ВСТУП

Ми живемо на межі двох тисячоліть, коли людство вступило в епоху нової науково-технічної революції.

До кінця двадцятого століття люди оволоділи багатьма таємницями перетворення речовини та енергії і зуміли використати ці знання для покращення свого життя. Але крім речовини і енергії в житті людини величезну роль грає ще одна складова - інформація. Це найрізноманітніші відомості, повідомлення, звістки, знання, вміння.

У середині минулого століття з'явилися спеціальні пристрої - комп'ютери, орієнтовані на зберігання і перетворення інформації і сталася комп'ютерна революція.

Інформацією володіють і використовують її всі люди без винятку. Кожна людина вирішує для себе, яку інформацію йому необхідно отримати, яка інформація не повинна бути доступна іншим і т.д. Людині легко, зберігати інформацію, яка у нього в голові, а як бути, якщо інформація занесена в «мозок машини», до якої мають доступ багато людей.

З кінця 80-их початку 90-их років проблеми пов'язані із захистом інформації турбують як фахівців в галузі комп'ютерної безпеки так і численних рядових користувачів персональних комп'ютерів. Це пов'язане з глибокими змінами вносяться комп'ютерною технологією в наше життя. Змінився сам підхід до поняття "інформація". Цей термін зараз більше використовується для позначення спеціального товару який можна купити, продати, обміняти на щось інше і т.д. При цьому вартість подібного товару найчастіше перевершує в десятки, а то і в сотні разів вартість самої обчислювальної техніки, в рамках якої він функціонує.

Природно, виникає потреба захистити інформацію від несанкціонованого доступу, крадіжки, знищення та інших злочинних дій. Проте, велика частина користувачів не усвідомлює, що постійно ризикує своєю безпекою і особистими таємницями. І лише небагато хоч якимось

чином захищають свої дані. Користувачі комп'ютерів регулярно залишають повністю незахищеними навіть такі дані як податкова і банківська інформація, ділове листування та електронні таблиці. Проблеми значно ускладнюються, коли ви починаєте працювати або грати в мережі так як хакеру набагато легше в цей час дістати або знищити інформацію, що знаходиться на вашому комп'ютері.

РОЗДІЛ 1 ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

1.1 Суть технічної проблеми, що виникла на сучасному етапі розвитку науки, техніки і промисловості

З початку свого розвитку в 80-х роках минулого століття біометрична технологія не тільки стрімко просунулася у своєму розвитку, але і перетворилася в складну комплексну галузь з безліччю різних напрямків. Однак, якщо подивитися на кожну з біометричних технологій, упадає в око, що в той час як усі вони покликані вирішувати ті самі задачі в досягненні єдиної мети, їхні розроблювачі і виробники дотримують різних філософських і методологічних підходів до досягнення даної мети. При цьому, звичайно ж, кожна група фахівців упевнена, що рішення, що просувається ними, є найбільш ефективним.

У зв'язку з тим, що ідентифікація по відбитках пальців є найбільш просунутим біометричним напрямком, у яке з кожним роком утягує усе більше і більше гравців, саме у відношенні цієї технології мається найбільш розгорнута інформація. З ростом конкуренції ці самі гравці усе менше відгороджуються завісою таємності, тому що на конкурентному ринку вони повинні використовувати більш повні зведення про свій виріб або програмне забезпечення для того, щоб довести світові і своїм потенційним клієнтам перевага їхньої продукції над всіма іншими.

Відбитки пальців стали дійсно біометричним параметром, що найбільше широко використовується в усім світі і використовується більш ніж у 50% усіх сучасних біометричних систем. Біометрія, як наука вивчення математичних або статистичних властивостей у фізіологічних і поведінкових людських характеристиках, широко використовується у сфері захисту інформації. Використання відбитків пальців в якості біометрії є одним з найстаріших методів автоматизованої ідентифікації особи і водночас найбільш поширеною в наш час. До числа факторів, які сприяють поширенню використання систем такого типу можна віднести: незначні

розміри та вартість апаратури для обробки зображень відбитків пальців, високопродуктивне апаратне забезпечення, степінь та швидкість розпізнавання, що відповідають вимогам програмного забезпечення, різкий ріст та розвиток мережних технологій та Інтернету, а також усвідомлення необхідності простих, базових методів захисту та безпеки інформації.

Отже, суть технічної проблеми полягає в розробці нового підходу до обробки зображення відбитка пальця з метою ідентифікації особистості, та обмеження доступу до комп'ютерних ресурсів.

1.2 Способи вирішення технічної проблеми

Необхідність вирішення проблеми захисту інформації на державному рівні викликала включення цієї проблеми до стратегії національної безпеки та прийняття Закону "Про електронний підпис". Це не останній законодавчий акт в цьому напрямі, оскільки комплексне вирішення проблеми передбачає створення єдиної правової, організаційної та матеріально-технічної бази.

Коли говорять про захист даних, то мають на увазі дві основних небезпеки втрати даних: пошкодження даних і несанкціонованого доступу до них. Боротьба з обома небезпеками ведеться апаратними і програмними засобами та організаційними заходами.

1.3 Класифікація методів і засобів захисту інформації

У теперішній час розвиток комп’ютерної техніки та технологій призвів до впровадження інформаційних систем практично на усіх підприємствах, в організаціях, наукових установах, силових структурах, тощо. Сьогодні різні види інформації – наукова, технічна, технологічна, фінансова, тощо – накопичуються у електронній формі та використовуються співробітниками через комп’ютерні мережі. Зважаючи на шкоду, яку може завдати

несанкціонований доступ до таких даних чи їх спотворення, на перший план виходять проблеми захисту інформаційних систем.

Проблема захисту інформації є далеко не новою. Вирішувати її люди намагалися з давніх часів. Втрата недокументованих електронних даних спричиняла необхідність повторного виконання необхідної обробки інформації. В деяких випадках втрата вихідних даних робила неможливою повторну обробку інформації, а отже, і втрату важливих результатів.

Захист даних, а, отже, і захист інформації - комплексна проблема, яка є частиною національної безпеки. Необхідність вирішення проблеми захисту інформації на державному рівні викликала включення цієї проблеми до стратегії національної безпеки та прийняття Закону "Про електронний підпис". Це не останній законодавчий акт в цьому напрямі, оскільки комплексне вирішення проблеми передбачає створення єдиної правової, організаційної та матеріально-технічної бази.

Коли говорять про захист даних, то мають на увазі дві основних небезпеки втрати даних: пошкодження даних і несанкціонованого доступу до них. Боротьба з обома небезпеками ведеться апаратними і програмними засобами та організаційними заходами.

Існують різні класифікації методів та способів захисту інформації. За способами здійснення усі заходи забезпечення безпеки комп'ютерних мереж поділяються на: правові (законодавчі), морально-етичні, організаційні (адміністративні), фізичні, технічні (апаратно-програмні). За Воликом О.Ф. сукупність методів і засобів захисту інформації включає програмні й апаратні засоби, захисні перетворення та організаційні заходи (рис. 1.1).

Апаратний, або схемний, захист полягає в тому, що в приладах ЕОМ та інших технічних засобах обробки інформації передбачається наявність спеціальних схем, що забезпечують захист і контроль інформації, наприклад, схеми контролю на чесність, які контролюють правильність передачі інформації між різними приладами ЕОМ, а також екрануючими приладами, що локалізують електромагнітні випромінювання.

Рисунок 1.1 - Методи і засоби захисту інформації

Програмні методи захисту — це сукупність алгоритмів і програм, які забезпечують розмежування доступу та виключення несанкціонованого використання інформації.

Сутність методів захисних перетворень полягає в тому, що інформація, яка зберігається в системі та передається каналами зв'язку, подається в деякому коді, що виключає можливість її безпосереднього використання.

Організаційні заходи із захисту інформації містять сукупність дій з підбору та перевірки персоналу, який бере участь у підготовці й експлуатації програм та інформації, чітке регламентування процесу розробки та функціонування інформаційної системи.

Лише комплексне використання різних заходів може забезпечити надійний захист інформації, тому що кожний метод або захід має слабкі та сильні сторони.

1.4 Програмні методи захисту інформації

Під програмними засобами захисту інформації розуміють спеціальні програми, що включаються до складу програмного забезпечення інформаційних систем виключно для виконання захисних функцій. Програмні методи захисту призначаються для безпосереднього захисту інформації за трьома напрямками:

а) апаратури;

б) програмного забезпечення;

в) даних і керуючих команд.

До основних програмних засобів захисту інформації відносяться: програми ідентифікації і аутентифікації користувачів інформаційних систем; програми розмежування доступу користувачів до ресурсів інформаційних систем; програми шифрування інформації; програми захисту інформаційних ресурсів (системного і прикладного програмного забезпечення, баз даних, комп'ютерних засобів навчання) від несанкціонованої зміни, використання та копіювання.

Ідентифікація і аутентифікація - це перша лінію оборони, «прохідна» інформаційного простору організації або установи. Ідентифікація – процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою. Даний термін звичайно означає встановлення особистості користувача. Аутентифікація – процедура встановлення належності користувачеві в системі пред'явленого ним ідентифікатора. За допомогою аутентифікації система переконується, що суб'єкт справді той, за кого себе видає.

Існує дві найпоширеніших види ідентифікації:

– парольна ідентифікація. Кожен зареєстрований користувач системи одержує набір персональних реквізитів (звичайно використаються пари: логін-пароль).

– апаратна ідентифікація. Цей принцип ідентифікації ґрунтується на визначенні особистості користувача за певним предметом, ключем (електронні ключі, проксіміті-карти, смарт-карти, магнітні карти), що перебуває в його ексклюзивному користуванні.

Методи аутентифікації умовно можна поділити на однофакторні та двофакторні. Однофакторні методи діляться на:

– логічні (паролі, ключові фрази, які вводяться з клавіатури комп'ютера чи клавіатури спеціалізованого пристрою);

– ідентифікаційні (носієм ключової інформації є фізичні об'єкти: дискета, магнітна карта, смарт-карта, штрих-кодова карта тощо);

– біометричні (в їх основі - аналіз унікальних характеристик людини, наприклад: відбитки пальців, малюнок райдужної оболонки ока, голос, обличчя).

Надійна ідентифікація і аутентифікація уповільнюється низкою принципових причин. По-перше, комп'ютерна система ґрунтується на інформації в тому вигляді, в якому вона була отримана; строго кажучи, джерело інформації залишається невідомим. По-друге, майже всі аутентифікаційні відомості можна почути, вкрасти чи підробити. По-третє, є протиріччя між надійністю аутентифікації з одного боку, і зручностями користувача і системного адміністратора з іншого. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно вводити аутентифікаційну інформацію (адже на його місце могла сісти інша людина), але це підвищує вірогідність підглядання за введенням. По-четверте, чим надійніший засіб захисту, тим він дорожчий.

Найбільш поширеним засобом аутентифікації є паролі. Система порівнює введений і раніше заданий для даного користувача пароль; у разі збігу справжність користувача вважається доведеною. Інший засіб, поступово набирає популярність і забезпечує найбільшу ефективність, - секретні криптографічні ключі користувачів.

Останнім часом здобуває популярність аутентифікація шляхом з’ясування координат користувача. Ідея у тому, щоб користувач посилав координати супутників системи GPS (Global Positioning System), що знаходяться у зоні прямої видимості. Сервер аутентифікації знає орбіти всіх супутників, тому можна з точністю до метру визначити місцезнаходження користувача. Оскільки орбіти супутників не завжди стабільні, передбачити які дуже складно, підробка координат виявляється практично неможливою. Нічого не дає і перехоплення координат - вони постійно змінюються. Безперервна передача координат не потребує від користувача будь-яких додаткових зусиль, і тому він може легко багаторазово підтверджувати свою справжність. Апаратура GPS порівняно недорога і опробована, у тому випадку, коли легальний користувач має перебувати у певному місці, даний метод перевірки справжності є досить привабливим.

Дуже важливим і складним завданням є адміністрування служби ідентифікації і аутентифікації. Необхідно постійно підтримувати конфіденційність, цілісність і доступність відповідної інформації, що особливо непросто в мережевому різнорідному середовищі. Доцільно, поруч із автоматизацією, застосувати максимально можливу централізацію інформації. Досягти цього можливо, застосовуючи виділені сервери перевірки справжності (такі як Kerberos) чи кошти централізованого адміністрування (наприклад CA- Unicenter). Деякі операційні системи пропонують мережні сервіси, які можуть служити основою централізації адміністративних даних. Централізація полегшує роботу як системним адміністраторам, так і користувачам, оскільки це дозволяє реалізувати важливу концепцію єдиного входу. Раз пройшовши перевірку дійсності, користувач отримує доступ до всіх ресурсів мережі у межах своїх повноважень.

До переваг програмних засобів захисту інформації належать: простота тиражування; гнучкість (можливість налаштування на різні умови застосування, що враховують специфіку загроз інформаційній безпеці

конкретних інформаційних систем); простота застосування – одні програмні засоби, наприклад, шифрування, працюють в «прозорому» (непомітному для користувача) режимі, а інші не вимагають від користувача ніяких нових (порівняно з іншими програмами) навичок; практично необмежені можливості їх розвитку шляхом внесення змін для врахування нових загроз безпеці інформації.

Всі програми захисту, що здійснюють управління доступом до машинної інформації, функціонують за принципом відповіді на питання: хто може виконувати, які операції і над якими даними. Також до ефективних заходів протидії спробам несанкціонованого доступу відносяться засоби реєстрації. Для цих цілей найбільш перспективними є нові операційні системи спеціального призначення, що широко застосовуються в зарубіжних країнах і отримали назву моніторингу (автоматичного спостереження за можливою комп'ютерною загрозою).

Аналіз аналітичних даних дозволив встановити, що джерела загроз по відношенню до інформаційних систем можуть бути зовнішніми або внутрішніми (компоненти інформаційної системи – її апаратура, програми, персонал), а список загроз при забезпеченні цілісності інформації може бути таким: модифікація (спотворення) інформації; заперечення дійсності інформації; нав'язування хибної інформації. При забезпеченні ж доступності інформації можливе її блокування, або знищення самої інформації і засобів її обробки.

У разі безпосереднього впливу вірусу на систему, або при проведенні некваліфікованих лікувальних заходів компонентів інформаційної системи може бути втрачена інформація або спотворено програмне забезпечення. В умовах дії зазначених факторів тільки прийняття жорстких комплексних заходів безпеки за усіма можливими видами загроз дозволить контролювати постійно зростаючі ризики повної або часткової зупинки бізнес процесів в результаті вірусних заражень.

Таким чином, інформаційні системи та мережі просто не зможуть нормально функціонувати і розвиватися, ігноруючи проблеми захисту інформації. Організація надійної та ефективної системи захисту є одним з найважливіших завдань щодо забезпечення збереження інформації в мережі. Застосування ефективних засобів захисту інформації дозволить зменшити сумарні втрати від комп'ютерних злочинів, пов'язаних з несанкціонованих доступом до інформації.

1.5 Характеристика процесу вирішення проблеми

1.5.1 Обробка зображення відбитків

Після отримання зображення відбитка пальця необхідно здійснити його обробку. В процесі обробки, зображення повинне досягнути якомога кращої якості, що необхідно досягнути для здійснення коректного розпізнавання. Основні етапи процесу обробки зображення є наступними: усунення завад (шуму) та покращення чіткості, виявлення основних характеристик та саме розпізнавання.

Фільтрація зображення. У результаті того, що пальці можуть бути забруднені, пошкоджені, вологі чи сухі постає проблема максимально відфільтрувати зображення та зробити відображення папілярів та відстаней між ними більш чіткими. З цією метою виконуються 2 операції: адаптивна узгоджуюча і фільтрація та адаптивна порогова сегментація. Незважаючи на можливі обриви і неоднорідності окремих папілярів можна визначити їх напрям. Така фільтрація застосовується до кожного пікселя зображення. На основі даних про такого роду орієнтацію папілярів до кожного пікселя застосовується адаптивна узгоджуюча фільтрація для виділення папілярів, які орієнтовані в однаковому напрямку і приглушення на зображенні частинок протилежного напрямку. Проте і надалі можуть існувати шуми, які спричиняють ефект злиття сусідніх папілярів. Саме такі шуми можна забрати завдяки використанню узгоджуючих фільтрів. Фільтр є адаптивним оскільки

він сам орієнтується відносно напрямку папілярів, а узгоджуючим оскільки він має збільшувати та робити чіткішим зображення папілярів на пальцях. Після подавлення шумів проводиться виділення папілярів через бінаризацію зображення.

Проблема бінаризації полягає у нерівноміному розподілу яскравості по площині зображення. Наприклад, той самий папіляр може мати більшу інтенсивність посередині зображення, оскільки там палець був сильніше притиснений до сканера. Тому зазвичай, для обробки такого зображення використовується порогова сегментація. Тобто для кожної окремо взятої частини зображення визначаєтсья свій поріг контрасту. Останнім етапом виконання обробки зображення перед розпізнаванням є векторизація папілярів. Тобто товщина кожного папіляра зводиться до товщини одного пікселя.

Узгоджуюча фільтрація та векторизація вносять левову частку в часові затрати. Результати всіх подальших етапів обробки залежать від якості початкового зображення, яке надалі буде оброблятись. Тому економія заради збільшення швидкості обробки зображення не завжди виправдана в таких випадках. Це призведе до погіршення результатів розпізнавання, що в свою чергу спричинить необхідність повторів верифікації системою або визнання даних некоректними.

1.5.2 Виділення ключових ознак відбитку для ідентифікації

В даному випадку під ключовими ознаками потрібно вважати закінчення (кінець) папіляру та його роздвоєння. Саме по цим ознакам буде проводитись ідентифікація особ.

Як би детально не було зображення опрацьовано на попередніх етапах, все одно залишаться надлишкові та некоректні роздвоєння, які не були усунені і є своєрідним зашумленням рисунку. Наприклад, два закінчення папіляра, які знаходяться дуже близько один біля одного швидше за все

тепер будуть трактуватись як один суцільний папіляр, бо внаслідок зашумлення і не зовсім коректного аналізу він був розділений. Якщо знайдено дуже короткий папіляр, в якому відстань між його кінцями дуже коротка то це скоріш за все шум, який не буде братись до уваги і т.д.

1.5.3 Розпізнавання

На етапі розпізнавання відбиток який вимагає верифікації порівнюється з еталонним. Зазвичай таке розпізнавання робиться на основі порівняння сусідніх ознак на схожість. Кожна з таких ознак (тобто кінець папіляра або роздвоєння) містить три чи більше сусідніх ознак, кожна з яких знаходиться на певній відстані, та має певну орієнтацію відносно сусідніх ознак. Крім того, як уже зазначалось кожна ознака характеризується типом і напрямком, які теж порівнюються. Якщо в результаті розпізнавання виявляються дуже незначні відмінності між сусідніми ознаками на еталонному зразку і тому, який подано для верифікації, тоді вважається, що вони співпадають. Це проробляється для всіх ознак, і коли виявляється, що вони з заданою точністю співпадають тоді можна говорити про розпізнавання поданого на автентифікацію відбитку.

Результатом розпізнавання є виявлення кількості однакових ознак. Це число від 0 до n. Більша кількість співпадінь означає більшу ймовірність розпізнавання. Саме кількість співпадінь є мірою для встановлення порогової величини. Якщо ця кількість більша від порогової, тоді говорять про позитивну верифікацію, тобто відбитки відповідають еталонним, в іншому випадку це негативна верифікація. Значення порогу теж може коливатись. Є сенс збільшити порогове значення для підвищення надійності верифікації. Або відповідно навпаки – за зниженням порогової величини зменшується надійність верифікації і відповідно зменшується кількість неспівпадінь з еталоном.

Модифікації класичного підходу. Так як одна із найбільш складних задач обробки зображень відбитків пальців – це отримання чіткого зображення для виконання розпізнавання, є декілька методів її розв’язку. Більшість з цих методів використовують адаптивне розпізнавання окремих частин зображення [2,4,3]. Спочатку зображення розбивається на квадрати у яких визначаються характеристики папілярів та їх орієнтація. Орієнтація кожного участка визначається при обробці просторової чи частотної області виконанням двовимірного швидкого перетворення Фур’є.

Після бінаризації зображення, зазвичай виконується векторизація ліній папілярів. Однак існують методи обробки при яких етапи бінаризації та векторизації (обидва етапи вимагають значних обчислювальних витрат та можуть вносити шуми на зображення) опускаються. Є інший підхід, згідно з яким зображення папілярів отримуються з оригінального вхідного зображення в сірих тонах. Результатом є також зображення з виділеними кінцями та роздвоєннями на відбитку, як і в результаті традиційної обробки такого зображення. Розглянемо підхід детальніше.

Замість використання одного вікна(сегменту) для визначення розміщення та орієнтації папілярів використовується так званий мультивіконний режим, або режим мультирозширення [3]. Спочатку ведеться обробка зображення вибраного розміру. В ньому визначається орієнтованість папілярів, визначається наскільки чітко можна розрізнити кінці та роздвоєння. Якщо дане значення є меншим ніж визначений поріг, тоді дане вікно розділяється на чотири менші підвікна і те ж саме повторюється для кожного підвікна. Така процедура виконується до тих пір, поки отримане значення не стане більшим визначеного порогу для кожного підвікна. Цей метод використовується для уникнення згладжування на окремих частинах зображення, що дуже часто є характерним для центральної частини зображення.

Через значну складність порівняння характерних ознак на двох відбитках, порівняння сусідніх ознак, було одним з найдавніших способів

розв’язку задачі [13]. Спочатку ознаки групувались за близькістю розташування одна до одної. Таких сусідніх ознак могло бути від двох до чотирьох. І кожна з них порівнювалась відповідно з ознаками на іншому відбитку, що значно спрощувало завдання. Існує два етапи такого розпізнавання. Спочатку розпізнавання ведеться всередині окремих частин на обох відбитках. Потім проводиться глобальне розпізнавання, тобто аналізується повністю весь відбиток – вхідний і еталонний.

Проте через трудомісткість таких операцій було запропоноване певне покращення цього методу. Для цього визначається положення центра та дельт.

Центр і дельти зазвичай визначаються виходячи з напрямку папілярів. Кращим методом для визначення окремих точок на такій площині є використання індексів Пуанкаре [8,7]. Для кожної точки на схемі розташування сумуються кути розміщення відносно замкненої кривої в напрямку за годинниковою стрілкою. Для не вироджених точок ця сума рівна нулю, для центра вона рівна 180 градусів, а для дельти до 180 градусів.

Для зменшення часу обчислень при розпізнаванні було запропоновано також ряд інших методів розпізнавання характерних ознак. Один з підходів пропонує спочатку провести співставлення, а потім розпізнавати ознаки (це особливо актуально для методів, коли порівняння необхідно проводити раз, а розпізнавання багато разів). Лінійний перелік ознак складається при скануванні. Спочатку вибирається середина, а потім від неї рухаються до країв по спіралі. Таким чином одновимірні вектори, які містять характеристики кожної з ознак порівнюються на вхідному і еталонному відбитках. Іншим методом порівняння ознак є ступінчатий метод [10]. Будується граф атрибутів, в якому найближчі характерні ознаки сполучені ребрами, а вершинами є ознаки [9]. Ці вершини порівнюються на двох відбитках. Кількість співпадінь і визначає значення рівня ймовірності відповідності. Через такі незначні відмінності при порівнянні двох ознак розпізнавання може відбутись некоректно. Тому для кожної ознаки вводяться

додаткові характеристики, такі як довжина та кривизна папіляра, на якому її виявлено та аналогічні характеристики по відношенню до сусідніх ознак.

