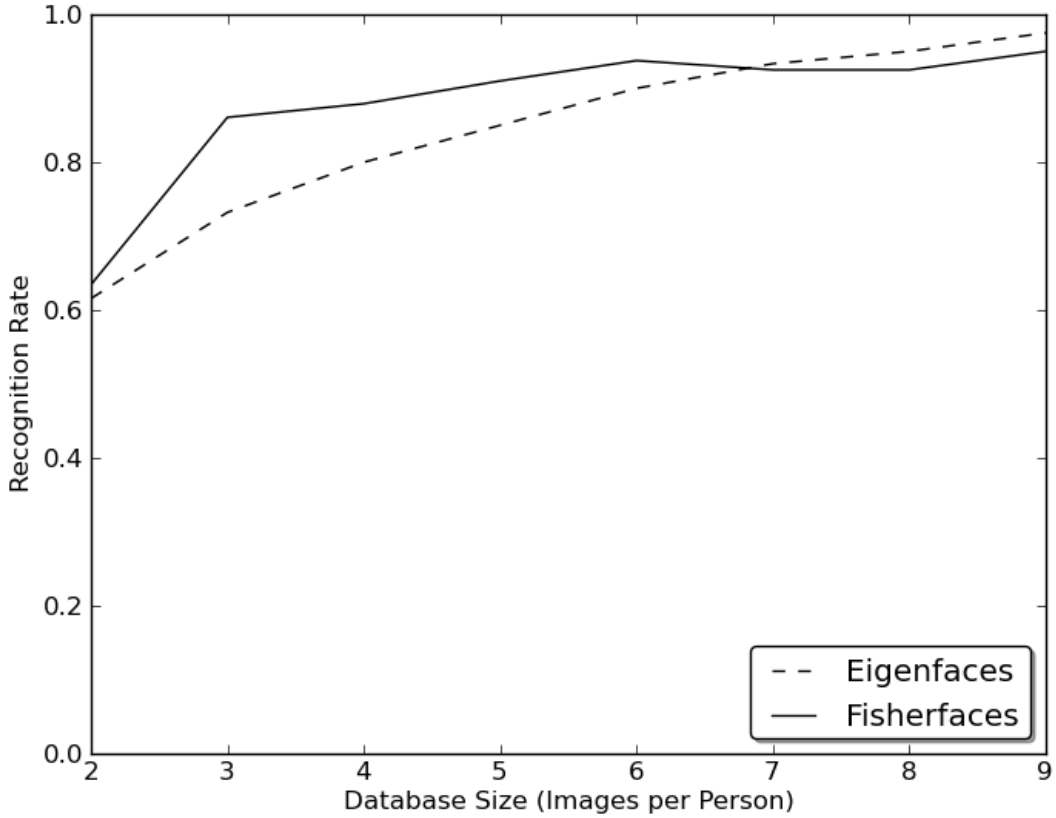


Рис – 2.4.2.2 Графіки Eigenfaces і FisherFaces на одній базі даних

2.4.3 Алгоритм Local Binary Patterns Histograms (LBPH)

Таким чином, деякі дослідження зосереджені на витягу з місцевих особливостей зображень. Ідея полягає в тому, щоб не дивитися на всі зображення в якості високої розмірності вектора, але описують лише локальні особливості об'єкта. Функції ви витягаєте цей шлях буде мати низьковимірних неявно. Прекрасна ідея! Але ви скоро спостерігати подання зображення нам дається не тільки страждають від варіацій освітлення. Подумайте про такі речі, як масштаб, переклад або обертання в зображеннях - ваше локальне опис має бути принаймні трохи стійким до цих речей. Так само, як SIFT, методологія локальні бінарні шаблони має свої корені в аналізі 2D текстури. Основна ідея локальні бінарні шаблони, щоб узагальнити локальну структуру зображення, порівнюючи кожен піксель з його околиці. Візьміть піксель як центру і порога його сусідів проти. Якщо інтенсивність центрального пікселя більше-одно його

сусід, то позначимо його з 1 і 0 якщо ні. Ви будете в кінцевому підсумку з двійкового числа для кожного пікселя, так само, як 11001111. Таким чином, з 8 оточуючих пікселів, в кінцевому підсумку з 2 ^ 8 можливих комбінацій, звані локальні бінарні шаблони або іноді називають LBP кодів. Перший оператор LBP описаний в літературі фактично використовується фіксований 3 x 3 околиці так само, як це:

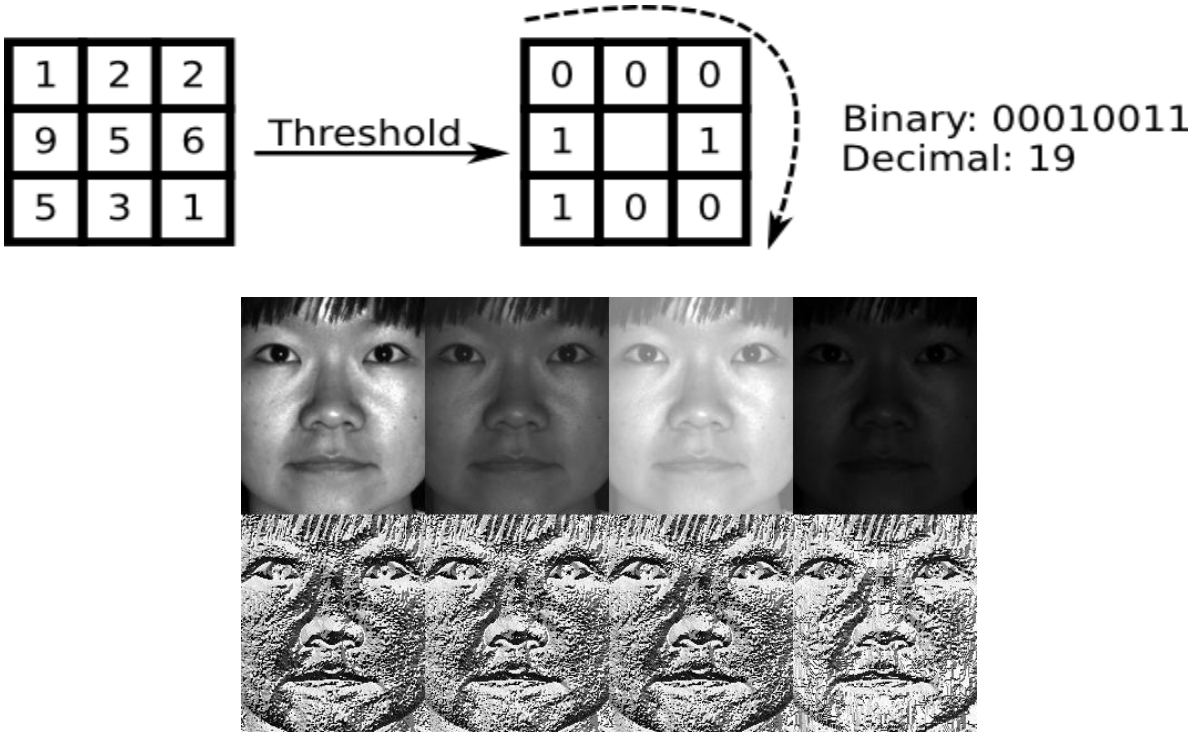


Рис – 2.4.3.1 приклад роботи LBPH

2.5 Висновок

Якість розпізнавання дуже сильно залежить від моделі навчання, яка, в свою чергу, залежить від кількості зображень, використаних при навчанні. Для досягнення найкращого результату, при навчанні рекомендується використовувати заздалегідь підготовлений набір зображень, що дає найбільш повний огляд визначеної особи. Бажано також приводити розміри зображень до одного стандарту.

Як було сказано раніше, можливістю оновлення моделі має тільки алгоритм LBPH. Це означає, що у нашому прикладі ми не зможемо після навчання моделі на одному наборі зображень «дообучить» її на додатковому

наборі. Тому, для динамічних, самонавчаючих систем, рекомендується використовувати алгоритм LBPH.

