УДК 621.391.01

Вовчук Д. А.

МОДЕЛЮВАННЯ СИСТЕМИ ПЕРЕДАВАННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ З ДОПОМОГОЮ ХАОТИЧНОГО МАСКУВАННЯ

У роботі розглянуто питання використання схеми хаотичного маскування для прихованого передавання цифрової інформації, де хаотичне коливання генероване схемою Чуа використовується в якості носійного сигналу. Інформаційний сигнал представляє собою хаотичне або шумове коливання, яке попередньо модульоване цифровим сигналом. Досліджено умови прихованості сигналу у каналі зв'язку та можливість відновлення інформації на приймальній стороні.

Ключові слова: *хаотичне маскування, цифровий сигнал, приховане передавання, ведучий та ведений генератори.*

1. Вступ

Сучасний стан телекомунікацій вимагає розробки нових цифрових систем зв'язку. Не останнє місце у вирішенні цих питань займають проблеми захисту інформації [1, 2]. Прихованість інформації, що передається, базується на використанні систем детермінованого хаосу, де генерований хаотичною системою сигнал, виконує роль носійного коливання. Це пов'язано із тим, що хаотичні коливання володіють великою інформаційною ємністю та суцільним спектром, що займає широку смугу частот.

Використання систем детермінованого хаосу у телекомунікація залежить від якості хаотичної синхронізації систем, що взаємодіють [3, 4]. Існує декілька видів хаотичної синхронізації та методів введення інформації у носійне коливання [5–9].

Метою даної роботи є дослідження модифікованої схеми хаотичного маскування для прихованого передавання інформації з допомогою MatLab-Simulink моделі.

2. Дослідження схеми хаотичного маскування

Хаотичне маскування є одним із способів передавання інформації з використанням синхронізації хаосу, що полягає у адитивному додаванні інформаційного сигналу до носійного коливання [10, 11]. Детальні дослідження показали її низький рівень прихованості та завадостійкості для практичного використання при передаванні цифрових сигналів.

Для підвищення прихованості передаваної інформації нами запропоновано використовувати попередню модуляцію інформаційного сигналу хаотичним або шумовим зі спектральними характеристики, близькими до носійного хаотичного коливання. З метою спрощення схеми у якості інформаційного сигналу можна використовувати інший хаотичний сигнал того ж генератора.

У роботі в якості ведучого генератора використано схему Чуа, яка у результаті декомпозиції розбивається на дві підсистеми, з'єднані у єдине кільце оберненого зв'язку і представляє собою автоколивальну систему. У веденому генераторі кільце оберненого зв'язку розірвано, в результаті чого він стає пасивним і при однонаправленому зв'язку та ідентичності параметрів взаємодіючих систем повторює динаміку ведучого генератора, тому можна говорити про встановлення хаотичного синхронного відгуку [6]. Маскування корисної інформації відбувається шляхом її адитивного додавання до носійного коливання. Схема такої системи наведена на рис. 1. Використання сигналу W_1 у якості інформаційного є доцільним, оскільки дослідження показали, що спектр потужності сигналу V_1 повністю перекриває спектр потужності W_1, що підвищує рівень прихованості інформації у каналі зв'язку (рис. 2).

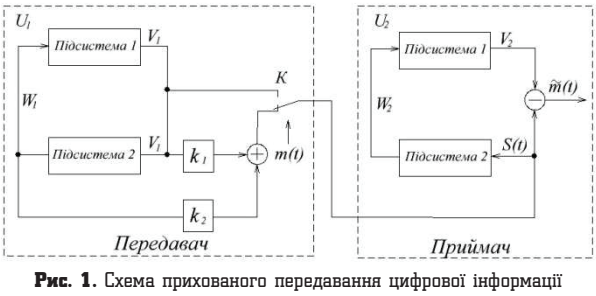

Рис. 1. Схема прихованого передавання цифрової інформації з використанням маскування хаотичного сигналу

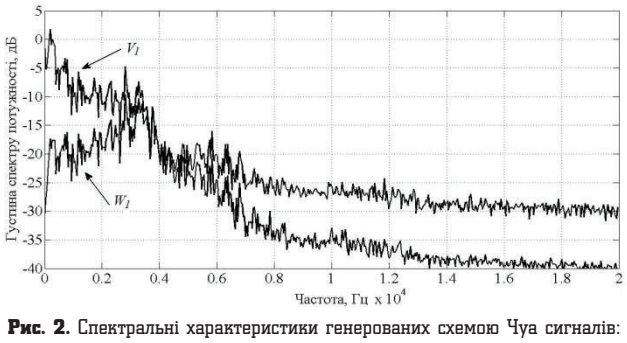

Рис. 2. Спектральні характеристики генерованих схемою Чуа сигналів: V_1 — носійного; W_1 — інформаційного