1.5.4 Порівняння

Відбитки можна порівнювати і через кореляцію. Якщо бути точним, то кореляція двох зображень включає в себе трансляцію одного зображення в інше. Виконується мультиплікація відповідних пікселів [15]. Тому пара відбитків, які співпадають, буде мати вище кореляційне значення. Порогове значення класифікації визначає чи достатньою є величина відповідності для того щоб даний відбиток був визначений як розпізнаний.

Кореляційний аналіз можна проводити не лише в просторовій, а і в частотній області [11]. Першим кроком в такому випадку буде виконання двовимірного швидкого перетворення Фур'є (ШПФ) над вхідним та еталонним зображеннями. Відбувається перетворення зображення в частотну область. Потім виконується перемноження кожного з пікселів двох перетворених зображень, а сума цих перемножених результатів в частотній області і є еквівалентом кореляційного значення, яке отримується таким самим чином в просторовій області. Перевагою виконання такої обробки в частотній області є те, що відбитки стають незалежними при перетворенні, це означає що вони не повинні вирівнюватись з точки зору перетворення, оскільки початки координат для двох зображень є нульове значення частоти.

Кореляція в частотній області може виконуватись не лише цифровими засобами [14], а й оптичними системами. Це досягається використанням лінз та лазерного освітлення. При розкладанні призмою променя в частотний ряд, відбувається частотне перетворення. Аналогічним чином вхідне та еталонне зображення відбитків пальців пропускаються за допомогою лазерного світла через лінзу для виконання перетворення Фур'є. Їхні накладання спричиняють

піки кореляції чиє значення є надзвичайно важливим при розпізнаванні відбитків. Перевагою такої оптичної обробки зображення є те, що швидкість операцій це і є по суті швидкість світла, що є значно швидшим, ніж швидкість обробки звичайними цифровими процесорами. В будь-якому випадку оптичні процесори не є настільки гнучко програмованими як цифрові, і в зв'язку з цим вони дуже рідко використовуються в комерційних проектах та системах.

Однією з модифікацій просторової кореляції є обробка не окремих пікселів самого зображення, а виконання операцій над рядками пікселів або над ознаками, які виявлені в даних рядках [5, 6]. Вхідне та еталонне зображення спочатку вирівнюються, а потім розділяються на частинки цими рядками. Характеристики папілярів визначаються для кожної частинки в рядку: середня інтенсивність кольору, напрям папіляра, частота, кількість папілярів у рядку. Відповідні частинки рядка порівнюються на наявність однакових ознак. Якщо значна частка ознак співпадає, тоді кажуть про високу ймовірність розпізнавання даного відбитка.

Кореляційний метод виконується швидше, особливо в системах, які виконують ШПФ на апаратному рівні. Проте він гірше справляється із зображеннями залежними від зовнішніх факторів та зашумленими зображеннями.

При проведенні верифікації відбитків пальців можна виділити наступні проблеми:

1. Зображення папілярів матимуть різні відповідні відображення. Можна встановити орієнтири такі як центр чи дельта, але якщо їх встановити чітко неможливо, тоді подальше розпізнавання не матиме сенсу.

2. На двох відбитках може бути різний кут повороту. Якщо на відбитку знайдено відповідний орієнтир, то можна спробувати обертати зображення для кращого співпадіння відносно цього орієнтиру. Проте, в процесі такої обробки можуть виникати помилки. А також в даному випадку будуть значні

обчислювальні витрати через те, що кожен раз повертаючи доведеться знову обробляти ціле зображення.

3. Через те що шкіра є еластичною, відбитки можуть співпадати по розміщенню і напрямку, проте окремі частини, особливо з країв можуть не співпадати.

4. І нарешті, неминуча проблема зашумлення зображення. Два зображення для яких треба зробити розпізнавання можуть бути різної якості і зображення відбитків пальців могло бути зроблене за різних умов (температура, вологість шкіри) чи різними пристроями, тому вони можуть відрізнятись.

Степінь розпізнавання. Основна міра рентабельності систем розпізнавання, в кожному окремому випадку, це степінь розпізнавання. Це значення описується двома величинами. Кількість прийняття хибних результатів (false acceptance rate - FAR) - це кількість виявлених хибних співпадінь в співвідношенні до всіх виконаних порівнянь. Альтернативною величиною є неприйняття хибних результатів (false rejection rate - FRR) – це співвідношення кількості хибних неспівпадінь до загальної кількості порівнянь. Значення FAR та FRR можуть заміняти одне одного.

Тобто система врівноважується коливанням цих двох величин - збільшення одної величини призводить до зменшення іншої і навпаки. FAR по-іншому називають рівнем хибних співпадінь або помилкою другого рівня, а FRR називають рівнем хибних неспівпадінь або помилкою першого рівня. Обидві величини визначаються на проміжку від 0 до 1, або у відсотковому співвідношенні.

Крива ROC (робоча характеристика отримувача) будується на основі залежності FAR та FRR харатеристик. FAR відкладається на осі x як незалежна величина. По осі y відкладається залежна величина FRR. Вісь x є логарифмічною. На рисунку 6 зображено дві криві суцільними лініями і три пунктиром. Суцільні лінії не відображають конкретних даних, вони наведені для того щоб відобразити межі характеристик.

Процедура обрахунків за допомогою такої кривої є наступною. Вибирається достатній рівень величини FAR. Пунктирна лінія встановлена на 0,01% FAR. FRR, який відповідає даному значенню в даному випадку буде приблизно на рівні 4%. Можна визначати дані і в зворотному порядку, тобто визначати FAR за FRR.

Проте дані які обчислюють за даними кривими не є стандартними і однаковими для всіх програм розпізнавання. Наприклад у військовій промисловості значення FAR є дуже важливе, і його намагаються мінімізувати наскільки це можливо (навіть до 0,001%). Однак, це відбивається на значенні FRR. В такому випадку його величина може досягати значення навіть 5-20%.

Для ведення та збору статистичної інформації необхідна наступна інформація: кількість зразків, опис типу процедури верифікації. Розмір зразка може містити таку інформацію: кількість людей, кількість відбитків, кількість відбитків для кожного пальця. Крім того кількість співпадінь і не співпадінь має бути усереднена. Наприклад, база буде містити дані про 100 людей. У кожної людини було взято відбитки двох пальців, по 4 зображення для кожного пальця. Тобто загалом є 100x4x2=800 відбитків у базі. Якщо кожне зображення для кожного пальця (200) порівнювати із іншими зображеннями для того ж пальця отримаємо 1200 порівнянь відбитків. Якщо зображення одного відбитка порівнюється з усіма відбитками для інших пальців , тоді це буде 158400 порівнянь при розпізнаванні. Це говорить про неефективність існуючих методів. Якщо у базу даних помістити кілька мільйонів відбитків, то чекати результату доведеться дуже довго. Для зменшення кількості операцій верифікації, відбитки можна класифікувати і відповідно пошук проводити по розбитим групам.

Цілий ряд компаній у своїй роботі виходить з допущення, що відбитки пальців можуть бути розділені на визначені категорії. Склалася загальна думка, що усі відбитки пальців по своєму типу підпадають під 5-7 категорій (у залежності від класифікаційної школи, на яку ви орієнтуєтеся). Таким

чином, теоретично, при перевірці конкретного відбитка по великій базі даних швидкість процесу ідентифікації значно зросте, тому що приблизно 4/5 (або 4/7) обсягу всієї бази даних можуть бути відразу ж виключені як невідповідні категорії даного відбитка.

Звичайно, це стало би ефектним проривом у справі ідентифікації, однак, на жаль, даний підхід ще вимагає доробки. Проблема полягає в тому, що поки не вироблено досить точні принципи, закладені в основу визначення параметрів кожної з категорій. При проведенні спробних тестів великої кількості відбитків експерти мали різну думку з приводу приналежності до конкретної категорії для 17% відбитків. Така погрішність, природно, є неприйнятною для ідентифікаційної класифікації. Однак, справедливості заради, варто визнати, що якщо уже вчені дотепер посилено просувають цю теорію, то за умови виділення їм необхідних інвестицій ми вже в недалекому майбутньому майже напевно побачимо застосування даної методології на практиці.

Порівняння по деталях або по зображенню в цілому. Найбільше широко використовувані сьогодні методи порівняння зводяться до двох:

– по окремих деталях відбитка;
– по його зображенню в цілому.

У першому випадку визначається набір координат для заздалегідь визначеної кількості "географічних" крапок відбитка пальця, таких як місця перетинання ліній, розташування потових пір, початку і кінця "хребтів" і "долин". Ці координати за допомогою спеціальної формули перераховуються, у результаті чого видається унікальний багатоцифровий ідентифікаційний номер для кожного конкретного відбитка, що згодом може бути використаний для пошуку найближчого за значенням номера при роботі з варіанта 1:N або точно такого ж номера при порівнянні по варіанті 1:1.

Використовувані параметри повинні бути точно визначені і погоджені, тому що існує імовірність того, що при фіксації того самого відбитка пальців у різний час можуть бути не абсолютно однакові значення

ідентифікаційного номера. Причиною таких розбіжностей можуть служити різні умови, що змінюються, такі як розходження в орієнтації пальця або його стани, електронний шум у програмної складові устаткування, швидкість переміщення пальця.

Другим найбільш розповсюдженим методом є порівняння по зображенню в цілому, коли зафіксоване зображення накладають на відбиток, наявний для порівняння, щоб визначити ступінь їхньої подібності. Звичайно, цей процес займає більше часу при ідентифікації по варіанті 1:N, але є досить швидким для порівняння 1:1 з даними смарт-карти, що містять всього одне зображення. Існує також ряд інших методів, заснованих на різновидах вищеописаних.

"За" и "Проти". Як у випадку будь-якої технології, в ідентифікації по відбитках пальців є і свої переваги, і свої слабкі сторони. Однак, з огляду на широке використання цієї методики, сильні сторони "переважують" і полягають, в основному, в удобстві практичного застосування, простоті використання і, звичайно ж, у тім, що, у першу чергу, хвилює споживача, - у ціні!

Переваги:

– перевірена і випробувана технологія - тривале практичне використання в порівнянні з іншими біометричними підходами;

– деталі відбитка пальця залишаються незмінними на всьому протязі життя;

– ефективне рішення з погляду вартості: ціни на зчитувачі відбитків пальців різко знизилися - приблизно від $100 усього кілька років назад до $10 у наші дні;

– прийнятна точність у порівнянні з іншими біометричними рішеннями і з урахуванням вартості;

– ненав'язливий метод ідентифікації, простому і швидкий у використанні;

– велика кількість потенційних можливостей застосування;

– легкий для мініатюризації з метою застосування в устаткуванні різних типів - наприклад, у мобільних телефонах, комп'ютерах, смарт-картах.

Недоліки:

– неможливість потайливого застосування в силу того, що для нормального функціонування вимагає повної взаємодії з конкретною людиною;

– клеймо, що усе ще зв'язує відбитки пальців із кримінальним світом;

– слабке розпізнавання може відбуватися через тимчасові зміни відбитка пальців, зв'язаних, наприклад, з порізами, шкірною хворобою, улученням бруду, стертими відбитками;

– слабке розпізнавання може відбуватися через розходження в розмірах і орієнтації відсканованого відбитка в порівнянні з зображенням, занесеним у базу даних.

В усім світі до цієї технології виявляється величезний інтерес - особливо в тих галузях, де ідентифікація по відбитках пальців може бути інтегрована досить просто і без особливих витрат у вже існуючі системи безпеки. У результаті в різних куточках планети з'являються всі нові і нові компанії, що спеціалізуються на проектуванні, розробці, виробництві і впровадженні біометричної технології, що використовує відбитки пальців.

Деякі з них - порівняно невеликі фірми, однак інших можна зарахувати до промислових гігантів. Нижче наведено список декількох компаній, що активно працюють у цій сфері:

– NEC Electronics Corp (США);

– IDTECK Co. Ltd. (Корея);

– ISL Informer Systems Ltd. (Великобританія);

– Lightuning (Тайвань);

– BMF Corporation (Японія);

– Identix (Великобританія);

– Digital Persona (США);

- Fingerprint Cards (Швеція);
- Idencom (Німеччина);
- Neurotechnologija Ltd. (Литва);
- SAFLINK Corp. (США);
- Technoimagia Co. Ltd. (Японія);
- TSSI (Великобританія).

1.6 Загальний висновок про доцільність розробки

Приведено класичний підхід для розпізнавання особи за відбитками пальців, методів захисту комп'ютерних ресурсів, та на базі нього проведено порівняльний аналіз методів ідентифікації та верифікації зображень відбитків пальців, та методів захисту комп'ютерних ресурсів. Виділено переваги та недоліки існуючих методів, проблеми які виникають на етапах обробки зображень, процесу ідентифікації особи, методів захисту даних.

Враховуючи, що більшість методів представляє собою комерційну таємницю в даному випадку важко виділити кращий метод, оскільки порівнювати доцільно алгоритмічно-апаратний комплекс. Зараз проводяться розробки по зменшенню розмірів та ціни системи, збільшенню надійності роботи. Для систем, що вимагають особливі вимоги до безпеки, використовуватимуться мультимодальні біометрики. Використання біометричних засобів спрощує процедуру аутентифікації особи, а також піднімає надійність систем безпеки.

Сьогодні розроблено декілька методик для проведення ідентифікації особи за відбитками пальців, та механізмів захисту даних. Кожен із розроблених підходів має свої особливості, які ґрунтуються на властивостях як характеристиках візерунку відбитків пальців так і складністю захисту даних. Основна ідея полягає у визначенні оптимального методу між мінімізацією грошових та часових затрат ідентифікації і максимізації степені розпізнавання, та захисту даних. Основним завданням дослідження є

оцінювання найпоширеніших методів ідентифікації особи за відбитками пальців, та захисту комп'ютерних ресурсів.

1.7 Економічна доцільність нової розробки

1.7.1 Розрахунок собівартості нової розробки

Проведемо приблизний розрахунок собівартості одиниці нового виробу. Для цього скористаємося методом питомої ваги. Цей метод застосовується тоді, коли є можливість розрахувати хоча б одну з прямих витрат та встановити питому вагу цієї статті в собівартості аналога. Собівартість одиниці нової продукції S можна розрахувати за формулою:

$$S = \frac{В_п \times К_н \times 100\%}{П\%}, грн \qquad (1.1)$$

де $В_п$ – величина однієї із статей прямих витрат, яка вибрана за основу;

П – питома вага цієї статті витрат в собівартості аналога, %;

$К_н$ – коефіцієнт, який враховує конструктами та технологічні особливості нової методики, $К_п$=1…1,2.

$$S_2 = \frac{450 \times 1{,}1 \times 100\%}{50\%} = 990 \text{ (грн)}$$

1.7.2 Розрахунок величини капітальних вкладень

Величина капітальних вкладень визначається за формулою:

$$К = В \times А \times S = В \times Ц, грн \quad (1.2)$$

де В– коефіцієнт який враховує витрати на розробку, придбання, транспортування, монтаж та налагодження нової розробки; В≈1,2÷2,0;

А – коефіцієнт, який враховує прогнозований прибуток та податки, які повинен сплачувати виробник; А≈1,3÷2,3;

S – собівартість нової розробки;

Ц – ціна реалізації нової розробки, якщо вона була визначена раніше, грн.

Розрахуємо величину капітальних вкладень для нової розробки:

$$К_2 = 1{,}2 \times 1{,}6 \times 990 = 1{,}2 \times 1584 = 1900 \text{ (грн)}$$

Величина капітальних вкладень аналогу:

$$К_1 = 1{,}2 \times 4000 = 4800 \text{ (грн)}$$

1.7.3 Розрахунок величини експлуатаційних витрат

Експлуатаційними витратами є такі витрати, які забезпечують нормальне функціонування певного технічного рішення в період його експлуатації.

Величина експлуатаційних витрат в розрахунку за один рік може бути спрогнозована за формулою:

$$Е = k \times Ц \times \beta \times 12 = k \times А \times S \times \beta \times 12, \frac{грн}{рік} \quad (1.3)$$

де Ц– ціна реалізації нової розробки якщо вона була визначена раніше, грн./шт.,

k– коефіцієнт який ураховує витрати на амортизацію, електроенергію, обслуговування, ремонти тощо. В середньому, k =0,2÷0,4.

А – коефіцієнт який ураховує прогнозований прибуток та податки які повинен сплачувати виробник; А ≈ 1,7÷2,3.,

S – собівартість нової розробки, яка була с прогнозована приблизним способом;

β – доля часу який витрачає працівник на обслуговування технічної або інтелектуальної розробки в загальному часі своєї роботи. β =0,2

Величина експлуатаційних витрат нової розробки:

$$E_2 = 0{,}5 \times 1584 \times 0{,}3 \times 12 = 2851 \ \frac{\text{грн}}{\text{рік}},$$

Величина експлуатаційних витрат аналогу:

$$E_1 = 0{,}5 \times 4000 \times 0{,}3 \times 12 = 7200 \ \frac{\text{грн}}{\text{рік}},$$

Оскільки нова розробка та аналог мають однакове значення основного технічного показника, то порівняємо капітальні вкладення та експлуатаційні витрати:

$$К_1 > К_2 \text{ і } E_1 > E_2$$

Отже, маємо абсолютний ефект на капітальних вкладеннях в розмірі 2900 грн ($К_{еф} = 4800 - 1900 = 2900$ грн) та на експлуатаційних витратах — 4549 грн/рік ($E_{еф} = 7200 - 2851 = 4549$ грн/рік).

1.7.4 Загальний висновок про необхідність та доцільність розробки

Як бачимо новий прилад має переваги над аналогом за рахунок економії на експлуатаційних витратах та капітальних вкладеннях. Тому зробивши техніко–економічне обґрунтування нової розробки можна зробити висновок, що розробка даного програмного засобу буде доцільною.

РОЗДІЛ 2 ДОСЛІДЖЕННЯ МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Ідентифікувати людину можливо за ознаками, пов'язаними з її фізіологічними особливостями, які однозначно ідентифікують особу. До таких ознак можна віднести: геометричну будову руки, відбитки пальців, особливості малюнка сітківки ока, райдужну оболонку ока, портрет (наприклад, інфрачервону карту людини), характеристики і особливості мови, рукописний почерк, клавіатурний та комп’ютерний почерк, інші фізіологічні особливості людини, що робить її «особливою». Особливість ідентифікації за біометричними параметрами базується на їх винятковості. Ймовірність того, що знайдуться дві людини з однаковими ознаками, дуже мала (наприклад, ймовірність того, що в двох різних людей на однакових пальцях однієї руки збігатимуться відбитки пальців, рівна 1/24 млн, тобто практично є нульовою). Методи біометричної ідентифікації діляться на дві великі групи:

– статичні методи, які ґрунтуються на фізіологічних характеристиках людини;

– динамічні методи, які ґрунтуються на особливостях поведінки людини-підсвідомих рухах в процесі виконання якої-небудь дії.

Статичні та динамічні методи біометричної ідентифікації – це два взаємопов’язані та взаємодоповнюючі напрями. Основною перевагою статичних методів біометричної ідентифікації є їх відносна незалежність від психологічного стану користувача, малих затрат зусиль користувача, і, як

наслідок, можливість організації біометричної ідентифікації великих потоків людей. Біометрична ідентифікація на основі динамічних характеристик, як правило, простіша в реалізації, оскільки, як правило, не вимагає дорогого устаткування і може обмежуватися тільки програмним забезпеченням, яке вимагає мінімальну підтримку фахівця в процесі експлуатації.

Дактилоскопія – метод ідентифікації людини за відбитками пальців, заснований на унікальності рисунка шкіри. Предмет дослідження в даному розділі виступає зображення відбитка пальця.

Унікальність кожного відбитка пальця можна визначити за узором, який утворюють виступи і борозенки, а також за іншими його деталями.

Будова верхнього шару шкіри пальців рук людини, епідермісу, така, що він оберігає дерму, тобто власне шкіру, від механічних пошкоджень. Після будь-яких пошкоджень епідермісу, що не зачіпають дермальних горбків, папілярний узор в процесі загоєння відновлюється в колишньому вигляді, що підтверджене багатьма експериментами. Якщо ж дермальні горбки ушкоджуються, то утворюється рубець, в певній мірі деформуючий папілярний узор, але принципово не змінює первинного загального малюнка, причому сам рубець може бути використаний як вторинна ознака при ідентифікації.

2.1 Типи і види папілярних візерунків

Всі папілярні узори діляться на три основні типи (дугові, петлеві і завиткові) і можуть бути класифіковані таким чином (див. таблицю2.1).

Дугові узори утворюються зовнішнім потоком папілярних ліній і в середній частині узору мають вигин — внутрішню дугу, будова і форма якої служать для поділу їх на види.

Петлеві узори складаються із зовнішнього і внутрішнього потоків папілярних ліній і мають одну дельту. Утворюються внутрішнім потоком, папілярні лінії якого, починаючись з одного краю пальця, згинаються вгору і

до центру і, утворюючи петлю, повертаються до того ж краю. Петлевий візерунок складається з ряду петель, що знаходяться одна в іншій, але для віднесення узору до петлевого типу необхідно, аби в центрі узору хоч би одна лінія утворювала завершену голівку петлі або повну петлю.

Найбільш увігнута частина центральної петлі називається голівкою петлі, остання — її ніжками: верхня точка голівки петлі, що розділяє її на дві рівні частини — вершиною петлі. Внутрішня петля може мати складну будову за рахунок включення окремих ліній, фрагментів, точок. Залежно від форми петель, взаємного розташування ніжок петель і положення петель в площині внутрішнього потоку, вони підрозділяються нарізні види.

Таблиця 2.1 – Класифікація папілярних узорів

Дугові	Петлеві	Завиткові
Прості:	Прості: проста петля зігнута петля замкнута петля половинчаста петля	Прості: просте коло простий овал проста спіраль петля-спіраль
Складні: шатровий з невизначеним центром	Складні: паралельні петлі зустрічні петлі	Складні: петлі-спіралі петля-равлик петлі-клубки зігнута петля незавершені
Помилкові: помилково-петлевий дуговий помилково-завитковий дуговий рідко зустрічаються, які відносяться до дугових	Помилкові: помилково-завитковий петлевий рідко зустрічаються, які відносяться до петлевих	Помилкові: рідко зустрічаються, які відносяться до завиткових
Аномальний По десятипальцевій дактилоскопічній класифікації аномальні папілярні узори		

прирівнюються до дугових і позначаються цифрою 1		

Завиткові візерунки складаються із зовнішнього і внутрішнього потоків папілярних ліній і мають дві дельти (рідше - три і більше). Утворюються внутрішнім потоком, папілярні лінії якого в середній частині зігнуті у вигляді кругів, овалів, спіралей, потоків, що огинають один одного або створюють різні поєднання. Різновиди завиткових візерунків обумовлені особливостями їх внутрішньої будови.

