Для імітації виконання функцій елементів, що використовуються в лабораторних роботах, написана програма ініціалізації мікроконтролера, в якій реалізована підпрограма обслуговування кожної лабораторної роботи. Програма мікроконтролера написана на мові програмування asm51.

Технічні характеристики пристрою:

- стенд виконано на інтегральних мікросхемах серії КМОП – КР1564;
- тип процессора – мікроконтролер W78E365D сімейства x514
- засоби індикації – світлодіоди АЛ307 та індикатор АЛС324А;
- спосіб спряження з ЕОМ – USB-порт;
- допустимі способи живлення – мережа живлення 220 В або акумуляторна батарея GPT112 700mAh/6V;
- режим використання акумулятора – автоматичне включення при зникненні напруги живлення основного джерела та автоматична підзарядка при відновленні напруги живлення основного джерела
- споживаний струм – 262 мА.
- споживана потужність – 1310 мВт.
- габаритні розміри пристрою: 240 мм х 150 мм х 60 мм.

Стенд повинен застосовуватись учнями для надбання практичних навиків в збиранні схем різних пристроїв та апробації теоретичних знань з дисципліни. Для цього було розроблено 8 базових лабораторних робіт. Ведуться роботи по розширенню спектру реалізовуваних на стенді схем.

Висновки. Запропонований прилад реалізовано у формі навчального стенду як сучасний програмно-апаратний комплекс, призначений для використання в ході проведення лабораторних робіт по всіх основних розділах дисципліни “Комп’ютерна схемотехніка”. Стенд розрахований на використання в навчальному процесі при підготовці фахівців за напрямом “Комп’ютерна інженерія”, а також на тих, хто бажає самостійно розібратися в азах схемотехніки. Лабораторний стенд може бути використаний для навчання студентів різних спеціальностей середніх спеціальних і вищих навчальних закладів, а також учнів професійно-технічних училищ, що вивчають дисципліни «Схемотехніка», «Цифрова електроніка» та інші.

Література

1. Учебное оборудование и пособия [Електронний ресурс]. Режим доступу до ресурса: http://www.e-import.ru/.

2. Новый стиль [Електронний ресурс]. Режим доступу до ресурса: http://newstyle-y.ru/high-school/.

3. Центр комплексного снабжения учебных заведений Ректор [Електронний ресурс]. Режим доступу до ресурса: http://www.rektor.ru.

4. Учебное оборудование KandH Products [Електронний ресурс]. Режим доступу до ресурса: http://www.kandh.com.tw.

Надійшла 25.4.2011 р.

УДК 004

В.М. ДЖУЛІЙ, Я.А. РОГОЗА, В.М. ЧЕШУН
Хмельницький національний університет

МЕТОДИКА ІДЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ ЦИФРОВИХ ГРАФІЧНИХ ЗОБРАЖЕНЬ У ПОШУКОВИХ СИСТЕМАХ НА ОСНОВІ ХЕШ-ФУНКЦІЙ

Розглянуті можливі способи ідентифікації цифрових зображень. Запропонована методика ідентифікації та авторизації цифрових зображень без додавання надлишкової інформації до об’єкту ідентифікації.

Identification methods for digital images are reviewed. The technique and algorithm for digital images identification and authorization without adding any excessive data to object has been proposed.

Ключові слова: ідентифікація, зображення, пошукова система.

Вступ

З появою поняття цифрового зображення з’явилося чимало програмного забезпечення, яке дозволяє редагувати зображення та змінювати його параметри. Постало питання про можливість ідентифікації та авторизації цифрових зображень по певним ознакам. Як один з варіантів була запропонований і введений стандарт EXIF (Exchangeable Image File Format) [1, 2]. Його суть полягає у тому, що камера при створенні зображення додає до нього метадані, у яких може міститися різна інформація, яка, в свою чергу, може виступати як ідентифікатор зображення.

Проте, стандарт EXIF не забезпечив всіх аспектів ідентифікації зображення. Поширеною проблемою, наприклад, залишилася конвертація зображень у інші формати.