У канал зв'язку подається сигнал, що отримується в результаті виконання наступної умови:

$$S(t)=\begin{cases}V_1, & \text{якщо } m(t)=1;\\ k_1V_1+k_2W_1, & \text{якщо } m(t)=0,\end{cases} \quad (1)$$

де k_1 використовується для того, щоб сигнали, що відповідають різним бітам, не можна було розрізнити за значенням їх енергії, k_2 — коефіцієнт підсилення сигналу W_1.

В результаті віднімання вхідного сигналу приймача та вихідного сигналу підсистеми 1 веденого генератора при відсутності шумів отримаємо:

$$\tilde{m}(t)=\begin{cases}0, & \text{якщо } m(t)=1;\\ (1-k_1)V_1-k_2W_1, & \text{якщо } m(t)=0.\end{cases} \quad (2)$$

Для оцінки працездатності схеми була розроблена її імітаційна модель у середовищі Simulink (рис. 3) відповідно до математичної моделі системи:

$$\begin{cases}\dot{x}_1=\alpha(y_1-x_1-f(x_1));\\ \dot{y}_1=x_1-y_1+z_1;\\ \dot{z}_1=-\beta y_1;\\ \dot{x}_2=\alpha(y_2-x_2-f(x_2));\\ \dot{y}_2=S(t)-y_2+z_2;\\ \dot{z}_2=-\beta y_2,\end{cases} \quad (3)$$

де α та β — параметри керування системи; x_i, y_i, z_i — динамічні змінні, при чому i = 1, 2, що відповідає ведучій та веденій системам.

Нелінійний елемент реалізовано у вигляді окремої підсистеми і позначений на схемі Nr. Для імітування сигналу повідомлення використано блок Pulse Generator. Блок Band-Limited White Noise використовується для моделювання впливу завад у каналі зв'язку.

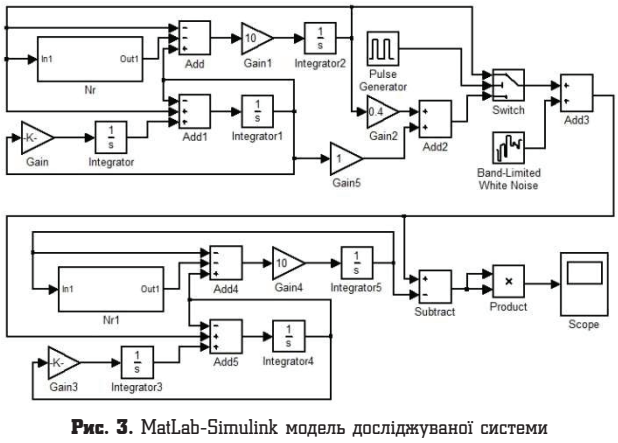

Рис. 3. MatLab-Simulink модель досліджуваної системи

Результат дослідження моделі системи наведений на рис. 4, з якого випливає, що у випадку відсутності шумів у каналі зв'язку, відновити інформаційний сигнал можна з високою імовірністю (рис. 4, *в*). З допомогою варіювання величиною значення коефіцієнтів k_1 та k_2 було досягнуто рівного значення енергій бітів «0» та «1». Із часової діаграми сигналу у каналі зв'язку випливає, що візуально неможливо розрізнити, який з інформаційних бітів передано (рис. 4, *б*).

Наявність шумів у каналі зв'язку призводить до спотворення інформації та некоректного її відновлення. Для підвищення рівня ймовірності безпомилкового відновлення, необхідно збільшити тривалість біту, а також потужність інформаційного сигналу, щоб досягти необхідного рівня відношення сигнал/шум. Осцилограми інформаційного сигналу та сигналів у каналі зв'язку та на виході приймача наведені на рис. 5.