За пару останніх десятиліть так склалося, що до кожного прикута така ж увага, як і до першої особи держави або сверхпопулярної знаменитості, а ваше життя, подібно журналістам, які висвітлюють всі ті, хто твитит про вас, згадує вас в блогах, читає ваші записи, стежить за вашим рейтингом і за тим, що ви творите з собою. Мережеві татуювання не менш красномовні. Поки ви роздумуєте над тим, які ж можливі наслідки, від цього ставати все складніше втекти — поширюються не тільки мережеві татуювання, розвиваються і алгоритми розпізнавання осіб. Варто лише зняти кого-небудь на iPhone, як отримаєш імена всіх тих, хто на знімку, хоча, знову-таки, часом трапляються непорозуміння.

Є компанії зразок face.com, які надають онлайн доступ до архіву з 18 мільярдів зображень осіб. А ось новини про цю компанію. Є й інші компанії, що розміщують камери, подібні до цієї, — до Facebook це відношення не має — камери знімають вас, зіставляють з даними про вас в соцмережах, з'ясовують будь-яку інформацію.

3 РЕАЛІЗАЦІЯ ТЕХГОЛОГІЇ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ В МОБІЛЬНИХ ПРИСТРОЯХ

Реалізація методів розпізнавання для аутентифікації на мобільних пристроях має деякі обмеження:

- Потужності пристрою
- Можливості фронтальної камери
- Змінне оствітлення

Для реалізації методу розпізнавання обличчя на мобільній платформі будемо використовувати бібліотеку OpenCV, у якій реалізовані такі методи як EigenFaces, FisherFaces та LBPH (детальний опис яких можна знайти у розділі 2, підпункті 4).

Вибір OpenCV зумовлений тим, що вона реалізована на мові C++ і методи, реалізовані на базі цієї бібліотеки можуть бути скомпільовані у динамічну бібліотеку і використані при розробці додатків для самих поширених операційних систем (Android, iOS). Також цей підхід дозволить використовувати реалізацію алгоритмів і на комп’ютерах, обладнаних веб-камерою.

3.1 OpenCV

OpenCV – de facto найпопулярніша бібліотека комп'ютерного зору. Вона написана на C/C++, її вихідний код відкрито. бібліотека містить більше 1000 функцій і алгоритмів. Вона розробляється з 1998 р., спочатку в компанії Інтел, тепер у Itseez при активній участі співтовариства. Про високої популярності бібліотеки свідчить кількість завантажень, їх більш 6000000 завантажень (без урахування svn/git трафіку).

Існують бібліотеки, більш просунуті функції, наприклад, Halcon. Є більш спеціалізовані бібліотеки, що роблять акцент на будь-якої конкретної задачі, наприклад, libmv. OpenCV – найбільша бібліотека за широтою тематики.

Бібліотека поширюється за ліцензією BSD, що означає, що її можна вільно і безкоштовно використовувати як у відкритих проектах з відкритим кодом, так і в закритих, комерційних проектах. Бібліотеку не обов'язково копіювати цілком у свій проект, можна використовувати шматки коду. Єдина вимога ліцензії – наявність у супроводжуючих матеріалах копії ліцензії OpenCV.

Через ліберальної ліцензії бібліотека використовується багатьма компаніями, організаціями, університетами, наприклад, NVidia, Willow Garage, Intel, Google, Stanford University. Компанії NVidia і WillowGarage частково спонсорують її розробку.

Є підстава думати, що не усі компанії, що використовують OpenCV, афішують це. Наведемо невеликий перелік відомих авторам проектів, в яких використовується OpenCV:

Система зору робота PR2, розробленого компанією WillowGarage (www.willowgarage.com). Проект PR2 націлений на рішення складної задачі – створення платформи для персональної робототехніки.

- Аудіо-візуальна інсталяція в Музеї Сучасного Мистецтва (Сан-Франциско).
- Контроль якості монет, виготовлених Центробанком Китаю.
- Курси комп'ютерного зору в Стенфорді.
- Панорами вулиць в картах Google.

Багатовимірна архітектура проекту представлена на рис. 4.1. Бібліотека складається з 16 модулів. Реалізовано близько 1000 алгоритмів. Функціональність доступна на різних мовах: C, C++, Python, CUDA, Java. Підтримуються основні операційні системи: MS Windows, Linux, Mac, Android, iOS. Є можливість використання сторонніх бібліотек, наприклад, для роботи з пристроєм Kinect (OpenNI), розробки паралельних програм (TBB) та ін.

Проект використовує систему безперервної інтеграції. Кожну ніч останні робочі версії OpenCV викачуються з репозиторію і компілюються на 50 різних конфігураціях (різні операційні системи, різні платформи, різні параметри і т.

д.), після чого запускаються регресійні тести. Наприклад, проводиться реальне тестування на Android-планшетах.

Основні модулі бібліотеки можна віднести до 4 групи (розділами):

- Модулі core, highgui, що реалізують базову функціональність (базові структури, математичні функції, генератори випадкових чисел, лінійна алгебра, швидке перетворення Фур'є, ввід/вивід зображень і відео, ввід/вивід в форматах XML, YAML та ін).
- Модулі imgproc, features2d для обробки зображень (фільтрація, геометричні перетворення, перетворення колірних просторів, сегментація, виявлення особливих точок і ребер, контурний аналіз та ін).
- Модулі video, objdetect, calib3d (калібрування камери, аналіз руху та відстеження об'єктів, обчислення положення в просторі, побудова карти глибини, детектування об'єктів, оптичний потік).
- Модуль ml, що реалізує алгоритми машинного навчання (метод найближчих сусідів, наївний байєсовський класифікатор, дерева рішень, бустинг, градієнтний бустинг дерев рішень, випадковий ліс, машина опорних векторів, нейронні мережі та ін).

Звернемо увагу на підтримку роботи з xml-файлами. Результати проміжних обчислень можна зберігати в xml-файлах, а потім їх прочитати, наприклад, в іншій програмі, що полегшує розробку алгоритму по частинах, роботу над алгоритмом цілою командою.

Зауважимо, що бібліотека OpenCV реалізує, як правило, тільки базові операції, що використовуються в комп'ютерному зорі. Таким чином, її можна розглядати як у цілому низькорівневу бібліотеку комп'ютерного зору. Для вирішення серйозних завдань необхідно на основі наданих бібліотекою цеглинок створювати складні додатки.

Все починається з захоплення зображень (модуль highgui). Ви читаєте зображення з файлу або читаєте відео з мережевої камери через мережевий протокол.

Далі здійснюється попередня обробка (модуль imgproc), така, як усунення шуму, вирівнювання яскравості, контрасту, виділення і видалення відблисків, тіней. Наприклад, один і той же об'єкт при різному освітленні виглядає по-різному. В яскравому світлі червона машина, рух якої, необхідно відстежувати, буде яскраво-помаранчевою. У похмуру погоду та ж машина буде виглядати червоно-рожевої. У цьому випадку на зображенні необхідно виконати вирівнювання кольорів. Передобробка може бути простий, але може містити в собі цілу складну технологію.

Наступний етап – виділення особливостей (модулі imgproc, features2d). Наприклад, в задачі стеження за об'єктом це може бути пошук спеціальних точок на об'єкті, за якими легко спостерігати; завдання для детектування (тобто виявлення на зображенні) особи – обчислення опису кожного пікселя.

Далі відбувається детектування цікавлять нас об'єктів, виділення значущих частин, сегментація зображення (модулі imgproc, objdetect). Якщо, наприклад, камера нерухома, а зображення рухливе, можна використовувати алгоритми віднімання фону.