Оскільки багато цифрових форматів включають у себе зменшення обсягу даних самого зображення, це несе за собою зміну самого зображення [3]. Наслідком постають проблеми ідентифікації самого

зображення та визначення наявності його модифікацій.

При проведенні аналізу результатів порівняння потрібно робити висновки, чи дійсно є значні зміни у зображенні, порівняно з оригіналом, чи самі зміни є просто результатом перетворення зображення у формат з частковою втратою даних.

В будь-якому разі, кінцева мета аналізу зображень – виявлення наявності та критичнисті змін і визначення автора графічного об'єкта даних.

На даний момент існують два основні криптографічні примітиви для забезпечення достовірності:

- коди ідентифікації повідомлення (Message authentication code MAC);
- цифрові системи підпису (Digital signage DS).

У згаданих системах для ідентифікації об'єкту **m** використовується алгоритм генерації, що дозволяє отримати ознаки ідентифікації **t**. У результаті отримується комбінація ознаки та об'єкту **m||t**. Ця комбінація дає змогу використовувати ідентифікатор для подальшого порівняння, яке повертає 0 або 1 залежно від того, рівні ідентифікатори порівняння або ні [4, 5].

Система ідентифікації повідомлення включає в себе два однакових ключі: ключ генерації і верифікації. У випадку, якщо ці ключі не однакові – один легко може бути визначений з іншого. Дана система називається симетричною ключовою системою.

Недоліком симетричних ключових систем є те, що вони не забезпечують «неможливості відмови від авторства»: відправник може відхилювати повідомлення, яке він послав.

У системах цифрового підпису код ідентифікації також називається підписом і використовується не тільки для ідентифікації, а і для забезпечення ознаки авторства з подальшою неможливістю відмови від нього.

Недоліком систем цифрового підпису таких систем є те, що вони потребують високої продуктивності апаратних засобів для проведення великої кількості обчислень.

Постановка задачі

Розвиток глобальної мережі Інтернет та значене збільшення пропускної здатності мережевих каналів за останні роки дали можливість вільного доступу до зображень та засобів їх поширення. На сьогоднішній день цифрові зображення стало одним з найпопулярніших засобів передачі інформації, що використовується надзвичайно поширено.

За таких умов виникає потреба створення надзвичайно великих баз для зберігання зображень, що породжує проблему пошуку та індексації в таких базах.

Керування базами даних потребує багато апаратних ресурсів та маніпулювання великими об'ємами даних. Для визначення наявності зображень у базі даних потрібно провести велику кількість обчислень, яка навіть при наявності потужних систем, займає багато часу.

Пошук за метаданими не є ефективним, оскільки графічні редактори мають можливість вносити туди зміни. Також візуально однакові зображення можуть мати різні формати, що ускладнює побітове порівняння для комп'ютерних систем.

Розвиток нейронних мереж дозволив використовувати спеціальні матриці для порівняння зображень. Використання таких матриць дає досить достовірні результати, але не вирішує проблему низької швидкодії процесу ідентифікації.

Стандарти хешування MD5 і SHA-1 не підходять для порівняння зображень, оскільки, як було згадано вище, побітовий процес порівняння унеможливлює наявність відмінностей форматів повідомлень [3, 6].

Цифрові зображення зазвичай підлягають різним маніпулюванням, таким як, наприклад, компресії, збільшенню, масштабуванню, впорядковуванню тощо. Функція виділення характерних ознак (хешування) повинна ідентифікувати зміни у візуальній області і створювати результат, організований лише на візуальному представленні зображення [8].

Іншими словами, значення хеш, одержані за допомогою функції хешування до візуально подібних зображень, повинні залишатися однаковими. Для візуально різних зображень, функція хешування повинна генерувати різні значення хешування.

Метою проведених досліджень є визначення методики виділення характерних ознак графічних зображень на онові функції хешування, що задовольняє зазначеним вимогам.

