Магістерська кваліфікаційна робота

На тему:

«Підвищення захищеності мовної інформації аналогового телефонного зв’язку на основі скремблера зі зміною коефіцієнтів вейвлет перетворення»

Виконав: студент групи УБ-19м Гереш Денис
Науковий керівник: к. т. н., доцент каф. МБІС: Карпінець Василь Васильович

Мета роботи: підвищення захищеності мовної інформації аналогового телефонного зв’язку на основі скремблера зі зміною коефіцієнтів вейвлет перетворень.

Актуальність обраної теми:

- ✓ залишається велика кількість аналогових засобів зв’язку;
- ✓ популярність телефонних мереж як засобів ведення переговорів;
- ✓ наявність великої кількості методів НСД до інформації в системах передачі;
- ✓ значна частина несанкціонованого перехоплення інформації припадає саме на телефонні розмови;
- ✓ вразливість існуючих скремблерів аналогового зв’язку.

Сфера застосування

Сьогоднішній науково-технологічний розвиток вимагає забезпечення високого рівня інформаційної безпеки.

Найбільш популярними засобами комунікації є аналогові, цифрові системи та радіозв’язок. Існування великої кількості загроз вимагає здійсненню відповідних заходів захисту.

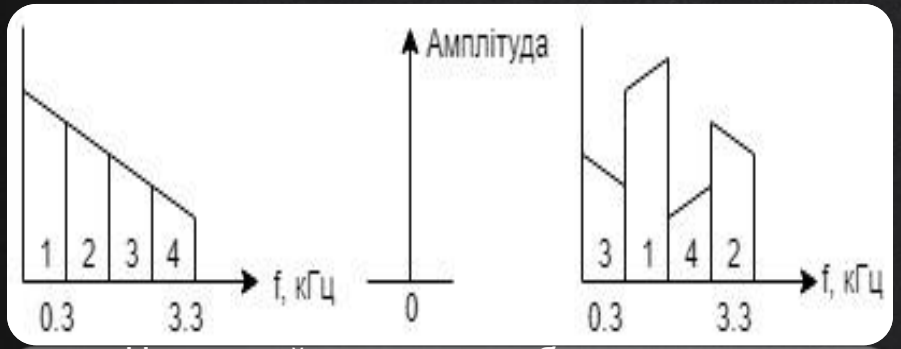
Серед всіх наявних методів захисту інформації в телекомунікаційних системах одним із найкращих методів захисту є застосування пристроїв шифрування сигналу в процесі його передачі каналом зв’язку – скремблерів.

Скремблер – це пристрій, призначений для шифрування мовної інформації, що передається по лінії зв’язку з подальший її відновленням до початкового стану використовуючи відповідну пару ключів.

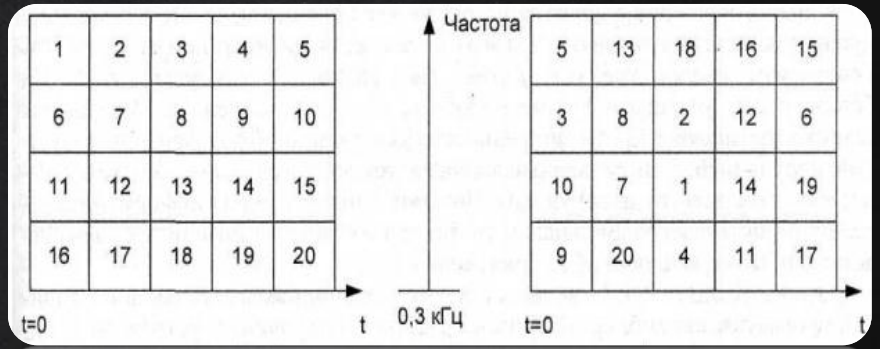
Типи скремблерів

- Аналогові
  - частотні;
  - часові;
  - комбіновані;
- Цифрові
  - застосування криптографічних алгоритмів;
  - застосування операції XOR інформації із створеною послідовністю;

