УДК 004.056.5:655.25

АНАЛІЗ СУЧАСНИХ МЕТОДІВ І ЗАСОБІВ ЗАХИСТУ ЕТИКЕТКОВО-ПАКУВАЛЬНОЇ ПРОДУКЦІЇ НА ОСНОВІ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ

Ю. В. Грик, Н. Ю. Гриньох, З. М. Сельменська

Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Досліджено тенденції розвитку сучасних методів ідентифікації/аутентифікації в технології захисту поліграфічної продукції, зокрема етикетково-пакувальної, від підробок. На сьогодні українські і закордонні виробники упаковки та етикетки розробляють, вдосконалюють і пропонують світовому ринку нові технічні рішення із захисту бренду, продукту і споживачів, впроваджуючи в упаковку новітні ІТ-розробки.

Проаналізовано наявні методи комп'ютерних технологій, які набувають актуальності під час захисту інформації в інформаційно-комунікаційних системах, так і при захисті поліграфічної продукції. Визначено, що «ідентифікація», «аутентифікація» і «авторизація» — це три взаємопов'язані між собою поняття, котрі становлять основу системи безпеки. Протокол аутентифікації — це так званий тип протоколу комп'ютерного зв'язку чи криптографічного протоколу, котрий був спеціально розроблений для передачі даних аутентифікації між двома об'єктами. Метою аутентифікації є підтвердження особистості, проте набір методів аутентифікації дуже широкий та може варіюватися по-різному. Розглянуто поширені методи аутентифікації: аутентифікація за допомогою пароля; аутентифікація за допомогою смарт-карти; біометрична аутентифікація; аутентифікація за допомогою цифрового сертифіката. Кожен з наведених методів аутентифікації має своє застосування проте і свої недоліки. У досліджуваній технології використовується біометрична аутентифікація, яка ґрунтується на виміряних відбитках пальців — в нашому випадку це ЕпіКод. Одною з основних цілей технології була розробка економічно ефективних та захищених від підробки процедур маркування та аутентифікації як для продуктів, так і для процесів та створення комплексних концепцій шляхом поєднання окремих технологічних, організаційних та юридичних варіантів.

Ключові слова: *підробка, фальсифікація, етикетка, упаковка, ідентифікація, аутентифікація, матричні коди.*

Постановка проблеми. Кількість українських інновацій у сфері упаковки і етикетки без перебільшення йде на десятки і сотні. Завдяки їм світові виробники використовують технологічні рішення, що зберігають продукт не тільки у фізичному сенсі, а й у ширшому — захищають від підробок.

На сьогодні етикетково-пакувальна галузь створює один з головних бар'єрів, який досі рятує споживчий ринок від потоку контрафактної продукції. Роки активної діяльності української пакувальної індустрії дали чітке усвідомлення, що найважливіша місія упаковки — збереження якості продукції. Екологічна і харчова безпека, економічна і маркетингова ефективність, захист від підробок — ось завдання, які світовий ринки диктують виробникам етикетково-пакувальної галузі. Українські виробники упаковки розробляють і пропонують світовому ринку нові технічні рішення із захисту бренду і споживачів, впроваджуючи в упаковку новітні ІТ-розробки [1, 2].

Для того щоб боротися з підробками виробники почали впроваджувати різні елементи захисту своєї продукції від підробки. Оскільки впровадити якісні елементи захисту в структуру самого товару неможливо, було обрано виготовлення оригінальної упаковки товару з елементами, які важко відтворити в незначних обсягах та в домашніх умовах без застосування спеціальних технологій друку.

Історичний аспект проблем фальсифікації та захисту від зловживань на різних етапах виготовлення продукції показує, що прогрес технологій захисту поліграфічної продукції від фальсифікації відбувається невідривно від прогресу в індустрії фальсифікації. Ці два аспекти однієї проблеми не можна розглядати і аналізувати окремо.

Аналіз останніх досліджень та публікацій. Фальсифікація — це створення зразка продукції, максимально наближеного до оригіналу, для підміни останнього з метою отримання прибутку [1]. Розвиток копіювальної техніки дав нові можливості для створення підроблених примірників поліграфічної продукції. У сучасному світі покращуються й можливості фальсифікаторів: кожен новий спосіб друку або спрощує створення підробки, або примушує фальсифікаторів обходити цей спосіб за допомогою інших, у такий спосіб удосконалюючи процес друку. Проблема фальсифікації полягає у фінансовому і моральному збитку виробника і споживача, особливо важливою є шкода, що наноситься здоров'ю людини. Говорячи про етикетково-пакувальну продукцію, потрібно зазначити, що поліграфічна підробка є вторинною щодо підробки самого продукту, проте захисну функцію має саме вона. Ринок етикетково-пакувальної продукції дуже привабливий для фальсифікаторів. Це зумовлено великими і незмінно зростаючими обсягами виробництва і прибутку [2, 4].

