УДК 004.056.53

О.А. Нємкова, З.А. Шандра, С.С. Гапій
Львівський інститут банківської справи,
Національний університет "Львівська політехніка"

ЗАСТОСУВАННЯ ЛУНА-СИГНАЛІВ ДЛЯ АВТЕНТИФІКАЦІЇ ЗВУКОВИХ ФАЙЛІВ

Розглянуто автентифікацію звукових повідомлень з використанням луна-сигналів. Автентифікаційна інформація впроваджується у DTMF-сигнал.

Ключові слова: автентифікація, луна-сигнал, DTMF-сигнал.

This paper is devoted to the authentication audio message using echo-signals. Authentication information is implemented in the DTMF-signal.

Key words: authentication, echo-signal, DTMF-signal.

Вступ

Сучасні системи телефонного зв'язку широко використовуються для автоматичного надання послуг клієнтам про стан заборгованості за телефон, вхід в автоматичне сервісне меню операторів мобільного зв'язку або в сервісне меню інтернет-провайдерів; навіть банки і платіжні системи надають послугу управління рахунком по телефону. При цьому для доступу до конфіденційних даних та сервісів використовується система автентифікації введенням номера користувача (угоди, контракту, рахунка, телефону тощо) і певного пароля (PIN-коду). В цьому випадку користувач використовує тоновий режим роботи телефону (режим генерації DTMF-сигналів) для передачі даних.

Звичайно, використання відкритого телефонного каналу дає можливість злочинцю порушити конфіденційність інформації. Не будемо вдаватися в те, яка його мета, але публікації в хакерських виданнях дають підстави робити висновок, що ця робота ведеться достатньо активно.

Відомо, що найпростіший спосіб злому системи автентифікації за припущення, що відомі номер угоди, контракту, рахунка тощо, полягає в звичайному переборі усіх можливих варіантів PIN-коду. Переважно PIN-код складається з чотирьох цифр, кількість можливих комбінацій в цьому випадку 10^4. Якщо на один варіант витрачати хоча б півхвилини, то для для перебору усіх варіантів потрібно 85–90 годин. Для людини ця робота є достатньо важкою, але для комп'ютера це не є проблемою. Єдине, що треба зробити, – це навчити комп'ютер розрізняти за отриманою аудіовідповіддю, чи введене значення PIN-коду є правильним, чи неправильним. З'явились публікації про автоматизацію цієї роботи з використанням брутфорсера, детальна інформація щодо цього напряму подана в [1].

Застосування луна-сигналів для приховування інформації

Ефективним засобом боротьби з брутфорсом у банкоматах є блокування дій з платіжною карткою при кількаразовому неправильному введенні PIN-коду. У телефонному банкінгу цей запобіжний засіб не використовується, тому не виключається можливість шахрайських дій типу брутфорсингу. Отже, якщо не використовувати процедуру блокування системи після введення заданої кількості PIN-кодів, то необхідно змінити процедуру автентифікації. Наприклад, до PIN-коду додавати деяку секретну інформацію, що перетворена за допомогою хеш-функції, про існування якої зломник не підозрює. Використання хеш-функції потрібне для підвищення стійкості автентифікації. Якщо зломник може перехопити сигнал у телефонній лінії, поміняти частину інформації і передати сигнал далі, то у випадку застосування хеш-функції таке перехоплення нічого не дасть. Для того, щоб було практично неможливо зламати хеш-функцію, слід використовувати систему разових паролів на базі генератора випадкових чисел. Сучасні надійні генератори випадкових чисел мають довжину 10^5, що набагато менше ніж кількість звернень однієї людини упродовж її життя до послуг банку.

Для цього можна застосувати будь-який стеганографічний метод, що використовує аудіо-контейнери. Огляд різних стеганографічних методів наведено в [2]. З описаних методів з міркувань більш-менш простої реалізації становить інтерес метод впровадження інформації за рахунок зміни часу затримки луна-сигналу.

Цей метод дає змогу впроваджувати дані в сигнал прикриття, змінюючи параметри луна-сигналу. До параметрів луни, що містить впроваджувану інформацію, належать: початкова амплітуда і зсув (час затримки між вихідним сигналом та сигналом відлуння). При зменшенні зсуву два сигнали змішуються. У певній точці людське вухо перестає розрізняти два сигнали, і луна сприймається як додатковий резонанс. Цю точку важко визначити точно, тому що вона залежить від вихідного запису, типу звуку і слухача. У загальному випадку для більшості типів сигналів і для більшості слухачів злиття двох сигналів відбувається, якщо відстань між ними близько 0,001 с.

