

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В АУДІОСИГНАЛАХ

Ткаченко О.Р., Садовий М.С., В'юхін Д.О.

Харківський Національний університет радіоелектроніки, м. Харків, Україна

Зростання обсягів передавання мультимедійних даних та поширення мережевих сервісів створює нові виклики у сфері інформаційної безпеки. В умовах, коли традиційні криптографічні підходи можуть привертати увагу потенційного зловмисника, методи приховування інформації в аудіосигналах дозволяють забезпечити не лише захист змісту повідомлення, але й сам факт його існування.

Частотні алгоритми та адаптивні психоакустичні методи є сучасними підходами до приховування інформації в аудіосигналах. Порівняння цих алгоритмів дозволяє оцінити їхні переваги та обмеження для практичного застосування [1].

Мета роботи полягає у проведенні порівняльного аналізу частотних алгоритмів та адаптивних психоакустичних методів приховування інформації в аудіосигналах, а також у визначенні їх ефективності за ключовими критеріями - прихованістю, стійкістю до обробки, ємністю даних і складністю реалізації.

У межах роботи передбачається дослідити особливості функціонування FFT-алгоритму, адаптивних психоакустичних підходів і базових методів стеганографії, встановити їх переваги та обмеження, а також обґрунтувати доцільність використання кожного з них залежно від вимог конкретної інформаційної системи.

У сучасній стеганографії важливо оцінювати ефективність алгоритмів не лише за технічними характеристиками, а й за практичними критеріями, такими як прихованість, стійкість до обробки та ємність даних.

У випадку використання методу прихованих символів (LSB або подібних підходів) зміни відбуваються на рівні окремих бітів цифрового представлення сигналу. Такі модифікації є мінімальними та практично не впливають на загальну структуру аудіофайлу. Однак через відсутність урахування особливостей людського слуху ці зміни можуть бути виявлені при детальному аналізі або після обробки сигналу (наприклад, стиснення чи фільтрації).

При застосуванні FFT-алгоритму зміни відбуваються у частотній області сигналу. Модифікуються амплітуди або фази окремих спектральних компонентів, що дозволяє більш гнучко контролювати вплив на сигнал. У результаті аудіофайл зазнає структурних змін у спектрі, але при цьому зберігає прийнятну якість звучання. Такі зміни є менш помітними для користувача, однак можуть бути виявлені при спектральному аналізі.

Адаптивні психоакустичні алгоритми змінюють аудіосигнал з урахуванням моделей сприйняття звуку людиною. Інформація вбудовується у ті частини сигналу, які маскуються більш гучними або домінуючими компонентами. У цьому випадку зміни є найбільш складними за структурою,

оскільки вони динамічно залежать від характеристик сигналу. Це забезпечує високий рівень прихованості, а самі модифікації практично неможливо виявити без спеціалізованого аналізу [2].

Результати аналізу ефективності алгоритмів за технічними характеристиками та практичними критеріями представлені у таблиці 1.

Таблиця 1 – Ефективність алгоритмів за технічними характеристиками та практичними критеріями

Критерій	Метод прихованих символів	FFT-алгоритм	Адаптивний психоакустичний алгоритм
Прихованість	40%	60%	90%
Стійкість до обробки	20%	70%	95%
Ємність даних	30%	60%	40%
Складність реалізації	10%	50%	80%

З аналізу таблиці видно, що давні алгоритми, хоча й прості у реалізації, мають низьку прихованість і стійкість, а їхня ємність обмежена [3]. FFT-алгоритм забезпечує середній рівень прихованості та достатню стійкість до стандартної обробки, зберігаючи при цьому помірну ємність даних. Адаптивний психоакустичний метод демонструє максимальну прихованість та стійкість, проте має обмежену ємність і високу складність реалізації.

FFT-алгоритм підходить для задач із середньою прихованістю та стійкістю, де важлива простота реалізації.

Адаптивний психоакустичний метод ефективний для систем з підвищеними вимогами до прихованості та стійкості, хоча має нижчу ємність та вищу складність реалізації. Вибір алгоритму визначається пріоритетами конкретної системи.

Список літератури

1. Голубничий, Д.Ю., Северінов, О.В., Коломійцев, О.В., Місюра, О.М., Третяк, В.Ф., Власов, А.В., Крук, Б.М. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загрозами: кібербезпеки, інформаційної безпеки та безпеки інформації.
2. Zhang J., Li S. A Survey of Audio Steganography. Journal of Information Security. 2018. 327 p.
3. Картушин, О. А. Дослідження моделей приховування інформації в мультимедійних даних з використанням стеганографічних перетворень.
4. Bhat V., Kamath S. Audio Steganography Techniques: A Review. International Journal of Computer Applications. 2015. 289 p.