Сучасні засоби захисту поліграфічних продуктів від фальсифікації є різноманітнішими порівняно з арсеналом фальсифікаторів. Будь-яка продукція за правильного технологічного підходу може бути захищена таким чином, щоб не залишилося можливості для підробки. Підробити можна будь-який найдосконаліший продукт. Проте вартість підробки, що перевищує економічний ефект від її застосування, апріорі робить фальсифікацію нерентабельною. Саме в тому, щоб забезпечити умови недоцільності фальсифікації, і полягає завдання фахівців із захисних технологій [3]. Отже, перед тим, як прийняти рішення про доцільність і необхідність захисту того чи іншого продукту від різних видів зловживань,

необхідно відповісти на низку питань. Тільки після аналізу цих питань щодо конкретного продукту можна компетентно розробити комплекс організаційних, інформаційних і технологічних заходів щодо захисту конкретного продукту від всіх видів можливих зловживань [5, 6, 7, 8].

Зараз біометричні технології активно використовуються в багатьох царинах, що потребують захисту доступу до конфіденційної інформації, матеріальних цінностей, при захисті етикетки та упаковки тощо. Оскільки біометричні дані є таємними й часто стають об'єктом атак, то вони підлягають захисту, а в середовищах обміну такими даними має використовуватись криптографічний захист [9, 12].

Мета статті — дослідження методів, особливостей використання сучасних методів і засобів проведення ідентифікації/аутентифікації друкованих матричних кодів з метою ідентифікації товару (упаковки). Для досягнення поставленої мети потрібно вирішити завдання: дослідити тенденції розвитку та напрями впровадження сучасних технологій ідентифікації/аутентифікації [3].

Виклад основного матеріалу дослідження. Методи захисту від фальсифікації залежно від рівня складності і доступності ідентифікації наявності захистів у продукті поділяють на три види:

1. Оголошені методи захисту.
2. Сертифіковані методи захисту.
3. Приховані методи захисту.

Оголошені методи захисту — це така група методів захисту, наявність і опис яких присутні безпосередньо на поліграфічному продукті (у вигляді сигнальних ліній) або повсюдно поширені в інформаційних посібниках. Зрозуміло, ефективніші сигнальні лінії на продукті, оскільки в цьому випадку інформація про застосування захисту невідокремлена від продукту. Отже, ця форма застосовується для умов неконтрольованого оточення. Дані захисту мають бути візуально контрольовані без застосування спеціальної апаратної бази. Ця група методів захисту насамперед розрахована на непідготовленого користувача. На жаль, застосування відкритого захисту методом сигнальних ліній у вітчизняній практиці мало поширене. Сертифіковані засоби захисту — це комплекс технічних заходів від фальсифікації, застосування яких відомо лише учасникам контрольованого оточення обігу продукції. Наявність і опис таких захисних заходів, так само як і метод їх ідентифікації, описані в сертифікаті захищеності продукту (сертифікат якості), переданому виробником організатору звернення (замовнику) разом з накладом продукції. Отже, ця форма комплексних заходів доповнює групу оголошених захистів, формуючи другий рівень контролю достовірності у процесі обігу. Приховані методи захисту застосовуються виробником захищеного поліграфічного продукту без опису їх замовнику або організатору обігу продукту. Передбачається, що ці технологічні заходи можуть бути ідентифіковані тільки в умовах професійного оточення (тобто в експертних лабораторіях і обладнаних сертифікаційних центрах). Інформування про їхню наявність замовника позбавлене сенсу через технічну неможливість останніми ідентифікувати продукцію. Необхідно зазначити, що найпоширеніша помилка при виборі методів та форм захисту для конкретного

поліграфічного виробу — це вибір будь-якої однієї форми. Успіх полягає саме в оптимальному використанні комбінації всіх трьох методів. Тільки тоді виріб може вважатися повноцінно захищеним від зловживань [8, 9].

Концепція захисту продукту базується на ідентифікації та аутентифікації. Ідентифікація — це процедура розпізнання користувача в системі за допомогою заздалегідь визначеного імені чи іншої інформації про нього. Така процедура є початковою у процесі надання доступу до системи та після неї здійснюється аутентифікація та авторизація. Аутентифікація — це процедура перевірки належності ідентифікатора об'єкта, встановлення чи підтвердження дійсності, а також перевірка чи є об'єкт або суб'єкт, що перевіряється, насправді тим, за кого він себе видає. Проаналізувавши друкування матричних кодів, з'ясовано, що вони мають свої індивідуальні неповторювані характеристики. Якщо код наноситься на вторинну упаковку, його вміст використовується для ідентифікації товару. Його унікальний відбиток, що отримується в результаті фізичної взаємодії між середовищем і підкладкою у процесі друку, може бути використаний для ідентифікації оригінальності продукту. Отже, основною задачею систем ідентифікації і аутентифікації є визначення та верифікація необхідного набору повноважень суб'єкта при доступі до інформаційної системи. Водночас ідентифікація дає змогу суб'єкту (користувачу чи процесу, який діє від імені користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я). Поняття аутентифікації «ідентифікація», «аутентифікація» і «авторизація» — це три взаємопов'язані між собою поняття, котрі становлять основу системи безпеки. Ідентифікація — це передача ідентичності ІС. Перед аутентифікацією заявник зазвичай надає ІС посвідчення (наприклад, логін або адресу електронної пошти), а монітор стверджує посвідчення шляхом аутентифікації (наприклад, за допомогою пароля). Користувачі ідентифікуються з використанням різних механізмів аутентифікації. У системі безпеки процес аутентифікації перевіряє інформацію, надану користувачем, за допомогою бази даних [10, 11]. Нарешті, авторизація це надання користувачеві привілеїв.