Кодер використовує дві тривалості затримки: одну для кодування нуля, другу для кодування одиниці. Ці тривалості затримки менші від тих, на яких людське вухо може розпізнати луну.

На рис. 1 показано спосіб кодування «одиниці» і «нуля». Затримка між вихідним сигналом та сигналом відлуння залежить від впроваджуваних у цей момент даних. Одиниці відповідає затримка δ_1, а нулю – затримка луна-сигналу δ_0.

Для того щоб закодувати більше від одного біта, вихідний сигнал розділяється на ділянки тривалістю δ. Кожна ділянка розглядається як окремий сигнал, і в нього впроваджується один біт інформації. Результуючий закодований сигнал (що містить кілька бітів впровадженої інформації) являє собою комбінацію окремих ділянок.

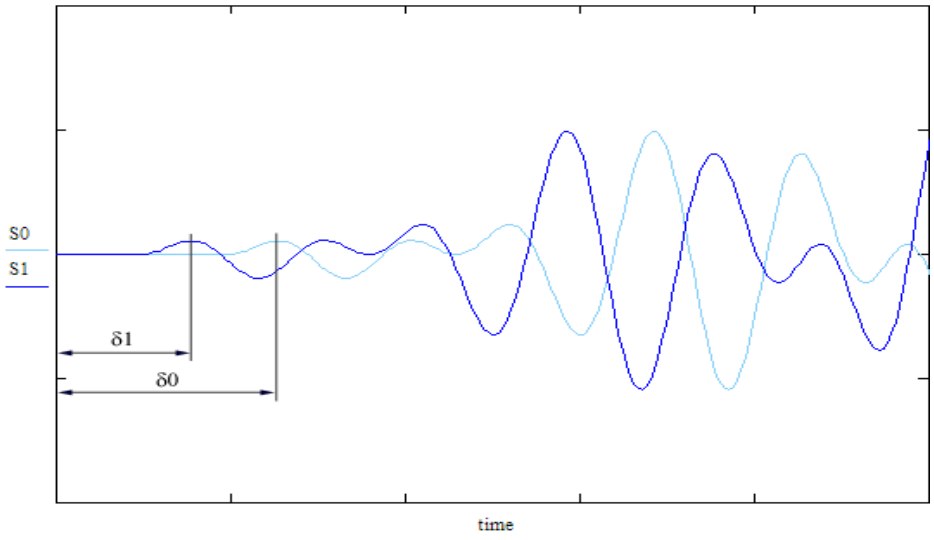

Рис. 1. Кодування інформації

Для досягнення мінімуму помітності спочатку створюють два сигнали: один, який містить лише "одиниці", й інший – містить лише нулі.

Потім створюють два перемикальних сигнали – нульовий і одиничний (рис. 2). Кожен з них являє собою бінарну послідовність, стан якої залежить від того, який біт повинен бути впроваджений в певну ділянку звукового сигналу.

Далі обчислюється сума добутків нульового перемикального сигналу й аудіосигналу із затримкою «нуль», а також одиничного перемикального сигналу й аудіосигналу із затримкою «одиниця». Інакше кажучи, коли в аудіосигнал необхідно впровадити «одиницю», на вихід подається сигнал із затримкою «одиниця», в іншому випадку – сигнал із затримкою «нуль» (рис. 3).

Оскільки сума двох перемикальних сигналів завжди дорівнює одиниці, то забезпечується плавний перехід між ділянками аудіосигналу, в які впроваджені різні біти. Блок-схема стегокодера показана на рис. 4.