Після цього ви вирішуєте основну задачу, таку, як обчислення розташування об'єкта в 3d, реконструкцію 3d структури, аналіз структури, реєстрацію і т. п. (модулі calib3d, contrib, video, stitching, videostab, ml). Наприклад, у завданні склейки панорам зображень – це зіставлення різних частин кадрів, визначення потрібного перетворення. У задачі відеоспостереження це відновлення траєкторій об'єктів і т. д.

В кінці відбувається розпізнавання та прийняття конкретних рішень (модуль ml). Наприклад, у системі відеоспостереження: з'явився небажаний об'єкт в кадрі чи ні. У задачі детектування тексту – детектирован текст, що саме за текст і т. д.

3.2 Використання OpenCV у Visual Studio

Для реалізації обраного методу необхідно завантажити та встановити бібліотеку OpenCV.

Спершу потрібно завантажити файл інсталяції. Зробити це можна на сайті проекту (http://opencv.org/)

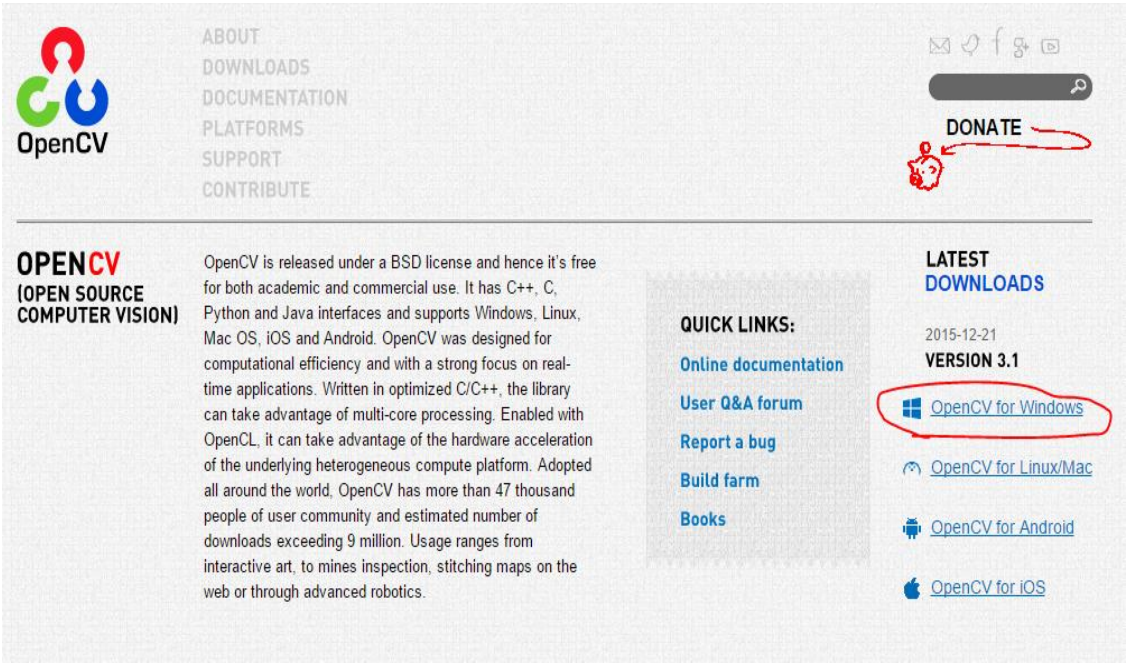


Рис - 3.2.1 Сайт OpenCV

Після того, як файл буде завантажено, запускаємо його і вибираємо каталог для установки: встановити можна куди вам захочеться (по суті це просто саморозпаковується архів). Виберемо наприклад диск D:\ (Створювати папку не треба: при розпакуванні у обрану директорію додасться папка "opencv").

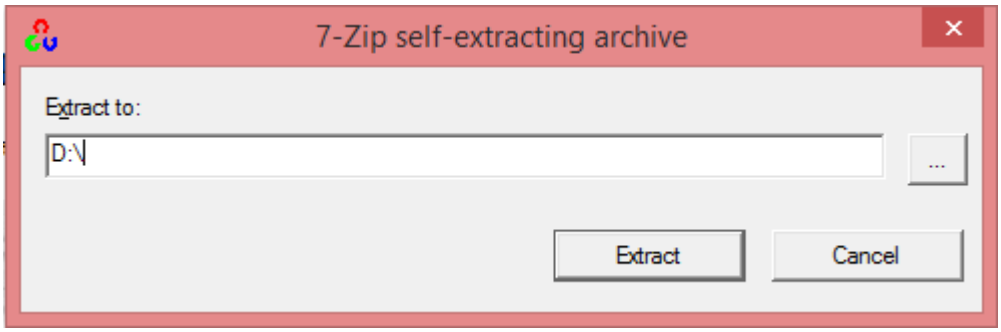


Рис - 3.2.2 Розпакування архіву

Після встановлення необхідно налаштувати змінні середовища. Для відкриваємо: "Панель керування" -> "Система" -> "Додаткові параметри системи" ->Додатково->"Змінні середовища..."

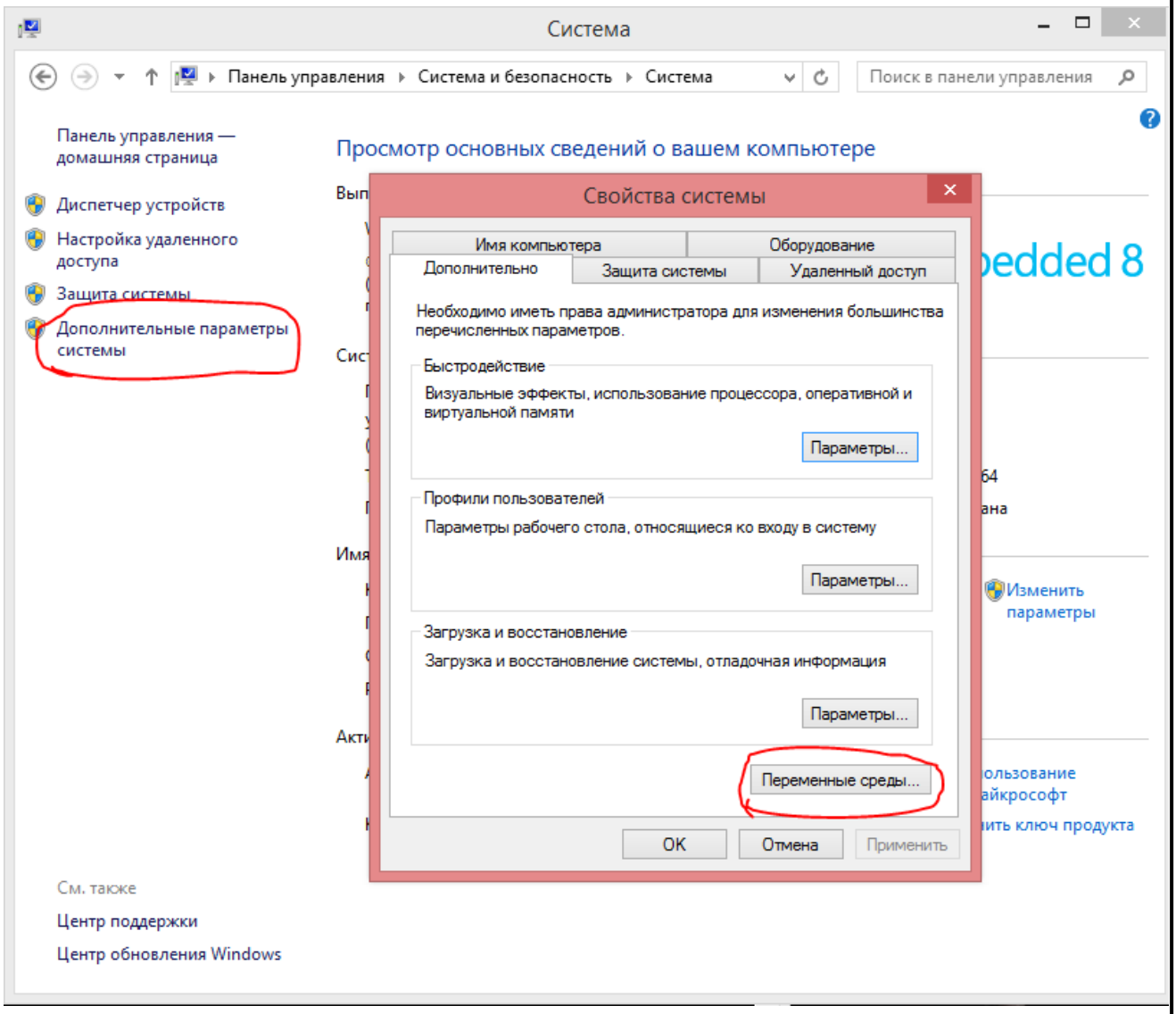


Рис – 3.2.3 змінні середовища

Створимо таку системну змінну:

