УДК 004.056.53

Д. Ю. Гереш

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ МОВНОЇ ІНФОРМАЦІЇ АНАЛОГОВОГО ТЕЛЕФОННОГО ЗВ'ЯЗКУ НА ОСНОВІ СКРЕМБЛЕРА ЗІ ЗМІНОЮ КОЕФІЦІЄНТІВ ВЕЙВЛЕТ ПЕРЕТВОРЕННЯ

Вінницький національний технічний університет

Анотація

Підвищено захищеність аналогового скремблера за рахунок виконання операції XOR та перестановки коефіцієнтів вейвлет перетворень відповідно до секретного ключа. Виконано дослідження характеристик отриманого сигналу.

Ключові слова: захист інформації, скремблер, вейвлет перетворення, латинські квадрати.

Abstract

The security of the analog scrambler is increased due to the XOR operation and permutation of the wavelet conversion coefficients according to the secret key. A study of the characteristics of the received signal.

Keywords: Data protection, scrambler, wavelet transformation, Latin square.

На сьогоднішній день майже неможливо уявити собі світ без щоденного застосування різноманітних засобів зв'язку або переоцінити їхній вплив на повсякденне життя. Це насамперед пов'язане із зручністю даного виду комунікації. Розвиток сучасних систем передачі інформації дозволяє кожний день передавати неймовірну за обсягами кількість інформації.

Значна частина несанкціонованого перехоплення інформації припадає саме на телефонні розмови, адже зазвичай телефонні мережі не мають достатнього рівня захисту [1]. Тому необхідним є забезпечення конфіденційності розмов, запобіганню несанкціонованому доступу до систем передачі даних.

Одним із найбільш ефективних засобів захисту є застосування різноманітних скремблерів, які являють собою кардинальний захід з метою запобігання прослуховування телефонної мережі [2].

Скремблер – це пристрій, призначений для зміни мовної інформації, що передається по лінії зв'язку з подальший її відновленням до початкового стану використовуючи відповідний ключ [3].

Класифікація скремблерів відбувається відповідно до систем передачі інформації в яких вони застосовуються. У системах зв'язку відомі два основні методи скремблювання мовних сигналів: аналогове скремблювання і цифрове скремблювання. Основними характеристиками скремблерів є якість скремблювання, розбірливість сигналу після зворотного перетворення та залишкова розбірливість сигналу після перетворення початкового сигналу [4].

Найбільш простими і популярними є аналогові методи скремблювання. Вони можуть перетворювати сигнал за трьома параметрами: амплітуді, частоті і часу. Однак, дані методи на сьогодні не здатні забезпечити достатній рівень захищеності сигналу [4].

В процесі розвитку інформаційно-телекомунікаційних систем широко застосування здобули методи скремблювання з перетворенням аналогового сигналу в цифровий. Дані методи забезпечують значно вищий рівень захищеності мовної інформації в процесі шифрування. Цифрові системи скремблювання додатково поділяються на такі, що у процесі шифрування застосовують ПВП та криптографічні алгоритми. Однак, дані системи вимагають значних апаратних потужностей, в іншому випадку вносять значні затримки у канал зв'язку [5].

В більшості випадків наявні скремблери дозволяють захистити інформацію на достатньому рівні. Особливо це характерне для пристроїв захисту стільникових телефонних мереж. Гірша ситуації спостерігається із аналоговими системами передачі даних в яких значна кількість скремблерів використовують прості методи захисту, які не здатні забезпечити високий рівень захищеності.

Основними шляхами покращення захищеності інформації було розширення можливої кількості часових або частотних перестановок. Збільшення можливих варіантів часових перестановок є небажаним, адже будуть створюватись значні затримки. Тому покращення досягається за рахунок збільшення варіативності частотних перестановок. Однак, найкращі рівень захищеності досягається у випадку комбінування частотно- часових перестановок [4].

Вейвлет перетворення – інтегральне перетворення, яке представляє собою згортку вейвлет-функції з сигналом. Вейвлет перетворення переводить сигнал з часового представлення в частотно-часове. Яке надає змогу більш детально вивчити, або дозволяє стиснути вихідний набір даних. Вейвлет перетворення сигналів є узагальненням спектрального аналізу. Вейвлети - це узагальнена назва математичних функцій певної форми, які локальні в часі і по частоті і в яких всі функції виходять з однієї базової, змінюючи її [6].

Враховуючи наявну інформацію, підвищення захищеності було вирішено досягти шляхом модернізації алгоритму за рахунок виконання операцій перестановок, XOR у відповідності до ключа скремблера – латинського квадрату. За рахунок застосування перестановки вейвлет коефіцієнтів у відповідності до латинських квадратів вдалось значно збільшити можливу кількість ключів скремблера не створюючи затримок у каналі зв'язку. А додаткове виконання операції XOR з отриманим після зворотного вейвлет перетворення сигналом створить додатковий захист від атаки прямим перебором.

