

РЕАЛІЗАЦІЯ МЕТОДУ БЛОКОВОГО ПРИХОВУВАННЯ ТЕКСТОВОГО ПОВІДОМЛЕННЯ У ЗВУКОВИХ ФАЙЛАХ

Хомич І. В.

Кухарська Н. П., ЛДУ БЖД, доцент, канд. фіз.-мат. наук, доцент

До аудіо-сигналів можна застосувати як методи стеганографічних перетворень, що придатні для всіх мультимедіа контейнерів (наприклад, метод заміни молодших значущих біт), так і методи, що враховують особливості аудіо-даних і слухової системи людини (ССЛ). ССЛ хоч і працює в широкому динамічному і частотному діапазонах, проте має деякі особливості, які можна використати для приховування інформації, наприклад, можливість впровадження повідомлень в абсолютну фазу (відносна різниця фаз при цьому залишається незмінною), можливість використання шумових контейнерів, а також можливості, засновані на ефектах пре- і пост-маскування.

Методи впровадження даних в аудіофайли діляться на дві групи.

До першої групи належать методи, які здійснюють приховування в просторово-часовій області. Наприклад, метод заміни молодших значущих біт контейнера або LSB-метод (з англійської “Last Significant Bit”) [1]; DSSS-метод (з англійської “Direct Sequence Spread Spectrum encoding” – пряме послідовне розширення спектра), розроблений Bender W. і Morimoto N. [2]; метод Bassia P. і Pitas I. амплітудної модифікації сигналу з псевдовипадковим розподілом повідомлення по контейнеру [3].

До другої групи методів, які здійснюють приховування в частотній області, відносяться, наприклад, метод Bender W. і Morimoto N. впровадження інформації шляхом модифікації фази аудіо-сигналу [4], метод M.Ramkumar і Ali N. Akansu, заснований на модифікації коефіцієнтів дискретного перетворення Фур’є.

Мета цієї роботи – описати стеганографічний метод блокового приховування повідомлення у звукових файлах, алгоритмів його реалізації і створених на їх основі програмних продуктів.

Метод блокового приховування належить до, так званих, LSB-методів. У LSB-методі вбудовування повідомлень здійснюється в молодші найменш значущі біти (НЗБ) файлу-контейнера. Вважається, що молодші біти аудіо- та відеоінформації, представленої в форматах файлів без втрат, не несуть істотних відомостей про сигнал, тому що перебувають на рівні шуму. Людина не здатна помітити зміни в цих бітах. Фактично молодші біти є похибкою в будь-якому медіа форматі, для якого кількість біт у відліку дорівнює вісьмом або більше. У таких форматах неможливо ні візуально, ні на слух виявити наявність прихованого повідомлення.

Опишемо алгоритм методу блокового приховування інформації, який є більш стеганостійкий у порівнянні з класичним LSB-методом. ASCII-коди символів текстового повідомлення, що необхідно приховати, подаємо у вигляді вектора бітів. Послідовність звукових амплітуд файла-контейнера розбиваємо на n блоків, де n – кількість біт повідомлення. Приховуючи i -ий біт повідомлення, здійснюємо такі дії. В i -ому блоці аудіо-файла сумуємо за модулем 2 НЗБ усіх його елементів. Отриману суму порівнюємо із значенням біта повідомлення. Якщо вони не дорівнюють один одному, інвертуємо НЗБ будь-якого, обраного випадковим чином, елемента блоку. У підсумку отримуємо, що у кожному блоці аудіо-сигнала буде “зашито” по одному бітові повідомлення. Під час процедури видобування їх отримуємо, додаючи за модулем 2 НЗБ елементів блоків.

Розроблений нами комплекс програм приховує записані у TXT-файлах повідомлення в аудіофайли формату WAVE будь-якої частоти дискретизації та бітності.

На рис. 1 подані осцилограми порожнього контейнера та контейнера з вбудованим повідомленням. Порівнюючи їх, не зауважуємо жодних візуальних змін.

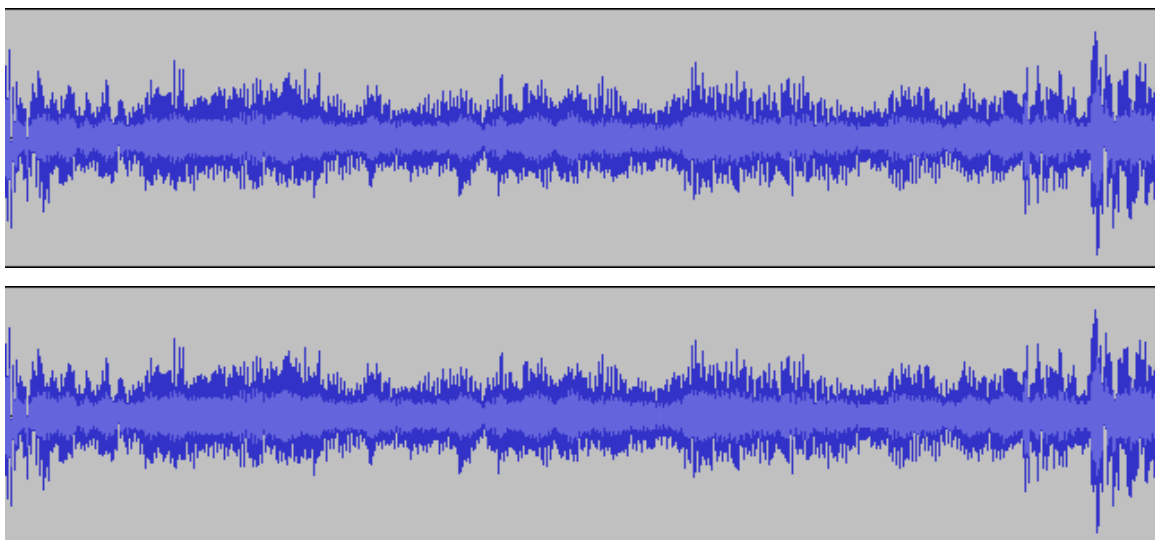


Рис. 1. Осцилограми порожнього контейнера та контейнера з вбудованим повідомленням

ЛІТЕРАТУРА

1. Arnold, M. MP3 robust audio watermarking / M. Arnold, S. Kanka // Proceedings of International Watermarking Workshop, Erlangen, Germany, October 5-6, 1999. – Fraunhofer-Publica, 1999. – P. 382-392.
2. Techniques for Data Hiding / W. Bender [et al.] // IBM systems journal. – 1996. – Vol. 35, № 3-4. – P. 313-336.
3. Bassia, P. Robust audio watermarking in the time domain / P. Bassia, I. Pitas // Multimedia, IEEE Transactions on. – 2001. – Vol. 3, № 2 – P. 232-241.
4. Applications for data hiding / W. Bender [et al.]// IBM Systems Journal. – 2000. – Vol. 39, № 3-4. – P. 547-568.