УДК 004.056.53

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

ЗАСТОСУВАННЯ ЛУНА-СИГНАЛІВ ДЛЯ АВТЕНТИФІКАЦІЇ ЗВУКОВИХ ФАЙЛІВ/ THE APPLICATION OF THE ECHO SIGNALS FOR SOUND FILES'S AUTHENTICATION

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

Keywords - authentication, echo-signal, DTMF-signal

У статті розглянуто автентифікація звукових повідомлень з використанням луна-сигналів. Автентифікаційна інформація впроваджується у DTMF-сигнал.

Ключові слова – автентифікація, луна-сигнал, DTMF-сигнал

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 шляхом вводу номера користувача (угоди, контракту, рахунку, телефону і т.д.) і певного пароля (PIN-коду). В даному 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 то, яку мету він переслідує, але публікації в хакерських виданнях дають підстави робити висновок, що ця робота ведеться достатньо активно.

Відомо, що самий простий спосіб злому системи автентифікації в припущенні, що відомі номер угоди, контракту, рахунку і т.д. 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 варіатів 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 по отриманій аудіовідповіді, що введене значення PIN-коду є вірним або невірним. З'явились публікації про автоматизацію цієї роботи шляхом використання брутфорсера, детальна інформація по цьому напрямку дається 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. Таким чином, 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 зломщик не підозрює. Використання хеш-функції потрібно для підвищення стійкості автентифікації. Якщо зломщик в змозі 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 на протязі її життя до послуг банку.

Для цього може бути застосований будь-якій стеганографічний метод, що використовує аудіоконтейнери. 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 дозволяє впроваджувати дані в сигнал прикриття, змінюючи параметри луна-сигналу. До параметрів луни, що несе впроваджувану інформацію, відносяться: 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 при відстані між ними близько 0,001 секунди.

Кодер використовує дві тривалості затримки: одну для кодування нуля, другу для кодування одиниці. Ці тривалості затримки менше того, на які людське вухо може розпізнати луна.

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

Для того щоб закодувати більше 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 біт впровадженої інформації) являє собою комбінацію окремих ділянок.

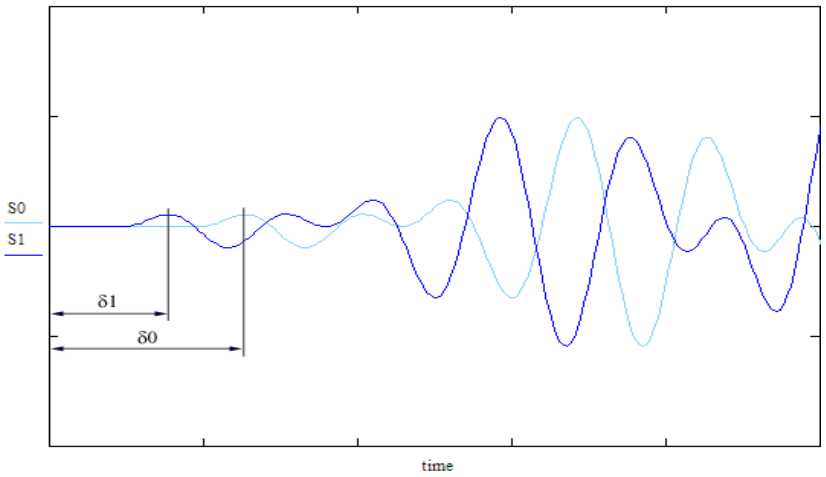

Рис.1. Кодування інформації

Для досягнення мінімуму помітності спочатку створюються два сигнали: один, який містить лише "одиниці", і інший - містить лише нулі.

Потім створюються два переключаючих сигнали - нульовий і одиничний (рис. 2). Кожен з них представляє собою бінарну послідовність, стан якої залежить від того, який біт повинен бути впроваджений в дану ділянку звукового сигналу.

Далі обчислюється сума добутків нульового переключаючого сигналу і аудіосигналу з затримкою «нуль», а також одиничного переключаючого сигналу і аудіосигналу з затримкою «одиниця». Іншими словами, коли в аудіосигнал необхідно впровадити «одиницю», на вихід подається сигнал із затримкою «одиниця», в іншому випадку - сигнал із затримкою "нуль" (рис.3).