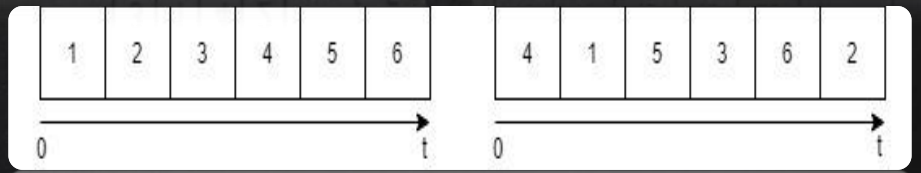
Аналогові скремблери



Частотний метод скремблювання

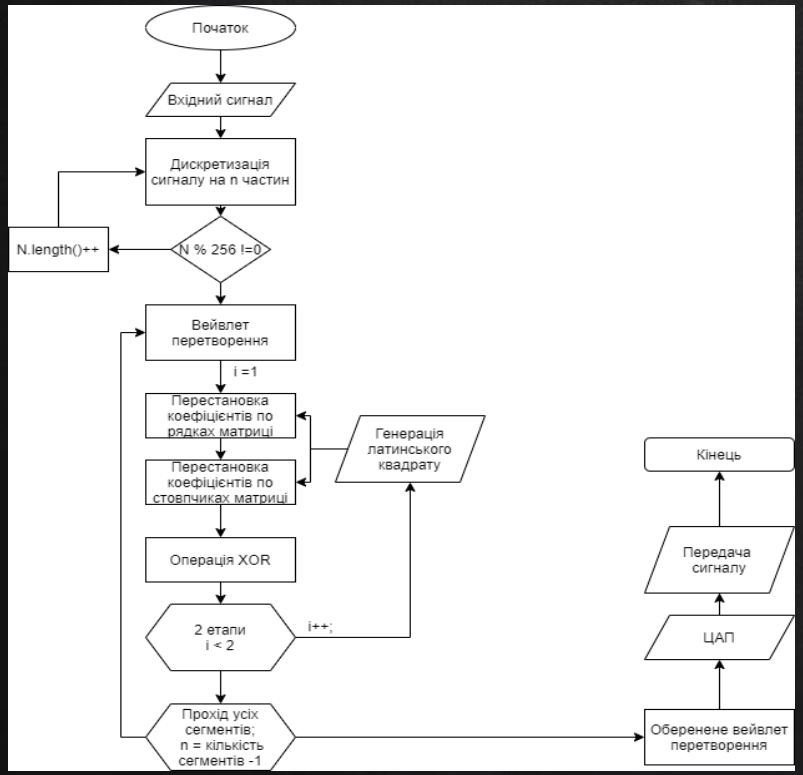


Комбінований метод



Часовий метод скремблювання

Алгоритм вдосконалення

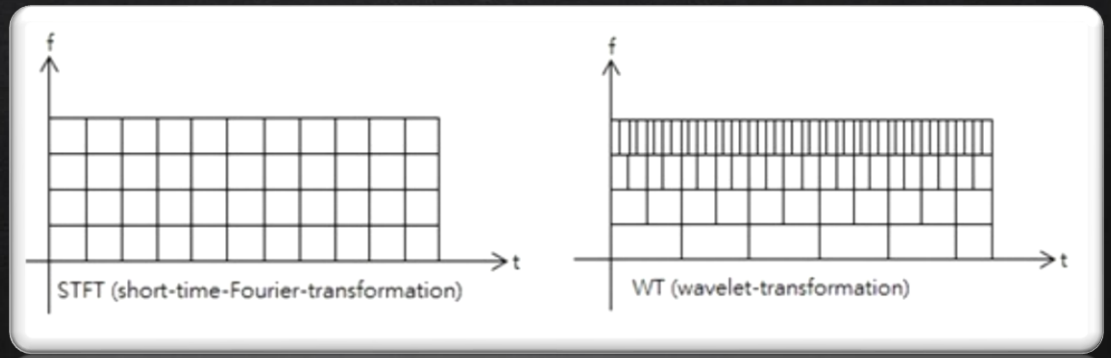


1 – Дискретне вейвлет перетворення
2 – Два етапи перестановки отриманих коефіцієнтів
3 – Два етапи операцій XOR з ключем
4 – Зворотне вейвлет перетворення

Вейвлет перетворення

Вейвлет перетворення — інтегральне перетворення сигналу у згортку вейвлет-функцій локалізованих у часі та частоті.