Змінна: OPENCV_DIR

Значення: [Місце установки opencv]\opencv\build\x64\vc14 (У нашому випадку: D:\opencv\build\x64\vc14)

Далі виправляємо змінну Path:

Додаємо в кінець її значення наступну рядок: ;%OPENCV_DIR%\bin

Після додавання змінної середовища необхідно перезавантажити комп'ютер.

Тепер переходимо до налаштування Visual Studio.

Якщо під час попередніх кроків Visual Studio була запущена, її необхідно перезапустити.

У проекті, де необхідно використовувати OpenCV відкриваємо властивості проекту (Проект->Властивості або Alt+F7)

Перед внесенням змін виберіть конфігурацію "конфігурації", а платформу "x64".

В закладці C/C++ Вказуємо додаткові каталоги, у які включаються файлів: $(OPENCV_DIR)\..\..\include

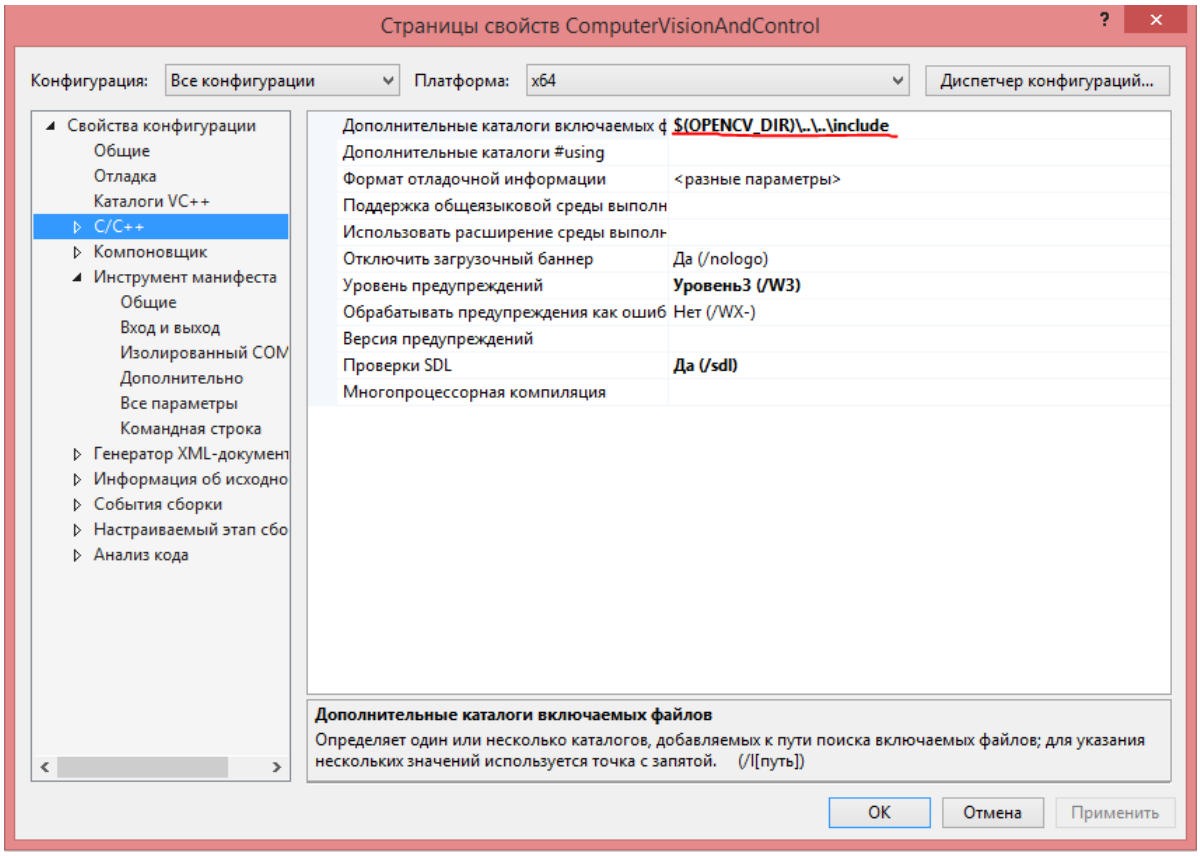


Рис - 3.2.4 Додаткові каталоги Visual Studio

В закладці Компонувальник->Загальні вказуємо додаткові каталоги бібліотек: $(OPENCV_DIR)\lib

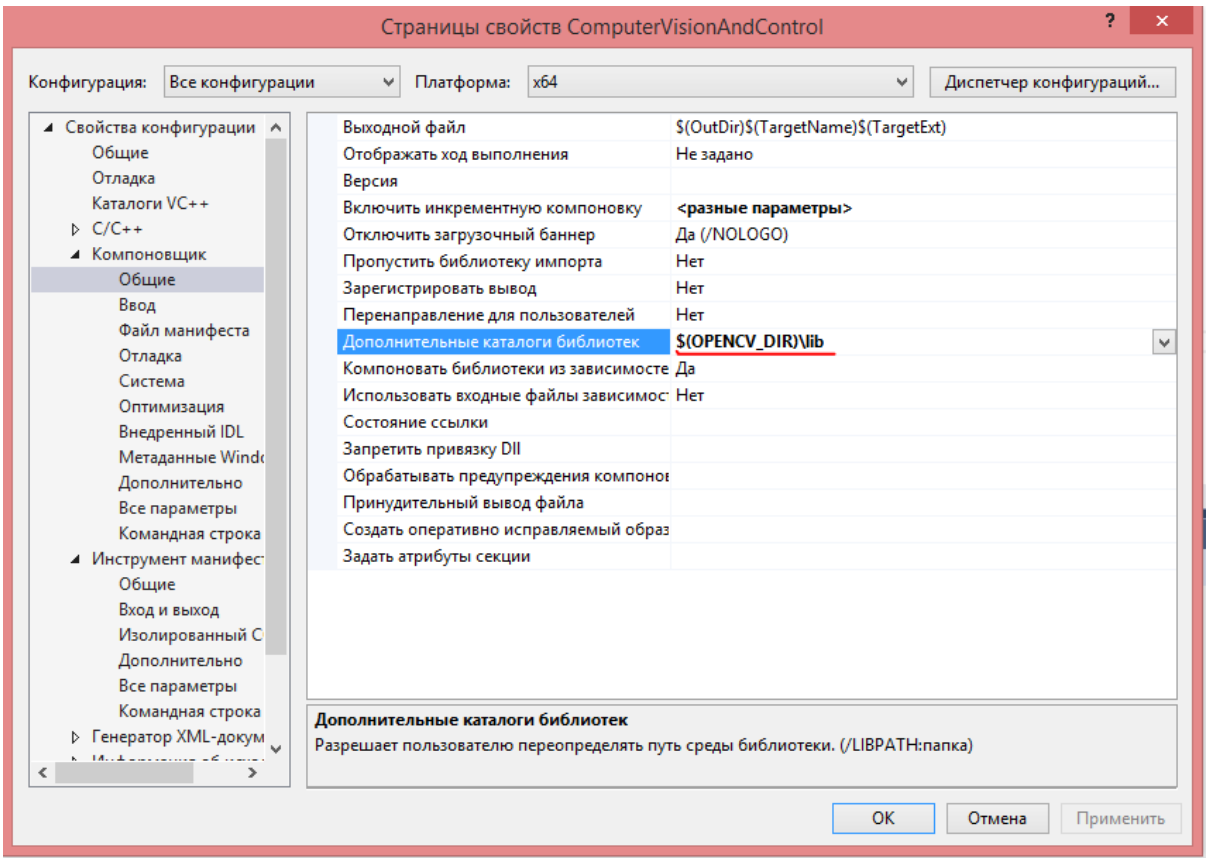


Рис - 3.2.5 додаткові бібліотеки

В закладці Компонувальник->Enter вказуємо додаткові залежності: opencv_world310.lib;opencv_world310d.lib;