Результати дослідження

У основі пропонованої методики лежить стратегія випадкової обробки сигналу для необоротної компресії зображень у випадкові бінарні послідовності, що є ефективним проти зміни зображення, яке з'являється внаслідок компресії, геометричного спотворення та інших атак. Такий підхід вносить в зображення прямий аналог Повідомлення Достовірності Кодів (MAC) з криптографії, в якій головна мета – надати значення хешування набору чітких незалежних парних вхідних значень. Як наслідок, зменшується вірогідність співпадання значень хешу, навіть коли вхідні значення генеруються не випадково.

Рішення, засновані на кодах, що корегують помилки, служать для зменшення довжини значення хешування і одночасно підтримують вірогідність колізій на низькому рівні [5, 1]. Статистичні властивості значень хеш для різних зображень подібні до таких, що використовуються в криптографії для мінімізації зациклень та виникнення помилок.

Основною перевагою методики є те, що вона забезпечує фактичну модифікацію пікселів зображення.

Методика базується на положеннях:

- процес хешування отримує два вхідних значення, зображення **I** і секретний ключ **K;**
- отримані значення використовуються для генерування значення хеш **h = H (I; K);**
- ознака **K** функціонує як початкове значення для генератора псевдовипадкових чисел, що використовується на різних стадіях алгоритму хешування.

При наявності аналогічних зображень і використанні різних ключів отримуване значення хеш я буде статистично незалежним і тому повністю іншим. Значення ключа є секретним і значення хеш запропонованого зображення не може бути обчисленим або перевіреним.

Для реалізації методики використаємо використовувати криптографічно сильний псевдо-випадковий генератор **G (s)** з випадковим секретним ключем (рандомізований алгоритм «підкидання монети» в необхідному напрямку).

Розглянемо основні етапи алгоритму реалізації пропонованої методики.

Алгоритм А1.

А1.1. На початку обчислюється розпад невеликої хвилі зображення і кожна підгрупа випадково групується в маленькі прямокутники.

А1.2. Статистика кожного прямокутника (середні величини або змінні, залежно від підгрупи) підраховуються та квантуються за допомогою методу рандомізованого округлення (тобто, вірогідне квантування), що є критичним і гарантує результат значення хешування у формі бінарної послідовності, яка є випадковою. Ці квантовані статистики можуть бути представлені як елементарні ознаки зображення, багато з яких є відносно ефективними проти атак.

А1.3. Квантована статистика підлягає стадії декодування з відповідно обраним кодом, що виправляє помилки, для отримання фінального значення хеш. Даний етап допомагає впевнитись в тому, що значення хеш-суми залишається таким же, якщо вхід дешифратора залишається в межах відповідно визначеного регіону декодування, який задається заздалегідь.

А1.4. Завершення алгоритму.

Алгоритм реалізації пропонованої методики сможна описати наступним чином.

Спочатку відбувається регенерація групування та обчислення статистики.

При цьому проходить процес генерації випадкового групування кожної підгрупи зображень, як ілюструє рис. 1.

Рис. 1. Трьохрівневе мікрохвильове розкладення

Зазначений процес може бути представлений як рандомізований аналог методів для обчислення інтегралів через наближення.

Кількість зразків достатньо велика, щоб гарантувати достатність інформації про початкове зображення, представляючи навмисно незворотність та непередбачуваність.

Середні величини коефіцієнтів в прямокутниках підраховуються в великій підгрупі, а змінні підраховуються в інших підгрупах. Результатом цього є довжина – **l** зображення статистичний вектор **m = σ (I; K)**, де **I** – це зображення, **σ** – це особливість (статистика), **K –** це ключ, який визначає групування

Далі виконується випадкове округлення (ця операція використовується у теоретичній комп'ютерній науці в дизайні алгоритмів). Статистичний вектор **M** вираховується з попереднього етапу і квантується за допомогою рандомізованого кванту **Q**. Це надає наближеній статистиці більшу ефективність проти атак.

Реалізуємо скорочення для мінімізації вірогідності співпадання будь-яких вхідних значень, кожен вихідний біт функції хешування повинен бути рандомізованим, і значення хешування повинне бути попарно незалежним.

Рахується, що вхідні значення були згенеровані невідомими джерелами і рандомізоване округлення – це критичне джерело випадковості (або ентропія) у вихідному значенні функції хешування.