Латинський квадрат – таблиця розміру $n \times n$ заповнена n різними елементами так, що в кожному стовпці і кожному рядку всі елементи зустрічаються по одному разу та кожний із них належить певній множині чисел M = { 1,2,3 … n } [7].

Кількість можливих варіантів при збільшені розрядності зростає на декілька порядків, при n = 4 кількість квадратів 576, при n = 6 кількість можливих варіантів визначається мільйонами. Дана властивість робить їх застосування ефективної схемою перестановок коефіцієнтів вейвлет перетворення. Скремблювання виконується над блоками коефіцієнтів сигналу, кожний блок є однаковий за довжиною і відповідає розмірності латинського квадрату.

Вдосконалений алгоритм скремблера зображено на рисунку 1:

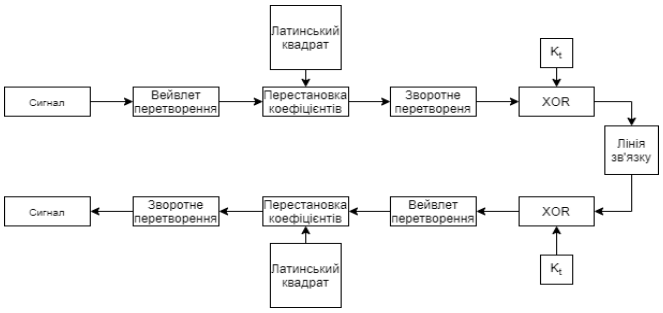

Рисунок 1 – Алгоритм скремблювання

Властивості вейвлет перетворень дозволяють точно здійснювати визначення коефіцієнтів з сигналу та виконання оберненої операції із точним відтворення початкового сигналу.

Отриманий в результаті роботи скремблера сигнал буде змінений у частотно-часовій часовій області. Порівняння спектрів сигналів зображено на рисунку 2.

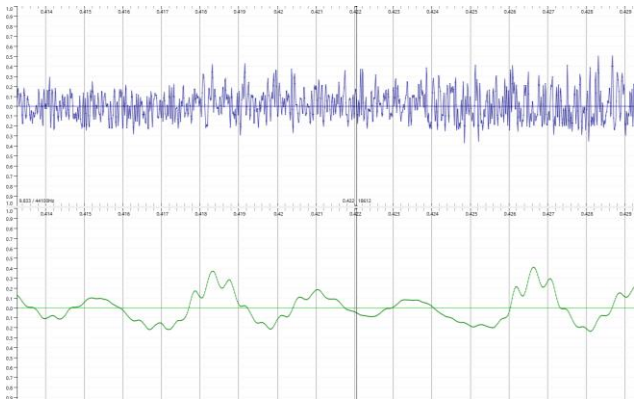

Рисунок 2 – Порівняння сигналів після та до роботи скремблера

Проведення статистичного аналізу сигналів на схожість дозволить дослідити захищений сигнал на відсутність надлишковості.

Визначимо значення MSE, яке дозволить додатково переконатись, що сигнал створений користувачем та отриманий після виконання процедури скремблювання відрізняються, а сигнал отриманий легітимним користувачем відповідає створеному сигналу. Для тестування було створено 5 пар таких сигналів. Результати MSE зображено в таблиці 1.

Таблиця 1 – Результати MSE досліджуваних сигналів

MSE/№	1	2	3	4	5
S_{syph}	0.09514	0.05372	0.06157	0.046096	0.040916
S_{dsyph}	0.00001	0.00002	0.00001	0.00001	0.000009

Результати даного тесту показують, що у всіх досліджених сигналах значення MSE скрембльованого сигналу не дорівнює нулю. MSE для дескрембльованих сигналів набуває значень близьких до нуля. Отже, алгоритм скремблера працює коректно. Оригінальний та скрембльований сигнал не є схожими, а оригінальний і дескрембльований однакові.

Іншим ефективним методом визначення рівня схожості двох сигналів є коефіцієнти кроскореляції. Даний метод дозволяє визначити в наскільки досліджувані послідовності є схожими шляхом пошуку більш коротких ідентичних послідовностей. Отримане значення кореляції знаходиться в діапазоні від -1 до 1. При значені кореляції близько 0, вважається про повну відмінність досліджуваних сигналів. Чим ближче значення до 1 або -1, тим сильніша кореляція двох сигналів і тим більше вони схожі, що є неприпустимим в системах скремблювання. Значення кореляції для досліджуваних сигналів наведено в таблиці 2.

