УДК 621.391.7

ПРИМЕНЕНИЕ ПОМЕХОУСТОЙЧИВЫХ КОДОВ В СТЕГАНОГРАФИИ

К. т. н. А. В. Шишкин

Одесская национальная морская академия
Украина, г. Одесса
shiskin@te.net.ua

Предложен метод встраивания устойчивых цифровых водяных знаков (ЦВЗ) на основе блоковых помехоустойчивых кодов. Формирование ЦВЗ реализовано с использованием алгоритма перевертывания бита на графе Таннера. По результатам компьютерного моделирования алгоритма для кода Хемминга эффективность встраивания информации составляет около 2 бит/инверсию при устойчивости ЦВЗ, определяемой корректирующей способностью кода.

Ключевые слова: цифровые водяные знаки, код Хемминга, алгоритм перевертывания бита.

Стеганографическая система характеризуется количеством скрываемой информации, ее устойчивостью к атакам и вносимыми искажениями. Данные параметры противоречивы и должны выбираться на основе компромиссного решения. В настоящей работе в качестве носителя рассматривается двоичная последовательность длиной n бит $\boldsymbol{x}=\{0,1\}^n$. Предполагается, что допустимы некоторые искажения (инверсии) битов последовательности для скрытной передачи r бит информации. Длина стегопоследовательности $\boldsymbol{y}=\{0,1\}^n$ при этом сохраняется. В [1] показано, что одна инверсия на блок длиной n позволяет передать r бит при использовании кода Хемминга (n,k), $n=2^r-1$, $r=3,4,5,\ldots$, $k=n-r$. Эффективность встраивания информации E, определяемая отношением количества скрываемой информации к числу инверсий [2], близка к r. Цифровой водяной знак (ЦВЗ) в таком методе является хрупким. Искажение любого бита в блоке приводит к потере всего ЦВЗ длиной r бит. В настоящей работе предложен метод формирования устойчивых ЦВЗ, сохраняющих целостность при атаках в канале.

Проверочная матрица линейного блокового кода (n,k) может быть представлена в треугольной форме: $H=(T,A)$, $H=\{0,1\}^{(r\times n)}$, где T — верхнетреугольная матрица $(r\times r)$, A — матрица $(r\times k)$. Исходный блок носителя запишем в виде префикса длиной r и суффикса длиной k: $x=(x_p, x_s)$. Блок с встроенными данными будем искать в виде $y=(y_p, y_s)$. Потребуем выполнение равенств $T\boldsymbol{y}_p^T=M$, $A\boldsymbol{y}_s^T=M$, где M — встраиваемые данные (r бит), «^{T}» — символ транспонирования. Последовательность $\boldsymbol{y}$ при этом будет кодовым словом, удовлетворяющим условию $H\boldsymbol{y}^T=0$. Префикс $\boldsymbol{y}_p$ однозначно вычисляется исходя из M. Суффикс $\boldsymbol{y}_s$ может быть вычислен с минимальными искажениями (по Хеммингу): $d(\boldsymbol{y}_s, \boldsymbol{x}_s)=\min$.

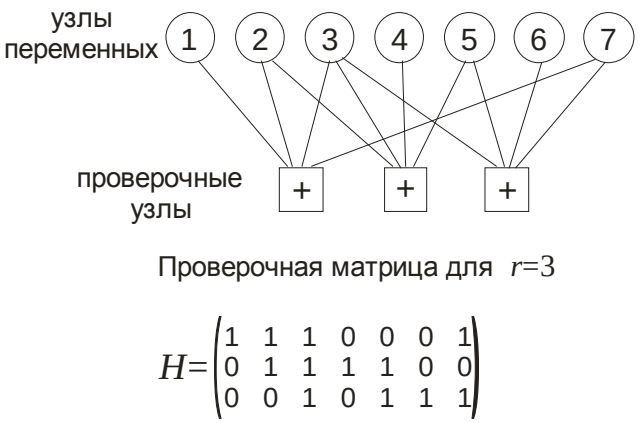
Для нахождения $\boldsymbol{y}$ был применен алгоритм распространения доверия в форме алгоритма перевертывания бита (WBF) [3] на графе Таннера. Пример графа Таннера для кода Хемминга (7,4) представлен на рис. 1. Алгоритм вычисления вектора включает два этапа:

1) вычисление префикса $\boldsymbol{y}_p$ из условия $T\boldsymbol{y}_p^T=M$;

2) вычисление суффикса $\boldsymbol{y}_s$ по алгоритму перевертывания бита. Изначально полагаем $\boldsymbol{y}_s=\boldsymbol{x}_s$. На каждом шаге вычисляется синдром $S=(s_1,s_2,\ldots,s_r)^T=H_s\boldsymbol{y}_s^T$, и инверсии подвергается бит, имеющий наименьшую надежность. При достижении $S=M$ процесс останавливается.