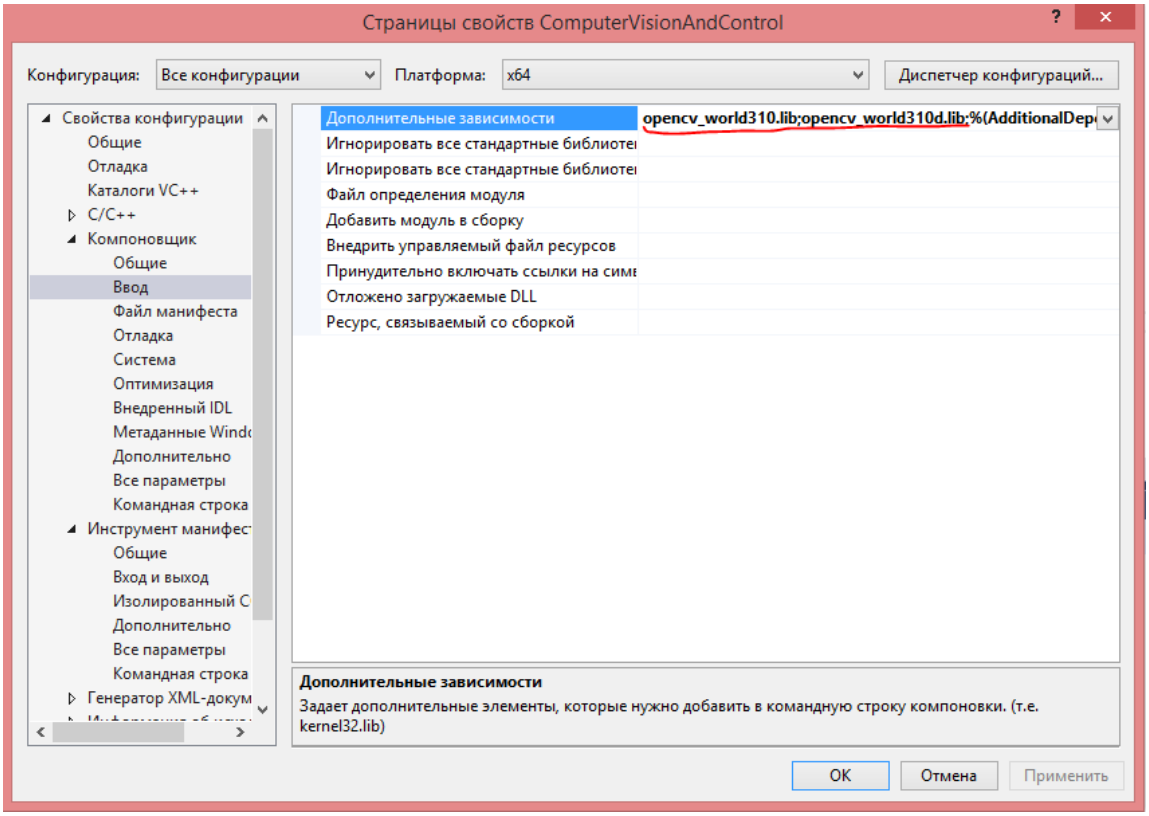


Рис 3.2.6 додаткові залежності.

Якщо усі кроки були виконані, бібліотеку можна використовувати у серидовищі.

Приклад коду методу LBPH можна знайти у додатку А.

3.3 Тестування реалізованих методів

Для тестування був підібраний навчальний набір фотографій із різними кутами положення обличчя відносно камери.

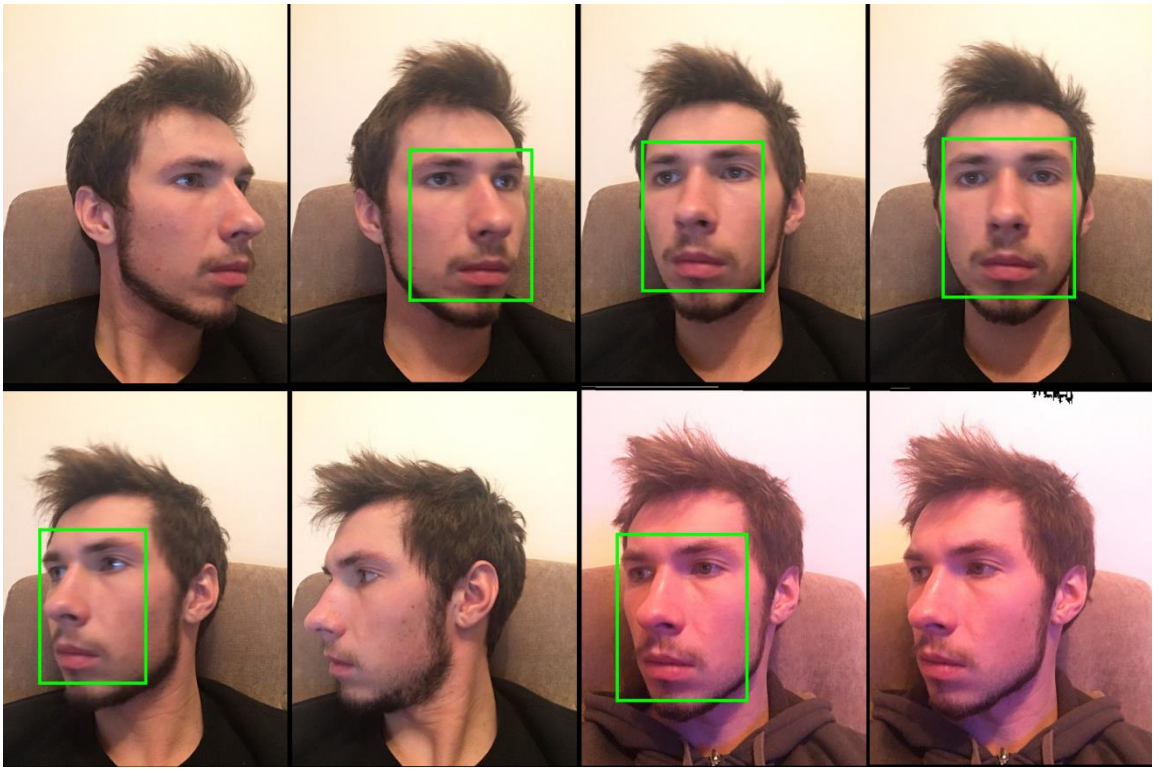


Рис – 3.3.1 Навчальний набір фотографій

Знаходження обличчя на фотографії виконується завдяки методу каскадів Хаара. Як можна побачити з рисунку 3.3.1, він досить чутливий до кута обличчя відносно камери. Цей метод може знайти обличчя на фотографії якщо воно відхиляється не більше ніж на 30 градусів.

Для створення навчального набору для обраних методів оптимальна кількість фотографій лежить у межах від 10 до 20 фотографій. Для більш чіткої роботи алгоритмів, при навчанні моделі необхідно робити фотографії під різним освітленням і різним кутом (але допустимим для методу виділення обличчя).

