

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ ИЗБЫТОЧНЫХ КОДОВ И ИХ ПРИМЕНЕНИЕ В СТЕГАНОГРАФИИ

Стеганография – наука о передаче сокрытых данных внутри других, открытых данных [1]. Стеганография делает сообщение незаметным, пряча его в других данных тем или иным способом.

Избыточные коды в стеганографии относятся к методам использования дополнительной информации или структуры данных внутри сокрытых сообщений.

Одним из методов использования избыточных кодов в стеганографии является «кодирование ошибок». В этом методе используются дополнительные биты, кодирующие информацию об ошибках, которые могут возникнуть при передаче или изменении данных.

Другой метод использования избыточных кодов в стеганографии основан на принципе «канального кодирования». В этом случае дополнительные биты кодируются вместе с исходными данными, что обеспечивает дополнительную защиту от ошибок и помогают восстановить исходные данные при наличии искажений или потерь.

Избыточные коды могут быть использованы для сокрытия информации внутри структуры данных носителя. При извлечении данных, например, из пикселей изображения эти дополнительные биты будут служить для обнаружения и коррекции ошибок.

К современным избыточным кодам относятся фонтанные коды (fountain code) и коды с малой плотностью проверок на чётность (LDPC).

Фонтанные коды представляют собой класс кодов стирания со свойством, заключающимся в том, что неограниченная последовательность символов кодирования может быть сгенерирована из заданного набора исходных символов таким образом, что исходные символы в идеале могут быть восстановлены из любого подмножества символов кодирования соответствующего размера равно или лишь немного больше количества исходных символов [2].

Фонтанные коды применяются в стеганографии при встраивании информации в контейнер, например, в виде изображений, аудиофайлов, видеофайлов, текстовых файлов, чтобы обеспечить конфиденциальность и незаметность передачи сообщений.

Процесс встраивания скрытой информации включает генерацию фонтанных кодов. Затем эти кодовые символы встраиваются в носитель с помощью различных методов.

Преимущества фонтанных кодов:

- гибкость и эффективность, так как они позволяют генерировать и встраивать неограниченное количество кодовых символов в носитель;
- устойчивость к атакам, так как они обладают высокой способностью обнаруживать и исправлять ошибки;
- расширяемость, так как они могут быть легко адаптированы для передачи различных типов данных;
- возможность отправлять данные по ненадежным каналам связи;
- обеспечение высокой эффективности передачи данных, так как они могут достигать предела Шеннона;
- возможность адаптации к изменяющимся условиям канала, так как они способны компенсировать потери и помехи в канале путем простой передачи дополнительных кодовых символов.

LDPC (low-density parity-check) коды являются классом линейных блочных избыточных кодов, которые широко используются в области кодирования и коррекции ошибок [3]. Отличием от большинства блочных кодов является определение их как low-density: их матрицы проверки на четность должны быть разреженными, то есть это коды, заданные матрицей проверки четности, содержащей в основном нули и лишь небольшое количество единиц.

LDPC коды используются в стеганографии для скрытой передачи информации в носителях, например, в изображениях, аудиофайлах, видеофайлах, текстовых файлах.

Одним из методов внедрения скрытой информации с использованием LDPC кодов в стеганографии является «стеганография на основе изменения четности». В этом методе, сообщение, представляется в виде битового вектора, который затем кодируется с использованием LDPC кода в дополнительные биты, называемые битами изменения четности. Эти биты изменения четности добавляются к носителю различными методами согласно LDPC коду.

Использование LDPC кодов в стеганографии позволяет достичь эффективной и незаметной передачи данных, так как они имеют низкую плотность проверочной матрицы и хорошие способности коррекции ошибок.

Преимущества LDPC-кодов:

- низкая плотность проверочной матрицы, что упрощает процесс кодирования и декодирования данных;
- обладание близкой к пределу Шеннона способностью коррекции ошибок;
- возможность использования в стандартах беспроводной связи.

В данной работе был произведен сравнительный анализ рассмотренных современных избыточных кодов: фонтанного кода и LDPC кода; и известного избыточного кода Хэмминга. Все перечисленные коды анализировались по следующим параметрам:

1. Эффективность исправления ошибок – качественная характеристика, отражающая способность кода восстанавливать исходную скрытую информацию с высокой степенью точности и надежности при наличии различных искажений или ошибок, возникающих в процессе передачи, хранения или обработки данных. 10 баллов – высокая способность исправления ошибок. 5 баллов – относительно хорошая способность исправления ошибок. 0 баллов – низкая способность исправления ошибок.

2. Пропускная способность – характеристика, отражающая возможность кода генерировать неограниченное количество кодовых слов различной длины при передаче данных. 10 баллов – высокая пропускная способность. 5 баллов – относительно хорошая пропускная способность. 0 баллов – низкая пропускная способность.

3. Отношение эффективности к длине кодового слова – характеристика, которая показывает, насколько эффективно коды используют дополнительные биты для исправления ошибок при относительно небольшом увеличении длины кодового слова. 10 баллов – высокая способность исправления ошибок при относительно небольшом увеличении длины кодового слова. 5 баллов – относительно хорошая способность исправления ошибок при относительно небольшом увеличении длины кодового слова. 0 баллов – низкая способность исправления ошибок при относительно небольшом увеличении длины кодового слова.

4. Гибкость адаптации – характеристика, которая позволяет настраивать пропускную способность и надежность в зависимости от условий канала. 10 баллов – высокая гибкость адаптации. 5 баллов – относительно хорошая гибкость адаптации. 0 баллов – низкая гибкость адаптации.

5. Сложность реализации – характеристика, которая показывает, насколько сложной является структура кода, которая требует большого количества вычислительных ресурсов для алгоритмов кодирования и декодирования информации. Код, требующий больших

вычислений, может привести к высокому качеству сокрытия, что также может повлечь увеличение времени на выполнение алгоритма, но в некоторых случаях время выполнения может играть большую роль. 10 баллов – невысокая сложность реализации. 5 баллов – относительно невысокая сложность реализации. 0 баллов – высокая сложность реализации.

На основе сравнительного анализа по нескольким параметрам можно сделать вывод о каждом избыточном коде. Анализ показал, что наиболее хорошим для использования является фонтанный код.

Таблица – сравнительный анализ избыточных кодов

	Фонтанный код	LDPC код	Код Хемминга
Эффективность исправления ошибок	5	10	0
Пропускная способность	10	5	0
Отношение эффективности к длине кодового слова	10	5	0
Гибкость адаптации	10	5	0
Сложность реализации	5	0	10
Итоговая оценка	40	25	10

Полученные результаты могут свидетельствовать о рациональности использования фонтанного кода в стеганографии в силу его преимуществ. Однако нельзя ориентироваться только на итоговую оценку, необходимо подбирать код по определенным критериям. В каждом коде есть свои достоинства и недостатки. При выборе кода важно обращать внимание на объем информации, на факторы угрозы безопасности информации и на высокое качество сокрытия и устойчивости.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие / П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.
2. MacKay, D. J. C. Fountain Codes / D. J. C. MacKay // IEEE Communications. – 2005. – Vol. 152, № 6. – P. 1062-1068.
3. Giuseppe, C. LDPC coding for interference mitigation at the transmitter / C. Giuseppe, D. Burshtein, S. Shamai // 40th Annual Allerton Conference on Communications, Control and Computing. – 2002. – P. 217–226.