Протокол аутентифікації — це так званий тип протоколу комп'ютерного зв'язку чи криптографічного протоколу, котрий був спеціально розроблений для передачі даних аутентифікації між двома об'єктами [4].

Метою аутентифікації є підтвердження особистості, проте набір методів аутентифікації дуже широкий та може варіюватися по-різному. Розглянемо декілька поширених методів аутентифікації: аутентифікація за допомогою пароля; аутентифікація за допомогою смарт-карти; біометрична аутентифікація; аутентифікація за допомогою цифрового сертифіката. Кожен з наведених методів аутентифікації має своє застосування, проте і свої недоліки. Наприклад, такени чи смарт-карти можуть бути викрадені, системи розпізнавання можуть бути зламані. Отже, можна визначити, що метою аутентифікації є перевірка ідентичності об'єкта із заданим рівнем довіри. За умови, якщо метод перевірки аутентичності не вважається цілком надійним, надана перевірка також не може вважатися надійною.

Ідентифікація, аутентифікація і авторизація — це три взаємопов'язані поняття, які становлять основу системи безпеки. Аутентифікація — це процес, під час якого відбувається підтвердження особи користувача. Системи аутентифікації дають відповіді на такі питання, як «хто є користувачем?» і «чи дійсно користувач є тим, за кого він себе видає?». Класифікація аутентифікації відбувається з точки зору методу (пароль, смарт-карта, сертифікат, біометрія), а також з погляду кількості використаних методів (однофакторна, двофакторна, трифакторна, чотирифакторна) та з точки зору рівня безпеки («сильна», безперервна, електронна). Атаки на процес аутентифікації поділяються на три основних типи: атаки на користувацький інтерфейс, атаки на базу даних шаблону, атаки на системні модулі та взаємозв'язки між модулями. Найпоширеніші атаки: метод грубої сили, за словником, сніффінг, спуфінг. Жоден з цих методів не є цілком безпечним, тому зараз найбільш актуальним є метод багатофакторної аутентифікації [12].

В аналізованій технології використовується біометрична аутентифікація. Основні біометричні характеристики людини, за допомогою яких найчастіше здійснюється її ідентифікація. Ідеальна характеристика має легко збиратися, бути універсальною, унікальною і постійною [12, 13, 14]. Універсальність — це змога представлення людини однією характеристикою. Унікальність означає, що не має бути двох людей з абсолютно ідентичними характеристиками. Зазвичай при класифікації біометричних технологій виділяють дві групи систем за типом біометричних параметрів. Перша група використовує статичні параметри: відбитки пальців, геометрію руки, райдужна оболонка ока тощо. Друга група — динамічні параметри: відтворення підпису або рукописного ключового слова, тембр голосу тощо. У всіх біометричних технологіях можна виділити однакову базову модель. Спочатку створюється первинний реєстраційний шаблон користувача. Шаблон створюється збиранням декількох зразків за допомогою будь-якого біометричного сенсора. Потім із зібраних зразків добуваються характерні для них ознаки, і отримані результати з'єднуються згідно з певним алгоритмом в шаблон. Первинний шаблон програма зберігає як контрольний і еталонний шаблон. Отже, при аутентифікації користувача з сенсора отримується зразок, обробляється та зіставляється з раніше зареєстрованим контрольним шаблоном. Цю форму біометричної аутентифікації називають верифікацією, тому що проводиться перевірка того, чи є користувач тим, за кого видає себе. Біометричні технології застосовують й іншу форму аутентифікації, яку називають ідентифікацією. Під час проведеня процесу ідентифікації користувачу не потрібно вказувати свою особистість. У цьому процесі оброблені зразки користувача порівнюються із базою контрольних шаблонів і ухвалюється рішення, який з них має найбільший ступінь схожості. Біометрична ідентифікація — процес порівняння поданих біометричних даних з усіма шаблонами в базі даних для визначення відповідності та в разі, якщо відповідність визначено, ідентифікації відповідної особи. Можлива архітектурна реалізації вищенаведеної базової моделі зображена на рис. 1 [12].