Полученный вектор $\boldsymbol{y}$ является кодовым словом поскольку $H\boldsymbol{y}^T=0$. В декодере вначале исправляются возможные под воздействием атак ошибки в канале. Устойчивость ЦВЗ гарантируется

способностью исправления ошибок корректирующим кодом. Далее оценка скрытой информации производится по формуле $\hat{M} = T\,\boldsymbol{y}_p^T$.



Проверочная матрица для r=3

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Рис. 1. Граф Таннера кода Хемминга (7,4)

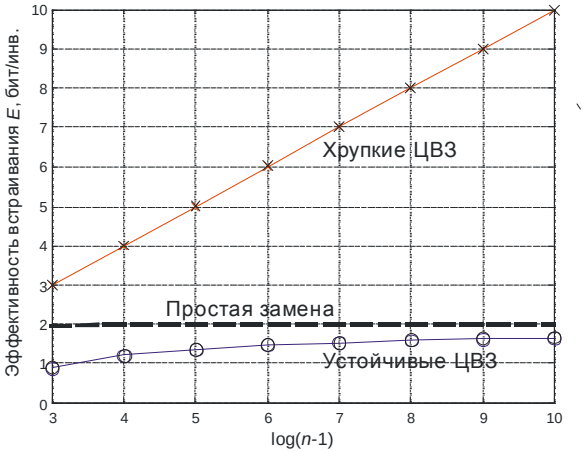


Рис. 2. Результаты моделирования

На рис. 2 представлены результаты моделирования алгоритмов формирования хрупких и устойчивых ЦВЗ в виде зависимости эффективности встраивания информации (бит/инверсия) от длины блока. Эффективность встраивания по предложенному алгоритму близка к эффективности в методе простой замены $(E = 2)$, однако ЦВЗ устойчивы к атаке в канале в пределах корректирующей способности кода.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Шишкин А. В. Синдромный метод формирования цифровых водяных знаков и стеганографической передачи с использованием дополнительной информации о носителе // Изв. вузов Радиоэлектроника.— 2010.– № 1.– С. 12 –19.

2. Cox I. J., et al. Digital watermarking and steganography. Second Edition – Morgan Kaufmann Publishers, 2008.– 594 p.

3. Zhu Q., Wu L. Weighted-Bit-Flipping-Based Sequential Scheduling Decoding Algorithms for LDPC Codes // Mathematical Problems in Engineering.– Vol. 2013, Article ID 371206, 6 p. http://dx.doi.org/10.1155/2013/371206

A. V. Shishkin

Application of error correcting codes in steganography.

A method for robust digital watermarking is designed on the basis of linear block error correcting codes. In general, parity-check matrix of block code (n,k) may be presented in the triangular form $H = (T, A)$, $H = \{0,1\}^{(r\times n)}$, $r = n - k$, where T is upper triangular matrix $(r \times r)$, A is matrix $(r \times k)$. Processing routine for embedding M bits in the host block of length n $\boldsymbol{x} = (\boldsymbol{x}_p, \boldsymbol{x}_s)$ relies on the bit flipping algorithm for Tanner graph and includes the next steps: 1) prefix $\boldsymbol{y}_p$ calculation of watermarked block from equation $T\,\boldsymbol{y}_p^T = M$, and 2) suffix $\boldsymbol{y}_s$ estimation by means of bit flipping algorithm until equality $H_s \boldsymbol{y}_s^T = M$ is reached. Watermarked block $\boldsymbol{y} = (\boldsymbol{y}_p, \boldsymbol{y}_s)$ constitutes code word because of $H\boldsymbol{y}^T = 0$, that guaranties error correction in the decoder. Estimation of extracted data is performed via $\hat{M} = T\,\boldsymbol{y}_p^T$. Embedding efficiency is near 2 bits per flip.

Keywords: *digital watermarks, Hemming code, bit flipping algorithm.*