Гибридный метод шифрования аудиосигналов на основе DCT и преобразования Уолша–Адамара с использованием хаотических отображений Хенона и логистического отображения

Davit Hovhannisyan, Sergo Episkoposyan

National Polytechnic University of Armenia

Конференция 2025

Мотивация

- Рост цифровых коммуникаций усиливает необходимость защиты аудиоконтента.
- Классические методы (AES, LWT и др.) — либо медленные, либо недостаточно стойкие.
- Цель: **разработать гибридный метод шифрования аудиосигналов**, сочетающий криптостойкость и эффективность.

Основная идея

- Комбинация **DCT + WHT + хаотические карты (Хенон и логистическая)**.
- DCT — энерго-компакция, уменьшает избыточность.
- WHT — усиливает декорреляцию данных.
- Хаотические карты — обеспечивают псевдослучайность и запутанность.
- Ключ генерируется адаптивно из статистики аудиофрейма, без внешнего хранения.

Дискретное косинусное преобразование (DCT): идея

- DCT переводит сигнал из временной области в частотную, концентрируя энергию в низких частотах.
- Используется для сжатия и шифрования аудиосигналов.
- Формула прямого DCT:

$$X(u) = \frac{2}{N} c(u) \sum_{m=0}^{N-1} x[m] \cos\left(\frac{\pi(2m+1)u}{2N} \right),$$

где

$$c(u) = \begin{cases} \frac{1}{2}, & u = 0, \\ 1, & u > 0. \end{cases}$$

DCT: визуальное объяснение

- DCT можно рассматривать как разложение сигнала по базису косинусных волн.
- Низкочастотные коэффициенты несут основную энергию аудио.
- Высокочастотные — детали и шум.

Интерпретация

DCT «собирает» энергию сигнала в первые коэффициенты, что уменьшает количество данных, требующих шифрования.

DCT: свойства и применение

- Применяется в MP3, AAC, JPEG, MPEG и др.
- Обратимость DCT:

$$x[m] = \frac{2}{N} \sum_{u=0}^{N-1} c(u) X(u) \cos\left(\frac{\pi(2m+1)u}{2N}\right)$$

- Основные свойства:
  - Энергетическая компакция.
  - Линейность.
  - Устойчивость к шуму.

В нашем методе

DCT подготавливает аудио к шифрованию, снижая избыточность и повышая стойкость к ошибкам.

Преобразование Уолша–Адамара (WHT): основа

- WHT — ортогональное дискретное преобразование, использующее только значения ± 1.
- Построено на матрице Адамара:

$$H_1 = [1], \quad H_{2N} = \begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix}$$

- Прямое преобразование: $X = H_N x$
- Обратное: $x = \frac{1}{N} H_N X$

WHT: пример и вычислительная эффективность

- Для $N = 4$:

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

- Вычисляется с помощью **Fast Walsh–Hadamard Transform (FWHT)**.
- Сложность $O(N \log N)$, только сложения и вычитания — без умножений.

Преимущество

WHT быстро выполняется и подходит для систем реального времени.

WHT: свойства и значение для шифрования

- WHT равномерно распределяет энергию сигнала между коэффициентами.
- Повышает чувствительность — малое изменение входа вызывает глобальные изменения выходных данных.
- Снижает корреляцию между отсчётами сигнала на 15% по сравнению с DCT.
- Усложняет статистический анализ при криптоанализе.

Результат

После WHT сигнал становится похож на белый шум — идеальный вход для хаотического шифрования.

Отображение Хенона

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n, \\ y_{n+1} = bx_n \end{cases}$$

- Применяется для перестановки коэффициентов (Permutation).
- Параметры: $a = 3.58$, $b = 0.56$ — оптимальны для NPCR и UACI.
- Создаёт нелинейные перестановки, усиливающие запутанность данных.

Логистическое отображение

$$x_{n+1} = r x_n (1 - x_n)$$

- Используется для операции замены (Substitution).
- При $r = 3.99$ система находится в полностью хаотическом режиме.
- Генерирует псевдослучайный поток ключей для XOR-подстановки.
- Обеспечивает высокую чувствительность к начальному значению x_0.

Бифуркационная диаграмма логистического отображения

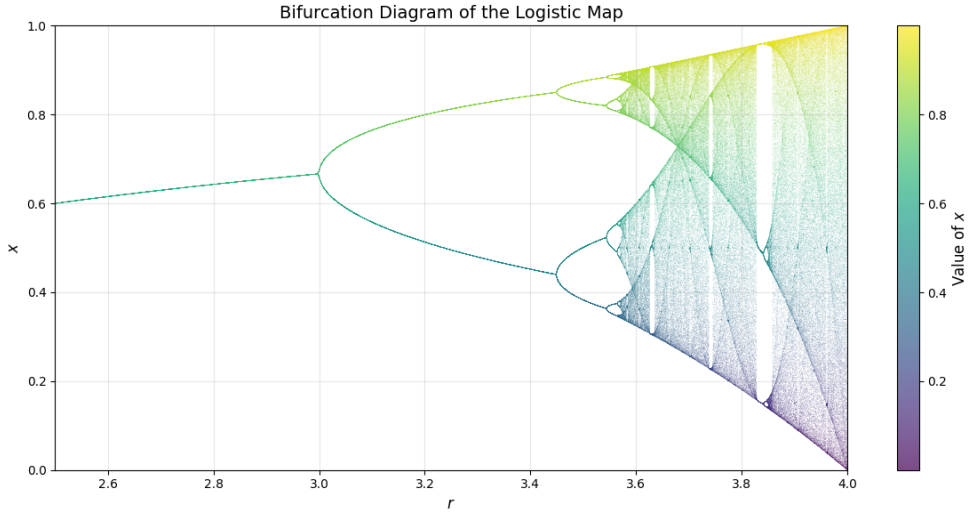

Рис : Бифуркационная диаграмма логистического отображения при изменении параметра r