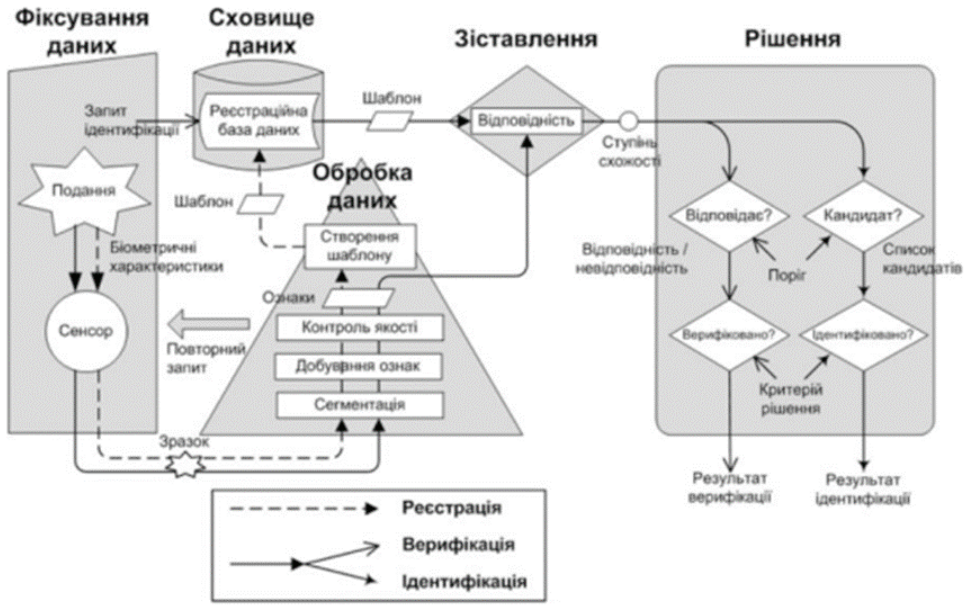


Рис. 1. Концептуальна схема узагальненої біометричної системи

Система складається з таких підсистем: фіксування, обробки і зберігання даних, зіставлення й ухвалення рішення. Вищенаведена схема показує процеси реєстрації, верифікації й ідентифікації. Проте елементи, надані в цій концептуальній моделі, можуть відрізнятися, тобто бути відсутніми чи не відповідати безпосередньо фізичним компонентам у реальній біометричній системі. Підсистема фіксації даних збирає зображення або сигнали біометричних характеристик суб'єкта, що були представлені біометричному сенсору, та видає це зображення або сигнал у вигляді біометричного зразка. Зразки, ознаки та шаблони можна передавати з використанням стандартних форматів обміну біометричними даними. Біометричний зразок можна ущільнити та/або зашифрувати перед передачею та розгорнути та/або дешифрувати до використання. Також зразок може бути модифікованих у процесі передавання через сторонній шум у каналах передачі або через втрати у процесі ущільнення та розширення. Можна визначити кілька рівнів обробки біометричних даних (рис. 2):

Рис. 2. Послідовність обробки біометричних даних

1) здобуті дані — необроблені дані, отримані з сенсора;

2) проміжні дані — оброблені дані, але у формі непридатній для зіставлення, — на такі дані посилаються, як на дані зображень або поведінки;

3) оброблені дані — дані у формі, придатній для зіставлення — дані ознак [12].

У випадку реєстрації підсистема обробки сигналів створює шаблон із отриманих біометричних ознак. Підсистема зберігання даних містить реєстраційну базу для зберігання шаблонів. Кожний шаблон містить якусь інформацію про суб'єкт реєстрації. Шаблони можуть зберігатися в пристрої біометричної фіксації, на переносному носії або в централізованій базі даних. Підсистема зіставлення даних порівнює біометричні дані із шаблонами та передає інформацію про ступінь схожості до підсистеми ухвалення рішень. Ступінь схожості визначає ступінь відповідності ознак шаблонам, з якими вони порівнювалися. При проведенні верифікації один визначений запит суб'єкта реєстрації ініціює один розрахунок ступеня схожості. У випадку ідентифікації декілька або всі шаблони можуть бути порівняні з ознаками, вихідний ступінь схожості буде отриманий для кожного порівняння. Підсистема ухвалення рішення використовує ступені схожості, створені однією або більше спробами, для ухвалення вихідного рішення на запит верифікації або ідентифікації. При верифікації порівняння ознак та шаблону вважається успішним за умови, якщо ступінь схожості вищий, ніж встановлене граничне значення. Підтвердження реєстрації суб'єкта ухвалюється згідно з правилами прийняття рішень, котрі можуть вимагати або допускати декілька спроб проходження верифікації. При ідентифікації зареєстрований шаблон є потенційним кандидатом для суб'єкта, коли ступінь схожості більший, ніж встановлене граничне значення. Підсистема керування (не зображена на схемі) керує правилами, реалізацією і використанням біометричної системи відповідно до узаконених, юрисдикційних і соціальних обмежень та вимог [13, 14].