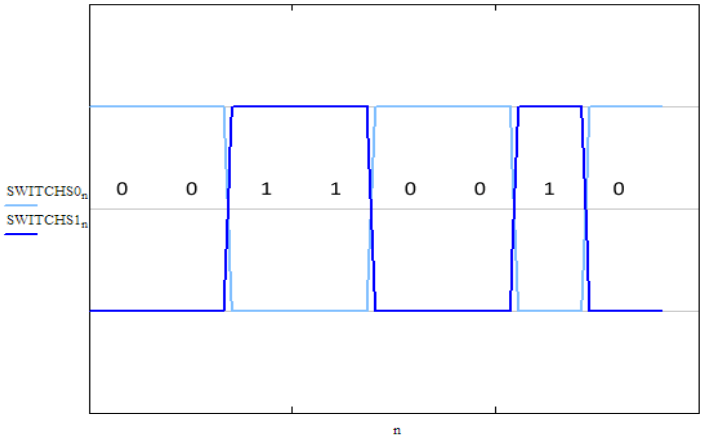

Рис.2. Перемикальний сигнал

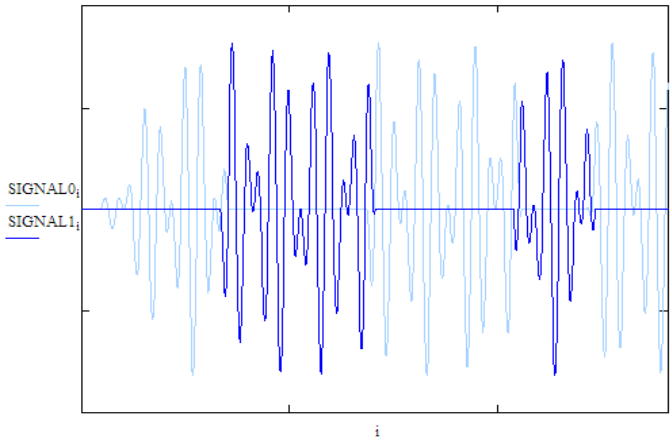

Рис.3. Запис «1» (темна лінія) або «0» (світла лінія) при використанні DTMF-сигналів

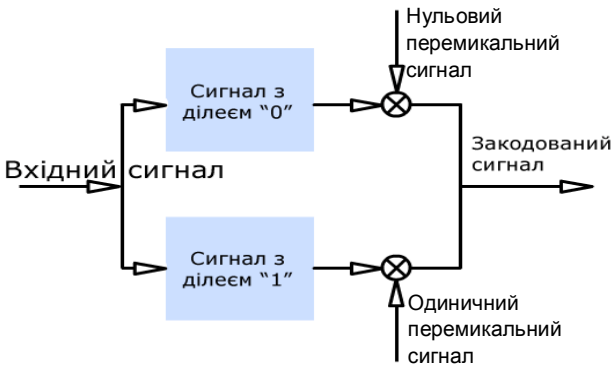

Рис. 4. Блок-схема стегокодера

Декодування впровадженої інформації являє собою визначення проміжку часу між первинним DTMF-сигналом і луною. Для цього необхідно розглянути амплітуду автокореляційної функції дискретного косинусного перетворення логарифма спектра потужності (кепстра).

В результаті обчислення кепстра вийде послідовність імпульсів (відлуння, дубльоване кожні δ секунд). Для визначення проміжку часу між сигналом і його луною необхідно розрахувати автокореляційну функцію кепстра.

Сплеск автокореляційної функції відбуватиметься через δ_1 або δ_0 секунд. Правило декодування основане на визначенні проміжку часу між вихідним сигналом і сплеском функції

автокореляції. При декодуванні "одиниця" приймається, якщо значення автокореляційної функції через δ_1секунд більше ніж через δ_0 секунд, в іншому випадку – "нуль".

Однак використання автокореляційної функції кепстра добре працює для сигналу із складним спектром, наприклад, мовного сигналу. У випадку, коли контейнером слугує DTMF-сигнал, декодування з використанням функції кепстра не спрацьовує, що було визначено нашими попередніми дослідженнями [3]. Для декодування запропоновано методику визначення зсуву луна-сигналу розрахунком коефіцієнтів кореляції двох функцій – початкового DTMF-сигналу і сигналу із впровадженою інформацією. Ця методика дає змогу однозначно визначити зсув за знаком коефіцієнта кореляції.

Виникнення шумів під час впровадження інформації

У цій роботі містяться результати дослідження спектрів DTMF-сигналів із впровадженою у них інформацією. Методика експерименту полягала у тому, що генерувався DTMF-сигнал, а також визначався спектр цього сигналу з використанням пакета MATLAB. Для цього використано функцію easyspec. За допомогою аудіоплеєра цей сигнал прослуховувався. Далі DTMF-сигнал був оцифрований з частотою дискретизації 44100 Гц і відбувалося впровадження інформації в описаний вище спосіб. Отриманий сигнал знову прослуховувався і паралельно визначався його спектр.

Було виявлено, що сигнали із записаною інформацією:

1.Шумлять.

2.Спектральна характеристика сигналу в області досліджуваних частот піднімається.