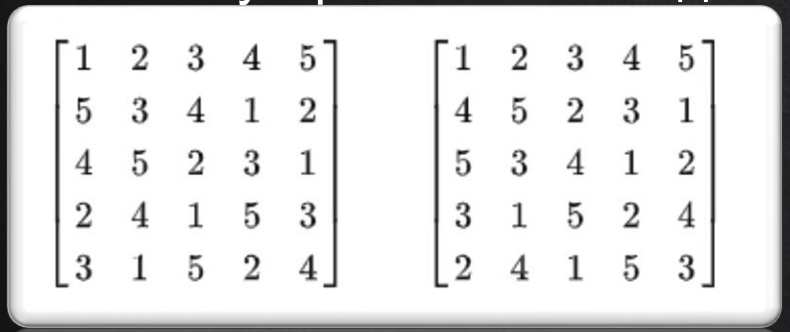
Завдяки своїм частотно-часовим властивостям вейвлет-перетворення є ефективним інструментом в скремблерах.



Розкладання сигналу Фур'є та Вейвлет перетворення

Латинський квадрат

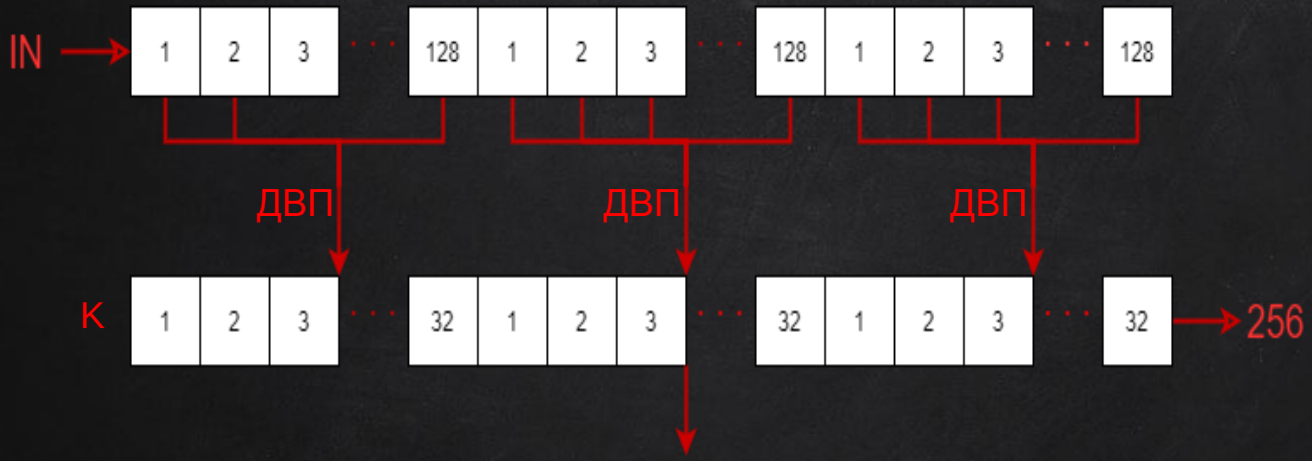
Латинський квадрат – таблиця розміру n × n заповнена n різними елементами так, що в кожному стовпці і кожному рядку всі елементи зустрічаються по одному разу



$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \\ 4 & 5 & 2 & 3 & 1 \\ 2 & 4 & 1 & 5 & 3 \\ 3 & 1 & 5 & 2 & 4 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \\ 5 & 3 & 4 & 1 & 2 \\ 3 & 1 & 5 & 2 & 4 \\ 2 & 4 & 1 & 5 & 3 \end{bmatrix}$$