Важливе значення і для класифікації, і для порівняльного дослідження по загальних ознаках має визначення умовного центру петлевого узору, що багато в чому визначає складність його внутрішньої будови.

Умовним центром петлевого візерунку прийнято вважати точку на вершині внутрішньої петлі або одній з ліній, що знаходяться всередині неї і що входить в голівку петлі. У випадках, коли внутрішня петля «чиста», центром візерунку буде вершина петлі.

Таким чином, у кожному відбитку пальця можна визначити два типи ознак:

1. Глобальні:

а) папілярний узор – специфічний узор, що формується сукупністю виступів і западинок;

б) виступ – лінія відбитка пальця підноситься і утворює виступ;

в) западинка (борозенка) – жолобок між виступами;

г) центр (ядро) – пункт, локалізований у середині відбитка або у деякій виділеній області; точка найбільшої кривизни виступу;

ґ) дельта – зона, де виступ розгалужується на три лінії, а потім вони сходяться в одній точці;

д) область інтересу – виділений фрагмент відбитка, в якому локалізовані всі ознаки (як правило, центральна область відбитка пальця).

У традиційній дактилоскопії папілярні узори пальців рук діляться на три основні класи: дугові (близько 5% усіх відбитків), петлеві (65%) і завиткові (30%). Для кожного класу проводиться детальнша класифікація на підкласи. Виділяються основні п'ять класів: завиток (W), права петля (R), ліва петля (L), дуга (A) і півсфера (T) (рис. 2.1) [2].

2. Локальні – це унікальні для кожного відбитка ознаки, що визначають пункти зміни структури папілярних ліній (закінчення, роздвоєння, розриви і т.д.), орієнтацію папілярних ліній і координати в цих пунктах. Кожен відбиток містить до 70 деталей.

Рисунок 2.1 – Зображення сканованого відбитка

Стандарти на відбитки пальців В основному використовуються стандарти ANSI і ФБР США. У них визначені такі вимоги до способу відбитка:

– кожен образ представляється у форматі нестисненого TIF;

– образ повинен мати дозвіл не нижче 500 dpi;

– образ повинен бути напівтоновим з 256 рівнями яскравості;

– максимальний кут повороту відбитка від вертикалі не більше 15 градусів;

– основні типи мінуцій: закінчення і роздвоєння.

Звичайно в базі даних зберігають більше, ніж один образ, що дозволяє поліпшити якість розпізнавання. Образи можуть відрізнятися один від одного зрушенням і поворотом.

Масштаб не змінюється, тому що всі відбитки отримують з одного пристрою.Відбиток, отриманий за допомогою спеціального сканера, датчика або сенсора, перетворюється в цифровий код і порівнюється з раніше введеним еталоном.

Переваги доступу за відбитком пальця – простота використання, зручність і надійність. Процес ідентифікації триває секунди і не вимагає зусиль. Сам пристрій займає мало місця. Але ідентифікація за відбитком пальця має один недолік. Приблизно у 1% людей пальці не можуть бути оброблені біометричною системою. Тобто, у них або немає відбитків, або вони мають такий вигляд, який неможливо перетворити в цифровий код.

Проблема пошкодження (поріз, опік) пальця вирішується просто. Якщо пошкодження не носить «складний» характер (папілярний узор відновлюється повністю), тоді систему необхідно лише "переучити" розпізнавати палець. На випадок, якщо палець пошкоджений серйозно, як правило, реєструється «резервний» відбиток (один або декілька, інколи для простоти реєструються відразу всі відбитки).

2.2 Напрям і крутизна потоків папілярних ліній

Папілярні візерунки петлевого і завиткового типів підрозділяються за ознакою відносного напряму потоків папілярних ліній:

а) по напряму ніжок петель:

– ульнарні - ніжки петель направлені у бік мізинця руки (мізинні);

– радіальні - ніжки петель направлені у бік великого пальця руки;

У відбитках пальців правої руки ульнарными будуть петлеві узори, ніжки петель яких направлені вправо, а у відбитках пальців лівої руки – вліво.

У відбитках пальців правої руки радіальними будуть петлеві узори, ніжки петель яких направлені вліво, а у відбитках пальців лівої руки - вправо (ця ознака використовується на практиці при визначенні руки і пальця, якими залишені сліди: праві петлеві узори відповідають правій руці, а ліві - лівій (за винятком 30% для вказівних пальців рук);

б) по напряму папілярних ліній центрального потоку завиткових узорів:

– правосторонні - закручування ліній в спіраль від центру узору до його периферії за годинниковою стрілкою (приведені характеристики змінюють прийняте в теорії дактилоскопії положення, що стосується лише розкручування папілярних ліній від центру завиткового узору до його периферії. Сенс умисної зміни характеристики полягає в тому, що закручування збігається з визначенням руки, якою залишений слід: праве закручування - права рука; ліве закручування - ліва рука);

– лівосторонні - закручування ліній в спіраль від центру узору до його периферії проти годинникової стрілки.

Для напряму папілярних ліній у відбитках вказівних пальців з узорами завиткових типів існує таке ж виключення, як і для петлевих.

Правило поширюється на ті види завиткових узорів, де чітко видимими є потоки ліній по спіралі: проста спіраль; петля-спіраль; петлі-спіралі і равлики.

Папілярні узори всередині свого типу і вигляду можуть розрізнятися (окрім вказаних ознак) по відносному напряму (нахилу) осей потоків папілярних ліній до основи узору - міжфалангової складки (рис. 2.1). Ця

ознака може успішно використовуватися не лише в процесі порівняльного дослідження схожих по будові узорів, але і як самостійна при визначенні руки і пальця, що залишили сліди. Якоюсь мірою нахил визначає і крутість потоків папілярних ліній, що також використовується в узорах одного типу і вигляду.

У дактилоскопічному десятипальцьовому обліку при виведенні додаткової частини формули радіальні петлеві узори позначаються цифрою 2; ульнарні - залежно від кількості папілярних ліній від дельти до центру узору - цифрами 3, 4, 5, 6.

У папілярних узорах петлевого і завиткового типів самостійно досліджується ознака взаєморозташування частин папілярного узору:

– центрів петлевих узорів - по відношенню до дельти;

– центрів завиткових узорів - по відношенню до правої і лівої дельт;

– дельт завиткових узорів відносно одна одної.

Для центрів і дельт петлевих узорів їх взаємно розташування розглядається в двох аспектах:

– по-перше, розташування дельти узору відносно центру по вертикалі, яке визначається висотою дельти відносно довжини петель внутрішнього потоку (нижнє, середнє, верхнє);

– по-друге, відстань від центру до дельти, виражена через гребневий рахунок - кількість папілярних ліній між їх центральними точками. Ця ознака використовується в дактилоскопічному 10-пальцевому обліку як класифікуюча петлеві узори при виведенні додаткової частини формули з їх цифровим позначенням:

а) цифра 3 - від 1 до 9 ліній;

б) цифра 4 - від 10 до 13 ліній;

в) цифра 5 - від 14 до 16 ліній;

г) цифра 6 - 17 ліній і більше.

Для центрів і дельт папілярних узорів використовується лише варіант підрахунку ліній від правої або лівої дельти до умовного центру узору, який в деяких випадках (із складною будовою центру) може визначатися чисто суб'єктивно.

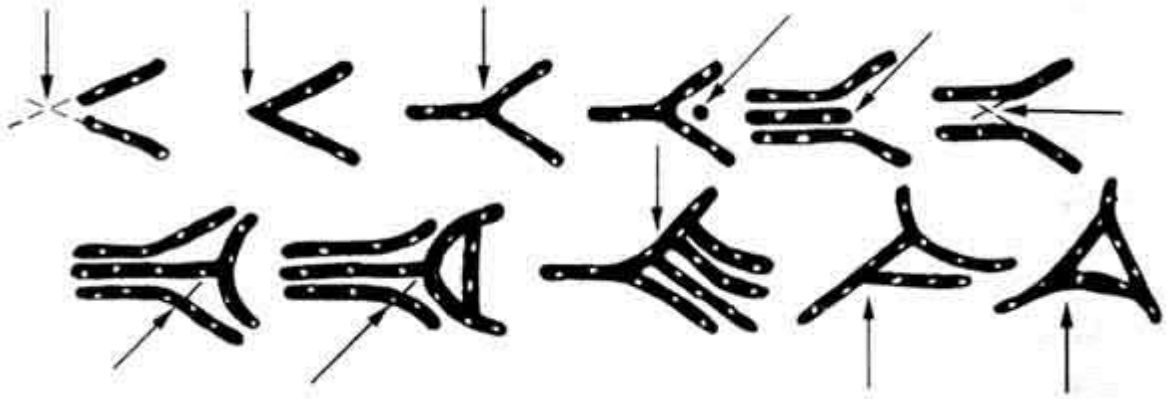


Рисунок 2.2 - Визначення вихідної точки в розташуванні дельт папілярних візерунків

Ознака взаєморозташування дельт в узорах завиткового типу є класифікуючою в 10-пальцевому дактилоскопічному обліку, за основу якого взято положення лівої дельти відносно правої, що визначається кількістю папілярних ліній між їх нижніми рукавами:

а) внутрішнє положення лівої дельти — на три і більше лінії вище правої - позначається цифрою 7;

б) середнє положення лівої дельти — її нижній рукав сполучений з нижнім рукавом правої дельти або число ліній між ними не більше двох - цифрою 8;

в) зовнішнє положення лівої дельти — на три і більше лінії нижче правої - цифрою 9.

При проведенні дактилоскопічних експертиз і порівняльного дослідження взаємнорозташування частин і елементів може визначатися поза зв'язком з їх точними кількісними виразами, загальними характеристиками: вище-нижче, правіше-лівіше, менше-більше.

2.3 Математична модель складних текстурних зображень

В наш час існуючі засоби технічної реалізації дуже близькі до потреб практики, що виражається в серійному випуску відеодатчиків, обчислювальних засобів, орієнтованих на застосування в системах ідентифікації. Проте відсутність ефективного спеціального програмного забезпечення призводить до дуже рідкого поширення дорогих надійних біометричних систем автоматичної ідентифікації. В результаті в таких системах використовується парольний захист з властивимийому недоліками.

У даному розділі вирішується завдання побудови структурного опису і на основі квазієнтропіного підходу — обчислення глобальних, інваріантних повороту ознак, таких як складність, регулярність і орієнтація.

Розглянемо текстурне зображення як об'єкт цифрової обробки.

В системах цифрової обробки процес створення оптичного образу об'єкту здійснюється системами, що містять оптичні і неоптичні елементи, які впливають на зміну поширення світлових хвиль або на перетворення світлової енергії в не світлову. Будь-яке зображення можна представити розподілом енергії джерела світлового випромінювання по просторових координатах X, Y, часу t і довжинам λ як функцію $F=f(x,y,t,\lambda)$.

Енергія випромінювання пропорційна квадрату амплітуди електромагнітного поля, отже, є дійсною позитивною величиною, обмеженою зверху величиною рівня насичення формуючої системи $A \geq f(x,y,t,\lambda) \geq 0$, де A — максимальна яскравість зображення.

Кінцеві розміри сприймаючого рецепторного поля також накладають обмеження і на розміри формованого зображення. В цілях спрощення вважатимемо, що зображення задане лише в прямокутної області, для якої

$$-L_x \leq x \leq L_x;$$

$$-L_y \leq y \leq L_y.$$

Після формуючої підсистеми відбиток є плоским однобарвним статичним зображенням *f(x, y)*.

В процесі кодування зображення випробовує ряд перетворень. Перш за все, змінюється сама природа величини, що описує зображення. Наприклад, розподіл освітленості перетвориться електронно-оптичною системою в розподіл щільності фотоструму.

У реальних умовах зображення схильні до дії шумів, які виникають на самому сприйманому об'єкті (непродрукування, заливка і т.д.) і в тракті передачі зображення.

В системи цифрової обробки зображень поступають масиви чисел, що є дискретними відліками яскравості, де значення функції в цих відліках замінюються квантованими по рівню величинами і далі перетворяться в цифровий код. Проте, при цьому неминучі погрішності, пов'язані з вибором кроку дискретизації і числа рівнів квантування.

Вимоги витримки товщини ліній відбитку і відстаней між ними не менше трьох елементів дискретизації призвели до граничних розмірів числової матриці *256×256* елементів. Контрастність вихідного зображення відбитку дозволяє обійтися всього двома рівнями квантування сигналу яскравості, що дає бінарну матрицю *F(i,j)*.

2.4 Визначення складності, регулярності зображень відбитку

Інтуїтивне поняття про складність бінарних зображень пов'язане з характером контурних ліній, їх напрямом, зв'язками ліній в деяких точках і т.д. Виділити на контурі самого зображення деякі фрагменти (лінії, дуги, кути і т.д.), які були б кінцевим набором елементів, придатних для опису або представлення будь-якого контурного або силуетного зображення, тобто деякий кінцевий набір непохідних елементів цього порядку, не надається можливим. У кожному конкретному випадку це буде часткове рішення. В той же час, саме однотипність елементів, незалежність їх від конкретного

зображення дозволить вирішити завдання оцінки складності форми і структури зображень.

Сповна природним представляється прийняти як такий непохідний елемент - елемент дискретизації, оскільки для бінарних зображень одиничні елементи утворюють структуру, адекватну структурі аналізованого зображення. Проте вихідні елементи дискретизації не можуть служити елементами аналізу складності, оскільки вони не несуть в собі інформації про характер зв'язків. Отже, як такі повинні виступати деякі сукупності вихідних елементів дискретизації, що містять інформацію про зв'язки елементів в площині і їх конкретному розподілі в образі. Встановлено, що основну інформацію про структуру образу несуть контури зображення.

Будь-яке вихідне зображення можна розглядати як сукупність монотонних відрізків контуру певної орієнтації: вертикальні, горизонтальні, похилі вліво і вправо. Їх кількість і величина визначають "витіюватість" форми контурної лінії. Чим більше виділених монотонних відрізків, тим більш складну форму вони представляють. При відомій загальній кількості N елементів, які складають контурну лінію, залежно від його складності виділяють m однорідних відрізків, кожен з яких складається з n_i елементів ($i=1,m$). Тоді відношення $p_i = \frac{n_i}{N}$ є вагомим вкладом кожного відрізку в порушення монотонності, або в складність контуру [16].

Для додання залежності, як мірі складності, явного вигляду необхідно зажадати виконання наступних умов :

а) міра складності не має бути негативною;

б) просте зображення типу лінії повинне мати міру складності, рівну нулю;

в) повинен виконуватися принцип адитивності вкладу кожного i-го відрізку;

г) міра складності має бути нормованою.

Апріорну невизначеність появи *i*-го відрізку у складі зображення можна оцінити виразом $H_i = \log_a \frac{1}{p_i}$.

Величину, що характеризує невизначеність окремої (і-тої) події, прийнято називати частковою ентропією. Невизначеність і кількість інформації для всієї сукупності випадкових подій можна отримати усереднюванням по всіх подіях

$$I = \sum_{i=1}^{m} p_i \log_a \frac{1}{p_i} = -\sum_{i=1}^{m} p_i \log_a p_i \tag{2.1}$$

$$H = \sum_{i=1}^{m} p_i \log_a \frac{1}{p_i} = -\sum_{i=1}^{m} p_i \log_a p_i \tag{2.2}$$

Оскільки величина $p_i = \frac{n_i}{N}$ не є вірогідністю появи *i*-го відрізку в зображенні, а лише її деякою наближеною оцінкою, але враховуючи, що $\sum_{i=1}^{m} p_i = 1$ можна говорити про квазіентропію зображення, яка задається виразом $H = \sum_{i=1}^{m} \frac{n_i}{N} \log_a \frac{N}{n_i}$.

Для визначення нормуючого коефіцієнта необхідно проаналізувати за яких умов складність зображення, що складається з *N* контурних елементів, буде максимальна. Як відомо ентропія має максимум при рівній вірогідності всіх подій, тобто при $n_i=1$ і $m=N$.

Підставимо ці значення і отримаємо

$$S_{\max} = \sum_{i=1}^{N} \frac{1}{N} \log_2 N = \log_2 N \tag{2.3}$$

Тоді вираз для оцінки складності бінарного зображення має вигляд

$$S = \frac{1}{\log_2 N} \sum_{i=1}^{m} \frac{n_i}{N} \log_2 \frac{N}{n_i} \qquad (2.4)$$

Отримана залежність повністю відповідає вимогам, пред'явленим до оцінки міри складності. Слід зазначити, що стосовно зображень, регулярною вважається форма, що має правильну постійну організацію, фрагменти, що повторюються. Тоді, враховуючи, що складність є мірою гетерогенності зображення об'єкту, можна представити, що регулярність відображає міру впорядкованості елементів зображення і визначається виразом

$$R = \frac{1}{S} = \frac{1}{\frac{1}{\log_a N} \sum_{i=1}^{m} \frac{n_i}{N} \log_a \frac{N}{n_i}} \qquad (2.4)$$

Узагальнена оцінка характеризує інтегральну регулярність зображення, а для однозначного орієнтування необхідна така характеристика проекції, значення якої різко міняється при повороті зображення. Дану вимогу задовольняють часткові оцінки, що характеризують міру регулярності аналізованого зображення уздовж однієї з чотирьох осей орієнтації. В цьому випадку регулярність відносно вертикальної, горизонтальної, ліво- і правонахиленої осей визначається виразами:

$$R_V = \frac{1}{S_H + S_L + S_P}; \quad R_H = \frac{1}{S_V + S_L + S_P};$$

$$R_L = \frac{1}{S_H + S_V + S_P}; \quad R_P = \frac{1}{S_H + S_L + S_V}.$$

Запропоноване аналітичне визначення складності і регулярності зображення засноване на тій частині об'єктивних властивостей зображень, які реально включаються людиною в його суб'єктивну оцінку - кількості монотонних ділянок контурної лінії і їх величини.

2.5 Висновки

У розділі здійснено дослідження зображень відбитків пальців як об’єкту обробки. Запропоновано математичну модель і метод розпізнавання зображень відбитків пальців. Розроблено математичний апарат визначення таких характеристик зображень відбитків як складність та регулярність.

2.8 Розробка алгоритмів опису і порівняння відбитків та заборони доступу до папки

2.9 Визначення тренду потоків ліній на відбитку пальця

Після оцінки міри регулярності зображення по всіх осях, проведеної методом описаним в розділі 2.4, вибираються максимальні величини з пар R_V, R_H, R_L, R_P і, як їх геометрична сума, визначається напрям максимальної регулярності, відносно якого задається еталонна орієнтація. Кут нахилу зображення відносно осі X визначається як [17,18]:

$$\varphi = arctg(\max\{R_V, R_H\} + \max\{R_L, R_P\}) . \qquad (2.5)$$

Якщо в даній зоні зображення присутні лише вертикальні або лише горизонтальні складові, то кут нахилу не обчислюється, а приймається рівним 90° або 0°, відповідно. За відсутності ліній відбитку у виділеній зоні вектор кута нахилу не будується взагалі.

2.10 Побудова глобального опису відбитку пальця

При аналізі структури з метою здобуття додаткових інформативних ознак проводиться декомпозиція оцінок складності, регулярності і кута орієнтації на часткові оцінки, що характеризують окремі фрагменти зображення. Для обліку зв'язності ліній сусідніх фрагментів логічно ці фрагменти вибирати з перекриттям. Для кожного фрагмента розраховується кут тенденції орієнтації ліній і будується відрізок під розрахованим кутом.

Отримана матриця величин кутів орієнтації ліній у фрагментах і їх відображення у вигляді орієнтованих відрізків є портретом регулярності елементів текстури (ПРЕТ) [17], представленим на рис.2.3. Від розмірів фрагментів залежить об'єм ПРЕТ і його детальність. Відмінною особливістю

портрета є здатність повторення геометрії рисунка відбитку із збереженням основних ознак, прийнятих в криміналістиці.

Графічне зображення відбитку є матрицею розміром *256×256*точок (пікселів). Для побудови портрета регулярності даний малюнок розбивається на зоні розміром *16×16* пікселів, для кожної з яких визначається кут нахилу і будується відповідний відрізок. Таким чином "гладке" зображення відбитку замінюється набором дискретних відрізків. Для згладжування і зменшення погрішності при аналізі вибиралися зони, що перекриваються, розміром *32×32*, але відрізок будується для елементу зображення розміром *16×16*.

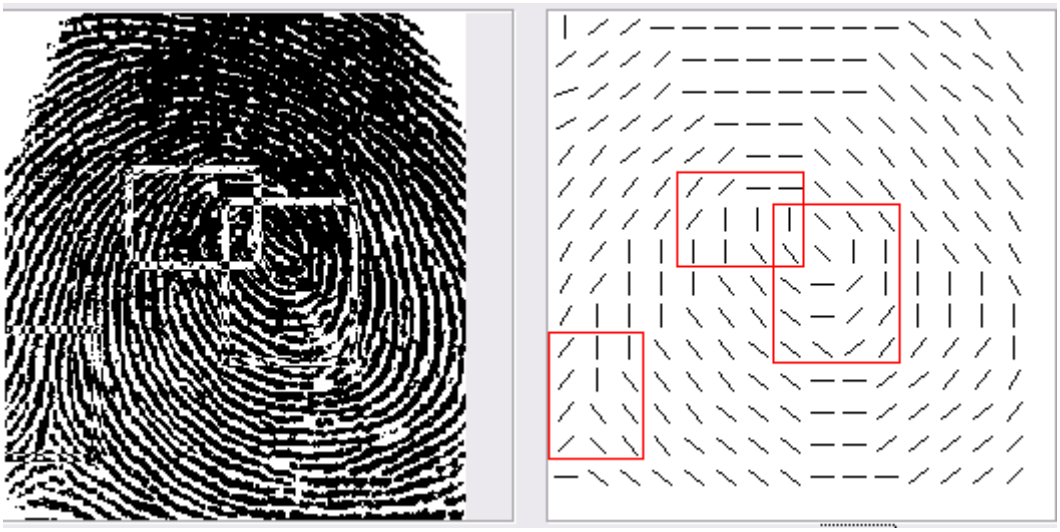


Рисунок 2.3 - Отримання портрета відбитку

В результаті проведеного перетворення графічного зображення відбитку з вибраною кількістю фрагментів отримано*256 (16×16)*зон значень кута нахилу і портрет регулярності. Для здобуття ще ближчого дискретного еквіваленту вихідного зображення відбитку використовується алгоритм інтерполяції, який дозволяє поєднати відрізки на межі зон, що є сусідніми.

ПРЕТ відбитку несе в собі стислу інформацію про його структуру. Тому його можна використовувати для попередньої ідентифікації, результатом якої має бути одне з двох тверджень:

– ПРЕТ відбитку, що пред'являється, корелює з відповідним еталонним ПРЕТом;

– кореляція між ПРЕТамі відбитку, що пред'являється, і вказаного еталону не спостерігається.

У першому випадку для подальшої точної ідентифікації необхідно порівняти структуру пред'явленого відбитку з еталонним. Причому для скорочення часу повної ідентифікації необхідно порівнювати структури найбільш інформативних фрагментів невеликих розмірів.

У другому випадку формується негативний результат ідентифікації і подальшого порівняння не відбувається.