Після навчання моделі можна тестувати додаток на розпізнавання обличчя.

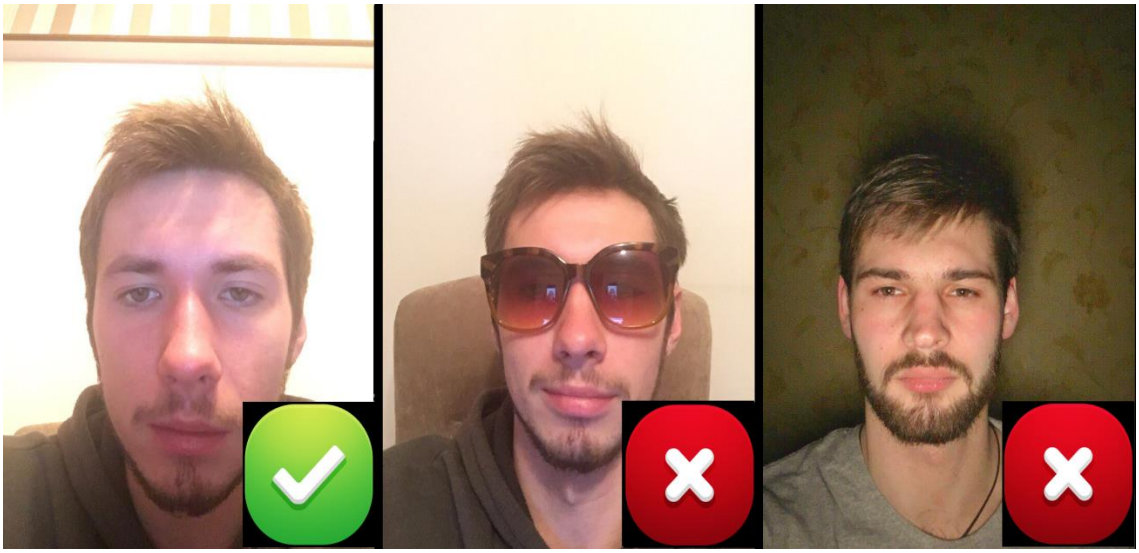


Рис - 3.3.2 Демонстрація роботи додатку

Як можна побачити з рисунку 3.3.2, розпізнавання обличчя спрацювало, але така зміна обличчя, як поява окулярів не дала змоги розпізнати користувача.

Тепер можемо порівняти методи EigenFaces, FisherFaces та LBPH. Для цього проведемо порівняння при штучному і природньому освітленні.

Таблиця 3.3.1 – Результати роботи алгоритмів ідентифікації на тестовій множині.

	Вероятность верной идентификации			Вероятность ложной идентификации		
№	LBPH	Eigen Faces	Fisher Faces	LBPH	Eigen Faces	Fisher Faces
Естественное освещение						
1	0,79	0,30	0,50	0,14	0,33	0,35
2	0,88	0,00	0,00	0,05	0,54	0,79
3	0,76	0,69	0,68	0,12	0,30	0,18
Искусственное освещение						
1	0,50	0,03	0,13	0,20	0,50	0,50
2	0,77	0,00	0,00	0,15	0,90	0,90
3	0,75	0,00	0,00	0,18	1,00	1,00

3.4 Висновок

Проаналізувавши існуючі методи розпізнавання обличчя, а також обмеження встановленні за рахунок використання мобільного телефону, як цільового пристрою, було прийнято рішення реалізовувати такі методи як: EigenFaces, FisherFaces та LBPH. Головною перевагою їх над іншими методами є швидкодія, невеликий навчальний набір фотографій та використання не великих апаратних потужностей.

Реалізувавши додаток та протестувавши його, можна зробити висновки, що алгоритми працюють досить надійно при умовах з природнім освітленням. При зміні освітлення, алгоритми можуть давати збій. Вирішенням цієї проблеми може бути попередня обробка фотографії, яку також можна реалізувати у автоматичному режимі.

Також, у ході тестування було виявлено, що додаток можна “обманути”, якщо показати йому фотографію із обличчям, на якому була навчена модель. Вирішити цей недолік можна або другим фактором авторизації, таким як пароль або голос, або реалізувати метод, який би фіксував моргання, що ідентифікувало би живу людину перед камерою.

Порівнюючи методи було виявлено, що метод LBPH показує кращі результати у розпізнаванні, що рекомендує його до використання.

4 КЕРУВАННЯ ТЕРМІНАМИ ВИКОНАННЯ ДИПЛОМНОЇ РОБОТИ. КЕРУВАННЯ РИЗИКАМИ

Тема: «Реалізація технології розпізнавання облич при аутентифікації користувачів в мобільних пристроях»

Для досягнення мети були поставлені наступні завдання:

- Зробити огляд існуючих методів аутентифікації;
- Розглянути існуючі методи розпізнавання обличь;
- Виділити методи розпізнавання обличь, базуючись на обмеженнях мобільних пристроїв.
- Реалізувати метод аутентифікації обличь, базуючись на проведеному аналізі.
- Розробити мобільний додаток із аутентифікацією користувача завдяки розпізнаванню його обличчя.

Об’єкт дослідження – дослідження методів аутентифікації та методів розпізнавання обличь.

Предмет дослідження – мобільний додаток із реалізованим прикладом роботи розпізнавання обличчя у якості методу аутентифікації.

3.1 Керування термінами виконання дипломної роботи

Діаграма Ганта:

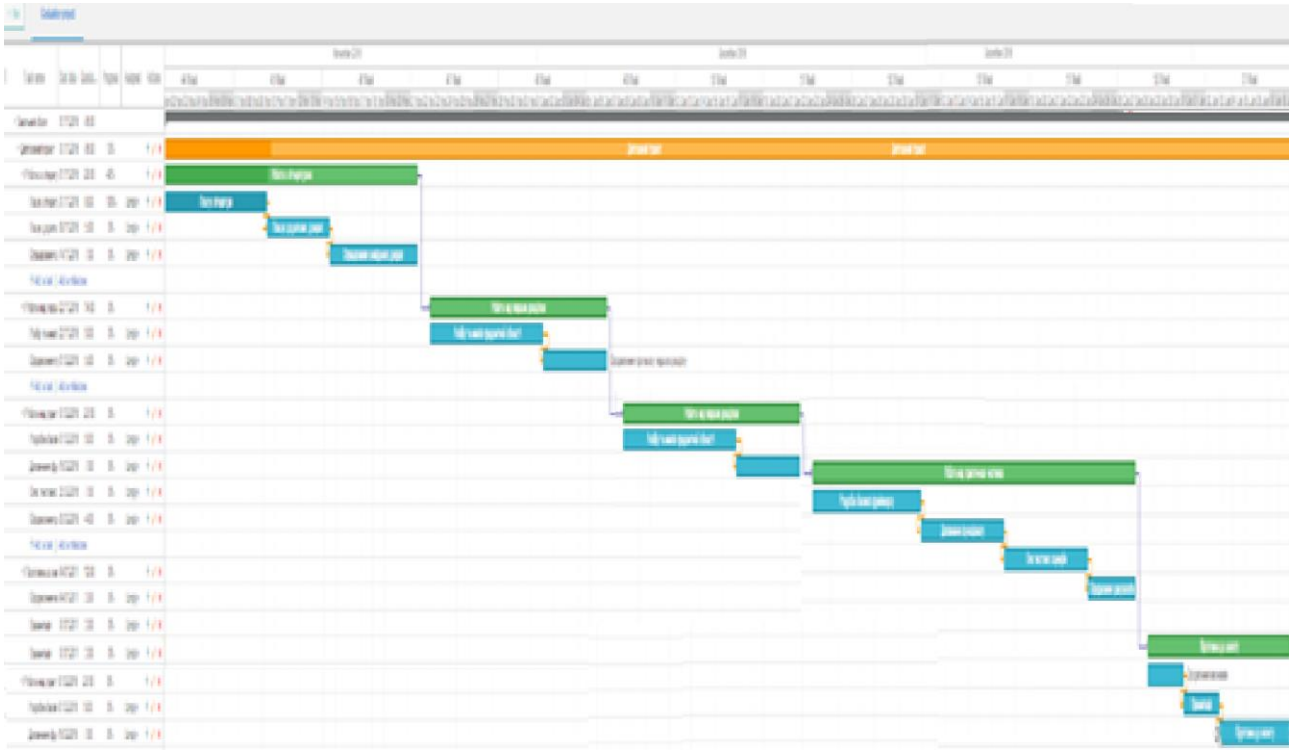


Рис. – 4.1.1 Діаграма Ганта по процесу роботи над дипломним проектом

План роботи:

