УДК 629.391

Д.В. БАРАННИК, А.Э. БЕКИРОВ

КОНЦЕПЦИЯ СТРУКТУРНОГО СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ С МАСКИРОВАНИЕМ

Рассматривается использование неравновесного позиционного кодирования в качестве функционального преобразования для числа с встроенной информацией. Обосновывается появление структурной избыточности в процессе неравновесного позиционного кодирования. Предлагается использовать наличие потенциальной избыточности для стеганографического встраивания информации. Разрабатывается стеганографический метод на основе прямого и обратного функционального преобразования для неравновесного позиционного числа с имплантированным элементом, обеспечивающий встраивание и изъятие скрываемой информации. Формулируется правило встраивания информации для структурного стеганографического кодирования.

1. Введение

Одним из возможных путей повышения безопасности информационных ресурсов является использование стеганографических методов скрытия данных в изображении – контейнере.

Наиболее распространенными стеганографическими методами являются алгоритмы непосредственного встраивания информации в элементы пространственно-временного представления изображения - контейнера. Но для таких систем существуют недостатки, обусловленные внесением значительных визуальных искажений в значения пространственно – временных элементов изображения – контейнера и низкой устойчивостью встроенных данных к активным атакам злоумышленника. В связи с этим наиболее актуальным является нахождение новых подходов для разработки альтернативных стеганографических алгоритмов непосредственного встраивания.

Возможным решением проблемы улучшения показателей визуальной устойчивости стеганограммы, а также стойкости к трансформации и атакам является разработка функционального преобразования для элемента с встроенными данными. В качестве кодообразующего функционала, соответствующего требованиям относительно процесса скрытия данных, предлагается использовать кодообразующую функцию для неравновесного позиционного числа. Отсюда, *цель исследований* состоит в разработке метода стеганографического кодирования неравновесного позиционного числа с имплантированным элементом.

2. Разработка метода стеганографического кодирования с маскированием структурной стеганографической избыточности

В процессе реализации функционального преобразования на основе неравновесного позиционного кодирования область исходного изображения, содержащая совокупность видеопоследовательностей, рассматривается как множество неравновесных позиционных чисел $\{A(j)\}$. Здесь неравновесное позиционное число $A(j)$ без имплантации для j-го столбца массива видеоизображения состоит из m элементов:

$$A(j)=\{a_{1,j};...;a_{i,j};...;a_{m,j}\}.$$

Имплантацию в число $A(j)$ предлагается проводить поэлементно, т.е. один элемент b_ξ на позицию γ-го разряда числа $A(j)$. Здесь b_ξ - ξ-й элемент встраиваемой последовательности $B=\{b_1;...;b_\xi;...;b_\nu\}$, $b_\xi \in [0;\,255]$, $\xi=\overline{1,\nu}$. В этом случае имплантация задается следующей формулой:

$$A(j)' = A(j) \cup b_\xi, \qquad b_\xi = a'_{\gamma,j}.$$

В результате имплантации, число $A(j)'$ примет следующий вид:

$$A(j)' = \{ a_{1,j};...;a'_{\gamma,j};...;a_{i,j};...;a_{m+1,j} \},$$

где $A(j)'$ – число с имплантированным элементом $a'_{\gamma,j}$ в γ-й разряд числа; $(m+1)$ – количество элементов в числе с имплантацией.

На следующем этапе число $A(j)'$ с имплантированным элементом кодируется, проводится встраивание скрываемой информации в коде-контейнера. Другими словами, реализуется стеганографическое кодирование или процесс одновременного встраивания информации и построения кода-контейнера. В этом случае значение кода-контейнера, содержащее скрываемую информацию, называется стеганокодом.

Значения стеганокода $N(j)'$ для НП числа с имплантацией определяется по следующей формуле:

$$N(j)' = (\sum_{i=1}^{\gamma-1} a_{i,j}\ V'_{i,j}) + a'_{\gamma,j}V'_{\gamma,j} + \sum_{i=\gamma+1}^{m+1} a_{i,j}\ V'_{i,j}\ .$$

Здесь $V'_{i,j}$ – весовой коэффициент элемента $a_{i,j}$; j – количество столбцов в массиве фрагмента видеоизображения, $j=\overline{1,n}$; $V'_{\gamma,j}$ – весовой коэффициент имплантированного элемента $a'_{\gamma,j}$.