Для більш наочного представлення відрізки, які виходять при побудові портрета можна з'єднати. Для цього необхідно весь портрет розбити на ділянки, що перекриваються, і в кожній ділянці проаналізувати нахили ліній, аби визначити які лінії необхідно з'єднати. Тобто ділянка перевіряється на наявність певних комбінацій відрізків. Якщо такі комбінації є, то відрізки в цих комбінаціях з'єднуються лінією (рис.2.4).

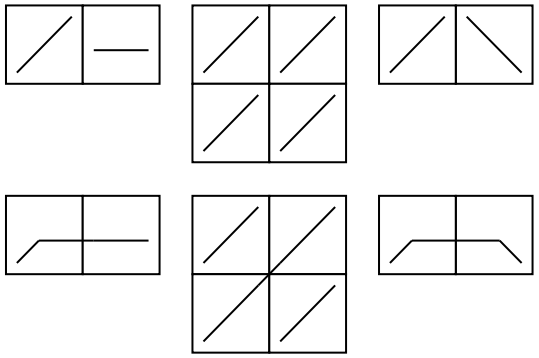


Рисунок 2.4 - Приклади варіантів з'єднання відрізань

Такий згладжений портрет також можна використовувати для порівняння з еталоном. При цьому можна виділити певні ознаки у відбитку, такі як «дельта» або «завиток» і перевірити, чи є такі ж в еталонному портреті (рис.2.5).

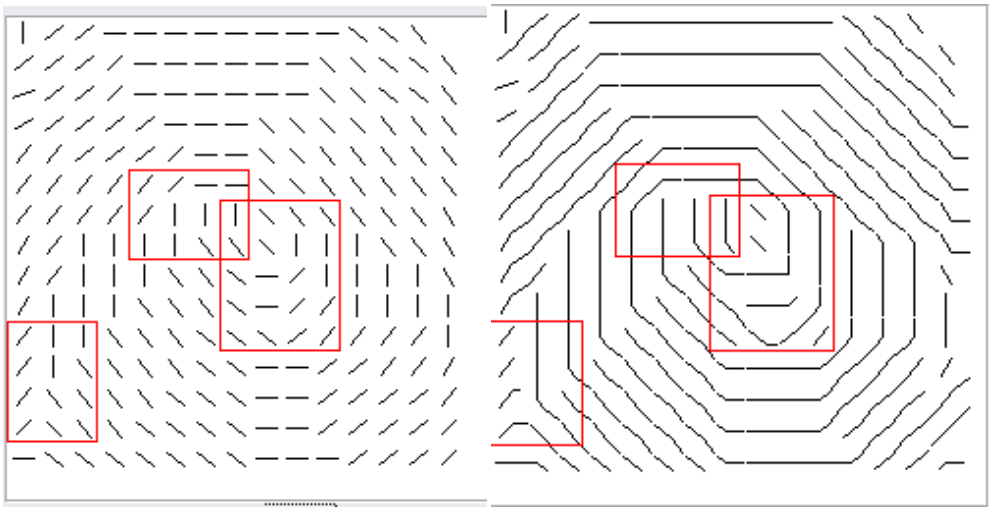


Рисунок 2.5 - Згладжування портрету

Як показує величезний досвід криміналістики, найбільш інформативними, з точки зору ідентифікації, є фрагменти з яскраво вираженими порушеннями регулярності папілярних ліній, що в ПРЕТ відповідає різкій відмінності значень кутів нахилу ліній в сусідніх зонах. Для автоматичного знаходження таких зон паралельно з формуванням ПРЕТ формується його загрублений варіант, в якому одним числом кодується не конкретне значення кута, а деякий інтервал кутів. Практичні дослідження показали, що для надійного виділення таких ознак як: очки, завитки, дельти, розташування яких є індивідуальним для кожної людини, досить виділити чотири таких інтервали:

– $0 \le j \le 22,5$ і $180 \le j < 157,5$ (горизонталь);
– $22,5 < j \le 67,5$ (лівонахилені лінії);
– $67,5 < j \le 112,5$ (вертикаль);
– $112,5 < j \le 157,5$ (правонахилені лінії).

За центр інформаційної зони береться точка, в якій граничать три або чотири різні елементи огрубленого ПРЕТ. Величина зони приймається рівною *48×48* елементів. В разі, якщо дві або більше зони граничать або стикаються, то розміри інформаційної зони відповідно збільшуються (рис.2.6).

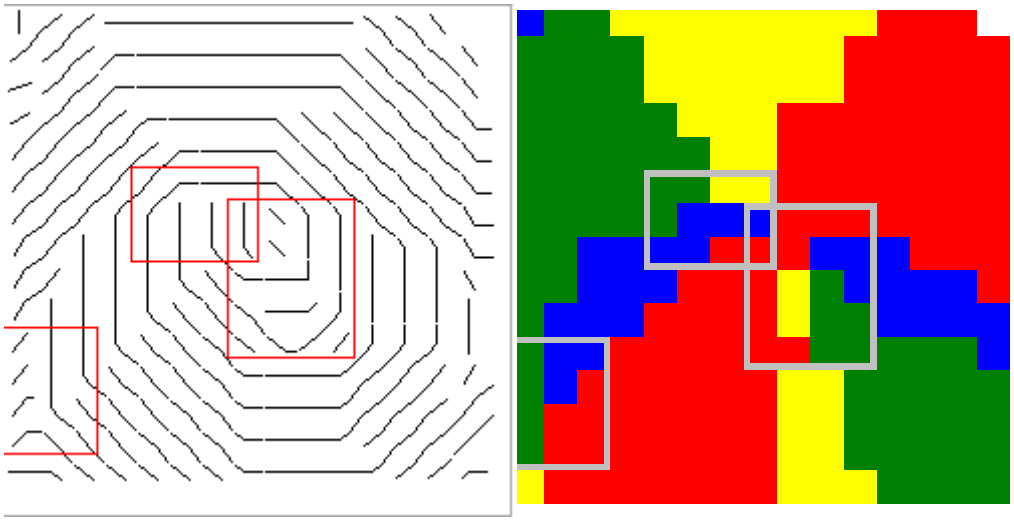
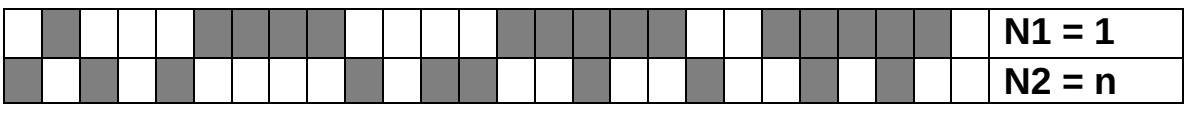


Рисунок 2.6 - Виділення інформативних зон відбитку

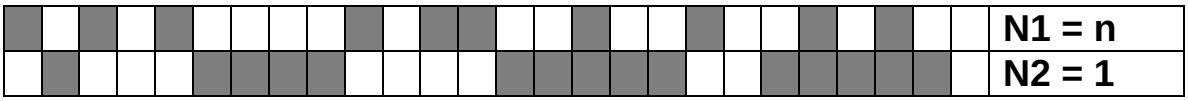
2.11 Побудова локального опису структури відбитку

Для детальнішого опису виділених інформативних зон в них виділяються такі ключові ознаки: початок (П), кінець (К), вузол верхній другого порядку точковий (ВВ2Т), вузол верхній другого порядку протяжний (ВВ2П), вузол верхній третього порядку точковий (ВВ3Т), вузол верхній третього порядку протяжний (ВВ3П), вузол нижній другого порядку точковий (ВН2Т), вузол нижній другого порядку протяжний (ВН2П), вузол нижній третього порядку точковий (ВН3Т), вузол нижній третього порядку протяжний (ВН3П). Інші ознаки описують зображення — трек лівий, трек правий, вертикаль, горизонталь, вузол вироджений верхній, вузол вироджений нижній, вузол помилковий враховуватися не будуть, оскільки вони не несуть корисної інформації, необхідної для подальшого порівняння, і для опису інформативної зони відбитку вибраного набору цілком достатньо, а його збільшення приведе лише до громіздкості опису і збільшить час ідентифікації[18].

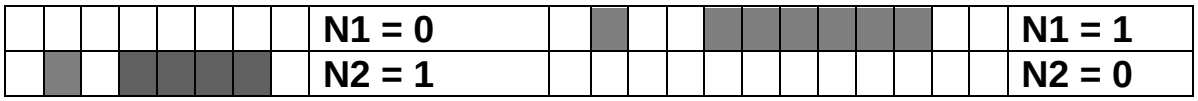
Приклади структурних ознак «вузли верхні»



Приклади структурних ознак «вузли нижні»

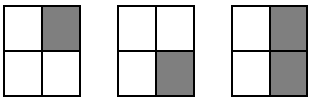


Приклади структурних ознак «початок» і «кінець»

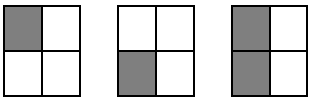


Опишемо детально алгоритм виділення структурних ознак.

Зліва направо аналізуються відразу два рядки. Поява однієї з таких комбінацій



координата такої комбінації запам'ятовується як початок ознаки $J_П$. Рядки аналізуються далі, і при появі однієї з комбінацій



запам'ятовується координата кінця ознаки J_K. Так виділяються межі ознаки. На всьому протязі рядків може знаходитися декілька ознак.

Тепер аналізується кожен рядок окремо в межах знайденої ознаки. У кожному рядку підраховується кількість безперервних відрізків (N_1 для першого рядка і N_2 для другого). З пари чисел N_1 і N_2 відразу видно яка з ознак була виявлена (табл.2.2).

Вузол помилковий не бере участь в описі.

Аби розрізнити точковий і протяжний вузол аналізується довжина верхнього відрізку (для верхнього вузла) або нижнього (для нижнього вузла). Якщо ця довжина більше деякої константи, яка обмежує довжину точкового вузла, то це вузол протяжний, якщо менше — точковий.

Таблиця 2.2 - Використовувані ознаки для опису локальної структури

N1	N2	Ознака
0	1	Початок
1	2	ВВ2Т(П)
1	3	ВВ3Т(П)
2	1	ВН2Т(П)
3	1	ВН3Т(П)
>1	>1	Вузол помилковий
1	0	Кінець

Таким чином обробляються всі рядки. Перехід по рядках здійснюється з накладенням. Для опису інформативної зони запам'ятовується тип кожної ознаки з його абсолютними координатами.

2.12 Дослідження методів порівняння відбитків

Зображення відбитку пальця людини, є сукупністю папілярних ліній. Їх взаємне розташування, власне, і визначає унікальність відбитку.

Існує чотири рівні ознак розрізнюваності відбитків.

Перший - тип узору, який визначається характером розташування папілярних ліній. Розрізняють кругові, дугові і завиткові типи. Це найбільш загальна характеристика відбитку.

Другий - макроелементи відбитку: центри і дельти. Їх типи (дельти бувають ліві і праві, центри з напрямом і без), взаєморозташування і спрямованість конкретніше характеризують відбиток в порівнянні з типом узору.

Третій - елементи відбитку:характерні особливості, що представляють собоюпочаток/закінчення папілярних ліній і злиття/розгалуження. Взаєморозташування і спрямованість цих особливих елементів в основному і визначає унікальність відбитку.

Четвертий же рівень став доступний до вивчення лише з появою високоякісної апаратури сканування. Йдеться про мікроскопічні пори на папілярних лініях - виходи потових залоз. Їх розташування також унікальне.

Проте жодна система дактилоскопічної ідентифікації не використовує даний критерій у зв'язку з необхідністю обробки величезного об'єму інформації і нестабільністю прояву даних елементів, пов'язаною із забрудненням, запітненням відбитку.

У криміналістиці для ідентифікації використовують перші три рівні ознак.

Виходячи з вищеописаних критеріїв розпізнаваності відбитків пальців, криміналіст-експерт здійснює їх порівняння по наступному алгоритму.

Виробляється визначення і порівняння типів узору на обох відбитках. В разі їх збігу аналізується розташування макроелементів (подібність типів, напряму, відстаней і т.д.). Якщо всі ознаки збігаються, робота переходить на точковий рівень. Аналізується наявність однакових елементів на обох відбитках. І в разі виявлення хоч би однієї розбіжності (наприклад, на відповідній ділянці паралельних ліній в іншого відбитку знайдене злиття/розгалуження) - приймається рішення про неспівпадання відбитків. Лише в разі повного повторення розташування елементів робиться протилежний висновок.

Більшість пропонованих систем дактилоскопічної ідентифікації більшою чи меншою мірою використовують саме такий підхід, перевірений практикою і часом. Хоча є розробки, що використовують і інші методи, запозичені з різних математичних теорій обробки зображень. Один з них - кореляційне порівняння зображень двох відбитків. Суть його полягає в накладенні двох зображень відбитків пальців в різних положеннях і визначення найкращого коефіцієнта збігу. При перевищенні апріорі заданого порогу збігу - відбитки визнаються ідентичними.

У табл. 2.3 приведені позитивні і негативні сторони цих двох поширених підходів.

Якісними показниками функціонування алгоритмів дактилоскопічної ідентифікації служать: помилка ідентифікації (вірогідність пропуску 'чужого') і відмова ідентифікації (вірогідність не пропуску 'свого'). На

графіках показані відповідності помилки і відмови ідентифікації для більшості існуючих систем дактилоскопічної ідентифікації.

Таблиця 2.3 - Різні підходи до ідентифікації

Підходи до ідентифікації	Позитивні аспекти	Негативні аспекти
Криміналістичний	Висока швидкість ідентифікації Інваріантність до повороту відбитку Стійкість до деформації відбитку Представлення відбитку в компактному коді	Складність реалізації алгоритмів Високий рівень помилки і відмови ідентифікації
Математичний	Простота реалізації алгоритмів	Високий рівень відмови ідентифікації, обумовлений нестійкістю алгоритмів до деформації повороту відбитку. Тривалий час ідентифікації Великий об'єм коду відбитку

Ідеальні характеристики системи - це рознесені показники помилки і відмови ідентифікації, коли одночасно при великій надійності ідентифікації (помилка 0,0001%) досягається відмова ідентифікації всього долі відсотка.

Показник помилки ідентифікації визначається вибраним підходом, якістю реалізації і налаштування алгоритмів ідентифікації.

Показник відмови ідентифікації визначається багатьма чинниками. До основних з них відносяться: міра збігу зареєстрованоїв якості еталону ділянки відбитку пальця і пред'являємої для ідентифікації, характеристики поверхні відбитку пальця (надмірно суха або волога, пошкоджена, стерта, забруднена і т.п. поверхня).

Якщо з першим недоліком «боротися» неможливо (по суті справи, це два різні відбитки), то недостатньо хороше зображення, пов'язане з неякісною поверхнею відбитку, може компенсуватися алгоритмами обробки, що враховують дані проблеми.

Наочний показник співвідношення помилки і відмови ідентифікації для будь-якої реалізації технології дактилоскопічної ідентифікації - наявність можливості пошукового режиму, коли відбиток користувача порівнюється з великим числом відбитків, що зберігаються в базі даних.

Більшість існуючих систем не можуть використовувати подібний режим у зв'язку з недостатнім показником надійності ідентифікації при малому відсотку відмови ідентифікації. Тому в таких розробках користувач повинен спочатку ввести своє ім'я, а лише потім підтвердити його відбитком пальця (підтверджуючий режим).

Явний недолік таких систем полягає в необхідності при доступі вказувати своє ім'я. Для цього потрібно встановлювати додаткове устаткування - цифрові наборники, карткові зчитувачі і т.п., що підвищує вартістю системи і створює додаткові незручності користувачам.

Для аутентифікації користувача потрібно два об'єкти – ім'я користувача і пароль. При використанні в процесі аутентифікації технології ідентифікації відбитків пальців ім'я користувача вводиться у вікні реєстрації, а відбиток пальця замінює пароль. Ця технологія використовує ім'я користувача як покажчик для отримання облікового запису користувача і перевірки відповідності “один до одного” між шаблоном зчитаного при реєстрації відбитку і раніше збереженим шаблоном для даного імені користувача. Такий пошук збігу “один до одного” по одному атрибуту називається “верифікацією”. Він відрізняється високою швидкістю і пред'являє мінімальні вимоги до обчислювальної потужності комп'ютера.

Деякі клієнти просили ввести в технологію ідентифікації відбитків пальців підтримку використання відбитку не лише замість пароля, але і замість імені користувача. Система вивчає ці функції, і вони можуть бути

реалізовані в майбутніх версіях системи. Такі засоби вимагають пошуку “один до багатьох”, який називається “ідентифікацією”. Іншими словами, введений при реєстрації шаблон відбитку пальця необхідно зіставити зі всім набором збережених шаблонів. Для пошуку “один до багатьох” необхідна набагато більша обчислювальна потужність, оскільки програмні алгоритми повинні виробити безліч порівнянь, аби виявити збіг.

Сучасна реалізація технології ідентифікації відбитків пальців на основі “верифікації” шаблону відбитку добре підходить для більшості комерційних застосувань. Вона забезпечує швидку аутентифікацію користувачів, а завдяки низьким вимогам до обчислювальної потужності комп'ютера її можна широко розвернути в існуючих середовищах клієнтів. При першій реєстрації в мережі по відбитку пальця потрібно буде ввести ім'я користувача, проте надалі це ім'я залишається заданим за замовчуванням до тих пір, поки не буде змінено. Таким чином, в комерційних середовищах, де на кожен ПК доводиться по одному користувачеві, своє ім'я користувачам зазвичай доведеться вводити всього один раз. У середовищах з машинами, що розділяються, ім'я користувача потрібно буде міняти, але і тут зберігаються всі переваги, пов'язані з відсутністю необхідності запам'ятовувати пароль.

2.13 Реалізація процедури порівняння відбитків

Процес верифікації включає такі обов'язкові пункти:

1. Зняття відбитків пальців.
2. Обробка отриманого зображення і отримання портрета регулярності елементів текстури.
3. Порівняння отриманого ПРЕТ з еталонним.
4. Якщо результат порівняння негативний, то об'єкт не верифікується, при позитивному порівнянні – наступний етап.
5. Виділення найбільш інформативних зон відбитку.
6. Формування опису структури виділених зон.

7. Порівняння описів структур виділених зон з остаточною верифікацією.

8. При невдалої верифікації - введення зображення другого пальця і повторна ідентифікація.

Узагальнений алгоритм повної верифікації представлений на рис.3.5. Зняття відбитків пальців проводиться спеціальним приладом, принцип дії якого може бути різними, але вихідними даними має бути чітке графічне зображення відбитку пальця, еквівалентне оригіналові. Важливою вимогою до формувача цифрового представлення зображення відбитку є обмеження можливості плоско-паралельного зсуву уздовж осей *X* і *У* величиною 16 елементів дискретизації в позитивну і негативну сторони, що відповідає величині зрушення на 2 мм. Другою вимогою є зниження до мінімуму можливості повороту пальця при його пред'явленні. Виконання цих вимог здійснюється використанням обмежувального тунелю.

Для порівняння двох портретів необхідно знайти різницю кутів нахилу відрізків у відповідних елементарних зонах портретів, що перекриваються. Формується масив різниць *Z* таким чином:

$$Zi=X1_i-X2_i, \tag{2.6}$$

де *X1* і *X2* — матриці кутів нахилу двох портретів.

Якщо відбитки ідентичні, то закон розподілу цих різниць буде схожий на закон нормального розподілу. Далі знаходимо математичне очікування отриманої матриці:

$$M=\frac{\sum_{i=1}^{n} Z_i}{n} \tag{2.7}$$

Аби мати всі характеристики нормального закону розподілу треба ще знайти дисперсію:

$$D = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(Z_i - M)^2} \qquad (2.8)$$

Маючи ці величини можна судити про ідентичність або не ідентичність відбитків. Надійність ідентифікації залежить від порогового значення цих характеристик.

Хай на еталонному зображенні розміром $N_x \times N_y$ зафіксована деяка множина $S=\{S_{i,j}\}$ структурних елементів, в якій $i=1,2...,n$ і характеризує безліч класів виділених структурних елементів, а $j=1,2...,m$ - кількість елементів в кожному класі. Поставимо у відповідність кожному виділеному елементу з множини S деяку зону $Z_{i,j}$ з центром в точці з координатами $(X_{i,j},Y_{i,j})$. Припустимо, що зона має форму прямокутника розміром $(2 \cdot W_x+1) \cdot (2 \cdot W_y+1)$, де величини W_x і W_y визначають апріорно встановлені гранично допустимі зрушення реалізації відбитку від еталону.

Після пред'явлення реалізації проводиться аналогічна процедура виділення структурних елементів, внаслідок чого формується множина $R=\{R_{i,m}\}$, $i=1,2,...,k$; $m=1,2,...,l$.

В результаті суміщення зображення пред'явленого відбитку з еталоном в межах виділених зон формуються вектори різниці t_{ij} шляхом з'єднання точок, в яких знаходяться елементи S_{ij} з точками, відповідними елементам R_{im} того ж класу.

При відповідності реалізації еталону в кожній зоні буде виділений вектор $t_{ij}=t_c$. В разі перекриття зон можливе утворення векторів $t_{ij}=t_n$, що є своєрідним шумом. Оскільки розподіл векторів t_{ij} на t_c і t_n апріорі невідомий, то в загальному випадку на вирішуючий пристрій поступає інформація про суму корисного сигналу t_c і перешкоди t_n. Для підвищення вірогідності ухвалення правильного рішення необхідно підвищити співвідношення корисний сигнал/шум. Враховуючи постійність вектору t_c у всіх зонах і

вважаючи перешкоду стаціонарним випадковим процесом, для цієї мети доцільно використовувати метод накопичення (рис. 2.6).