1. Робота з літературою
   1.1. Пошук літератури
   1.2. Пошук додаткових джерел
   1.3. Опрацювання знайдених джерел
2. Робота над першим розділом
   2.1. Розбір та аналіз предметної області
   2.2. Оформлення протоколу першого розділу
3. Робота над другим розділом
   3.1. Розбір та аналіз предметної області
   3.2. Оформлення протоколу другого розділу
4. Робота над практичною частиною
   4.1. Дослідження бібліотек для використання

4.2.Реалізація методів

4.3.Тестування

4.4.Оформлення результатів

5. Підготовка до захисту

5.1.Оформлення висновків

5.2.Презентація

5.3.Підготовка до захисту

Оцінка тривалості робіт (оптимістична (**О)**– песимістична (**Р)** – реалістична (**М)**).

1. Робота з літературою (20 – 30 – 22)
2. Робота над першим та другим розділом (14 – 20 – 16)
3. Робота над практичною частиною (27 – 35 – 30)
4. Підготовка до захисту (12 – 15 – 13)

Таблиця 4.1 – Оцінка параметрів дипломної роботи

№	Р	М	О	Дисп.	Ср.ст.от.	Те
1	30	22	20	2,56	1,6	23
2	20	16	14	1	1	16,(3)
3	35	30	27	1,7	1,33	30,(3)
4	15	13	12	0,25	0,5	13,1(6)
∑	100	81	73	20,25	4,5	82,8(3)

Z = 0,66; F(z) = 0,74

Відповідно, із вірогідністю 74% проект буде завершений за 85 днів

3.2 Керування ризиками

Таблиця 4.2 – Таблиця ризиків проекту

Ризик	Подія	Вірогідність	Вплив
Вихід з ладу робочого комп'ютера	Збереження даних в хмарних сховищах	Низька	Сильний
Зміна вимог до дипломної роботи	Розраховувати час із запасом	Висока	Середнє
Зміна ліцензії фреймворків, що використовуються у роботі	Переробка проекту з використанням засобів із відкритими ліцензіями	Низька	Сильний
Зайнятість наукового керівника	Підготовка чітко сформульованих питань на кожну з консультацій, підтримання спілкування в мережі	Середня	Сильний
Відсутність в мережі достатньої кількості літератури по темі дослідження	Заздалегідь дізнатися назви наукових журналів по даній тематиці, дізнатися наявність літератури в бібліотеці	Низька	Середній
Завантаження додатковою діяльністю (робота)	Виконання більшості задач заздалегідь до кінцевих строків	Середня	Середній
Відсутність достатніх знань та навичок у роботі з інструментами для виконання завдання	Виділення більшої кількості часу на вивчення та роботи над завданням, виконання більш чіткого планування	Середня	Слабкий

4.3 Висновки

У розділі було сплановано процес підготовки дипломного проекту, за розрахунками, вірогідність закінчення роботи в запланований термін дорівнює 74%, що є досить непоганим результатом для початкового планування, що свідчить добрій спланованості процесу. Однак, при більш детальному розпланування часу, якість процесу виконання можна підвисити. Також було описано таблицю ризиків та описано засоби запобігання та протидії цим ризикам.

ВИСНОВКИ

Під час написання даної роботи були розкриті дві досить великі теми: аутентифікація користувача і розпізнавання обличчя. Були проаналізовані методи аутентифікації особи, розглянутий такий великий пласт, як біометрична аутентифікація та обраний для використання і дослідження один із них – розпізнавання обличчя. Були розглянуті методи розпізнавання обличчя та виділені ті, які можуть бути використані на мобільних пристроях.

У третьому розділі були враховані всі обмеження, встановленні використанням додатку на мобільних пристроях та обрані методи розпізнавання обличчя, які задовольняли встановлені критерії. У цьому розділі було реалізовано додаток, використовуючи таку бібліотеку як OpenCV, ліцензія якої є вільною, а рівень самої бібліотеки – професійним.

Реалізувавши додаток були виявлені деякі місця для покращення додатку. Детально ці моменти і пропозиції їх вирішення описані у висновках третього розділу.

Ціль даної роботи була досягнута, результатами цієї роботи є аналіз методів аутентифікації, методів розпізнавання обличчя, а також розроблений мобільний додаток, який дав змогу протестувати методи у реальних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Анализ существующих подходов к распознаванию лиц. [Электронный ресурс]. - Режим доступа: https://habrahabr.ru/company/synesis/blog/238129/. - Дата доступа: 13.05.2016
2. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие.- СПб.: Изд-во СПбГУЭФ, 2010.- 267 с.
3. Галатенко В.А. Идентификация и аутентификация, управление доступом лекция из курса «Основы информационной безопасности». - Интернет Университет Информационных Технологий, 2010г.
4. Зиновьев А. Ю., Визуализация многомерных данных, Красноярск, Изд. КГТУ, 2000.
5. Метод главных компонент - Википедия. [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/ Метод_главных_компонент. - Дата доступа: 13.04.2016
6. Распознавание лиц [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/Распознавание_лиц. - Дата доступа: 13.05.2016
7. Тихонов И.А. Информативные параметры биометрической аутентификации пользователей информационных систем 2010. № 9. С. 26-32.
8. Цирлов В.Л. Основы информационной безопасности автоматизированных систем: краткий курс. - Феникс, 2008 г.
9. Face Recognition. [Электронный ресурс]. - Режим доступа: https://play.google.com/store/apps/details?id=com.vinisoft.facesdk.demo&hl=ru. - Дата доступа: 13.05.2016
10. Hyvdrinen A, Karhunen J., and Oja E., Independent Component Analysis, A Volume in the Wiley Series on Adaptive and Learning Systems for Signal Processing, Communications, and Control. — John Wiley & Sons, Inc., 2001.

11. Muresan D. D., Parks T. W., Adaptive Principal Components and Image Denoising, in: Image Processing, 2003, Proceedings 2003 IEEE International Conference on Image Processing (ICIP), 14-17 Sept. 2003, V. 1, pp. I-101-104
12. Rao, K., Yip P. (eds.), The Transform and Data Compression Handbook, CRC Press, Baton Rouge, 2001.
13. Scholz M., Fraunholz M., Selbig J., Nonlinear Principal Component Analysis: Neural Network Models and Applications, In: Gorban A. N. et al (Eds.), LNCSE 58, Springer, 2007 ISBN 978-3-540-73749-0
14. Zinovyev A., Cluster structures in genomic word frequency distributions, 14-17 Sept. 2003, V. 1, pp. I-101-104