Функція **Q** використовує псевдо-випадкове значення **K** з попереднього етапу для отримання імовірного розподілення, що використовується для квантування. Поточний етап продукує вектор з

трибітовими вхідними даними $x = Q(m, K) \in \{0,1,...,7\}^l$.

На наступному етапі вектор статистики $\boldsymbol{x}$ розшифровується дешифратором Ріда-Мюллера, що виправляє помилки, для отримання **n**-бінарного значення хешу $h = D(x) \in \{0,1\}^n$. Показник, що використовується для декодування є експоненціальною псевдо-нормою, що надає додаткової ефективності схемі декодування.

Стадія декодування зменшує кількість невеликих порушенн (які залишаються в сфері декодування) в квантизованій статистиці візуально подібних зображень, даючи таке ж значення хешу на різних зображеннях, що призводить до статистично некорельованого значення контрольної суми, а також локалізує випадковість, що виникає через рандомізоване округленням, в меншу кількість біт для досягнення випадкових результатів.

Остання стадія декодування лінійного коду з випадковими параметрами відображає проміжне значення хешування.

Всі етапи реалізації пропонованої методики можуть модифікуватися шляхом введення необмеженої кількості проміжних значень. Але у цьому питанні слід враховувати проблему швидкодії, яка була розглянута вище.

Також зазначені етапи можуть повторюватися з різними випадковими ключами і різними областями для надання багатьох незалежних випадкових послідовностей, а також може перевірятися узгодженість більшості значень хешування, що істотно збільшує ефективність генерації контрольних сум.

Висновки

Розглянута методика виявлення характерних ознак зображення трансформує зображення у згенеровані певним чином рядки біт, що дає змогу порівнювати два зображення, перевіряючи згенеровані рядки для точної рівності. Це зменшує кількість проблем у випадку порівняння частково змінених зображень в наслідок часткової втрати даних тощо.

Запропонована методика та алгоритм її реалізації дає змогу забезпечити стійкість у питанні відмови від авторства при загальному редагуванні зображення або редагуванні його частин. В основі алгоритму лежить використання ідей криптографії, які використовуються для корекції помилок сигналів тощо.

Методика має переваги порівняно з алгоритмами, які є поширеними на даний момент. Використання водяних знаків має ряд проблем: до зображення постійно потрібно додавати додаткові ознаки і сам алгоритм не є стійким до загальних змін. Використання нейронних мереж для ідентифікації зображень є досить ресурсомістким процесом і потребує високої продуктивності апаратних засобів. Порівняння ж зображень з використанням хеш-суми може модифікуватися у процесі використання для досягнення високої якості захисту і не потребує ніяких модифікацій об’єкту ідентифікації.

Література

1. Венбо Мао. Современная криптография – теория и практика / Венбо Мао. – М.: Вильямс, 2005. – 786 с.

2. Брассар Ж. Современная криптология / Брассар Ж.; пер. с англ. – М: Полимед, 1999. – 176 с.

3. Панасенко С. Алгоритмы шифрования / Панасенко С. – БХВ-Петербург, 2009. – 564 с.

4. Об определении подлинности документов // [Абламейко С.В., Гречихин Л.И., Шумский И.П. и др.] – Мн.: Ин-т техн. кибернетики НАНБ, 2001. – 256 с.

5. Гречихин Л.И. Многоуровневая автоматическая система принятия решения на основе нечетких исходных данных / Гречихин Л.И., Шумский И.П // Искусственный интеллект. – 2004. – № .3. – С.12-15.

6. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Блейхут Р. – М.: Мир, 1986. – 576 с.

7. Дружинин М. А. Применение электронной цифровой подписи для идентификации и шифрования /Дружинин М. А [Електронний ресурс]. Режим доступу до ресурса: http://www.astra-st.ru/en/node/478.

8. Джулій В.М. Алгоритм хешування графічних зображень / В.М.Джулій, К.В. Іванов // Вимірювальна та обчислювальна техніка в технологічних процесах ”. – 2007. – № 1. – С.74-75.

Надійшла 23.4.2011 р.