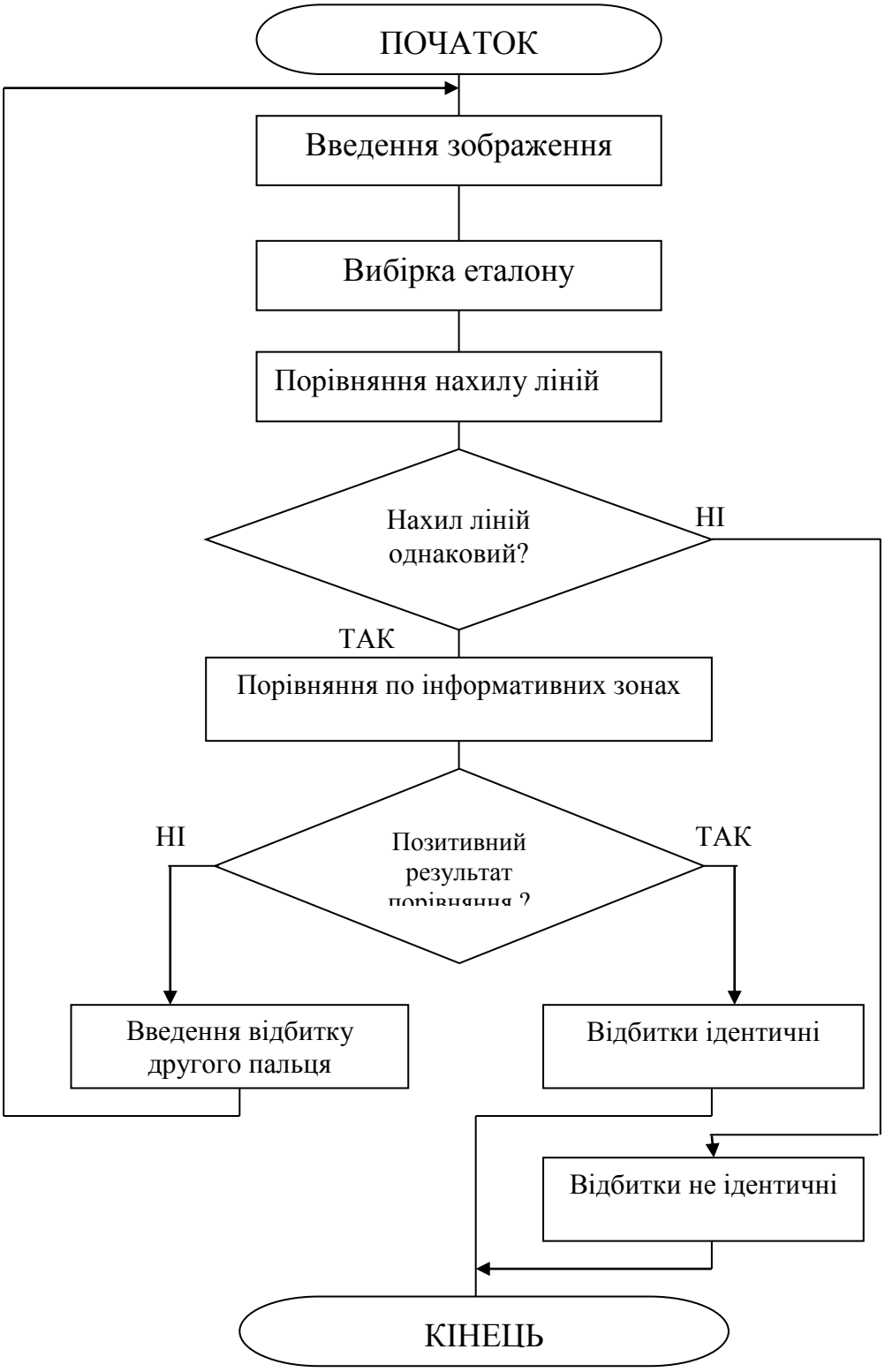


Рисунок 2.7 - Алгоритм ідентифікації

При цьому в гістограмі розподілу векторів t_i, побудованою за результатами аналізу виділених зон, характерним буде яскраво виражений

пік, який визначається векторами t_c. При невідповідності реалізації еталону результуючий вектор визначатиметься лише сумою шумових векторів t_n, яка із збільшенням числа оброблюваних структурних елементів рухатиметься до нуля.

2.14 Механізми захисту даних

2.14.1 Захист папок і файлів вбудованими засобами Windows

Приховувати свої папки та файли можна, використовуючи вбудовані можливості Windows - для цього достатньо у властивостях відповідних об'єктів включити атрибут "Прихований". Приховані таким чином папки та файли не будуть бачити в провіднику іншим користувачам системи, але лише за умови, що у властивостях містять їх батьківських папок включений прапорець «Не показувати приховані файли і папки". В принципі, цього може виявитися достатньо для захисту своїх даних від найбільш непідготовленою аудиторії. Однак приховані подібним чином об'єкти будуть видимі в додатках, які не використовують стандартний діалог для відображення файлів і папок (FAR, Total Commander і т.п.), тому подібний захист більш ніж ненадійна (рис. 2.8).

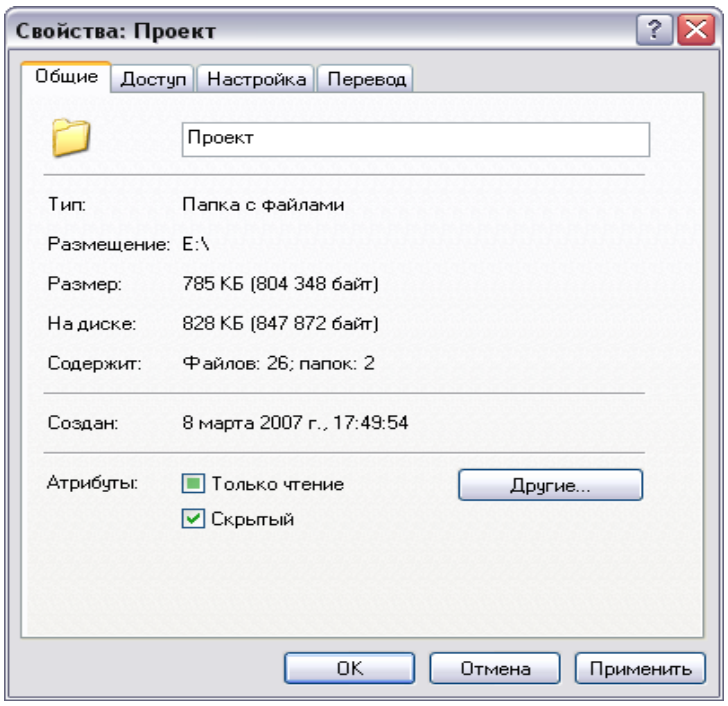


Рисунок 2.8 -Захист папок і файлів вбудованими засобами Windows

2.14.2 Шифрована файлова система (EFS)

Шифрована файлова система (EFS) дає можливість зберігати дані на диску в зашифрованому форматі, однак при перевстановлення системи або видаленні облікового запису користувача його зашифровані дані будуть безповоротно загублені, якщо не подбати про збереження сертифіката та ключів, створенні облікового запису агента відновлення.

Шифрована файлова система EFS використовується для зберігання шифрованих файлів на томах файлової системи NTFS 5.0. Після того як файл або папка зашифровані, з ними можна працювати так само, як і з іншими файлами або папками, тобто шифрування прозоре для користувача, зашифрований файл. Це означає, що перед використанням файл не потрібно розшифровувати. Можна, як звичайно, відкрити файл і змінити його.

Робота з EFS аналогічна використанню дозволів для файлів і папок. Задача обох методів — обмеження доступу до даних. Однак дозволу для файлів і папок не захистять вас, якщо зловмисник отримає фізичний доступ до ваших даних, наприклад, підключить ваш жорсткий диск до іншого комп’ютера або завантажиться за допомогою іншої операційної системи, що

має доступ до томів NTFS. При спробі ж відкрити або скопіювати зашифрований файл або папку він отримає вичерпну відповідь: «Ні доступу».

Як тільки ми зашифруємо якусь папку або файл, Windows створить для нас сертифікат і пов’язану з ним пару ключів (відкритий і секретний ключ), на підставі яких відбуватиметься шифрування і дешифрування файлів. Сертифікат — цифровий документ, використовуваний для перевірки справжності та безпечної передачі даних в загальнодоступних мережах (Інтернет, Інтернет, Екстранет), він пов’язує відкритий ключ з об’єктом, який містить відповідний закритий ключ (рис. 2.9).

Рекоменлується використовувати шифрування на рівні папки. Якщо шифрується папка, всі файли і підпапки, створені в зашифрованій директорії, автоматично шифруються. Ця процедура дозволяє створювати зашифровані файли, дані яких ніколи не з’являться на диску у вигляді звичайного тексту — навіть тимчасові файли, створювані програмами в процесі редагування, також будуть зашифровані.

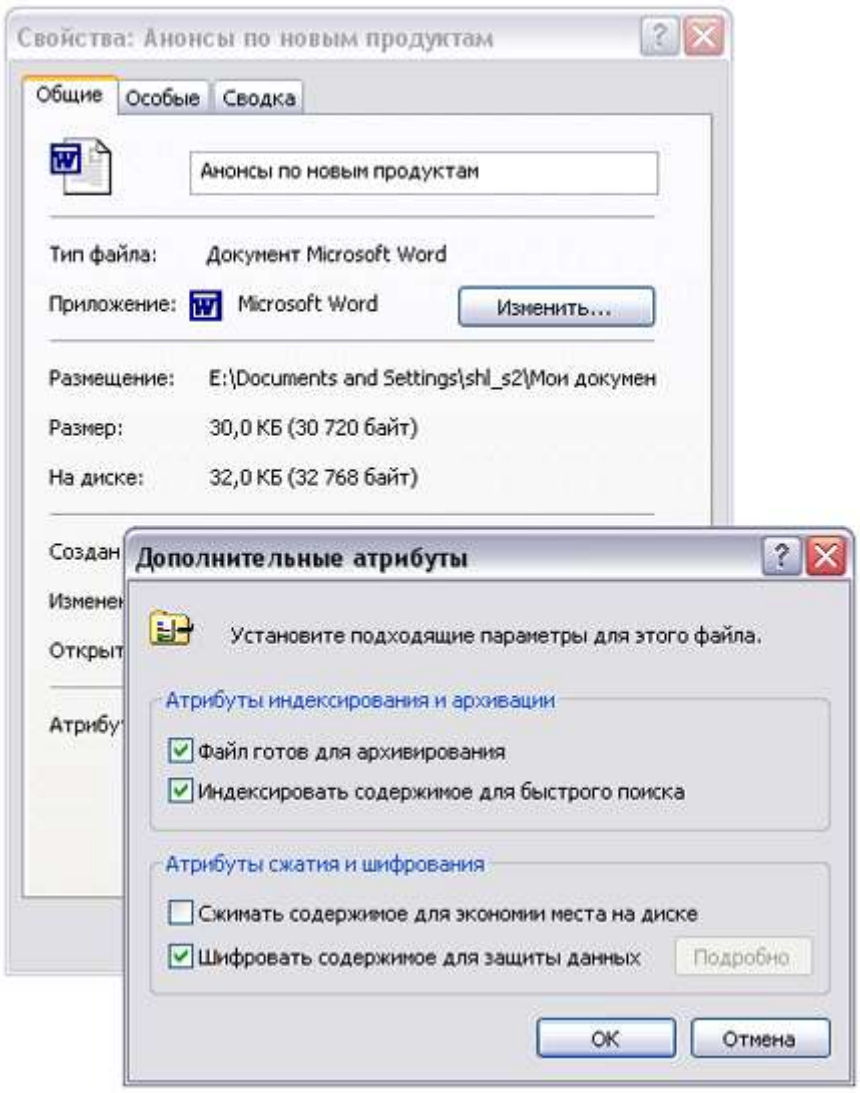


Рисунок 2.9 – Приклад шифрування системою EFS

При роботі з зашифрованими файлами і папками слід враховувати ряд моментів.

Можуть бути зашифровані тільки файли і папки, що знаходяться на томах NTFS. Стислі файли і папки не можуть бути зашифровані. Якщо шифрування виконується для стисненого файлу або папки, файл або папка перетворюються до стану без стиснення.

Зашифровані файли можуть стати розшифрованими, якщо файл копіюється або переміщується на тому, що не є томом NTFS. При переміщенні незашифрованих файлів в зашифровану папку вони автоматично шифруються в новій папці, проте зворотна операція не призведе до автоматичної розшифровці файлів, файли необхідно явно розшифрувати.

Не можуть бути зашифровані файли з атрибутом Системний і файли в системному каталозі. Шифрування папки або файлу не захищає їх від видалення — будь-який користувач, який має права на видалення, може видалити зашифровані папки або файли. З цієї причини рекомендується використання EFS в комбінації з дозволами системи NTFS. Можуть бути зашифровані або розшифровані файли і папки на віддаленому комп'ютері, для якого дозволено віддалене шифрування. Однак якщо зашифрований файл відкривається по мережі, передані при цьому по мережі дані не будуть зашифровані. Для шифрування даних, переданих по мережі, повинні використовуватися інші протоколи, наприклад SSL / TLS або IPSec.

Процес шифрування в Microsoft Windows на більш низькому рівні, щоб убезпечити себе від витрат шифрування, а саме — втрати даних.

Для початку згадаємо дві основні криптографічні системи. Найбільш проста — шифрування з використанням секретного (симетричного) ключа, тобто для шифровки і розшифровки даних використовується один і той же ключ. Переваги: висока швидкість шифрування; недоліки: проблема передачі секретного ключа, а саме можливість його перехоплення. Представники: DES, 3DES, DESX, AES. Відмінність шифрування з відкритим ключем (асиметричне шифрування) полягає в тому, що дані шифруються одним ключем, а розшифровуються іншим, за допомогою одного і того ж ключа не можна здійснити зворотне перетворення. Ця технологія шифрування припускає, що кожен користувач має в своєму розпорядженні пару ключів — відкритий ключ (public key) і особистий або закритий ключ (private key). Таким чином, вільно поширюючи відкритий ключ, ви надаєте іншим користувачам можливість шифрувати свої повідомлення, спрямовані вам, які зможете розшифрувати тільки ви. Якщо відкритий ключ і потрапить в «погані руки», то він не дасть можливості визначити секретний ключ і розшифрувати дані. Звідси і основна перевага систем з відкритим ключем: не потрібно передавати особистий ключ, однак є й недолік — низька швидкість

шифрування. Представники: RSA, алгоритм Ель-Гамаля, алгоритм Діффі-Хелмана.

В EFS для шифрування використовуються всі переваги вище перелічених систем. Дані шифруються за допомогою симетричного алгоритму із застосуванням ключа шифрування файлу (File Encryption Key, FEK). FEK — згенерований EFS випадковим чином ключ. На наступному етапі FEK шифрується за допомогою відкритого ключа користувача і зберігається в межах атрибута, званого полем розшифровки даних (Data Decryption Field, DDF) безпосередньо всередині самого файлу. Крім того, EFS шифрує FEK, використовуючи відкритий ключ агента відновлення, і поміщає його в атрибут Data Recovery Field — DRF. DRF може містити дані для безлічі агентів відновлення.

Агент відновлення даних (Data Recovery Agent, DRA) — користувач, який має доступ до всіх зашифрованих даних інших користувачів. Це актуально в разі втрати користувачами ключів або інших непередбачених ситуаціях.

Агентом відновлення даних призначається зазвичай адміністратор. Для створення агента відновлення потрібно спочатку створити сертифікат відновлення даних і визначити політику відновлення, а потім призначити одного з користувачів таким агентом. Політика відновлення грає важливу роль в системі шифрування Windows , вона визначає агентів відновлення, а їх відсутність або видалення політики взагалі забороняє використання користувачами шифрування.

За замовчуванням політика відновлення така, що права агента відновлення належать адміністратору. Якщо сертифікат агента відновлення за замовчуванням видалений, а іншого агента в політиці немає, комп’ютер буде мати порожню політику відновлення. Порожня політика відновлення означає, що агента відновлення не існує. Це відключає EFS, отже, забороняє користувачам шифрувати файли на цьому комп’ютері. Ми можемо створити обліковий запис адміністратора за допомогою агента відновлення та

провести для надійності операцію експорту його ключа, а можемо створити новий сертифікат відновлення і призначити іншого користувача в якості агента.

Часто недоліком шифрування за допомогою EFS вважають неможливість транспортування зашифрованих даних, тобто записати дані на «болванку», не втративши їх секретність, не вдасться. Але це не зовсім так — дійсно, просто записати їх не можна, але можна скористатися програмою архівації для Windows — NTBackup, в цьому випадку дані будуть скопійовані на вказаний носій без дешифрування, причому носій може не підтримувати NTFS 5.0. Після відновлення зашифровані дані залишаються в зашифрованому вигляді.

2.14.3 Маркер доступу Access token

Маркер доступу (англ. Access token) - програмний об'єкт операційних систем класу Microsoft Windows, містить інформацію з безпеки сеансу ідентифікує користувача, групу користувачів і користувальницькі привілеї.

Маркер доступу - це об'єкт, що інкапсулює дескриптор безпеки процесу. Доданий до процесу, дескриптор безпеки ідентифікує власника об'єкта. Поки маркер використовується для представлення тільки інформації з безпеки, він технічно вільний за своїм змістом і може містити будь-які дані. Маркер доступу використовується Windows, коли процес намагається взаємодіяти з об'єктами, дескриптори безпеки яких вимагають контроль доступу. Маркер доступу представлений системним об'єктом типу Token. Унаслідок того, що маркер - звичайний системний об'єкт, доступ до самого маркеру може бути проконтрольована за допомогою дескриптора безпеки, але це зазвичай ніколи не робиться на практиці.

Маркер доступу генерується сервісом входу в систему, коли користувач реєструється і його справжність успішно встановлена, визначаючи права користувача в дескрипторі безпеки, укладеному в маркер.

Маркер додається до кожного процесу, створеному сесією користувача (процеси, власником яких є користувач). Коли б такий процес ні запитував будь-який ресурс, доступ до якого контролюється, Windows дивиться в дескрипторі безпеки в маркері доступу, чи має користувач, власник даного процесу, право доступу до даних, і, якщо так, які операції (читання, запис / зміна) йому дозволені. Якщо операція дозволена в контексті даного користувача, Windows дозволяє процесу її продовжувати, якщо ні, то відмовляє в доступі.

2.14.4 Типи маркерів доступу

Існує два типи маркерів доступу:

– первинні маркери доступу можуть бути асоційовані тільки з процесом і являють собою суб'єкт безпеки процесу. Створення первинних маркерів і їх асоціація з процесом є привілейованими операціями, нужденними в двох різних привілеях (для поділу привілеїв) - типовий сценарій бачить створює маркер доступу сервіс ідентифікації та сервіс входу в систему, асоціює його з оболонкою операційної системи. Процес спочатку успадковує копію первинного маркера батьківського процесу. Імперсоналізіруючі маркери доступу можуть бути асоційовані тільки з потоками і являють собою суб'єкти безпеки клієнтського процесу.

– імперсоналізіруючий маркер доступу.

Імперсоналізація - це концепт безпеки властивий тільки Windows NT, що дозволяє серверному додатку тимчасово «бути» клієнтом для доступу до охоронюваного об'єкту. Імперсоналізація складається з трьох можливих рівнів: ідентифікація, що дозволяє сервера перевіряти справжність клієнта, імперсоналізація, що дозволяє сервера працювати від імені клієнта, і делегація, те ж, що і імперсоналізація, тільки розширена на роботу з віддаленими системами, з якими зв'язується сервер. Клієнт може вибрати

максимально можливий рівень імперсоналізації на сервері в параметрі підключення. Делегація і імперсоналізація - привілейовані операції.

2.14.5 Декриптори захисту і управління доступом

Маркери, які ідентифікують посвідчення користувача, є лише частиною виразу, що описує захист об'єктів. Інша його частина - інформація про захист, зіставлена з об'єктом і вказує, кому і які дії дозволено виконувати над об'єктом. Структура даних, яка зберігає цю інформацію, називається дескриптором захисту (security descriptor). Дескриптор захисту включає наступні атрибути:

– номер версії. Версія моделі захисту SRM, використаної для створення дескриптора;

– прапори. Необов'язкові модифікатори, що визначають поведінку або характеристики дескриптора. Приклад - прапор SE_DACL_PROTECTED, який забороняє спадкування дескриптором параметрів захисту від іншого об'єкта;

– SID власника Ідентифікатор захисту власника;

– SID групи Ідентифікатор захисту основної групи для даного об'єкта (використовується тільки POSIX);

– список управління виборчим доступом (discretionary access-control list, DACL) Вказує, хто може отримувати доступ до об'єкта і які види доступу;

– системний список управління доступом (system access-control list, SACL) Вказує, які операції і яких користувачів повинні реєструватися в журналі аудиту безпеки.

–

2.14.6 Список управління доступом ACL

Список управління доступом (access-control list, ACL) складається з заголовка і може містити елементи (access-control entries, ACE). Існує два типи ACL: DACL і SACL. В DACL кожен ACE містить SID і маску доступу (а також набір прапорів), причому ACE можуть бути чотирьох типів: «доступ дозволений» (access allowed), «доступ відхилений» (access denied), «дозволений об'єкт» (allowed-object) і «заборонений об'єкт» (denied-object).

Різниця між ACE типу «дозволений об'єкт» і «доступ дозволений», а також між ACE типу «заборонений об'єкт» і «доступ відхилений» полягає в тому, що ці типи використовуються тільки в Active Directory. ACE цих типів мають поле глобально унікального ідентифікатора (globally unique identifier, GUID), яке повідомляє, що даний ACE застосовується лише до певних об'єктів або під об'єктам (з GUID-ідентифікаторами). Крім того, необов'язковий GUID вказує, що тип дочірнього об'єкта успадковує ACE при його (об'єкта) створення в контейнері Active Directory, до якого застосований ACE. (GUID - це гарантовано унікальний 128-бітний ідентифікатор.)

За рахунок акумуляції прав доступу, зіставлених з індивідуальними ACE, формується набір прав, наданих ACL-списком. Якщо в дескрипторі захисту немає DACL (DACL = null), будь-який користувач отримує повний доступ до об'єкта. Якщо DACL порожній (в ньому немає ACE), доступу до об'єкту не отримує ніхто.

ACE, використовувані в DACL, також мають набір прапорів, контролюючих та визначають характеристики ACE, пов'язані зі спадкуванням. Деякі простору імен об'єктів містять об'єкти-контейнери і об'єкти-листи (leaf objects). Контейнер може включати інші контейнери і листи, які є його дочірніми об'єктами. Приклади контейнерів - каталоги в просторі імен файлової системи і розділи в просторі імен реєстру.

SACL складається з ACE двох типів: системного аудиту (system audit ACE) і об'єкта системного аудиту (system audit-object ACE). Ці ACE визначають, які операції, що виконуються над об'єктами конкретними

користувачами або групами, підлягають аудиту. Інформація аудиту зберігається в системному журналі аудиту. Аудиту можуть підлягати як успішні, так і невдалі операції. Як і специфічні для об'єктів ACE з DACL, ACE об'єктів системного аудиту містять GUID, який вказує типи об'єктів або під-об'єктів, до яких застосовується даний ACE, і необов'язковий GUID, контролюючий передачу ACE дочірніх об'єктів конкретних типів. При SACL, рівному null, аудит об'єкта не ведеться.

Спрощена схема об'єкта «файл» і його DACL представлена на рис .2.10

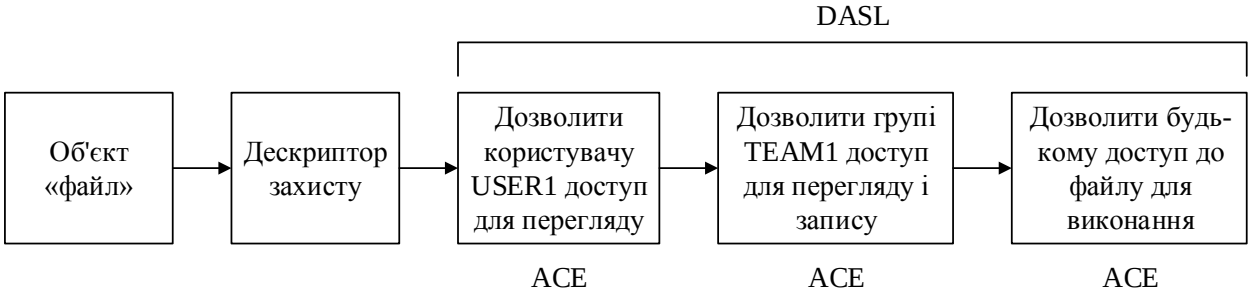


Рисунок 2.10 - Схема об'єкта «файл» і його DACL

Як показано на рис.2.10, перший ACE дозволяє USERl читати файл. Другий ACE дозволяє членам групи TEAM1 читати і записувати файл. Третій ACE надає доступ до файлу для виконання всім користувачам.