Значение весового коэффициента $V'_{i,j}$ для элемента $a_{i,j}$, позиция которого в числе $A(j)'$ старше позиции имплантированного элемента $a'_{\gamma,j}$, т.е. $i=\overline{1,\gamma-1}$, определяется на основе выражения:

$$V'_{i,j} = \psi'_{\gamma,j} \prod_{\xi=i+1}^{m+1} \psi_{\xi,j}\ ,$$

где $\psi_{\xi,j}$ – основание $(i;\ j)$-го элемента числа $A(j)'$ с имплантацией; $\psi'_{\gamma,j}$ – основание имплантированного элемента $b_\xi \le \psi'_{\gamma,j} - 1$.

Весовой коэффициент $V'_{i,j}$ элемента $a_{i,j}$, позиция которого в числе $A(j)'$ младше позиции имплантированного элемента $a'_{\gamma,j}$, т.е. $i=\overline{\gamma+1,m+1}$, вычисляется по формуле:

$$V'_{i,j} = \prod_{\xi=i+1}^{m+1} \psi_{\xi,j}\ .$$

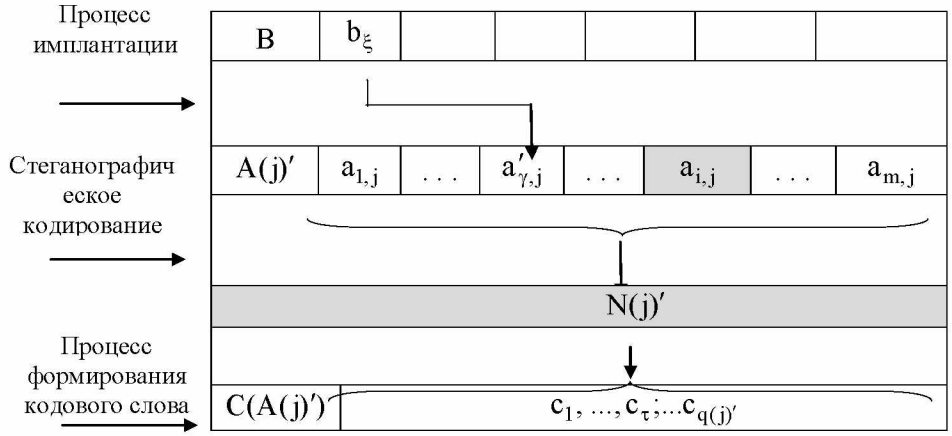
Весовой коэффициент $V'_{\gamma,j}$ имплантированного элемента $a'_{\gamma,j}$, равный накопленному произведению оснований старших элементов числа $A(j)'$, находится с помощью следующего выражения:

$$V'_{\gamma,j} = \prod_{\xi=\gamma+1}^{m+1} \psi_{\xi,j}\ .$$

Обобщив приведенные определения для весового коэффициента $V_{i,j}$, получим следующую систему выражений:

$$V_{i,j} = \begin{cases} \psi'_{\gamma,j} \prod\limits_{\xi=i+1}^{m+1} \psi_{\xi,j}, & \to i=\overline{1,\gamma-1}; \\ \prod\limits_{\xi=\gamma+1}^{m+1} \psi_{\xi,j} & \to i=\gamma; \\ \prod\limits_{\xi=i+1}^{m+1} \psi_{\xi,j}, & \to i=\overline{\gamma+1,m+1}. \end{cases}$$

В случае такого встраивания фрагмент исходной видеопоследовательности рассматривается, как позиционное число $A(j)' = \{ a_{1,j};...; a'_{\gamma,j};...; a_{i,j};...; a_{m+1,j} \}$ с имплантированным элементом $a'_{\gamma,j}$, $i=\overline{1,m+1}$. Для числа $A(j)'$ кодовое представление $C(A(j)')$ его



стеганокода $N(j)'$ в неравновесном позиционном базисе формируется в два этапа (рис. 1).

Рис 1. Структурная схема построения кодограммы стеганокода для числа $A'(j)$ с имплантацией

Первый этап включает в себя вычисление стеганокода $N(j)'$, как взвешенного суммирования величин $a_{i,j} V'_{i,j}$ и $a'_{\gamma,j} V'_{\gamma,j}$. Кодограмма $C(A(j)')$ стеганокода формируется на втором этапе для величины $N(j)'$:

$$C(A(j))' = \{c_1, ..., c_\tau, ..., c_{q(j)'}\},$$

где $q(j)'$ – длина кодограммы $C(A(j)')$.