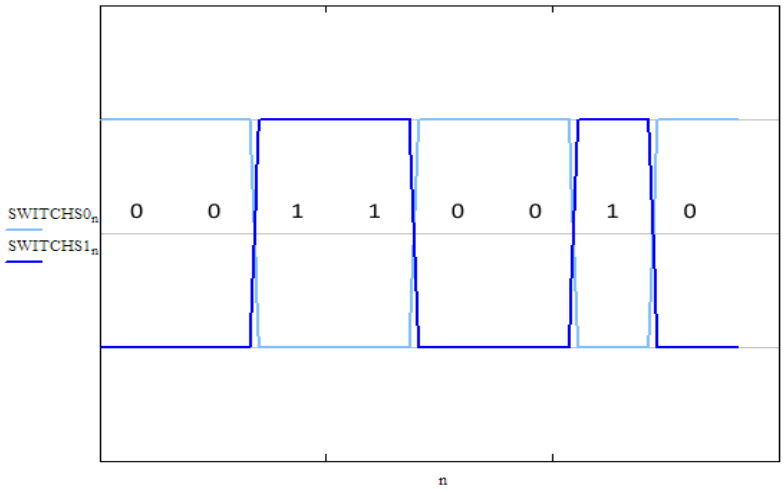

Рис.2. Переключаючий сигнал

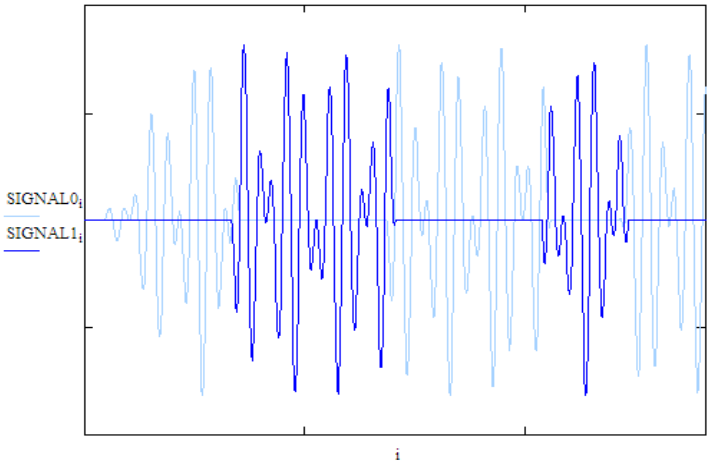

Рис.3. Запис «1» (темна лінія) або «0» (світла лінія) при використанні DTMF-сигналів

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

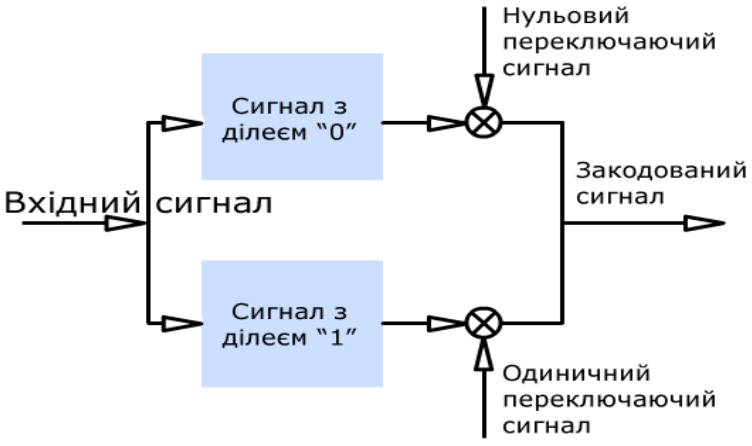

Рис.4. Блок-схема стегокодера

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 буде мати місце через δ_1 або δ_0 секунд. Правило декодування засноване 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 автокореляціонной функції кепстра добре працює для сигналу із складним спектром, наприклад, мовного сигналу. У випадку, коли в якості контейнера використовується DTMF-сигнал, декодування з використанням функції кепстра не спрацьовує, що було визначено нашими попередніми дослідженнями [3]. Для декодування було запропоновано методика визначення зсуву луна-сигналу шляхом розрахунку коефіцієнтів кореляції двох функцій – початкового DTMF-сигналу і сигналу із впровадженою інформацією. Ця методика дозволяє однозначно визначити зсув по знаку коефіцієнта кореляції.

Виникнення шумів при впровадженні інформації

В даній 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 пакету MATLAB. Для цього була використана функція 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.

Шум в системі може бути причиною появи помилок при передачі цифрових сигналів (помилки квантування), тому були проведені 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 біт інформації, на 1 біт припадало N = 176 семплів (відліків) - δ = 4 мс. В результаті спектральна характеристика заповненого контейнера суттєво змінилася; шляхом аудіального порівняння встановлено виникнення значного за амплітудою шуму (рис.6).