Дескриптор захисту містить два ACE типу «доступ дозволений», причому один з них вказує обліковий запис адміністратора (її можна розпізнати по RID, рівному 500), а інший - обліковий запис System (яка завжди виглядає як Sl-5-18). Без декодування бітів, встановлених в масках доступу в ACE і визначення того, яким типам доступу до процесів вони відповідають, дуже важко сказати, якими правами доступу до об'єкта «процес» для Winlogon володіє кожна з цих облікових записів. Однак, якщо ви зробите це, використовуючи заголовні файли з SDK, то виявите, що обидві облікові записи мають повні права доступу.

2.14.7 Список контролю доступу ACL

Список контролю доступу(AccessControlListабоACL) - список прав доступу до об'єкта, який визначає, хто або що може отримувати доступ до нього, и які самє операции дозволено або заборонено проводити над об'єктом.

Списки контролю доступу є основою систем з вибірковим управлінням доступом. У типових ACL кожензапис визначає суб'єкт впливу и операцію: наприклад, записи (Taras, delete) в ACL для файлу XYZ дають можливість користувачеві Taras ВИДАЛИТИ файл XYZ.

В системі з моделлю безпеки, заснованої на ACL, коли суб'єкт запитує виконання операції над об'єктом, система спочатку перевіряє список дозволеного для цього суб'єкта операцій, та тільки після цього дає (або не дает) доступ до запитуваної дії.

При централізованому зберіганні списків контролю доступу можна говорити про матрицю доступу, в якій по осях розміщені об'єкти и суб'єкти, а в клітінках - відповідні права. Однак у великій кількості систем списки контролю доступу до об'єктів зберігаються окремо для кожного об'єкта, найчастіше безпосередно з самим об'єктом.

Традиційні ACL системи призначають права індивідуальним користувачам. Варіантом цієї проблеми є призначення прав групам користувачів, а не персонально. Іншім варіантом цієї проблеми є «управління доступом на основі ролів», де функціональні підмножинні прав до ряду об'єктів об'єднуються в «ролі», і ці ролі призначаються користувач. Однак, у першому варіанті групи користувачів також часто називаються ролями.

2.14.8 Файлові системи з ACL

У файлових системах для реалізації ACL використовується Ідентифікатор користувача процесу (UID в термінах POSIX).

Список доступу представляє собою структуру даних (зазвичай таблицю), що містить записи, які визначають права індивідуального користувача або групи на спеціальні системні об'єкти, Такі як програми, процеси або файли. Ці записи також відомі як ACE (Access Control Entries) в операційних системах Microsoft Windows и OpenVMS. В операційній системі Linux и Mac OS X більшість файлових систем мают розширені атрибути, что виконують роль ACL. Кожен об'єкт в системі містіть показчик на свій ACL. Привілеї (або повноваження) визначаються спеціальні права доступу, що дозволяє користувачеві читати з (Read), писати в (Write), або виконувати (execute) об'єкт. У деяк реалізаціях ACE могут визначати право користувача або групи на зміну ACL об'єкта.

2.14.9 Ідентифікатор безпеки SID

Ідентифікатор безпеки (Security Identifier (SID)**)** - структура даних змінної довжини, яка ідентифікує обліковий запис користувача, групи, домену або комп'ютера (в Windows на базі технології NT (NT4, 2000, XP, 2003, Vista, 7,8)). SID ставиться у відповідність кожного облікового запису в момент її створення. Система оперує з SID'амі облікових записів, а не їх іменами. У контролі доступу користувачів до захищених об'єктів (файлів, ключів реєстру) беруть участь також тільки SID'и.

Для ідентифікації об'єктів, що виконують в системі різні дії, Windows використовує не імена (які можуть бути не унікальними), а ідентифікатори захисту (security identifiers, SID). SID є у користувачів, локальних і доменних груп, локальних комп'ютерів, доменів і членів доменів. SID являє собою числове значення змінної довжини, сформоване з номера версії структури SID, 48-бітного коду агента ідентифікатора і змінної кількості 32-бітних кодів субагентів та / або відносних ідентифікаторів (relative identifiers, RID). Код агента ідентифікатора (identifier authority value) визначає агент, який видав SID. Таким агентом зазвичай є локальна система або домен під

управлінням Windows. Коди субагентів ідентифікують піклувальників, уповноважених агентом, який видав SID, а RID - не більше ніж засіб створення унікальних SID на основі загального базового SID (common-based SID). Оскільки довжина SID досить велика і Windows намагається генерувати істинно випадкові значення для кожного SID, ймовірність появи двох однакових SID практично дорівнює нулю.

SID призначається комп'ютеру при установці Windows (програмою Windows Setup). Далі Windows призначає SID локальним облікових записів на цьому комп'ютері. SID кожної локального облікового запису формується на основі SID комп'ютера з додаванням RID. RID користувальницької облікового запису починається з 1000 і збільшується на 1 для кожного нового користувача або групи. Аналогічним чином Dcpromo.exe - утиліта, застосовувана при створенні нового домену Windows, - видає SID щойно створеного домену. Нові облікові записи домену отримують SID, що формуються на основі SID домену з додаванням RID (який також починається з 1000 і збільшується на 1 для кожного нового користувача або групи). RID з номером 1028 вказує на те, що його SID є 29-м, виданими доменом.

Winlogon створює унікальний SID для кожного інтерактивного сеансу входу. SID входу, як правило, використовується в елементі списку управління доступом (access-control entry, ACE), який дозволяє доступ на час сеансу входу клієнта. Наприклад, Windows-сервіс може викликати функцію LogonUser для запуску нового сеансу входу. Ця функція повертає маркер доступу, з якого сервіс може витягти SID входу. Потім цей SID сервіс може використовувати в ACE, дозволяючому звернення до інтерактивних об'єктів WindowStation і Desktop з сеансу входу клієнта. SID для сеансу входу виглядає як Sl-5-5-0, а RID генерується випадковим чином.

Параметри PsGetSid дозволяють транслювати імена облікових записів користувачів і комп'ютерів у відповідні SID і навпаки.

Якщо PsGetSid запускається без параметрів, вона виводить SID, призначений локального комп'ютера. Використовуючи той факт, що облікового запису Administrator завжди присвоюється RID, рівний 500, ви можете визначити ім'я цього облікового запису (у тих випадках, коли системний адміністратор перейменував її з міркувань безпеки), просто передавши SID комп'ютера, доповнений «-500», як аргумент командного рядка PsGetSid.

Ознайомившись з методами захисту даних, врахувавши всі переваги та недоліки вище описаних методів на рис. 2.11 побудований алгоритм захисту папок.

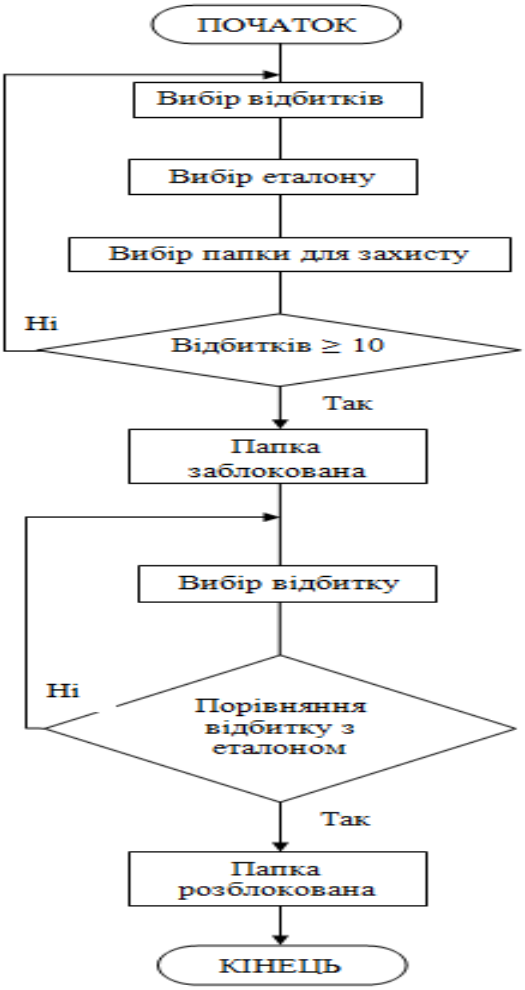


Рисунок 2.11 – Алгоритм захисту папки

2.15 Висновки

Запропонована методика ідентифікації складних зображень текстур завдяки інтегральному характеру основної класифікуючої ознаки - вектора різниці координат t_c володіє значною перешкодостійкістю від локальних спотворень, що виражаються в появі помилкових або зникненні вихідних структурних елементів. Запропонований механізм захисту даних дає можливість зберігати дані в зашифрованому форматі, також не дозволяє скопіювати або видалити дані. З допомогою програмних об'єктів відбувається обмеження доступу, та надається інформація про захист.

2.16 Програмна реалізація розроблених алгоритмів

2.17 Обґрунтування вибору мови програмування

Кожна мова спочатку проектувалася для максимально ефективного вирішення саме свого класу завдань. Тому мови програмування не можна порівнювати між собою поза зв'язком з завданнями, що розв’язуються, наприклад:

а) мова Фортран (Fortran - FORmula TRANslator - транслятор формул) - для чисельних обчислень;

б) мова Лісп (Lisp -LISt Processing - обробка списків) - для вирішення завдань штучного інтелекту;

в) мова Пролог (Prolog - PRO LOGic) - для програмування в термінах логіки і т.д.

Таким чином до написання програми підводиться питання вибору мови програмування, яка б надавала кращі засоби для вирішення поставленого завдання. Сформулюємо головні вимоги до програмної реалізації. Для реалізації поставленого завдання можна використовувати декілька мов програмування. Порівняємо їх характеристики і основне призначення в табл. 2.4.

Для реалізації програми вибрана мова програмування C++. Підкреслимо ті особливості мови, які визначили цей вибір:

C ++ - надзвичайно потужний мова, що містить засоби створення ефективних програм практично будь-якого призначення, від низькорівневих утиліт і драйверів до складних програмних комплексів самого різного призначення. Зокрема:

Підтримуються різні стилі та технології програмування, включаючи традиційне директивне програмування, ООП.

Є можливість роботи на низькому рівні з пам'яттю, адресами, портами.

Можливість створення узагальнених алгоритмів для різних типів даних, їх спеціалізація і обчислення на етапі компіляції, використовуючи шаблони.

Кросплатформеність. Доступні компілятори для великої кількості платформ, на мові C ++ розробляють програми для самих різних платформ і систем.

Ефективність. Мова спроектована так, щоб дати програмістові максимальний контроль над усіма аспектами структури та порядку виконання програми. Жодна з мовних можливостей, що призводить до додаткових накладних витрат, не є обов'язковою для використання - при необхідності мова дозволяє забезпечити максимальну ефективність програми

Переваги:

– швидкість роботи підсумкової програми (у порівнянні з Java / Python);

– пряме управління дімаміческой пам'яттю, що знову ж важливо для швидкості роботи.

Таблиця 2.4 - Порівняння мов програмування

Назва продукту	Основні переваги	Основне призначення
Visual C++	Універсальність. Найбільша швидкість роботи додатку.	Створення компонентів додатку для виконання критичних по

	Необмежена функціональність.	швидкості процесів, забезпечення функціональності, яка не допустима в інших засобах розробки
Object Pascal	Високий рівень об'єктної моделі. Висока швидкість обробки даних. Інтеграція об'єктно–орієнтованої мови програмування з операційною системою Windows.	Створення додатків масштабу підприємства. Створення додатків з великим рівнем важкості розробки.

2.18 Синтез програми

Вся програма складається з п'яти модулів, кожен з яких має своє власне вікно. Фрагменти тексту модулів представлені в додатку А.

При запуску програми на екрані з'являється основне вікно. У верхній частині вікна є меню, побудоване за допомогою компонентів MainMenu, яке і викликає основні функції програми. У нижній частині вікна –інформаційне вікно, в якому показано список використовуємих відбитків.

Перше вікно – це функція вибору зображень Images Select, за допомогою якої ми можемо обрати файли з зображенням відбитків, які будуть використовуватися під час роботи програми. Для ініціалізації діалогового вікна та вибору папки, в якій містяться зображення відбитків, використовуються функції DoModal та fileDialog.

Друге вікно використовується для виробу еталонного відбитку за допомогою функції EtalonSelect. Вибір папки та ініціалізація діалогового вікна відбуваються також за допомогою функцій DoModal та fileDialog.

Третє вікно використовується для вибору папки для закриття доступу за допомогою функції FolderSelect. На даному етапі використовується структура BROWSEINFO, що дозволяє керувати виглядом та поведінкою діалогу SHBrowseForFolder. Дана структура включає наступні компоненти:

- hwndOwner – визначає дескриптор вікна власника діалогу;
- pidlRoot – визначає корінь PIDL;
- pszDisplayName – повертає заголовок обраної папки;
- lpszTitle – дозволяє визначити текст, що відобразиться за допомогою діалогу;
- ulFlags – контролює тип папки, яку може обрати користувач.

Четверте вікно вмикає функцію заборони доступу до обраної нами папки у попередньому вікні за допомогою функції ClickedOn. Перед тим, як

увімкнути заборону доступу, програма здійснює перевірку наявності еталону, відбитків та кількості відбитків, шляху до папки, що потребує захисту. Якщо усі умови виконані, з’являється вікно з повідомлення про те, що папка заблокована.

П’яте вікно викликає функцію порівняння і повернення доступу ClickedOff. Якщо обраний відбиток співпадає з еталоном, повертається доступ до папки.

2.19 Випробування розробленої програми

Даний програмний продукт призначений для верифікації користувача по запропонованому зображенню відбитку пальця.

Програма висуває такі системні вимоги:

- IBM сумісний комп'ютер з 800 MHz процесором (або краще);
- маніпулятор миша;
- 64 Мбайт оперативної пам'яті;
- MS Windows 98 (і вище);
- роздільна здатність екрану: 1024x768 або вище.

Необхідний простір на жорсткому диску залежить від розміру бази даних з еталонами відбитків, мінімум 1Мб. Після запуску файлу fp_ukr на екрані з'являється вікно, показане на рис.2.12.

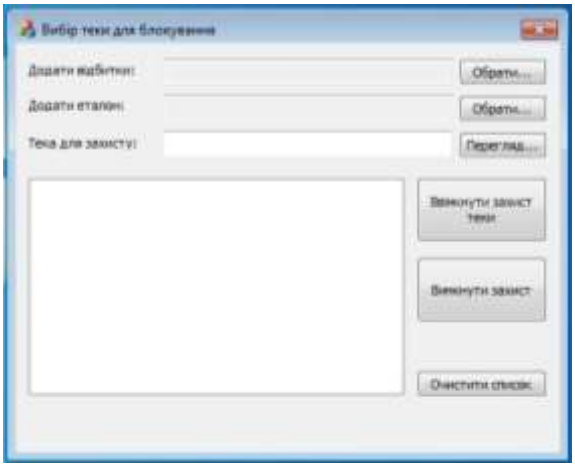


Рисунок 2.12 - Вікно після запуску програми

Розглянемо кожен пункт меню програми.

Вибір зображень. Цей пункт меню призначений для введення переліку графічних зображень відбитків, їх обробки з виділенням всієї необхідної інформації і запису на диск. Після активізації цього пункту меню на екрані з'явиться вікно, показане на рис.2.13.

Рисунок 2.13 - Вікно вибору зображень

У даному вікні обираються файли з графічним представленням відбитків (з врахуванням використовуваних форматів), натискувати кнопку Відкрити.

Вибір еталонного відбитку. Цей пункт меню призначений для введення графічного зображення еталонного відбитку, його обробки з виділенням всієї необхідної інформації і запису на диск. Після активізації цього пункту меню на екрані з'явиться вікно, показане на рис.2.14.

Рисунок 2.14 - Вікно вибору еталонного зображення

У даному вікні обирається файл з графічним представленням еталонного відбитку (з врахуванням використовуваних форматів), натискувати кнопку Відкрити.

Вибір папки для закриття доступу. Цей пункт призначений для вибору теки для закриття доступу, після активізації з’явиться вікно, зображене на рис. 2.15:

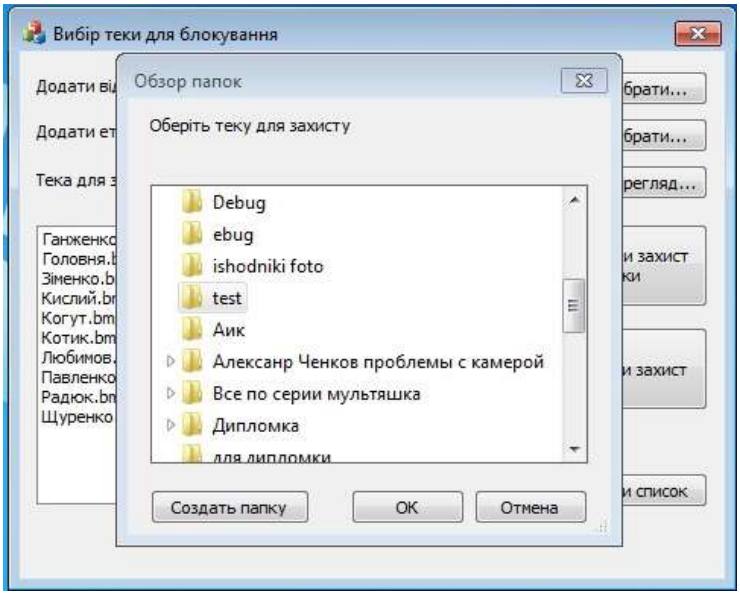


Рисунок 2.15 – Вікно вибору папки для захисту

Ввімкнення функції заборони доступу до теки. Цей пункт призначений для того, щоб ввімкнути заборону доступу до обраної у попередньому пункті теки. Після активації з’явиться повідомлення про блокування теки, зображене на рис. 2.16:

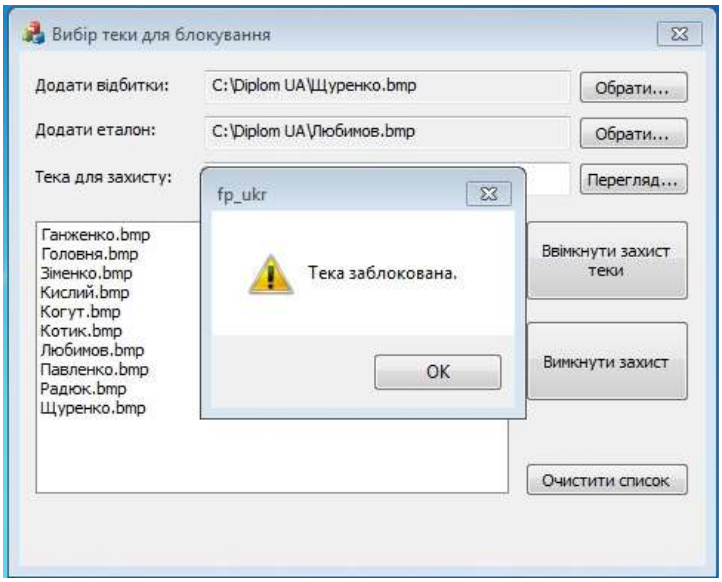


Рисунок 2.16 – Блокування доступу до папки

Якщо при виборі видбитків ми виберемо менше 10-ти зображень, то при використанні функції заборони доступу до обранної теки программа нас попередить про це (рис. 2.17):

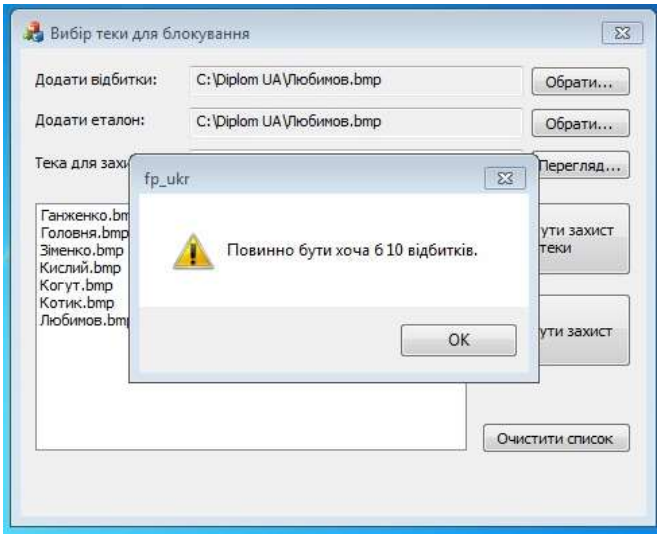


Рисунок 2.17 – Повідомлення щодо нестачі відбитків

Перевірка доступу до теки. Після виконання усіх попередніх пунктів, перевіримо доступ до заблокованої теки (рис.2.18-2.19):

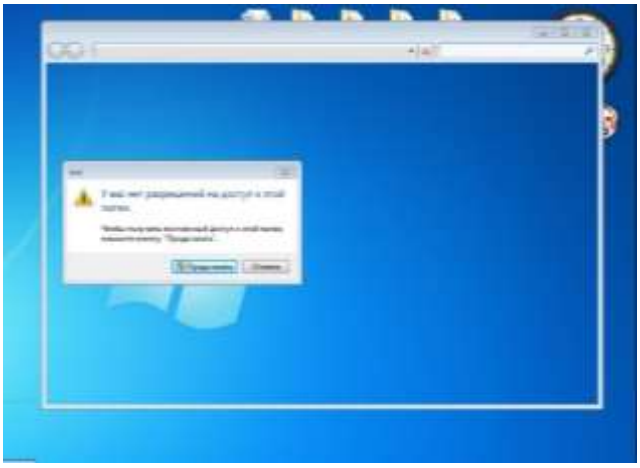


Рисунок 2.18 – Перевірка доступу

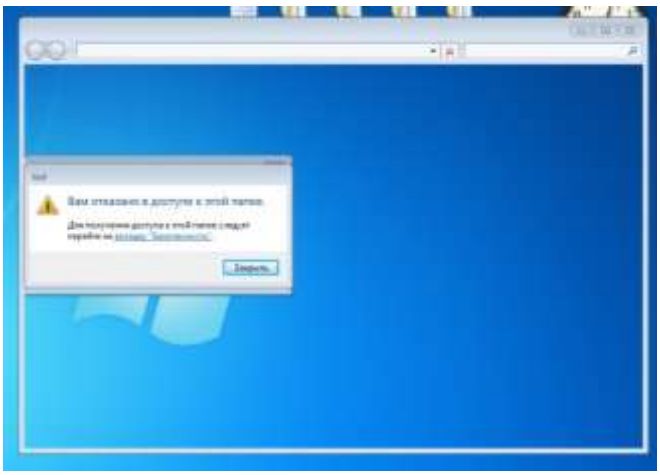


Рисунок 2.19 – Перевірка доступу

Як бачимо, ми не можемо зайти в обрану нами теку та скористатися данними, які в ній знаходяться.

Вибір відбитку для порівняння з еталоном. Цей пункт складається з двох підпунктів: «Відкрити файл та порівняти з еталоном», «Відкрити доступ до теки».Перший відкриває вибраний графічний файл з відбитком (рис. 2.20) і обробляє його, запитує ім'я файлу еталону, відкриває цей файл і порівнює з обробленим відбитком.