В результате стеганографического кодирования формируются кодовые комбинации, состоящие из двух частей: служебной $\Psi^{(1)}$ и информационной $N(j)'$ (значение стеганокода). Кодовую комбинацию, которая содержит служебную часть $\Psi^{(1)}$ (система оснований) и информационную часть (кодовое представление стеганокода $N(j)'$), будем называть стеганограммой.

Оценим длину $q(j)'$ кодограммы стеганокода $N(j)'$ для числа $A(j)'$ с имплантацией. Значение $q(j)'$ с учетом того, что имплантированный элемент $a'_{\gamma,j}$ имеет основание $\psi'_{\gamma,j}$, будет определяться по формуле:

$$q(j)' = |N(j)'|_2 = [\ell og_2 \psi'_{\gamma,j} + \ell og_2 \prod_{i=1}^{m} \psi_{i,j}] + 1 = [\log_2 \psi'_{\gamma,j} + \sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 1 \text{ (бит)},$$

где $|N(j)'|_2$ – длина стеганокода $N(j)'$.

Сравним значение $q(j)'$ с длиной $q(j)$ кодограммы кода-контейнера $N(j)$ числа $A(j)$ без имплантированного элемента. Значение $q(j)$ определяется на основе следующего выражения:

$$q(j) = |C(A(j))| = [\ell og_2 \prod_{i=1}^{m} \psi_{i,j}] + 1 = [\sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 1 \text{ (бит)}.$$

Из сравнения выражений для q(j) и q(j)′ можно сделать вывод, что имплантация бита в число A(j) увеличивает длину кодового представления на $(\log_2 \psi'_{\gamma,j})$ бит. Это описывается выражением: $q(j)' - q(j) = \log_2 \psi_{\gamma,j}$.

Отсюда можно заключить, что в процессе формирования стеганокода для числа A(j)′ с имплантированным элементом относительно варианта до встраивания вносится структурная стеганографическая избыточность.

Данная избыточность $R(j)_{стег}$ определяется как разность длины q(j)′ кодограммы стеганокода числа A(j)′ с имплантацией и длины q(j) кодограммы кода-контейнера для числа A(j) без встроенной информации, т.е. $R(j)_{стег} = q(j)' - q(j) \geq 0$.

Теперь оценим величину остаточной структурной избыточности $R(j)_{ост}$, которая образуется в результате формирования стеганокода для числа с имплантацией в неравновесном базисе оснований относительно кодового представления исходной видеопоследовательности. Для этого оценим длину $q(j)_{исх}$ кодового представления исходной видеопоследовательности. Длина $q(j)_{исх}$ кодового представления числа A(j) с постоянным основанием $\psi = 256$ определяется по формуле: $q(j)_{исх} = m \cdot \log_2 256 = 8 \cdot m$ (бит).

Сравним длину q(j)′ кодограммы стеганокода N(j)′ для числа A(j)′ с имплантацией с длиной $q(j)_{исх}$ кодового представления числа A(j) с постоянным основанием $\psi = 256$ без имплантированного элемента. Это описывается выражением: $R(j)_{ост} = q(j)_{исх} - q'(j)$.

Очевидно, что возможность встраивания информации в условиях обеспечения ее скрытности будет обеспечиваться, когда количество структурной избыточности не будет равно нулю, т.е. $R(j)_{ост} = q_{исх} - q(j)' \neq 0$.

Проведем оценку того, как влияет появление стеганографической избыточности на возможность выявления факта встраивания информации. В этом случае необходимо учитывать, что стеганограмма содержит как информационную часть (значение стеганокода N(j)′), так и служебную (систему оснований $\Psi^{(1)}$). Отсюда, неавторизированный пользователь имеет доступ к базису оснований $\Psi^{(1)}$, на основе которого сформирован стеганокод N(j)′. Для выявления факта встраивания информации неавторизированный пользователь может предпринять следующее:

1. На основе имеющейся в кодограмме системы оснований $\Psi^{(1)}$ существует возможность вычислить длину q(j) кодограммы для кода контейнера N(j), т.е.

$$q(j) = [\sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 1.$$

2. Это позволяет установить предполагаемую длину информационной части текущей кодограммы, в результате чего будет считано значение кода N(j)″. Однако в действительности передается стеганокод и величина q(j) не будет равна q(j)′. Длина кодового представления стеганокода превышает длину исходного кода-контейнера. Поэтому в общем случае считанное значение N(j)″ в информационной части кодограммы будет отличаться от исходного значения кода-контейнера, а именно: $N(j)'' \neq N(j)$.

