МУЛТИМЕДИЙНА МНОГОСТЕПЕННО ШИФРИРАНА ЗАЩИТА НА ДОКУМЕНТИ, ЦЕННИ КНИЖА И СТОКИ СРЕЩУ ФАЛШИФИКАЦИЯ

Основната идея на технологията представлява вграждане на различни нива на допълнителна скрита (секретна) информация във видимия образ (защита, номер и пр.). Така вградената на всяко отделно ниво информация е специфична, както за различните нива, така и за всеки един отделен обект на защита и е генерирана и предоставена от независими един от друг източници (производител, контролен орган и пр.). Връзката и съотношението между видимия образ (информация, номер и пр.) и вградената секретна (скрита) информация за дадено ниво се записва на неизтриваем носител CD-ROM, DVD-ROM, защитавайки я от нежелателни или неоторизирани корекции.

Предвид независимостта на отделните нива на защита, достъп до персонализацията имат само съответните органи, свързани с процеса на формиране и генериране на скритата образна информация (кодове) за конкретното ниво . Така се получават независими една от друга защити в защитата и ако по някакъв начин се фалшифицира информацията за дадено ниво, в резултат на корупция в съответната организация, тази от другите нива остава валидна в защитата. В резултат на това се ограничава възможността от измама и възпроизвеждане на оригинални защити, поради необходимостта от подмяна на информационните бази за всяко едно ниво по отделно.

РЕАЛИЗАЦИЯ НА ЗАЩИТАТА

Едно и двуизмерна (едно и двустепенна) реализация на защитата
Чрез промяната в пространствените координати на отворите по “X” и “Y” се създават скрити номера (кодове). Тези скрити номера допълнително осигуряват и персонализират защитения документ.

Триизмерна, тристепенна реализация на защита
Чрез разместване на знаците по координатите “X” и “Y” и различна дълбочина на гравиране (разместване по оста “Z”) се осъществяват три независими нива на защита.

Многодименсионна, многостепенна реализация на защита
Следният пример е реализиран върху защитна нишка, като тази в банкнотите.
Примерът илюстрира многовариантността на осъществяване на защитата.

М-код – видимата естествена микроструктура на материала

М-код е уникален метод за различаване на оригинал от негово много точно копие (фалшификат). Как на практика ясно разграничаваме точното копие от оригинала!? Подобно на човешките пръстови отпечатъци, които са уникални за всеки отделен индивид, при този метод се генерират също такива уникални отпечатъци (образи) на материала. След записа на многостепенната защита, се сканират и записват някои нейни елементи (напр. перфорирани отвори), посредством устройство с висока резолюция. Въпреки, че защитата се нанася върху подложка от един и същ материал, записващото устройство поставя отпечатъци - уникални по своята структура, както за всяка една отделна защита, така и за един обект – стока, документ, банкнота и пр. Тези отпечатъци на материала представляват М-код – уникалната видима микроструктура на материала, която не може да бъде копирана и по този начин диференцира защитата. Този метод може да бъде сравнен с физическите генератори на шум при формирането на секретните ключове в криптографията.

АРХИТЕКТУРА НА ЗАЩИТАТА

Запис

Скритата секретна информация се подава към записващата система от различните независими източници. Тя от своя страна осъществява процеса на запис и връща обратна информация към съответния източник за връзката между видимата и скритата секретна информация за определеното ниво на защита.

Записващо устройство

Запис може да се осъществи както чрез механични устройства, така и чрез лазерни, мастиленоструйни и други подобни системи.
Следващото решение е базирано на лазерна записваща система с CO_2 импулсен лазер. Системата състояща се от 1,3,4 и 5,12 (виж фиг.1) контролирани и управлявани от 2,6,7 записва на база кодовете предоставени от различни институции, имащи интерес от идентификацията на конкретния продукт, многостепенни мултимедийни шифрирани маркировки (13). Ако записващата система не се намира едно и също място с доставчика на кодове, то те се подават по защитени канали на база високоскоростни шифриращи устройства (11). Записаната маркировка се чете от 9 за проверка и обратна връзка и 10 записва връзката видима скрита информация в базата данни (на неизтриваем носител CD-ROM/DVD-ROM), или при отдалечен източник изпраща тази информация до него по установените защитени комуникационни канали.

База данни

Независими бази данни за всяко ниво на защита;
Съхраняват връзката между видимата и скритата информация;

Записани на CD-ROM или DVD-R. Информацията на такъв носител не може да бъде променяна, изтривана или добавяна, което елиминира риска от неоторизирани и злонамерени корекции;

Контрол и инспекция
Тази фаза представлява крайната видима част на целия процес на защита, даваща отговора «истински» или «фалшив».
Четящото устройство сканира защитата и извлича скритата секретна информация само за съответното ниво на защита, след което се извършва проверка дали тази информация съответства на тази от локалната (А) или отдалечената (Б) база данни.

Четене и контрол
Контролът трябва да се осъществява достатъчно бързо и ефективно. Скоростта е много съществен фактор на I-ва и II-ра линия, където една по бавна и задълбочена проверка би довела до значителни забавяния. Съвместната дейност и координация между съответните органи от различните региони и страни е абсолютно належаща. Много важен фактор е бързата обмяна на информация, а особено належащо е наличието и възприемането на единна система от препоръки, в областта на борбата срещу измамите и фалшифика-циите, което неимоверно би подобрило и улеснило процеса на проверка и контрол. В зависимост от вградените степени на защита и начините за тяхното имплементиране, съществуват следните начини за осъществяване на контрол и проверка:

Ръчно четене и контрол с помощта на лупа с растер за измерване и крипто карта с логиката за извличане на информацията за съответното ниво. Чрез лупата се измерват отместванията на елементите(точките) на образа (номера) и на база крипто картата се формира скритата информация. Следва проверка в мултимедийната антикорупционна база данни.
Автоматично четене със стационарни устройства за контрол в банки, митници, гранични и полицейски служби, магазини и пр. Четяща глава контролирана по X и Y сканира изображението, след което се извършва обработка, извличане и калкулиране на скритата информация(кодове) последвана от проверка в базата данни.
Автоматичен контрол с преносими устройства.
С помощта на устройство с висока разрешаваща способност се сканира защитата и по телекомуникационен път се изпраща до съответните органи (производител, контролни и пр.), където се обработва и се връща веднага отговор дали съответната стока, документ и пр. е фалшив.С започналото широко навлизане на 3G-трето поколение мобилни комуникации позволяващи високо скоростен обмен на информация и пренос на образи, нормалните мобилни телефони с превръщат в универсални четящи устройства, които сканират защитата и я изпращат на съответните органи и он-лайн се получава потвърждение за оригиналността на проверявания обект. По този начин всеки един човек от всяка една точка на света може да

осъществи проверка за валидност и да се включи директно в борбата с престъпността.

ПРИЛОЖЕНИЯ НА ТЕХНОЛОГИЯТА:

Маркиране на автомобили против кражба
Документи и лични карти
Етикети и опаковки
Метални изделия, резервни части и оръжия
Ценни книжа, свидетелства, банкноти