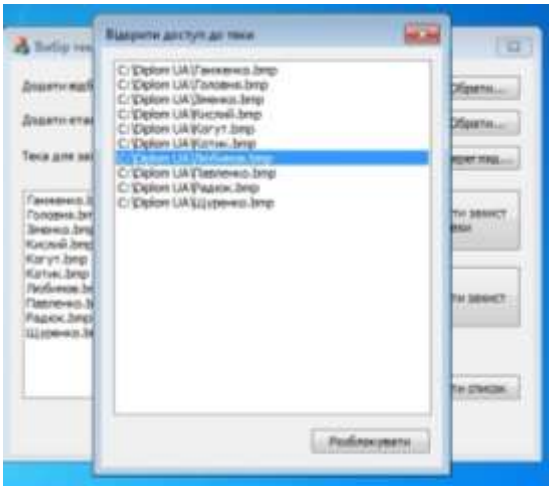


Рисунок 2.20 – Відкриття та порівняння файлу з еталоном

Другий підпункт відкриває доступ до теки якщо файли співпадають (рис. 2.21-2.22):

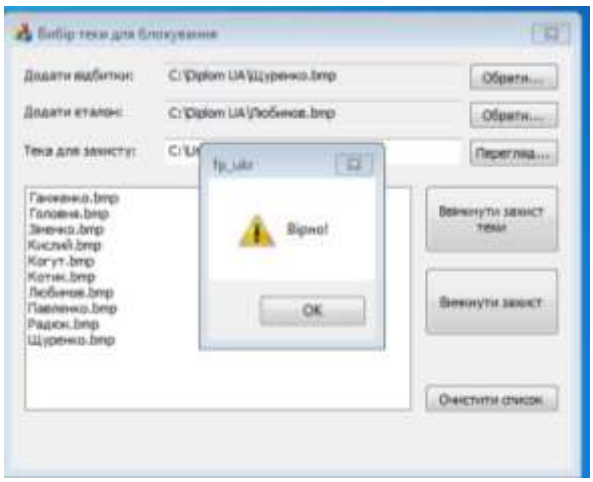


Рисунок 2.21 – Повідомлення про співпадання файлів

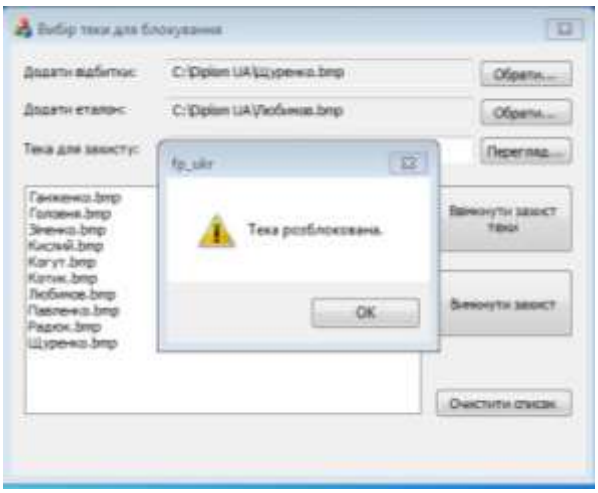


Рисунок 2.22 – Розблокування теки

Якщо відбитки не ідентичні, то доступ до теки не буде відкритий (рис. 2.23-2.24):

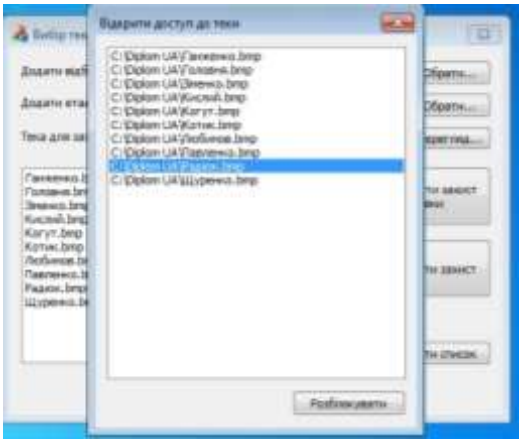


Рисунок 2.23 – Вибір невірного відбитку

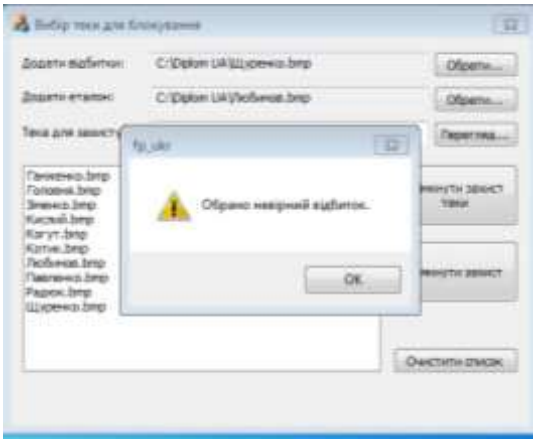


Рисунок 2.24 – Повідомлення про обрання невірного відбитку

Очищення списку відбитків. Цей етап полягає у виклику функції очищення відбитку, тобто видалення обраних на другому етапі відбитків з бази програми (рис. 2.25):

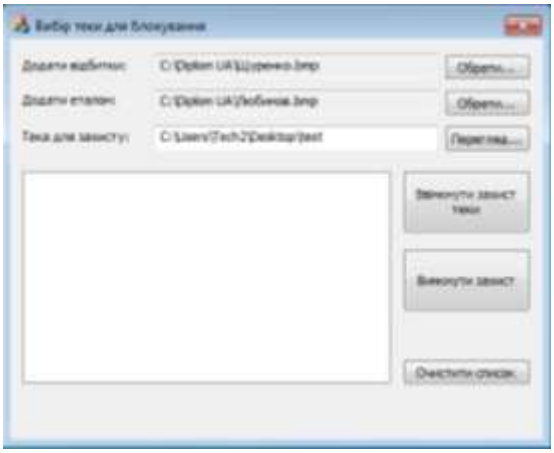


Рисунок 2.25 – Видалення списку відбитків

Програма не вимагає інсталяції. Для роботи програми необхідний файл fp_ukrta директорії з підготовленими відбитками.

2.20 Дослідження розроблених методів

Система шифрування EFS виконує чотири основні операції: відкриття, читання, запис і перетворення файлів. Оскільки EFS – прозорий сервіс, відкриття, читання і запис зашифрованих файлів не відрізняються від операцій зі звичайними файлами: додатки використовують звичайний Win32 API. Перетворення файлів – Це шифрування текстового файлу або

розшифровка зашифрованого файлу. Під час виконання процедури шифрування створюється тимчасвоий файл, в який записується вихідний файл. Потім вихідний файл усікається, дані зчитуються з тимчасового файлу і записуються в вихідний в незашифрованому вигляді.

Побічний ефект цієї процедури полягає в тому, що, коли тимчасовий файл видаляється, частини тексту можуть залишитися в невживаному дисковому просторі. Запустивши утиліту командного рядка cipher.exe з ключем / W, можна стерти вміст простору розділу, позначеного як вільне. Ця операція стирає залишилися після шифрування частини тексту файлів, що не вміщається в одну запис MFT (Master File Table). Розмір запису MFT залежить від розміру кластера диска і зазвичай становить 1024 байти. Вміститься чи файл в запис MFT, залежить від того, скільки місця залишилося в запису MFT після формування метаданих файлу. В MFT можуть міститися й інші дані, наприклад атрибути файлу або потоки. Крім того, у файлі може бути більше даних, ніж вміщує запис MFT. Додаткову інформацію про MFT см. в Microsoft Developer Network, в розділі Master File Table and MFT Zone документації Platform SDK.

Щоб повністю виключити ймовірність того, що на диску залишаться частини тексту, рекомендується ніколи не виконувати перетворення текстових файлів. Замість цього слід створити каталог і позначити його як зашифрований. Файл, який створюється в зашифрованому каталозі, відразу ж записується на диск в зашифрованому вигляді, а тимчасовий файл не створюється.

Очевидно, коли користувачеві потрібно зашифрувати вже існуючі файли, цей прийом не спрацює. У такому випадку рекомендується перетворити всі існуючі файли, які потрібно захистити, а потім з допомогою cipher.exe очистити весь вільний простір розділу. Після цього слід створювати всі файли, які потребують захисту, в зашифрованих каталогах.

Найважливішою характеристикою будь-якого розпізнавального пристрою його перешкодозахищеність - здатність протистояти впливу випадкових зовнішніх і внутрішніх перешкод, тобто забезпечити задану достовірність розпізнавання і точність визначення вхідного об'єкту за наявності випадкових перешкоджаючих дій, що призводять до невідповідності між еталонним і поточним вхідним зображенням, а отже, до деформації структур функції взаємної кореляції зображень, зниження відношення сигнал/шум.

Найважливішими з чинників, що впливають на відбиток, є наступні:

– нестаціонарність структури оброблюваного зображення;

– порушення плоско-паралельного зміщення реалізації відносно еталону;

– наявність зміщень, не кратних кроку дискретизації;

– похибки, що виникають в процесі виміру характеристик яскравості зображень.

Під нестаціонарністю структури зображення розуміється допустимість деякої зміни геометрії дактилоскопічного малюнка (подряпини на пальці, злиття ліній узору, розриви).

При дослідженні процесу верифікації відбитку аналізуватимемо, при якому рівні шуму він буде не розпізнаний або сприйнятий як чужий. При моделюванні процесу зашумлення розглянемо два варіанти: точковий шум (бруд) і лінійний (порізи).

Аналіз результатів моделювання дозволяє зробити наступні висновки:

1. При забрудненні відбитку ПРЕТ залишається досить стійкою ознакою, і аж до зашумлення 50% його площі залишається практично незмінним та не відбувається трансформації інформативних зон.

2. Порізи роблять сильніший вплив на правильність формування ПРЕТ, і вже при 20% інтенсивності відбувається його трансформація і зміна місця розташування інформативних зон.

3. При допустимому шумі верифікація здійснюється надійно.

На рис.2.26÷2.31 приведені результати верифікації відбитків при різній інтенсивності їх зашумлення. На рис.2.32 представлено зображення ідеального відбитку і його ПРЕТ з показом виділених інформативних зон.

На рис.2.33 і рис.2.34 представлені критично зашумлені відбитки. З цих малюнків видно, що ПРЕТ навіть в цьому випадку залишається практично незмінним.

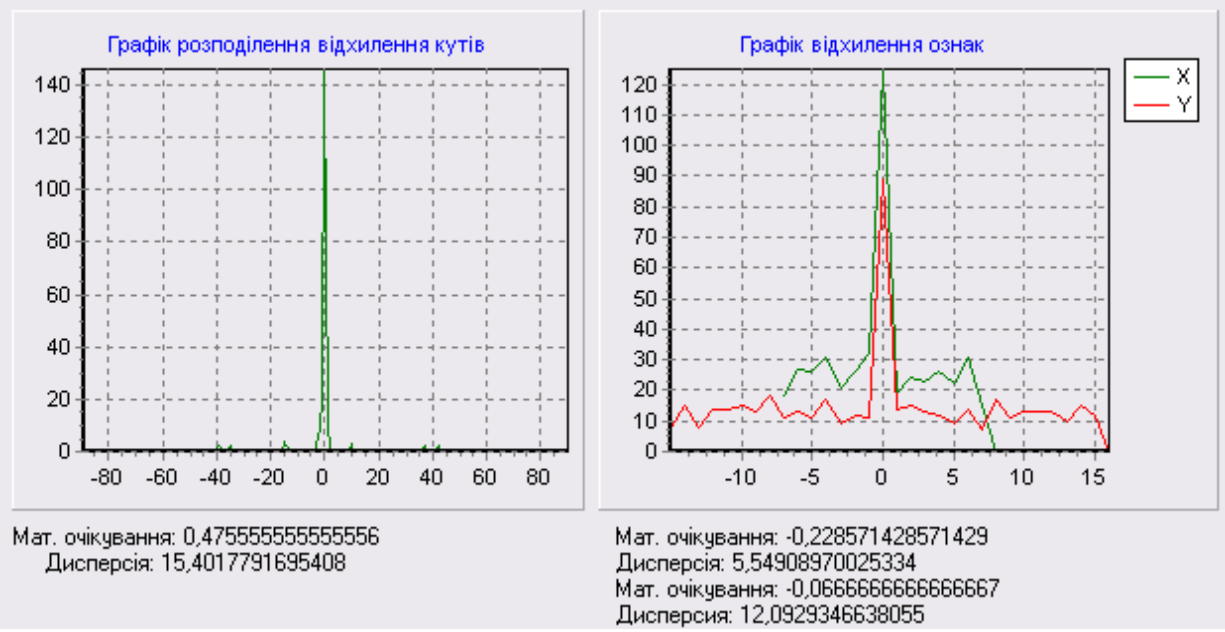


Рисунок 2.26– Результати порівняння однакових відбитків з інтенсивністю зашумлення 10%

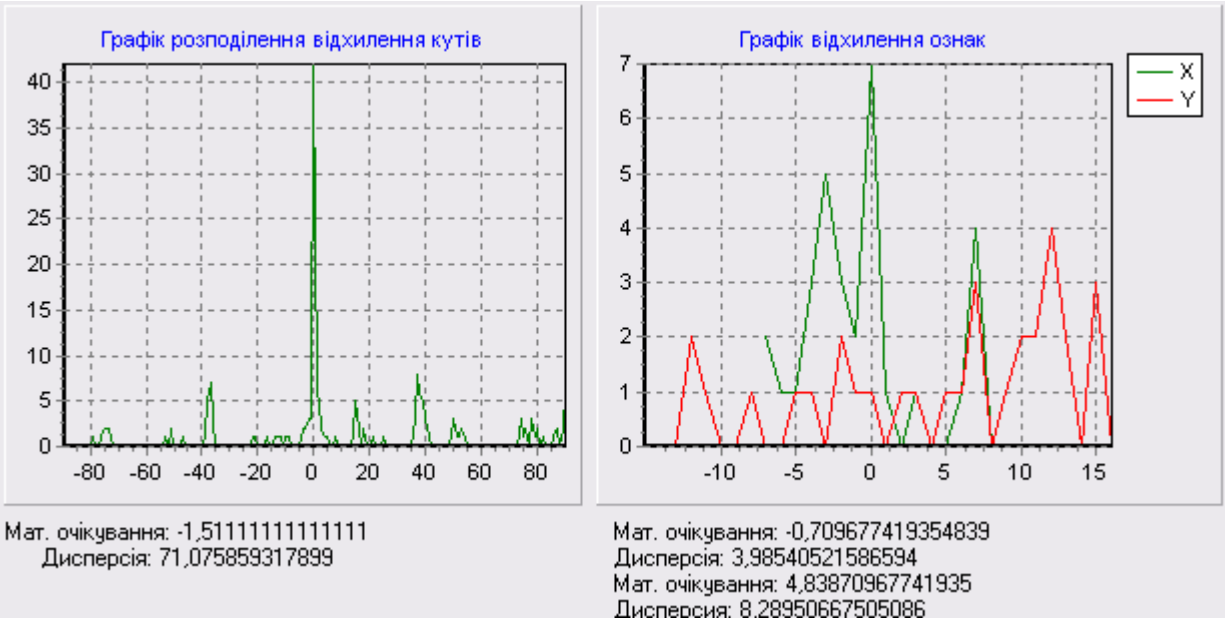


Рисунок 2.27– Типові результати порівняння різних відбитків без зашумлення

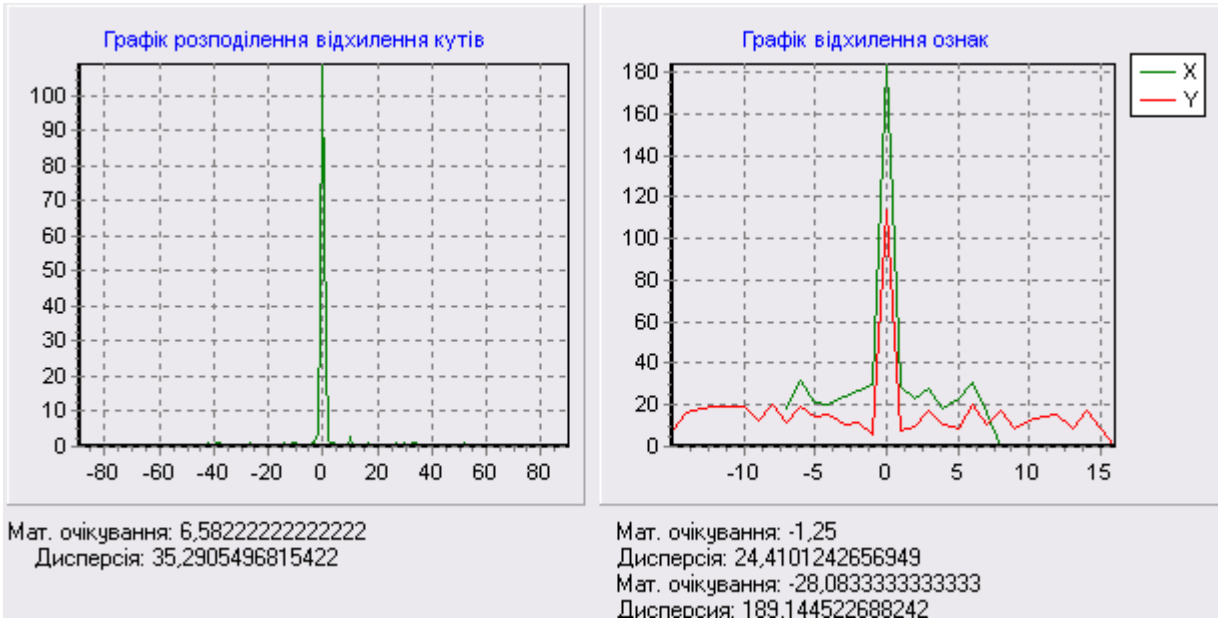


Рисунок 2.28– Результати порівняння однакових відбитків з інтенсивністю зашумлення 20%

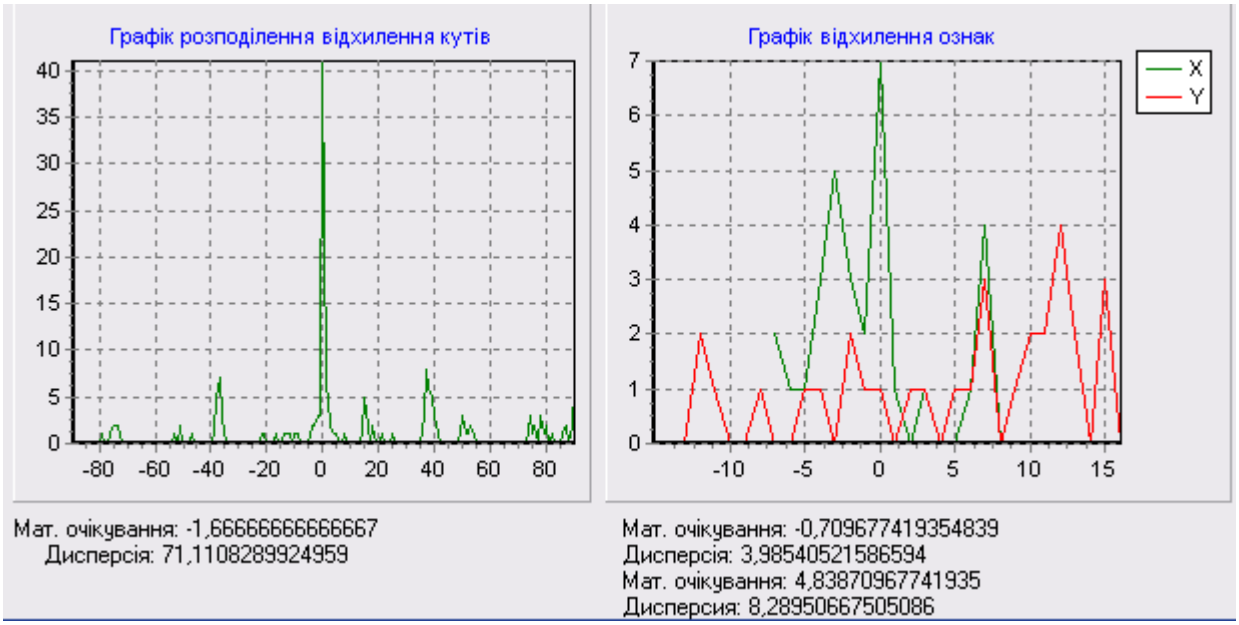


Рисунок 2.29– Типові результати порівняння різних відбитків без зашумлення

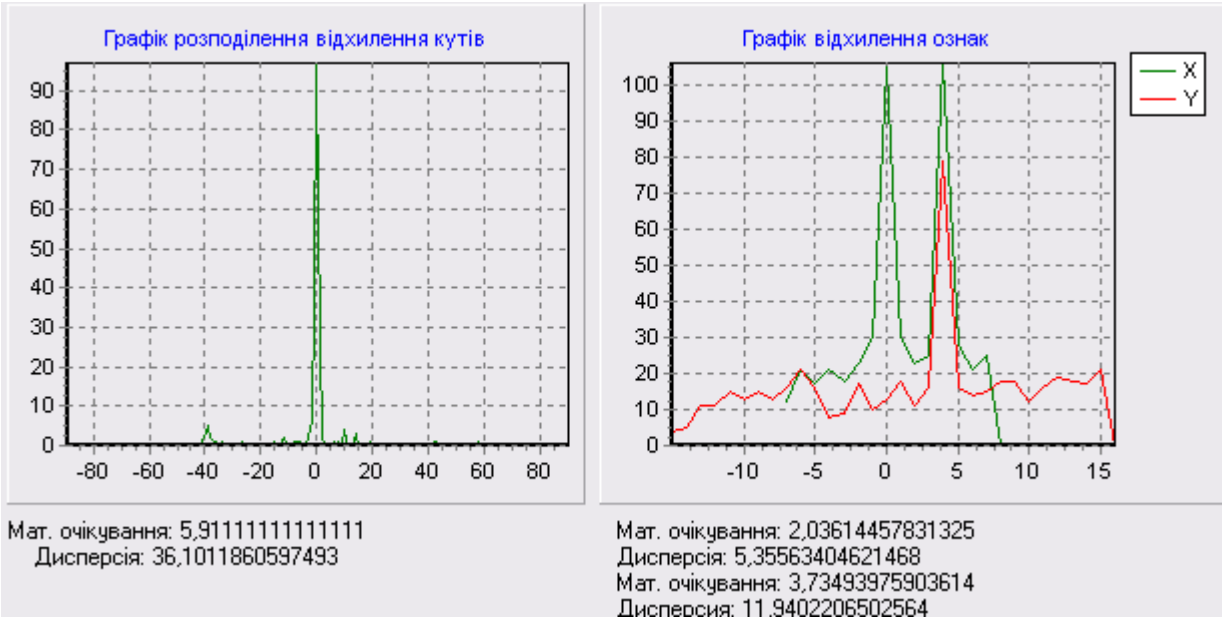


Рисунок 2.30– Результати порівняння однакових відбитків з інтенсивністю зашумлення 20% із зсувом на 4 пікселя