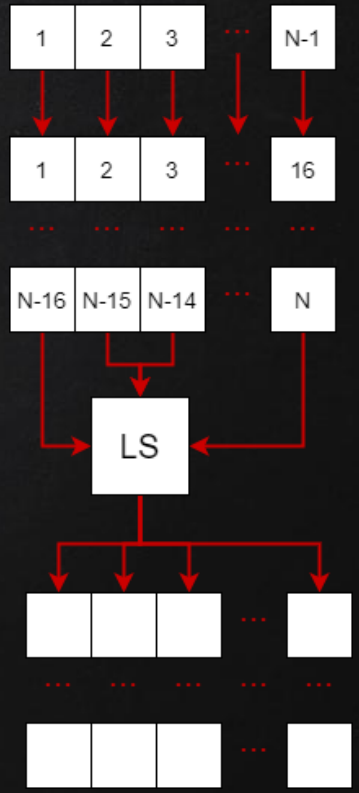
N	L(N)
3	12
5	161280
7	61479419904000
12	1.62 × 10^44

Алгоритм формування ключвих послідовностей



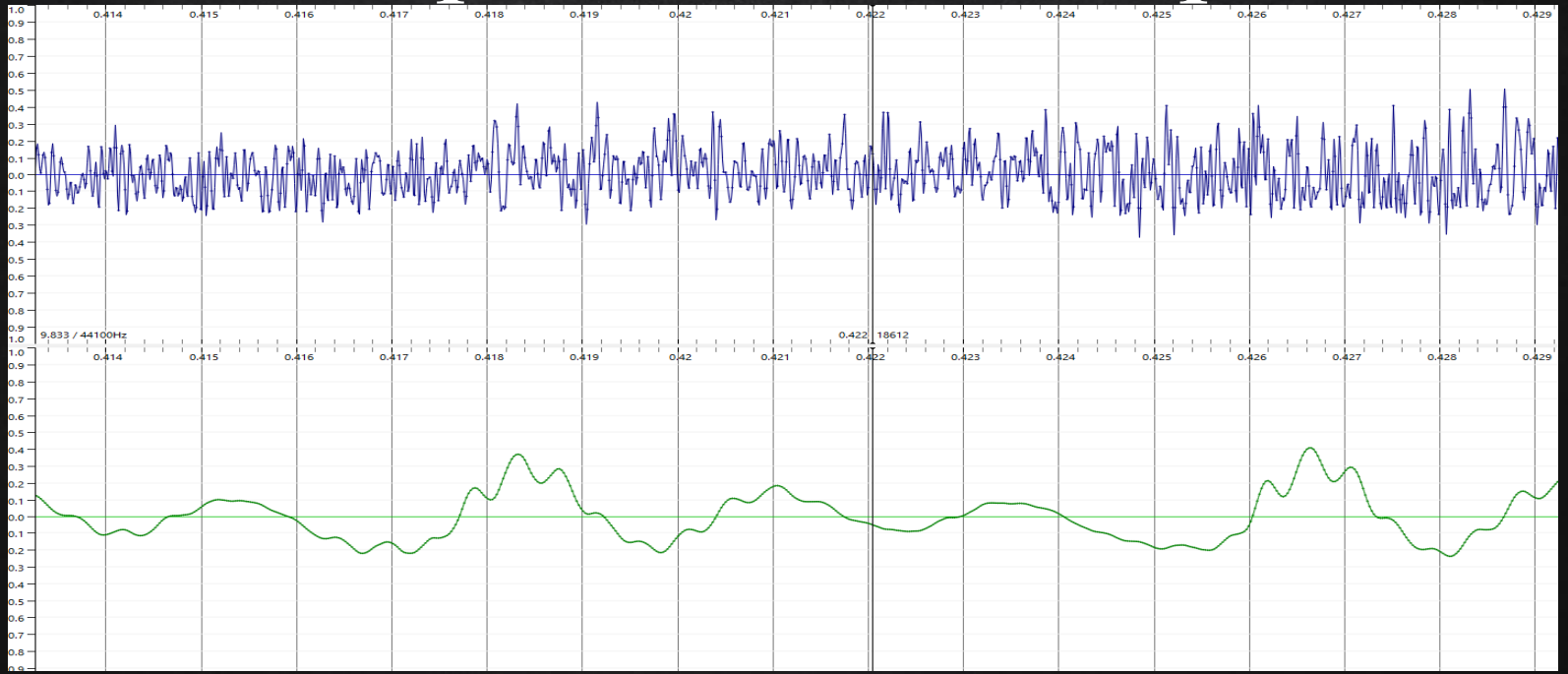
Формування N=256 послідовності

Ключові параметри $K = 2^{J-\iota}, \quad J = \log_2 N;$



Формування вихідної послідовностей

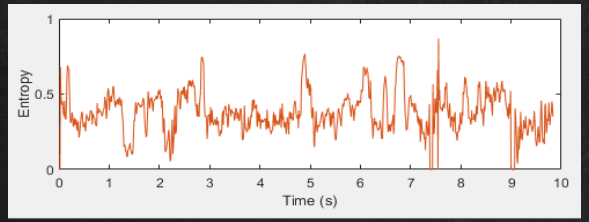
Порівняння спектрів

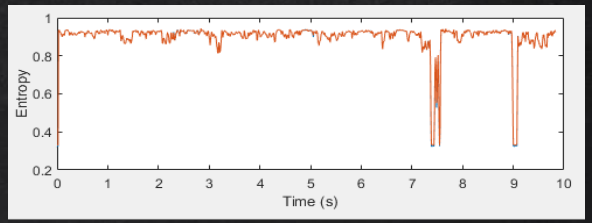


Синій – отриманий сигнал