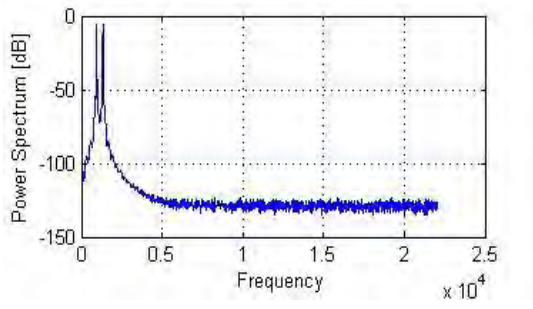

Рис. 5. Спектральна характеристика порожнього контейнера

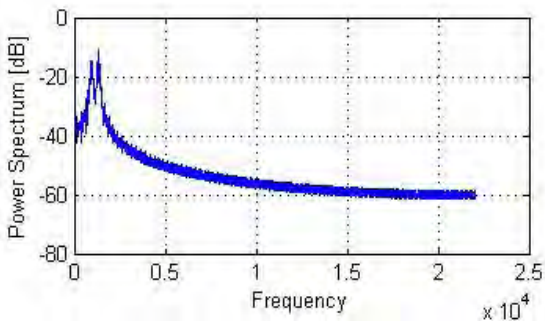

Рис. 6. Спектральна характеристика заповненого контейнера, δ =4 мс

Шум в системі може бути причиною появи помилок при передачі цифрових сигналів (помилки квантування), тому проведено додаткові дослідження впливу на спектральну характеристику інтервалу δ поділу сигналу на ділянки (кількість таких ділянок визначає кількість бітів впровадженої інформації).

Спектральна характеристика порожнього контейнера подана на рис. 5.

Була записана послідовність із 76 бітів інформації, на 1 біт припадало N = 176 семплів (відліків) – δ = 4 мс. В результаті спектральна характеристика заповненого контейнера суттєво змінилася; за допомогою аудіального порівняння встановлено виникнення значного за амплітудою шуму (рис. 6).

Зменшення щільності запису інформації до 1 біта на N=1408 семплів (δ =32 мс) призвело до зменшення рівня шумів (рис. 7). Це також відчувається під час прослуховування сигналу.

У таблиці подано залежність співвідношення початкового рівня DTMF-сигналу (порожній контейнер) до рівня сигналу заповненого контейнера від тривалості блока δ (ділянки розбиття), тобто від щільності запису (кількості семплів на один біт інформації). Видно, що зменшення впливу впровадженої інформації при використанні луна-сигналів досягається при щільності запису більше ніж 1584 семплів на 1 біт, і вже при щільності 4400 семплів на біт сигнали для порожнього і заповненого контейнерів різняться не суттєво. Дослідження цього впливу в широкому діапазоні значень δ показало, що наявний чітко визначений тренд на зниження шуму при зменшенні щільності запису інформації (рис. 8).

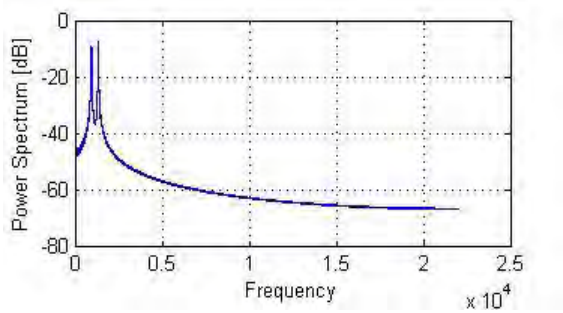

Рис. 7. Спектральна характеристика заповненого контейнера, δ =32 мс

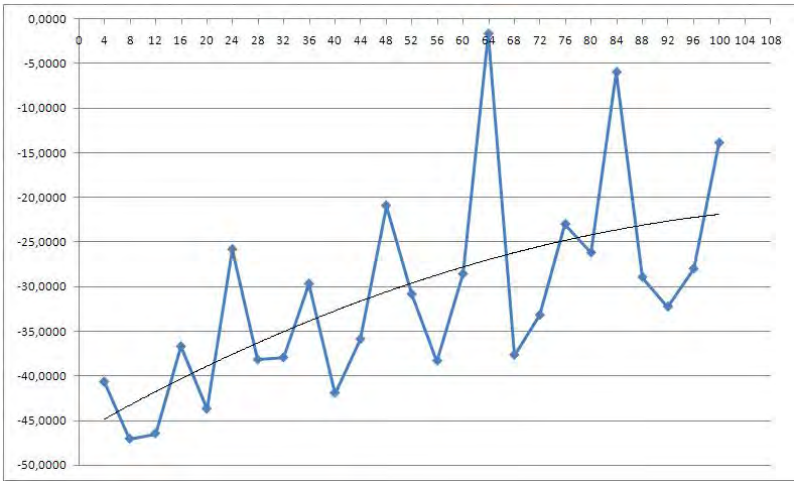

Рис.8. Залежність співвідношення початкового рівня DTMF-сигналу (порожній контейнер) до рівня сигналу заповненого контейнера від тривалості блока. Плавна лінія показує тренд залежності

Справді, дія перемикального сигналу проявляється у виникненні додаткових коливань – шуму. Тому зменшення кількості перемикань зменшує потужність шумів. Для підтвердження цього досліджено контейнер з одним типом бітів (повна відсутність перемикань, наприклад, тільки нулі). Спектральна характеристика такого контейнера була аналогічною, як на рис. 5.