Проаналізувавши способи захисту друкованої продукції, з метою захисту цієї продукції від підробок використаємо матричний код. Отже, для реалізації недорогого ефективного захисту маркування упаковок і етикеток був проаналізований матричний код. Основні технології ідентифікації та аутентифікації продукції з використанням матричного коду наведено на рис. 3.

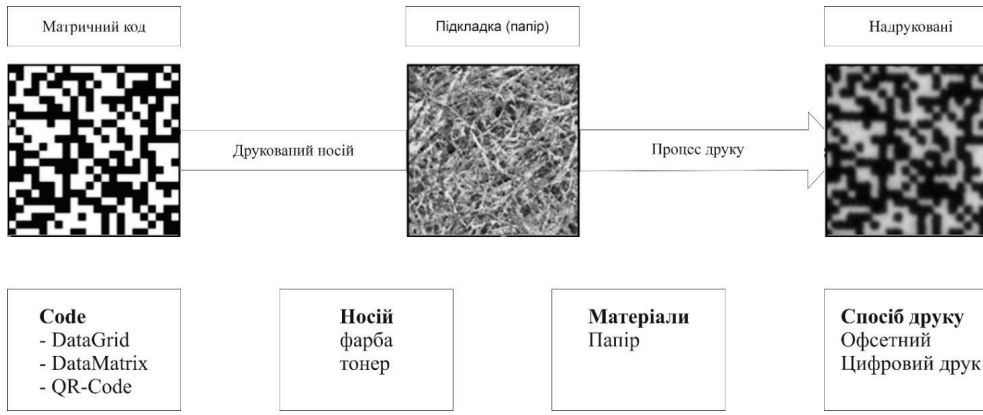


Рис. 3. Основні технології ідентифікації та аутентифікації продукції

У роботі проведено комплексний аналіз теоретичних та експериментальних досліджень дослідницького проєкту O-PUR [15]. Метою проєкту було промислове впровадження представленої технології, що містить реалізацію масштабованої концепції безпеки, досягнення найнижчих витрат на виробництво з використанням звичайних матеріалів. У проаналізованому проєкті O-PUR було успішно продемонстровано промислове виробництво захисних засобів з використанням офсетних пресів, що подаються листом і котушкою, цифрових принтерів, а також методів прямого маркування. Концепція захисту показала себе ефективно на коробках та етикетках.

На сьогодні поняття охорони поділяється на виробництво та експертизу захисного знака, як це наведено на рис. 4. Матричний код DataGrid містить зашифровані дані про продукт, а вбудована копія виявляє візерунок NanoGrid, який розглядається як штучний відбиток і використовується для аутентифікації (виявлення копій) без доступу до бази даних. Після друку коду на упаковці або етикетці унікальний відбиток EpiCode виникає в результаті взаємодії між папером і фарбою або тонером. EpiCode і ClusterCode можуть бути використані для аутентифікації в ланцюжку поставок тільки в тому випадку, якщо вони захоплені і збережені в базі даних під час виробничого процесу.

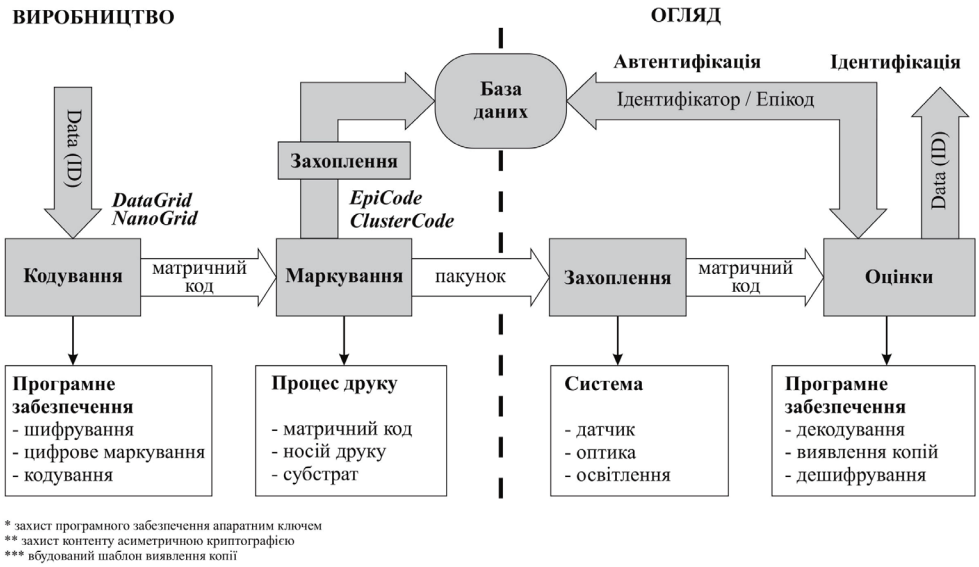
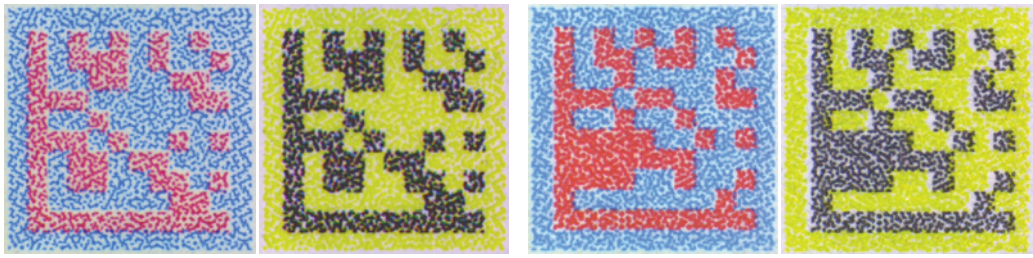