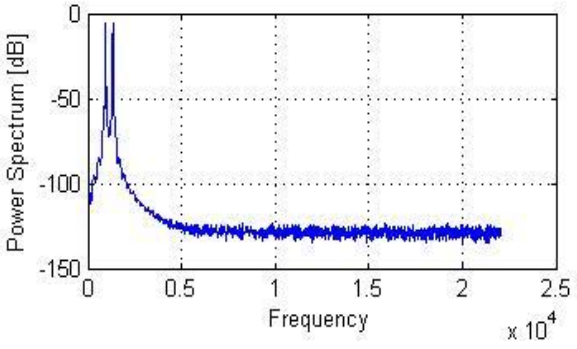

Рис. 5. Спектральна характеристика порожнього контейнера

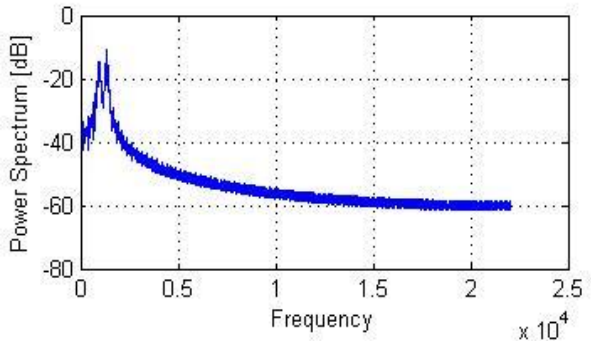

Рис. 6. Спектральна характеристика заповненого контейнера, δ =4 мс

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

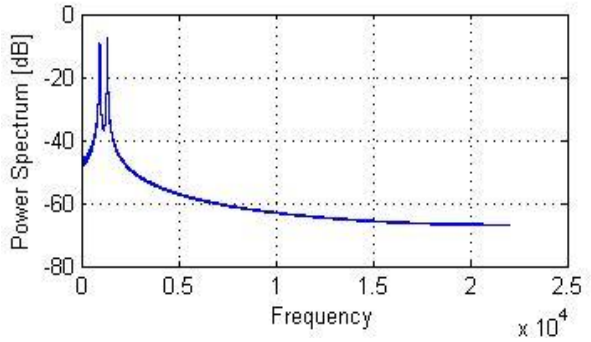

Рис. 7. Спектральна характеристика заповненого контейнера, δ =32 мс

В таблиці 1 подано залежність співвідношення початкового рівня DTMF-сигналу (порожній контейнер) до рівня сигналу заповненого контейнера від тривалості блоку 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 наявність чітко визначеного тренду на зниження шуму при зменшенні щільності запису інформації (рис.8).

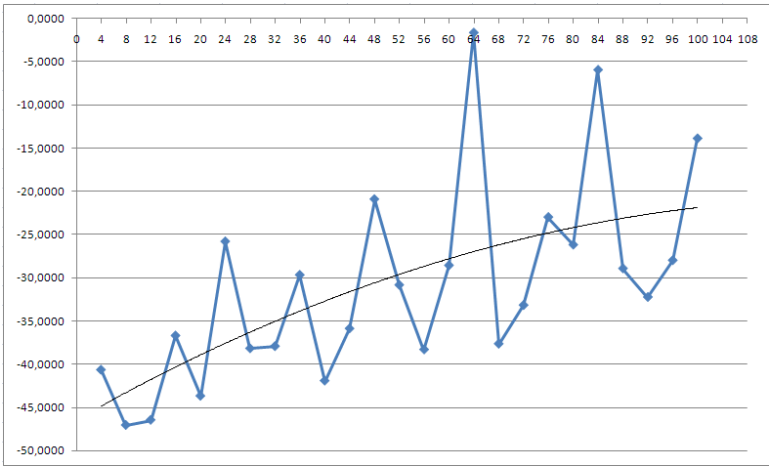

Рис.8. Залежність співвідношення початкового рівня DTMF-сигналу порожній контейнер) до рівня сигналу заповненого контейнера від тривалості блоку. Плавна лінія показує тренд залежності.

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

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

Таблиця 1

Вплив щільності запису інформації на зашумлення контейнера

№ з/п	N (кількість семплів на 1 біт стего)	δ(тривалість блоку), 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

Згідно стандарту тривалість DTMF-сигналу починається з 40 мс, але може бути збільшена. Виходячи з 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. Виходячи з міркувань, що впроваджувати слід не менш як 64 біти (об'єм деяких стандартних хеш-функцій), потрібно збільшувати тривалість аудіофайлу. Наприклад для δ = 32 мс тривалість аудіофайлу складає трохи більш, ніж 2 с.

Висновок

В результаті досліджень було виявлено, що при застосуванні луна-методу 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 випадку 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. Нємкова 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.