Процесс шифрования

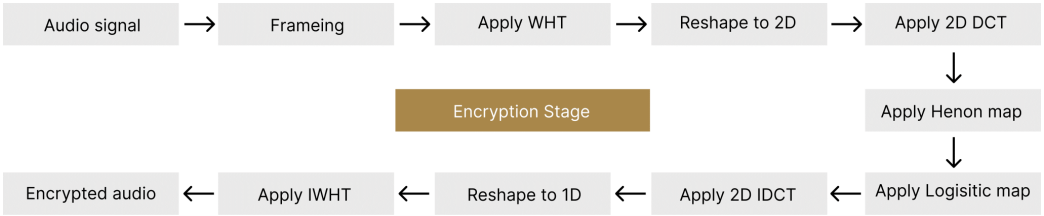

Рис.: Блок-схема шифрования

Этапы

Фреймирование аудио → DCT и WHT → перестановка (Хенон) → замена (логистическая карта)

Процесс дешифрования

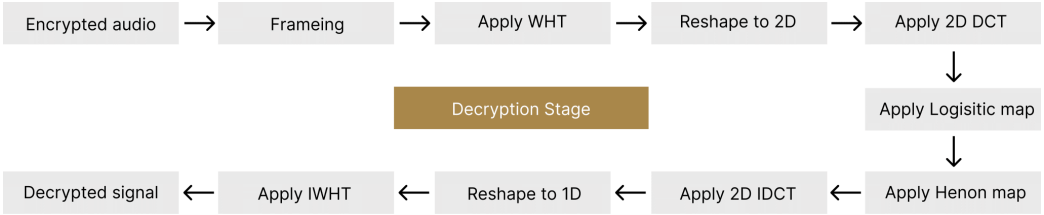

Рис.: Блок-схема дешифрования

Этапы

1. Инверсия логистической карты $\rightarrow$ 2. Henon $\rightarrow$ 3. IWHT и IDCT

Исходный аудиосигнал и гистограмма

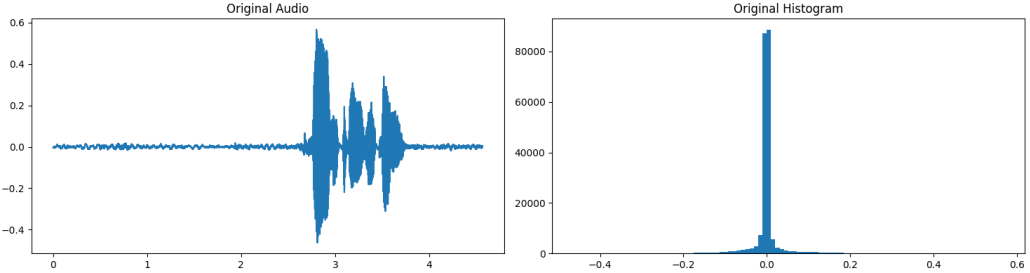

Рис.: Исходный сигнал и его гистограмма распределения

Зашифрованный аудиосигнал и гистограмма

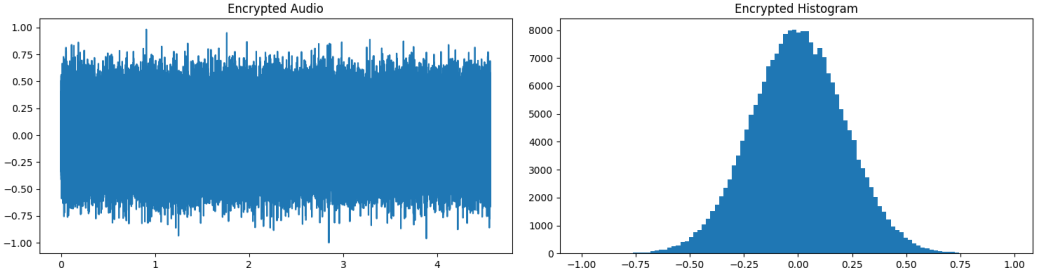

Рис.: Зашифрованный сигнал и его гистограмма

Сравнение методов: корреляция и MSE

Метод	Корреляция	MSE
DCT+WHT+Henon	0.000586	0.0205
DCT+Henon	0.000642	0.1370
WHT+Henon	0.000507	0.0206
Henon+LWT	0.000454	0.0354

Вывод

Комбинация DCT+WHT+Henon обеспечивает минимальную корреляцию и наименьшее среднеквадратичное отклонение (MSE).

Энтропия, NPCR и UACI

Показатель	Наш метод	Henon+LWT
Энтропия	5.18 бит	5.86 бит
NPCR	97.63%	98.47%
UACI	6.67%	15.57%

Вывод

Метод демонстрирует высокую энтропию и устойчивость к изменениям пикселей (NPCR), однако требует оптимизации параметров для повышения диффузии (UACI).

Выводы

- Разработан гибридный метод аудиошифрования на основе DCT, WHT и хаотических отображений.
- Метод обеспечивает высокую точность восстановления (RMSE = 0.0205).
- Ключ генерируется адаптивно, без хранения.
- Баланс между скоростью и безопасностью.

Thank You!