Зелений – оригінальний сигнал

Тестування

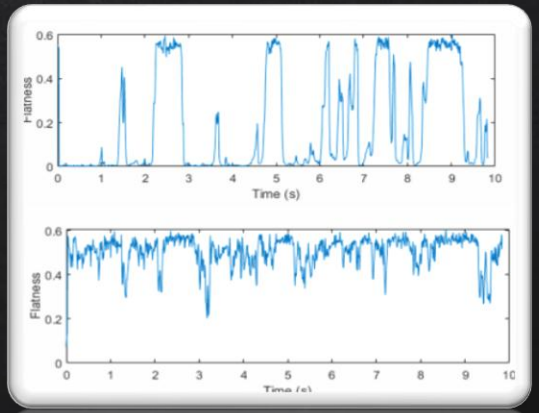
Ентропія



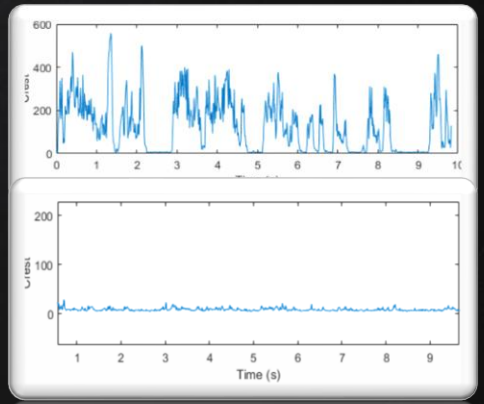


№	1	2	3	4	5
$S_{скрб}$	0.05006	0.043818	0.05582	0.030926	0.037227
$S_{дескр}$	0.99	0.99996	0.99	0.99995	0.99996
№	6	7	8	9	10
$S_{скрб}$	0.03727	0.03615	0.035524	0.03412	0.034752
$S_{дескр}$	0.99996	0.99994	0.99	0.99	0.999998

Кореляції



Ентропія Вінера



Коефіцієнти вершин

Дякую за увагу!