Таблиця 2 – Значення кореляції двох сигналів

№	1	2	3	4	5
S_{syph}	0.05006	0.043818	0.05582	0.030926	0.037227
S_{dsyph}	0.99	0.99996	0.99	0.99995	0.99996

З отриманих коефіцієнтів можна зробити висновок про відсутність кореляції між оригінальним та скрембльованим сигналом, що і є очікуваним на виході алгоритму. Для оригінального та дескрембльованого сигналу отриманні коефіцієнти свідчать, що дані сигнали є майже ідентичними. Отже, можна вважати про ефективну роботу алгоритму у випадку застосування коректних ключів скремблера.

Метод спектрального аналізу коефіцієнтів вершин дозволяє розрізнити у спектрі сигналу тональність та шум. Високі коефіцієнти дозволяють зрозуміти характер, силу, звучання тону. Низькі коефіцієнти характерні для шумів. Відповідно, вихідний сигнал алгоритму має мати низькі коефіцієнти, щоб не залишати зловмисникові дану інформацію. Спектри коефіцієнтів досліджуваних сигналів зображено на рисунку 3.

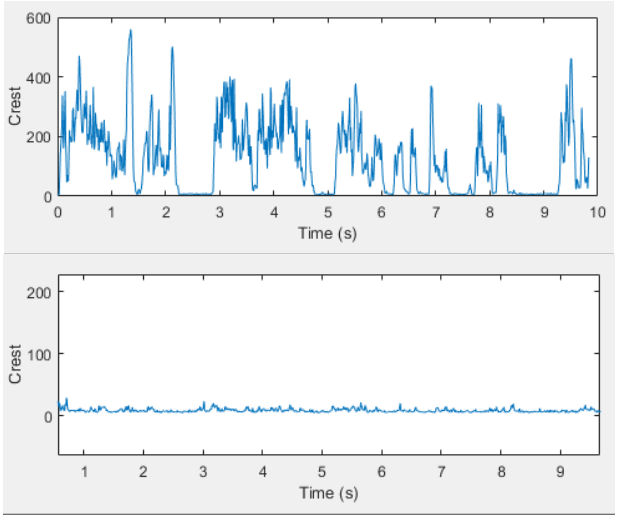

Рисунок 3 – Спектри коефіцієнтів вершин

Отже, в результаті виконання спектрального аналізу досліджуваних сигналів та перевірки даних

послідовностей з використанням статистичних тестів було встановлено коректність роботи алгоритму скремблювання, відсутність схожості між оригінальним та отриманими сигналами на виході розробленого алгоритму. Також встановлено, що застосування невірних ключі не погіршує статистичних характеристик скрембльованих сигналів.

Таким чином, застосувавши вейвлет перетворення для отримання відповідних коефіцієнтів та виконавши запропоновані операції вдалося підвищити захищеність аналогового скремблера. Застосування латинських квадратів в якості ключа системи є ефективною схемою перестановок, що не вносить значних затримок у канал зв'язку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конахович Г. Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов – К.: "МК-Пресс", 2005. — 288 с, ил.
2. Семеренко В.П. Реконструкция линейных скремблеров на основе автоматных моделей / В.П. Семеренко. – 2016. – 5с.
3. Сулименко Э.А. Методы скремблирования речевого сигнала / Э.А Сулименко. – 2017. – 5с
4. Методы и средства сокрытия данных путем скремблирования. [Електронний ресурс]. – Режим доступу: // https://ru.bmstu.wiki/ Методы_и_средства_сокрытия_данных_путем_скремблировния
5. Кукуш В.Д. Оценка эффективности применения полосовых скремблеров для защиты речевой информации в узкополосных системах связи / В.Д. Кукуш. – 2017. – 35с.
6. Калякін І.В Обнаружение и измерение характеристик локальных сигналов с помощью дискретного вейвлет преобразования // І.В. Калякін., СПб – 2018. –147с
7. Гарднер М. Новые математические развлечения // М. Гардер М.: АСТ—Астрель, 2009. — 319 с
8. Азарова А.О. Методичні вказівки до проведення практичних занять та до виконання самостійної індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 – «Менеджмент» та 6.170103 – «Управління інформаційною безпекою» / Азарова А.О., Карпінець В.В. – Вінниця: ВНТУ, 2013. – 44 с.

Гереш Денис Юрійович — студент групи УБ-19м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail:den.heresh@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** — кандидат технічних наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця

Heresh D.Y. — student, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnytsia, email : den.heresh@gmail.com

Supervisor: ***Karpinets Vasyl V.*** — Ph. D., assistant professor, Head of the Department of Management and Security of Information Systems, Vinnitsa National Technical University, Vinnytsia