Вплив щільності запису інформації на зашумлення контейнера

№ з/п	N (кількість семплів на 1 біт стего)	Δ (тривалість блока), мс	Нормований рівень сигналу, дБ
1	176	4	-40,6642
2	704	16	-36,7053
3	1056	24	-25,7967
4	1584	36	-29,6768
5	2112	48	-20,9037
6	3344	76	-22,9794
7	4400	100	-13,8637

Наявність різких сплесків на графіку рис.8 можна пояснити впливом інтерференції коливань, що виникають під дією перемикального сигналу. Попередні математичні оцінки підтверджують цей результат.

Згідно зі стандартом тривалість DTMF-сигналу починається з 40 мс, але може бути збільшена. З урахуванням проведених розрахунків легко отримати, що в аудіофайл такої тривалості з гарною якістю можна впровадити лише один біт інформації. Цього абсолютно недостатньо для практичного застосування методу. З міркувань, що впроваджувати слід не менш як 64 біти (об'єм деяких стандартних хеш-функцій), потрібно збільшувати тривалість аудіофайла. Наприклад, для δ = 32 мс тривалість аудіофайла становить трохи більш ніж 2 с.

Висновок

У результаті досліджень виявлено, що, застосовуючи луна-метод для передавання автентифікаційної інформації у випадку з малоінформативними та короткотривалими сигналами на кшталт DTMF-сигналів, потрібно шукати компроміс між щільністю запису інформації та зашумленням контейнера. Очевидно, що декодування DTMF-сигналу за наявності значних шумів стає проблематичним. Надсилання автентифікатора, вбудованого в тональний сигнал, можливе у разі зменшення обсягу цього автентифікатора та підвищення безпеки телефонної автентифікаційної системи криптографічними та технічними засобами.

1. Крис Касперски. Создание брутфорсера для голосового меню //www.inattack.ru/ article/ 583.html. 2. Грибунин В. Г. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с. 3. Немкова О.А. Визначення часового зсуву ехо-сигналу за методом розрахунку коефіцієнта кореляції // О.А. Немкова, З.А. Шандра, С.С. Гапій // Інформаційна безпека. – Луганськ. – 2011. – №2 (6). – С.93–98.

УДК 378.14:006.3

Р.М. Тріщ, В.А. Бруєва
Українська інженерно-педагогічна академія

КОМПЛЕКСНА МОДЕРНІЗАЦІЯ СИСТЕМИ МЕНЕДЖМЕНТУ У ВИЩІЙ ШКОЛІ ЯК ГОЛОВНИЙ ІНСТРУМЕНТ ПРИ ПІДГОТОВЦІ КОНКУРЕНТОСПРОМОЖНИХ ФАХІВЦІВ (НА ПРИКЛАДІ УКРАЇНСЬКОЇ ІНЖЕНЕРНО-ПЕДАГОГІЧНОЇ АКАДЕМІЇ)

Розглянуто актуальність удосконалення системи менеджменту організації навчального процесу в вищих навчальних закладах відповідно до міжнародного стандарту серії ISO 9001 : 2009. Запропоновано алгоритм концепції удосконалення системи організації навчального процесу в напрямку розроблення автоматизованої системи документообігу відповідно до міжнародного стандарту серії ISO 9001 : 2009.

Ключові слова: стандарт ISO 9001:2009, автоматизована система, менеджмент навчального процесу, концепція.

In the article examined the improvement of the management system of the educational organization process ISO 9001 : 2009 in the higher educational establishments. The algorithm of conception of improvement of the system of organization of educational process is offered in the direction of development system of documents circulation in accordance of international standard to the series of ISO 9001 : 2009.

Key words: ISO standard 9001 : 2009, automated system, management training process, concept.

Вступ

Сьогодні рівень та якість підготовки кадрів є найважливішим чинником та необхідною передумовою ефективного вирішення завдань розвитку економіки України. Сучасні економічні та соціально-політичні умови потребують працівника «нового типу» – професійно і соціально мобільного, такого, що має глибокі професійні знання з інтегрованих професій, володіє економічними і правовими знаннями, здатного до технічної та соціальної творчості, самовдосконалення, готового до роботи за різних форм організації праці та виробництва в умовах жорсткої конкуренції.