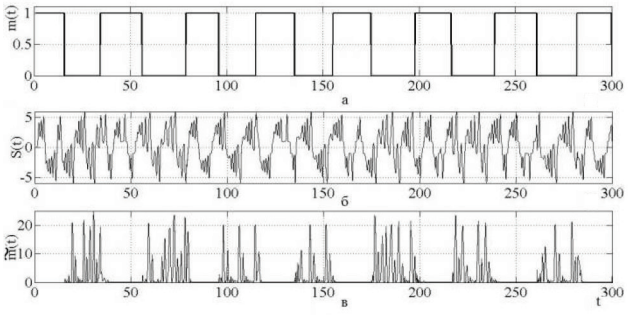

Рис. 4. Часові діаграми сигналів при використанні модуляції інформаційного сигналу хаотичним: *а* — інформаційний; *б* — у каналі зв'язку без шуму; *в* — відновлений сигнал

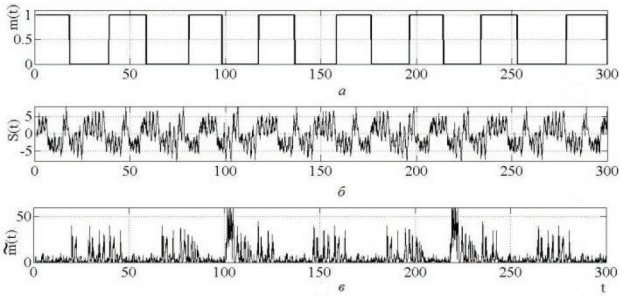

Рис. 5. Часові діаграми сигналів у каналі зв'язку та вихідного сигналу пристрою віднімання: *а* — інформаційний; *б* — у каналі зв'язку; *в* — відновлений сигнал

У якості інформаційного сигналу можна використовувати шумовий сигнал. Проте прихованість інформації може погіршитись, оскільки шумовий сигнал є широкосмуговим. Як і у випадку використання хаотичного сигналу, для ідеального каналу відновлення інформації є нескладною задачею (рис. 6).

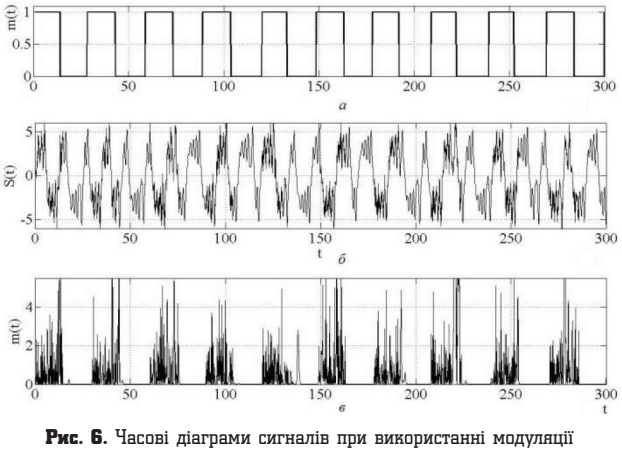

Рис. 6. Часові діаграми сигналів при використанні модуляції інформаційного сигналу шумовим: *а* — інформаційний; *б* — у каналі зв'язку без шуму; *в* — відновлений сигнал

Наявність шуму у каналі зв'язку потребує збільшення рівня потужності інформаційного сигналу унеможливлює виявлення бітів за допомогою аналізу часової діаграми сигналу (рис. 7, *б*).

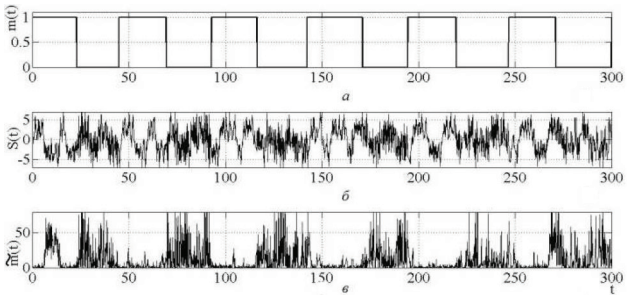

Рис. 7. Часові діаграми сигналів при використанні модуляції інформаційного сигналу шумовим: *а* — інформаційний; *б* — у каналі зв'язку з шумом; *в* — відновлений сигнал

3. Висновки

Дослідження моделі системи передавання цифрової інформації з використанням схеми хаотичного маскування показали потенційну придатність до практичного використання у системах зв'язку. Основною проблемою при відновленні інформації є перехідний процес при перемиканні бітів повідомлення та наявність шумів у каналі зв'язку. Вирішення цих питань вимагає пошуку компромісу між зменшенням рівня прихованості та швидкості передавання.