ДОДАТОК А. ПРИКЛАД КОДУ МЕТОДУ LBPH

```
#include
"lbp.hpp"
            using namespace cv;
            template <typename _Tp>
            void lbp::OLBP_(const Mat& src, Mat& dst) {
                  dst = Mat::zeros(src.rows-2, src.cols-2, CV_8UC1);
                  for(int i=1;i<src.rows-1;i++) {
                        for(int j=1;j<src.cols-1;j++) {
                              _Tp center = src.at<_Tp>(i,j);
                              unsigned char code = 0;
                              code |= (src.at<_Tp>(i-1,j-1) > center) << 7;
                              code |= (src.at<_Tp>(i-1,j) > center) << 6;
                              code |= (src.at<_Tp>(i-1,j+1) > center) << 5;
                              code |= (src.at<_Tp>(i,j+1) > center) << 4;
                              code |= (src.at<_Tp>(i+1,j+1) > center) << 3;
                              code |= (src.at<_Tp>(i+1,j) > center) << 2;
                              code |= (src.at<_Tp>(i+1,j-1) > center) << 1;
                              code |= (src.at<_Tp>(i,j-1) > center) << 0;
                              dst.at<unsigned char>(i-1,j-1) = code;
                        }
                  }
            }
            template <typename _Tp>
            void lbp::ELBP_(const Mat& src, Mat& dst, int radius, int neighbors) {
                  neighbors = max(min(neighbors,31),1); // set bounds...
                  // Note: alternatively you can switch to the new OpenCV Mat_
                  // type system to define an unsigned int matrix... I am probably
                  // mistaken here, but I didn't see an unsigned int representation
                  // in OpenCV's classic typesystem...
                  dst = Mat::zeros(src.rows-2*radius, src.cols-2*radius, CV_32SC1);
                  for(int n=0; n<neighbors; n++) {
                        // sample points
                        float x = static_cast<float>(radius) *
            cos(2.0*M_PI*n/static_cast<float>(neighbors));
                        float y = static_cast<float>(radius) * -
            sin(2.0*M_PI*n/static_cast<float>(neighbors));
                        // relative indices
                        int fx = static_cast<int>(floor(x));
                        int fy = static_cast<int>(floor(y));
                        int cx = static_cast<int>(ceil(x));
                        int cy = static_cast<int>(ceil(y));
                        // fractional part
                        float ty = y - fy;
                        float tx = x - fx;
                        // set interpolation weights
                        float w1 = (1 - tx) * (1 - ty);
```

```
                float w2 =      tx  * (1 - ty);
                float w3 = (1 - tx) *      ty;
                float w4 =      tx  *      ty;
                // iterate through your data
                for(int i=radius; i < src.rows-radius;i++) {
                        for(int j=radius;j < src.cols-radius;j++) {
                                float t = w1*src.at<_Tp>(i+fy,j+fx) +
w2*src.at<_Tp>(i+fy,j+cx) + w3*src.at<_Tp>(i+cy,j+fx) + w4*src.at<_Tp>(i+cy,j+cx);
                                // we are dealing with floating point precision, so add
some little tolerance
                                dst.at<unsigned int>(i-radius,j-radius) += ((t >
src.at<_Tp>(i,j)) && (abs(t-src.at<_Tp>(i,j)) >
std::numeric_limits<float>::epsilon())) << n;
                        }
                }
        }
}
template <typename _Tp>
void lbp::VARLBP_(const Mat& src, Mat& dst, int radius, int neighbors) {
        max(min(neighbors,31),1); // set bounds
        dst = Mat::zeros(src.rows-2*radius, src.cols-2*radius, CV_32FC1); //! Result
        // allocate some memory for temporary on-line variance calculations
        Mat _mean = Mat::zeros(src.rows, src.cols, CV_32FC1);
        Mat _delta = Mat::zeros(src.rows, src.cols, CV_32FC1);
        Mat _m2 = Mat::zeros(src.rows, src.cols, CV_32FC1);
        for(int n=0; n<neighbors; n++) {
                // sample points
                float x = static_cast<float>(radius) *
cos(2.0*M_PI*n/static_cast<float>(neighbors));
                float y = static_cast<float>(radius) * -
sin(2.0*M_PI*n/static_cast<float>(neighbors));
                // relative indices
                int fx = static_cast<int>(floor(x));
                int fy = static_cast<int>(floor(y));
                int cx = static_cast<int>(ceil(x));
                int cy = static_cast<int>(ceil(y));
                // fractional part
                float ty = y - fy;
                float tx = x - fx;
                // set interpolation weights
                float w1 = (1 - tx) * (1 - ty);
                float w2 =      tx  * (1 - ty);
                float w3 = (1 - tx) *      ty;
                float w4 =      tx  *      ty;
                // iterate through your data
                for(int i=radius; i < src.rows-radius;i++) {
                        for(int j=radius;j < src.cols-radius;j++) {
                                float t = w1*src.at<_Tp>(i+fy,j+fx) +
```

```
w2*src.at<_Tp>(i+fy,j+cx) + w3*src.at<_Tp>(i+cy,j+fx) + w4*src.at<_Tp>(i+cy,j+cx);
                                _delta.at<float>(i,j) = t - _mean.at<float>(i,j);
                                _mean.at<float>(i,j) = (_mean.at<float>(i,j) +
(_delta.at<float>(i,j) / (1.0*(n+1)))); // i am a bit paranoid
                                _m2.at<float>(i,j) = _m2.at<float>(i,j) +
_delta.at<float>(i,j) * (t - _mean.at<float>(i,j));
                        }
                }
        }
        // calculate result
        for(int i = radius; i < src.rows-radius; i++) {
                for(int j = radius; j < src.cols-radius; j++) {
                        dst.at<float>(i-radius, j-radius) = _m2.at<float>(i,j) /
(1.0*(neighbors-1));
                }
        }
}
/ now the wrapper functions
void lbp::OLBP(const Mat& src, Mat& dst) {
        switch(src.type()) {
                case CV_8SC1: OLBP_<char>(src, dst); break;
                case CV_8UC1: OLBP_<unsigned char>(src, dst); break;
                case CV_16SC1: OLBP_<short>(src, dst); break;
                case CV_16UC1: OLBP_<unsigned short>(src, dst); break;
                case CV_32SC1: OLBP_<int>(src, dst); break;
                case CV_32FC1: OLBP_<float>(src, dst); break;
                case CV_64FC1: OLBP_<double>(src, dst); break;
        }
}
void lbp::ELBP(const Mat& src, Mat& dst, int radius, int neighbors) {
        switch(src.type()) {
                case CV_8SC1: ELBP_<char>(src, dst, radius, neighbors); break;
                case CV_8UC1: ELBP_<unsigned char>(src, dst, radius, neighbors); break;
                case CV_16SC1: ELBP_<short>(src, dst, radius, neighbors); break;
                case CV_16UC1: ELBP_<unsigned short>(src, dst, radius, neighbors);
break;
                case CV_32SC1: ELBP_<int>(src, dst, radius, neighbors); break;
                case CV_32FC1: ELBP_<float>(src, dst, radius, neighbors); break;
                case CV_64FC1: ELBP_<double>(src, dst, radius, neighbors); break;
        }
}
void lbp::VARLBP(const Mat& src, Mat& dst, int radius, int neighbors) {
        switch(src.type()) {
                case CV_8SC1: VARLBP_<char>(src, dst, radius, neighbors); break;
                case CV_8UC1: VARLBP_<unsigned char>(src, dst, radius, neighbors);
break;
                case CV_16SC1: VARLBP_<short>(src, dst, radius, neighbors); break;
                case CV_16UC1: VARLBP_<unsigned short>(src, dst, radius, neighbors);
```

```
break;
                case CV_32SC1: VARLBP_<int>(src, dst, radius, neighbors); break;
                case CV_32FC1: VARLBP_<float>(src, dst, radius, neighbors); break;
                case CV_64FC1: VARLBP_<double>(src, dst, radius, neighbors); break;
        }
}
// now the Mat return functions
Mat lbp::OLBP(const Mat& src) { Mat dst; OLBP(src, dst); return dst; }
Mat lbp::ELBP(const Mat& src, int radius, int neighbors) { Mat dst; ELBP(src, dst,
radius, neighbors); return dst; }
Mat lbp::VARLBP(const Mat& src, int radius, int neighbors) { Mat dst; VARLBP(src,
dst, radius, neighbors); return dst; }
```