Это приводит к тому, что:

1) реконструкция элементов в исходной видеопоследовательности будет проводиться с ошибками;

2) разница между длинами кодовых представлений стеганокода q(j)′ и кодограммы q(j), которая остается не изъятой, будет восприниматься как первые биты служебной части следующей кодограммы N(j)″ (рис.2).

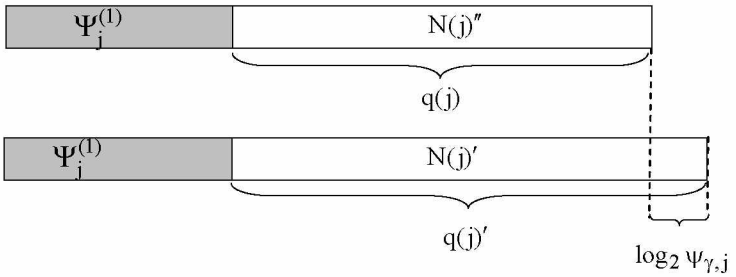


Рис. 2. Кодограммы для ошибочно изъятого стеганокода $N(j)''$ и стеганокода $N(j)'$

Поэтому можно заключить, что появление структурной стеганографической избыточности $R(j)_{стег}$ приводит к тому, что изображение будет декодироваться с наличием существенных искажений. Это позволит злоумышленнику установить факт наличия встроенной информации.

Рассмотрим, как влияет ошибочное значение $N(j)''$ кода-контейнера, считанное из информационной части кодограммы, в условиях, когда:

– с одной стороны, в реальности передается стеганокод $N(j)'$;

– с другой – неавторизированный пользователь будет считывать значение кода-контейнера $N(j)$.

В этом случае вместо того чтобы отобрать $q(j)'$ бит, неавторизированный пользователь выбирает $q(j)$ бит.

Рассмотрим процесс реконструкции элементов исходной видеопоследовательности, представленных как неравновесные позиционные числа в условиях использования ошибочного значения кода-контейнера $N(j)''$. Другими словами, проведем оценку влияния несоответствия длины стеганокода и кода-контейнера на процесс восстановления элементов исходной видеопоследовательности. Рассмотрим реконструкцию i-го элемента j-й видеопоследовательности. Для этого используем выражение:

$$a''_{i,j} = [N(j)''/V_{i,j}] - [N(j)''/\psi_{i,j}V_{i,j}]\psi_{i,j}$$

или

$$a''_{i,j} = N(j)''_i - \left[\frac{N(j)''_i}{\psi_{i,j}V_{i,j}}\right]\cdot\psi_{i,j},$$

где $a''_{i,j}$ – i-й элемент реконструированной видеопоследовательности; $N(j)''_i$ - остаточное значение кода неравновесного позиционного числа для декодирования очередного i-го элемента.

Из анализа этого выражения в условиях, когда

$$N(j)'' > N(j)',$$

следует, что как минимум начиная с некоторой β-й позиции, элементы видеопоследовательности будут обнуляться, т.е. $a''_{i,j} = 0$, для $i = \overline{\beta; m+1}$.

Значит, ошибочно установленная злоумышленником длина информационной части $N(j)''_i$ будет приводить к появлению искажений в процессе восстановления видеоизображения. Данные визуальные искажения могут служить дополнительным источником для стегоанализа.

Поэтому для устранения влияния стеганографической избыточности на возможность проведения атаки злоумышленником, в том числе установления факта наличия встроенной информации, необходимо разработать подход для устранения стеганографической избыточности. Для этого будем проводить локализацию количества избыточности путем маскирования структурной стеганографической избыточности.