Рис. 4. Загальна концепція безпеки захисту продукції
на основі ідентифікації та аутентифікації

Технологію вперше розробили в університеті прикладних наук Hochschule Mannheim. Однією з основних цілей була розробка економічно ефективних та захищених від підробки процедур маркування та аутентифікації як для продуктів, так і для процесів та створення комплексних концепцій шляхом поєднання окремих технологічних, організаційних та юридичних варіантів.

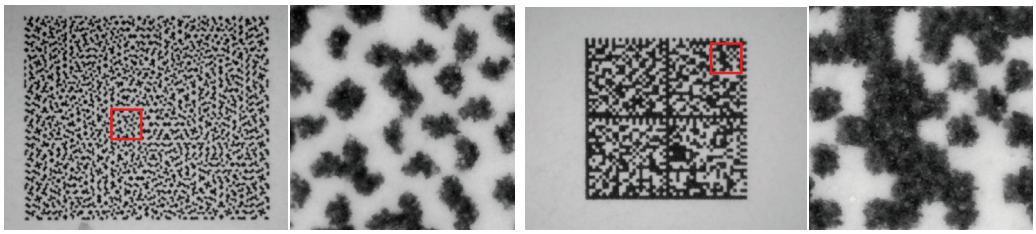
Концепція аутентифікації у цьому випадку базується на виміряних відбитках пальців — в нашому випадку це — EpiCodes витягнуто з друкованих DataGrids. Загалом EpiCodes розраховуються за сигналом помилки еквалайзера зворотного зв'язку рішень (DFE), описаного в публікації [15], і порівнюються з еталонними значеннями з бази даних. Результати порівняння обробляються з використанням методології біометричної оцінки [16]. Суть методу полягає в тому, що для перевірки якості аутентифікації техніки друку, яка використовується, друкується невелика партія одного цифрового тестового листа. Потім проводиться еталонне сканування (баз даних) і сканування аутентифікації (зонд), зазвичай сканується різними пристроями, які використовуються як для виробництва, так і для експертизи.



A *B*

Рис. 5. DataGrid (A, 4,1×3,8 мм, корисне навантаження до 180 байт) і DataMatrix (B, 3,1×3,1 мм, корисне навантаження 174 байт) з аналогічною щільністю даних, надрукованими звичайними фарбами і тонером з однаковою роздільною здатністю друку

Концепція аутентифікації також реалізована для стандартних кодів, наприклад, DataMatrix або QR-код, а також отримані коди використовуються так само для оцінки ефективності визнання.



DataGrid *DataMatrix*

Рис. 6. DataGrid з реалізованим кодом DataMatrix в колірному шарі, надрукованому на листових подачах Roland

Проаналізувавши вплив нанесеної друкарської фарби та різних матричних кодів на розпізнавання за формою, тестові відбитки показані на рис. 6.

Використання багатоколірних змішаних кодів додаткових індивідуальних властивостей, наприклад просторового зсуву фарби між різними кольорами, були вилучені та застосовані форми кольорових друкарських одиниць та відстань відтінку між тріадними кольорами, як зображено на рис. 6, для підвищення ефективності розпізнавання [17].

Висновки. На сьогодні можна зазначити, що біометричні технології аутентифікації мають дуже великі перспективи розвитку. При використанні систем на основі біометричних методів процедури доступу стають швидшими, безпечнішими та простішими. Проте біометричні технології також мають низку складнощів і проблем, таких як підготовка професійних кадрів, зменшення вартості пристроїв та інше.