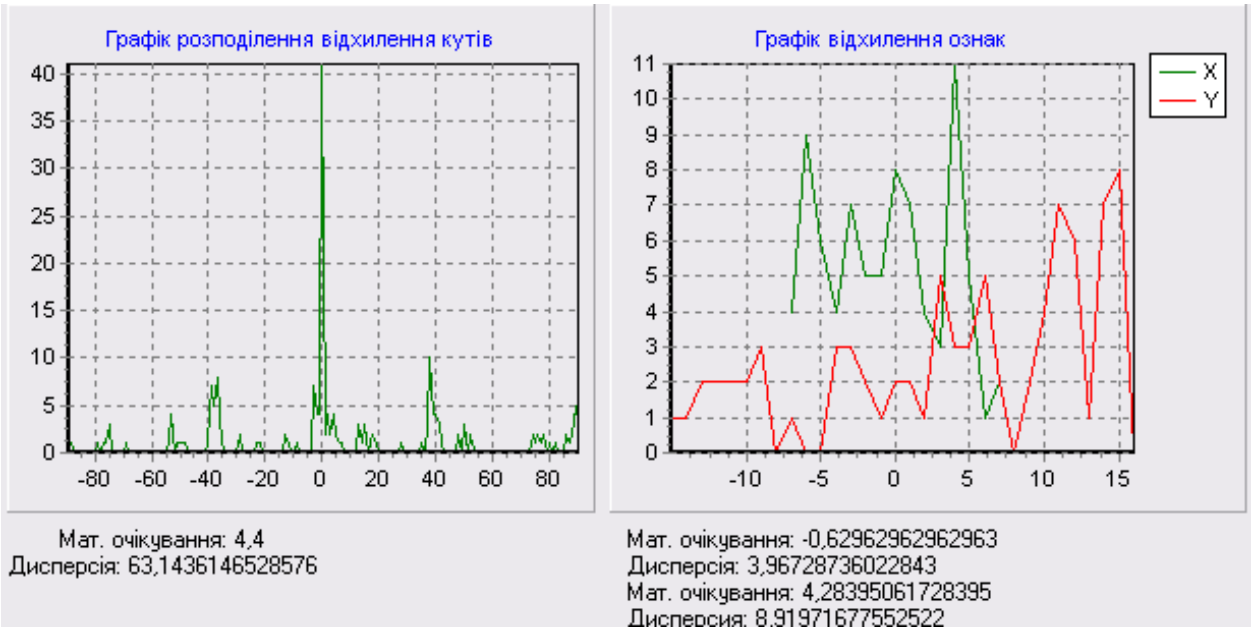


Рисунок 2.31– Типові результати порівняння різних відбитків з інтенсивністю зашумлення 20% із зсувом на 4 пікселя

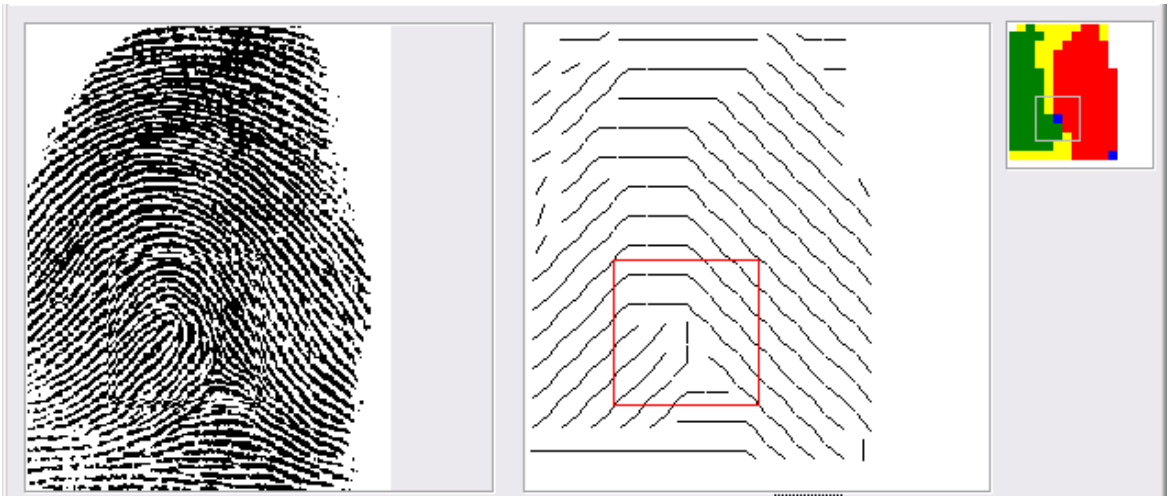


Рисунок 2.32 –Еталонне зображення відбитку і ПРЕТ

Рисунок 2.33– Зашумлення початкового відбитку точковим шумом з інтенсивністю 40%

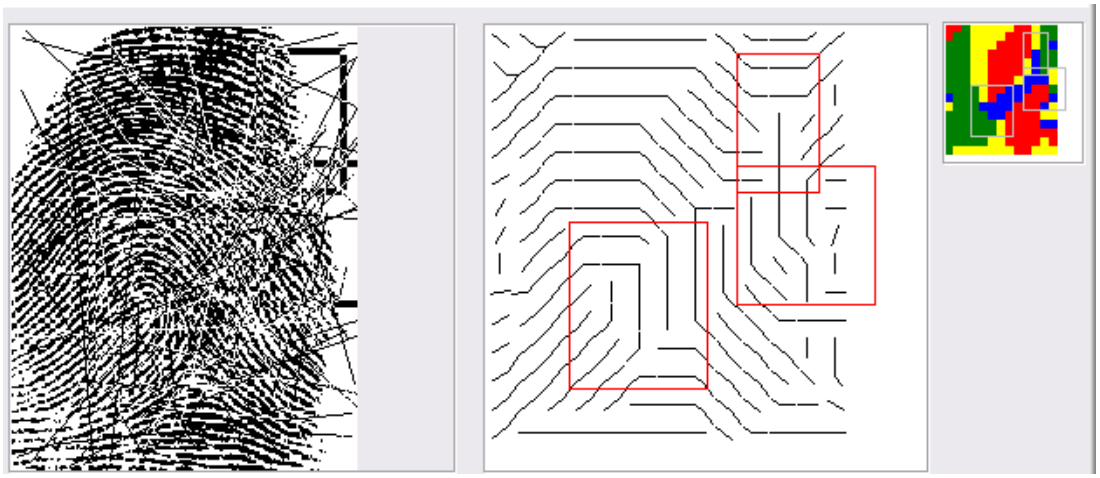


Рисунок 2.34– Зашумлення початкового відбитку лінійним шумом з інтенсивністю 40%

2.21 Висновки

Проведений аналіз системи шифрування, що використовується у розробленому програмному засобі, показав, що головним її недоліком є ймовірність копіювання частин текстових файлів на диск. Тому головною умовою запобігання незахищеності інформації залишається блокування не окремих документів, що повинні бути новостворенними, а тек з файлами.

Проведений аналіз роботи програми показав, що при зміщенні зображення відбитку більш ніж на 10 пікселів по обох осях навіть без зашумлення результат порівняння по інформативних зонах дає негативний результат по вертикальній осі, що пов'язане з дуже великою зоною, якааналізується при порівнянні координат інформативних ознак по вертикальній осі.

А також з'ясувалося, що при порівнянні кутів нахилу відрізків портрету велику роль грає шум у вигляді чорних і білих ліній різної товщини. Зате до точкового шуму цей алгоритм менш чутливий. При порівнянні інформативних зон все навпаки. Шум з чорних і білих ліній не позначається сильно на результаті верифікації. Зате при точковому шумі результат порівняння негативний навіть при невеликому відсотку зашумлення.

Це говорить про те, що ці два алгоритми потрібно використовувати разом, тим самим підвищуючи достовірність порівняння до 90% і вище.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

В дипломному проекті було розроблено програмне забезпечення яке ідентифікує особу завдяки обробці зображень пальців, та обмежує доступ до комп’ютерних ресурсів. Це програмне забезпечення використовує біометрію. В економічной частині буде проведено розрахунок економічної ефективності використання цього ПЗ, показник загального ефекту від впровадження системи інформаційної безпеки, коефіцієнт повернення інвестицій та коефіцієнт повернення інвестицій ROSI.

В нашому випадку розробник є одночасно і виробником, який на свій ризик та за свої власні кошти здійснює розробку нового технічного рішення для реалізації його споживачам.

5.1 Розрахунок капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Капітальні витрати на розробку та використання ПЗ розраховуються за формулою:

$$K = K_{\text{зпз}} + K_{\text{пз}} \quad (3.1)$$

де $K_{\text{зпз}}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;.;

$K_{\text{пз}}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн.

Для закупівлі ліцензійного основного й додаткового програмного забезпечення обрано безкоштовні програмні засоби які мають ліцензію, яка дозволяє їх використовувати для власних комерційних розробок. Вартість створення основного програмного забезпечення напряму залежить від кваліфікації розробників. Оцінивши складність розробки маємо наступні значення.

Результати розрахунку капітальних витрат наведені в таблиці 3.1.

Таблиця 5.1 – Розрахунок капітальних витрат

Вид витрат	Вартість, грн..
Закупівля ліцензійного ПЗ	0
Розробка основного ПЗ	6000
Всього	6000

5.1.1. Визначення витрат на створення програмного засобів захисту інформації

Для розробки програмного забезпечення необхідно виконати наступні, техніко-економічні розрахунки:

- визначення трудомісткості розробки та опрацювання ПЗ;
- розрахунок витрат на створення програмного продукту;
- оцінку швидкодії та надійності роботи програмного продукту.

5.1.1.1. Визначення трудомісткості розробки та опрацювання програмного продукту

Трудомісткість створення ПЗ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації, враховується робота одного програміста:

$$t = t_{mз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д}, \text{ годин} \quad (3.2)$$

$$t = 5 + 0.35 + 0.92 + 0.92 + 7.59 + 3.159 = 17.9, \text{ годин} \quad (3.2)$$

де $t_{mз}$ – тривалість складання технічного завдання на розробку ПЗ;
$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;
$t_{а}$ – тривалість розробки блок-схеми алгоритму;
$t_{пр}$ – тривалість програмування за готовою блок-схемою;
$t_{опр}$ – тривалість опрацювання програми на ПК;
$t_{д}$ – тривалість підготовки технічної документації на ПЗ.

Складові трудомісткості визначаються на підставі умовної кількості операторів у програмному продукті $\boldsymbol{Q}$ (з урахуванням можливих уточнень у процесі роботи над алгоритмом і програмою).

Умовна кількість операторів у програмі:

$$Q = q \cdot c\,(1 + p), \text{ штук,} \quad (3.3)$$

$$Q = 15 \cdot 1{,}5\,(1 + 0{,}08) = 24{,}3 \text{ штук,} \quad (3.3)$$

де q – очікувана кількість операторів;

c – коефіцієнт складності програми;

p – коефіцієнт корекції програми в процесі її опрацювання.

Тривалість вивчення технічного завдання:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k}, \quad \text{годин,} \tag{3.4}$$

$$t_в = 24.3 \cdot 1.2 / 75 \cdot 1.1 = 0.35 \text{ години,} \tag{3.4}$$

де В – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, В = 1,2...1,5;

k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом

Тривалість розробки блок-схеми алгоритму:

$$ta = \frac{Q}{(20...25) \cdot k}, \text{ годин.} \tag{3.5}$$

$$t_a = 24.3 / 22 \cdot 1.2 = 0.92 \text{ годин.} \tag{3.5}$$

Тривалість складання програми за готовою блок-схемою:

$$tпр = \frac{Q}{(20...25) \cdot k}, \text{ годин.} \tag{3.6}$$

$$t_{пр} = 24.3 / 22 \cdot 1.2 = 0.92 \text{ годин} \tag{3.6}$$

Тривалість опрацювання програми на ПК:

$$tonp = \frac{1{,}5Q}{(4...5)\cdot k},\ \text{годин.} \qquad (3.7)$$

$$t_{опр} = 1.5 \cdot 24.3 / 4 \cdot 1.2 = 7.59\ \text{годин} \qquad (3.7)$$

Тривалість підготовки технічної документації на ПЗ:

$$t_{Д} = \frac{Q}{(15...20)\cdot k} + \frac{Q}{(15...20)} \cdot 0{,}75 \qquad (3.8)$$

$$t_{д} = 24.3 / 15 \cdot 1.2 + (24.3 / 15) \cdot 0.75 = 3.159 \qquad (3.8)$$

3.1.1.2. Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту ***Кпз*** складаються з витрат на заробітну плату виконавця програмного забезпечення ***Ззп*** і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК ***Змч***:

$$К_{пз} = З_{зп} + З_{мч}\ . \qquad (3.9)$$

$$К_{пз} = 5958 + 42 = 6000. \qquad (3.9)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{ЗП} = t \cdot З_{ПР},\ \ \text{грн,} \qquad (3.10)$$

$$З_{зп} = 17.9 \cdot 332.84 = 5958,\ \ \text{грн,} \qquad (3.10)$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на ПК

визначається за формулою:

$$З_{мч} = t_{опр} \cdot C_{мч} + t_{д} \text{ , грн,} \quad (3.11)$$

$$З_{мч} = 7.59 \cdot + 3.159 = 42 \text{ , грн,} \quad (3.11)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_{д}$ – трудомісткість підготовки документації на ПК, годин;

3.2 Розрахунок експлуатаційних витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

У даному випадку експлуатаційні витрати розраховуються як:

$$C = C_{\text{а}} + C_{\text{тос}} \quad (3.12)$$

$$C_{\text{а}} = \frac{K}{n} = \frac{6000}{1} = 6000 \quad (3.12)$$

де $C_{\text{а}}$ – річний фонд амортизаційних відрахувань, грн.;

$C_{\text{тос}}$ – витрати на технічне й організаційне адміністрування та сервіс, грн.;

n – строк корисного використання основних засобів, становить один рік для розробленого ПЗ, враховуючи швидкість змін особливостей операційних систем.

Сума витрат на організаційне адміністрування та сервіс встановленого ПЗ визначається як 1-3% від вартості капітальних витрат і становить 180 грн.

Таким чином, річні експлуатаційні витрати складають 6180 грн.

3.3 Оцінка величини збитку

У комп'ютерах умовного підприємства, де буде встановлено розроблене ПЗ, постійно зберігається та обробляється інформація що має високу цінність. Величина збитку від несанкціонованого заволодіння нею третіми особами умовно становить 130 000 грн.

3.4 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження програми інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B * R - C \tag{3.13}$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн.;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Величина загального ефекту для умовного підприємства складатиме:

$$E = 50 * 0.2 - 6.180 = 3.82 \tag{3.13}$$

3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження програми інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на ТЗПІ, а отже:

$$ROSI = \frac{E}{K} = \frac{3.82}{1.6} = 2.38 \quad (3.14)$$

Для остаточної оцінки необхідно порівняти розрахункове значення ROSI з бажаним значенням показника ефективності $E_{\text{н}}$.

Проект системи інформаційної безпеки визнається доцільним за умови:

$$ROSI > E_{\text{н}} \quad (3.15)$$

В якості $E_{\text{н}}$ прийнято норму прибутковості від покладення коштів K на депозитний рахунок у банку:

$$E_{\text{н}} = (N_{\text{деп}} - N_{\text{інф}})/100 = (0.16 - 0.099)/100 = 0.00061 \quad (3.16)$$

де $N_{\text{деп}}$ – річна депозитна ставка, 16%;

$N_{\text{інф}}$– річний рівень інфляції за 2018 рік, 9.9%.

Оскільки $ROSI > 0.00061$, проект інформаційної безпеки є доцільним.

3.6 Висновок

В економічному розділі було розраховано витрати на розробку ПЗ, а також показник загального ефекту від впровадження системи інформаційної безпеки та коефіцієнт повернення інвестицій ROSI.

Значення показника загального ефекту становить 3.82, тобто у разі здійснення атаки на умовне підприємство, сума відвернених збитків становитиме 382 грн., що значно менше від загальної суми капітальних витрат.

Значення коефіцієнта ROSI становить 2.38, тобто кожна гривня капітальних інвестицій допоможе запобігти втраті двох гривень від можливого збитку внаслідок атаки, що набагато більше ніж прибуток від покладення суми капітальних витрат на депозитний рахунок.

Судячи з отриманих результатів, можна зробити висновок що запропонованого ПЗ є економічно доцільним.

ВИСНОВКИ

В даній дипломній роботі розглядається питання розробки спеціального програмного забезпечення для захисту ресурсів комп'ютера методами дактилоскопії. Здійснений детальний аналіз технічної літератури по питаннях ідентифікації та верифікації по відбитках пальців. Запропонована методика оцінки регулярності потоків ліній відбитку, яка дозволила отримати портрет регулярності елементів текстури (дискретний і безперервний), який ефективно може використовуватися як ознака при первинній верифікації. Здійснений детальний аналіз механізмів захисту даних. Запропонований метод захисту даних дозволив обмежити доступ до папки, скопіювати їх або видалити.

На підставі запропонованого підходу до оцінки складності бінарних зображень розроблені алгоритми:

– побудови портрета регулярності елементів текстури;

– оцінки інтегральної ознаки складності зображень;

– визначення місця розташування і орієнтації ліній на зображенні відносно базових точок.

Розроблений метод і алгоритм ідентифікації зображень відбитків, заснований на статистичній обробці виділених структурних ознак, і дозволяє значно скоротити час обробки цих зображень.

На підставі запропонованого підходу до захисту даних розроблені алгоритми:

– функція блокування папки;

– функція розблокування папки.

Проведене експериментальне дослідження показало високу ефективність роботи розроблених алгоритмів.

Оцінюючи проведену роботу по розробці програмного продукту можна відзначити, що методи і алгоритми, використовувані при побудові портрета відбитку, при виділенні інформативних зон, при виділенні ознак, при

ідентифікації відбитку, при блокуванні папки, а також розюлокуванні папки працюють ефективно і по багатьом параметрам не поступаються закордонним аналогам.

Результати аналізу роботи програми показали, що можливе введення додаткових методів порівняння, та механізмів захисту даних. Це дозволить збільшити достовірність результату ідентифікації, та більш надійніше захистити дані на комп'ютері.

У результаті економічного аналізу та обґрунтування з’ясовано, що новий прилад має переваги над аналогом за рахунок економії на експлуатаційних витратах та капітальних вкладень. Тому розробка даного програмного засобу буде доцільною.

У результаті проведення розрахунків термін окупності витрат складе майже 2 роки , тобто новий програмний засіб буде конкурентоспроможним і розробка даного програмного засобу є доцільною і економічно вигідною.

ПЕРЕЛІК ПОСИЛАНЬ

1. Lawrence O'Gorman, Veridicom Inc. "Fingerprint verification" 2000.

2. O. Nakamura, K. Goto, and T. Minami, "Fingerprint Classification by Directional Distribution Patterns," Systems, Computers, and Controls, Vol. 13, pp. 81-89, 1982.

3. L. O'Gorman and J. V. Nickerson, "An approach to fingerprint filter design", PatternRecognition, Vol. 22, No. 1, pp. 29-38, 1989.

4. E. Peli, "Adaptive Enhancement Based on a Visual Model," Optical Engineering, Vol. 26, No. 7, pp. 655-660, 1987.

5. E. C. Driscoll Jr., C. O. Martin, K. Ruby, J. J. Russell, and J. G. Watson, "Method and Apparatus for Verifying Identity Using Image Correlation, 1991.

6. L. Coetzee and E. C. Botha, "Fingerprint Recognition in Low Quality Images," PatternRecognition, Vol. 26, No. 10, pp. 1441-1460, 1993.

7. K. Karu and A. K. Jain, "Fingerprint Classification," Pattern Recognition, Vol. 29, No. 3, pp. 389-404, 1996.

8. M. Kawagoe and A. Tojo, "Fingerprint Pattern lassification," Pattern Recognition, Vol. 17, pp. 295-303, 1984.

9. M. A. Eshera and R. E. Sanders, "Fingerprint Matching System,"1997.

10. S. Ferris, R. L. Powers, and T. Lindh, "Hyperladder Fingerprint Matcher," 1997.

11. R. C. Gonzalez and Richard E. Woods, Digital Image Processing, Addison-Wesley, Massachusetts, 1992.

12. K. Asai, H. Izumisawa, H. Owada, S. Kinoshita, and S. Matsuno, "Method and Device for Matching Fingerprints with Precise Minutia Pairs Selected from Coarse Pairs,", 1987.

13. R. A. Marsh and George S. Petty, "Optical Fingerprint Correlator," ,1991.

14. A. Sibbald, "Method and Apparatus for Fingerprint Characterization and Recognition Using Auto-correlation Pattern," 1997.

15. M. K. Sparrow, “Fingerprint Recognition and Retrieval System,” 1988.

16. А.И. Гороховский, Данилюк Ю.С. Подход к оценке сложности изображений. Электронная техника.Сер. 10. Микроэлектронные устройства, 1984, вып.5(47).

17. А.И. Гороховский,Харьков А.М. Автоматическая идентификация по отпечатку пальца. В кн. «Приборостроение 2000», Калуга, стр. 238-243.

18. А.И. Гороховский, Кожемяко В.П., Шепетко А.Ф. Структурно-статистическая идентификация текстур. В кн.: Автоматизированные системы обработки изображений: Тез. докладовII Всесоюз.конф., 1986, Львов.

19. Чередниченко В. Б. Біометричні методи у системах захисту інформації / .

20.С. Бармен. Розробка правил інформаційної безпеки / Бармен С. [Пер. з англ.] – М.: Вид-во "Вільямс", 2002. — 208 с.

21. Лапонін О. Р. Основи мережевої безпеки: криптографічні алгоритми та протоколи взаємодії. – М.: Вид-во "Інтернет-університет інформаційних технологій - ІНТУІТ.ру", 2005. – 608 с.

22. Митні інформаційні технології : навч. посіб. / О. Ф. Волик, О.В. Кащеєва, І.В. Дорда та ін. ; за ред. П.В. Пашка ; передмова А.В. Толстоухова. — К.: Знання, 2011. — 391 с — (Митна справа в Україні).

23. В.П.Новосад, С.М.Ромашко. Методичні вказівки до модуля "Сучасні інформаційні технології в державному управлінні". Частина 7. Захист інформації. Перспективи розвитку інформаційних технологій - Львів: ЛРІДУ НАДУ, 2007. - 35с.

24. Мусієнко Д. Захист інформації в портативному ПК / Д. Мусієнко // Бизнес и безопасность, 2006.

25. Жицький О. С., Савельєва Т. В. Аналіз засобів захисту інформації в інформаційно-комунікаційних системах та мережах.

26. Гадецька З. М., Омельчук Д. Г., Литвин Р. В. Ідентифікація та аутентифікація – методи захисту від несанкціонованого доступу / З. М.

Гадецька, Д. Г. Омельчук, Р. В. Литвин // Восточно-европейский журнал передовых технологий. –2013. –Вип. 2(62). – С. 8-11.

27. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / Упоряд.: О.Ю. Гусєв, О.В. Герасіна, О.М. Алексєєв,О.В. Кручінін. – Дніпро: НГУ, 2018. – 50 с.