Література

1. Скопа, О. О. Принципи вибору формальних параметрів при побудові профілей захисту інфоресурсів [Текст] / Ю. В. Щербина, С. Л. Волков, О. О. Скопа // Восточно-Европейский журнал передовых технологий. — 2012. — Т. 5, № 2(59). — С. 31—33.
2. Скопа, О. О. Статистичне тестування симетричних криптографічних перетворень [Текст] / О. О. Скопа // Східно-Європейський журнал передових технологій. — 2011. — Т. 4, № 9(52). — С. 15—18.
3. Goldobin, D. S. Synchronization desynchronization of selfsustained by common noise [Text] / D. S. Goldobin, A. S. Pikovsky // Phys. Rev. E. — 2005. — Vol. 71, № 4. — 045201.
4. Пиковский, А. С. Синхронизация. Фундаментальное нелинейное явление [Текст] / А. С. Пиковский, М. Г. Розеблюм, Ю. Куртс. — М.: Техносфера, 2007. — 496 с.
5. Галюк, С. Д. Особливості синхронізації хаотичних систем (огляд) [Текст] / С. Д. Галюк, Л. Ф. Політанський, М. Я. Кушнір, Р. Л. Політанський // Складні системи і процеси. — 2011. — № 2. — С. 3—29.
6. Дмитриев, А. С. Динамический хаос: новые носители информации для систем святи [Текст] / А. С. Дмитриев, А. И. Панас. — М.: Издательство Физико—математической литературы. — 2002. — 252 с.
7. Политанский, Л. Ф. Непрерывная и импульсная синхронизация работы генераторов Чуа [Текст] / С. Д. Галюк, О. М. Элияшив, Л. Ф. Политанский, Н. Я. Кушнир, В. С. Танасюк // Технология и конструирование в электронной аппаратуре. — 2012. — № 1. — С. 21—26.
8. Политанский, Р. Л. Исследование зависимости корреляции между несущим и информационным сигналом в системах с динамическим хаосом [Текст] / Р. Л. Политанский, Л. Ф. Политанский, С. Д. Галюк, Н. Я. Кушнир // Восточно-Европейский журнал передовых технологий. — 2011. — № 2/3(50). — С. 58—63.
9. Политанский, Р. Л. Исследование свойств цикличности псевдослучайных последовательностей битов [Текст] / Р. Л. Политанский, Л. Ф. Политанский, М. Я. Кушнир // Восточно-Европейский журнал передовых технологий. — 2009. — № 6/2(42). — С. 64—66.
10. Политанский, Л. Ф. Хаотическое маскирование информационных сигналов с использованием генератора на базе системы Лю [Текст] / П. В. Иванюк, Л. Ф. Политанский, Р. Л. Политанский, О. М. Элияшив // Технология и конструирование в электронной аппаратуре. — 2012. — № 3. — С. 11—17.
11. Короновский, А. А. О применении хаотической синхронизации для скрытой передачи информации [Текст] / А. А. Короновский, О. И. Москаленко, А. Е. Храмов // ЖТФ. — 2009. — Т. 179, № 12. — С. 1282—1310.

МОДЕЛИРОВАНИЕ СИСТЕМЫ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ ХАОТИЧЕСКОГО МАСКИРОВАНИЯ

В работе рассмотрен вопрос использования схемы хаотического маскирования для скрытой передачи цифровой информации, где хаотическое колебание генерированное схемой Чуа используется в качестве сигнала носителя. Информационный сигнал представляет собой хаотическое или шумовое колебание, которое предварительно модулированное цифровым сигналом. Исследованы условия скрытости сигнала в канале связи та возможность восстановления информации в приемнике.

Ключевые слова: хаотическое маскирование, цифровой сигнал, скрытая передача, ведущий и ведомый генераторы.

***Вовчук Дмитро Анатолійович**, асистент, кафедра радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Україна, **e-mail: dimavovchuk@gmail.com**.*

***Вовчук Дмитрий Анатольевич**, ассистент, кафедра радиотехники и информационной безопасности, Черновицкий национальный университет имени Юрия Федьковича, Украина.*

Vovchuk Dmutro**, Yuriy Fedkovych Chernivtsi National University, Ukraine, **e-mail: dimavovchuk@gmail.com