Було показано що звичайний офсетний друк може ефективно забезпечити маркування, що убезпечує продукцію від підробок. Така технологія може використовуватися для масового виробництва, з огляду на її дешевизну. Копіювання або передрук кодів призведе до збільшення бітових помилок. Якщо рівень помилок перевищує певний діапазон це може призвести до не читання кодів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Захист інформації в поліграфії. Домашня контрольна робота «Життєвий цикл захищеної поліграфічної продукції» : навч. посіб. / КПІ ім. Ігоря Сікорського ; уклад.: Т. Ю. Киричок. Київ : КПІ ім. Ігоря Сікорського, 2020. 29 с.
2. Журнал «Світ упаковки». Розвиток українського ринку упаковки. URL: https://packaging.com.ua/content/4755.
3. Global packaging industry. URL: https://www.smitherspira.com/market-reports/globalpackaging-industry-expected-to-reach-820-billion-by-2016.aspx.
4. Ярема С. М., Гавва О. М. Етикетка. Київ : Ун-т «Україна», НУХТ, 2007. 635 с.
5. Технології захисту цінних паперів : навч. посіб. / Нац. ун-т «Львівська політехніка». 2-ге вид., допов. Львів : Вид-во Львів. політехніки, 2013. 152 с.
6. Інформаційна технологія формування графічних засобів захисту документів / Дурняк Б. В., Пашкевич В. З., Сабат В. І., Тимченко О. В. Львів : Українська академія друкарства, 2011. 152 с.
7. Киричок П. О., Коростіль Ю. М., Шевчук А. В. Методи захисту цінних паперів та документів суворого обліку. Київ : НТУУ «КПІ», 2008. 368 с.
8. Бизюк А. В., Жернова П. Е. Расчет обобщенного показателя защищённого полиграфического изделия для информационной системы. Бионика интеллекта. 2016. № 1 (86). С. 63–67.
9. Бизюк А. В., Шамо И. И. Решение задачи пространственного сегментирования с применением методов интеллектуального анализа данных. Информационные системы и технологи : материалы 2-й Международ. науч.-техн. конф. (16–22 сентября 2013, Евпатория-Харьков). Харьков, 2013. С. 134–135.
10. Кузьмина К. В., Бизюк А. В. Классификация методов защиты полиграфической продукции. Информационные системы и технологи : материалы 3-й Междунар. науч.-техн. конф. ИСТ-2014 (15–21 сент. 2014, Харьков). Харьков, 2014. С. 206–207.
11. Жернова П. Е., Бизюк А. В. Оптимизация выбора полиграфической защиты для упаковочно-этикеточной продукции. Информационные системы и технологи : материалы 2-й Международ. науч.-техн. конф. (16–22 сентября 2013, Евпатория-Харьков). Харьков, 2013. С. 142–143.
12. Романов В., Галелюка И., Клочан П. Биометрическая идентификация личности: современное состояние и перспективы развития в Украине. Электронные компоненты и системы. 2010. № 5. С. 16–20.

13. How can you prevent an authentication hacking attack. URL: https://www.acunetix.com/websitesecurity/authentication/ 28.09.2022.
14. Anonymous identification with cancelable biometrics. URL: https://ieeexplore.ieee.org/document/5297678 (дата звернення: 29.09.2022).
15. Дослідження в університетах прикладних Наук (проект ЕпіКод-3D). URL: https://www.ds.hs-mannheim.de/fileadmin/user_upload/institute/ds/pdf-Dateien/Preisverleihungen/Forschungsprojekt_des_Monats_Mai/Das_Projekt_EPICODE-3D.pdf, Федеральне міністерство освіти та досліджень (БМБФ), Німеччина.
16. Virnitser B., Sprague-Hernandez T. Deconvolution in linear scanners using a priori information, Proceedings of the SPIES - Image Reconstruction from Incomplete Data II. 2002. Vol. 4792. Pp. 156–163, Seattle, WA, USA.
17. Малешлійський С., Гарсія Ф. Інтеграція функцій боротьби з підробками в звичайні 2D-штрих-коди для мобільного маркування. Новий Орлеан, США, 2009.

REFERENCES

1. Zakhyst informatsii v polihrafii. Domashnia kontrolna robota «Zhyttievyi tsykl zakhyshchenoi polihrafichnoi produktsii» (2020) / KPI im. Ihoria Sikorskoho ; uklad.: T. Yu. Kyrychok. Kyiv : KPI im. Ihoria Sikorskoho (in Ukrainian).
2. Zhurnal «Svit upakovky». Rozvytok ukrainskoho rynku upakovky. Retrieved from https://packaging.com.ua/content/4755 (in Ukrainian).
3. Global packaging industry. Retrieved from https://www.smitherspira.com/market-reports/globalpackaging-industry-expected-to-reach-820-billion-by-2016.aspx (in English).
4. Yarema, S. M., & Havva, O. M. (2007). Etyketka. Kyiv : Un-t «Ukraina», NUKhT (in Ukrainian).
5. Tekhnolohii zakhystu tsinnykh paperiv (2013) / Nats. un-t «Lvivska politekhnika». 2-he vyd., dopov. Lviv : Vyd-vo Lviv. Politekhniky (in Ukrainian).
6. Durniak, B. V., Pashkevych, V. Z., Sabat, V. I., & Tymchenko, O. V. (2011). Informatsiina tekhnolohiia formuvannia hrafichnykh zasobiv zakhystu dokumentiv. Lviv : Ukrainska akademiia drukarstva (in Ukrainian).
7. Kyrychok, P. O., Korostil, Yu. M., & Shevchuk, A. V. (2008). Metody zakhystu tsinnykh paperiv ta dokumentiv suvoroho obliku. Kyiv : NTUU «KPI» (in Ukrainian).
8. Bizjuk, A. V., & Zhernova, P. E. (2016). Raschet obobshhennogo pokazatelja zashhishhjonnogo poligraficheskogo izdelija dlja informacionnoj sistemy: Bionika intellekta, 1 (86), 63–67 (in Russian).
9. Bizjuk, A. V., & Shamo, I. I. (2013). Reshenie zadachi prostranstvennogo segmentirovanija s primeneniem metodov intellektual'nogo analiza dannyh. Informacionnye sistemy i tehnologi : materialy 2-j Mezhdunarod. nauch.-tehn. konf. (16–22 sentjabrja 2013, Evpatorija-Har'kov). Har'kov, 134–135 (in Russian).
10. Kuz'mina, K. V., & Bizjuk, A. V. (2014). Klassifikacija metodov zashhity poligraficheskoj produkcii. Informacionnye sistemy i tehnologi : materialy 3-j Mezhdunar. nauch.- tehn. konf. IST-2014 (15–21 sent. 2014, Har'kov). Har'kov, 206–207 (in Russian).
11. Zhernova, P. E., & Bizjuk, A. V. (2013). Optimizacija vybora poligraficheskoj zashhity dlja upakovochno-jetiketochnoj produkcii. Informacionnye sistemy i tehnologi : materialy 2-j

Mezhdunarod. nauch.-tehn. konf. (16–22 sentjabrja 2013, Evpatorija-Har'kov). Har'kov, 142–143 (in Russian).
12. Romanov, V., Galeljuka, I., & Klochan, P. (2010). Biometricheskaja identifikacija lichnosti: sovremennoe sostojanie i perspektivy razvitija v Ukraine: Jelektronnye komponenty i sistemy, 5, 16–20 (in Russian).
13. How can you prevent an authentication hacking attack. Retrieved from https://www.acunetix.com/websitesecurity/authentication/ 28.09.2022 (in English).
14. Anonymous identification with cancelable biometrics. Retrieved from https://ieeexplore.ieee.org/document/5297678 (data zvernennia: 29.09.2022) (in English).
15. Doslidzhennia v universytetakh prykladnykh Nauk (proekt EpiKod-3D). Retrieved from https://www.ds.hs-mannheim.de/fileadmin/user_upload/institute/ds/pdf-Dateien/Preisverleihungen/Forschungsprojekt_des_Monats_Mai/Das_Projekt_EPICODE-3D.pdf, Federalne ministerstvo osvity ta doslidzhen (BMBF), Nimechchyna (in Ukrainian).
16. Virnitser, B., & Sprague-Hernandez, T. (2002). Deconvolution in linear scanners using a priori information, Proceedings of the SPIES - Image Reconstruction from Incomplete Data II, 4792, 156–163, Seattle, WA, USA (in English).
17. Maleshliiskyi, S., & Harsiia, F. (2009). Intehratsiia funktsii borotby z pidrobkamy v zvychaini 2D-shtrykh-kody dlia mobilnoho markuvannia. Novyi Orlean, USA (in Ukrainian).

doi: 10.32403/2411-3611-2022-2-42-54-66

ANALYSIS OF MODERN METHODS AND MEANS OF PROTECTION OF LABELLING AND PACKAGING PRODUCTS BASED ON IDENTIFICATION AND AUTHENTICATION

Y. V. Hryk, N. Y. Hrynokh, Z. M. Selmenska

Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine
zorselm@gmail.com

The paper studies the trends in the development of modern identification/authentication methods in the technology of protecting printed products, in particular, label and packaging, from counterfeiting. Today, Ukrainian and foreign packaging and label manufacturers are developing, improving and offering the new global market technical solutions to protect brands, products and consumers by implementing the latest IT developments in packaging.

The paper thoroughly analyses the existing methods of computer technologies that are becoming relevant in protecting information in information and communication systems and in protecting printed products. It is determined that "identification", "authentication" and "authorization" are three interrelated concepts that form the basis of the security system. An authentication protocol is a so-called type of computer communication protocol or cryptographic protocol that has been specially designed to

transfer authentication data between two objects. The purpose of authentication is to confirm an individual's identity, but the set of authentication methods is very wide and can vary in different ways. This paper discusses a list of common authentication methods: 1. password authentication; 2. smart card authentication; 3. biometric authentication; 4. authentication with a digital certificate. Each of the above authentication methods has its application, but also its drawbacks. The technology under study uses biometric authentication based on measured fingerprints - in our case, it is EpiCode. One of the main goals of the technology is to develop cost-effective and counterfeit-proof labelling and authentication procedures for both products and processes and to create integrated concepts by combining individual technological, organizational and legal options.

Keywords: *counterfeiting, falsification, label, packaging, identification, authentication, matrix codes.*

Стаття надійшла до редакції 11.10.2022.
Received 11.10.2022.