Локализацию структурной стеганографической избыточности в процессе формирования стеганокода в неравновесном базисе предлагается осуществлять на основе коррекции длины кодограммы C(A(j)′) стеганокода N(j)′. Процесс коррекции предусматривает приведение длины кодограммы стеганокода q(j)′ к значению длины q(j). В физическом плане реализация коррекции кодограммы заключается в отбрасывании $(\log_2 \psi'_{\gamma,j})$ наименее значимых бит кодограммы C(A(j)′), т.е.

$$C'''_j = [N(j)''']_2 = [N(j)'/\psi_{i,j}]_2,$$

где N(j)‴ – значение стеганокода, скорректированное в процессе маскирования структурной стеганографической избыточности; $[N(j)''']_2$ – двоичное значение скорректированного стеганокода N(j)‴; C'''_j – кодограмма кодового представления скорректированного стеганокода N(j)‴.

Как следует из выражения для $R(j)_{стег}$, степень локализации значения стеганокода, а значит и уровень его искажений, будет зависеть от значения основания $\psi'_{\gamma,j}$ встраиваемого элемента. Тогда для обеспечения минимального значения $R(j)_{стег}$ в процессе стеганографического кодирования должно выполняться условие: $(\log_2 \psi'_{\gamma,j}) \to \min$.

Поэтому для уменьшения уровня искажений стеганокода предлагается встраивать элементы в двоичном представлении, т.е. $b_\xi \in [0; 1]$. В этом случае основание встроенного элемента будет равно $\psi'_{\gamma,j} = 2$.

Определим длину q(j)′ кодограммы стеганокода N(j)′ числа A(j)′ с имплантацией двоичного элемента. Учитывая, что имплантированный элемент $a'_{\gamma,j}$ имеет основание $\psi'_{\gamma,j} = 2$, величина q(j)′ будет определяться по формуле:

$$q(j)' = [\ell og_2 \psi'_{\gamma,j} + \ell og_2 \prod_{i=1}^{m} \psi_{i,j}] + 1 =$$

$$= [\log_2 \psi'_{\gamma,j} + \sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 1 = [\sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 2 \quad \text{(бит)}.$$

Можно сделать вывод, что имплантация бита в число A(j) увеличивает длину кодового представления стеганокода относительно кода-контейнера на один бит. Количество $R(j)_{стег}$ структурной избыточности будет равно:

$$R(j)_{стег} = q(j)' - q(j) = 1 \quad \text{(бит)}.$$

Следовательно, встраивание двоичного элемента позволяет минимизировать степень несоответствия между значениями стеганокода и кода – контейнера. В этом случае правило локализации будет иметь вид:

$$C'''_j = [N(j)''']_2 = [N(j)'/2]_2.$$

Такой вариант локализации стеганографической избыточности заключается в использовании свойств устойчивости структурных характеристик и структурной избыточности кодов относительно обработки искаженных значений кодов неравновесного позиционного числа. После локализации стеганографической избыточности длина q(j)″ кодограммы скорректированного стеганокода N(j)‴ будет вычисляться с помощью следующей формулы:

$$q(j)'' = [(\sum_{i=1}^{m+1} \ell og_2 \psi_{i,j})/2] + 1 = q(j).$$

Несмотря на это, искажения в значение стеганокода все равно будут вноситься, причем наибольшим искажениям будут подвергаться младшие элементы неравновесного позиционного числа. Поэтому для повышения устойчивости встроенных данных предлагается размещать один бит скрываемой информации на позицию старшего элемента неравновесного позиционного числа. Вследствие такого встраивания число $A(j)'$ примет следующий вид:

$$A(j)' = \{a'_{1,j}; a_{2,j}; ...; a_{i,j}; ...; a_{m+1,j}\},$$

где $A(j)'$ – число с имплантированным битом $a'_{1,j}$ на позиции старшего элемента; $a'_{1,j}$ – имплантированный бит на позиции старшего элемента числа $A(j)'$, равный $a'_{1,j} = b_\xi$, $a'_{1,j} \in [0; 1]$, где b_ξ – ξ-й элемент встраиваемой последовательности $B = \{b_1; ...; b_\xi; ...; b_\nu\}$; $b_\xi \in [0; 1]$, $\xi = \overline{1, \nu}$; $(m+1)$ – количество элементов в числе $A(j)'$ с имплантацией.

В этом случае вес встраиваемого элемента $V'_{\gamma,j}$ в неравновесном позиционном числе будет наибольшим, т.е. $V'_{\gamma,j} = V'_{1,j} = \max\limits_{1 \le i \le m+1} .\{V'_{i,j}\}$.

Следовательно, встраиваемый элемент будет более устойчив к преобразованиям со стеганокодом. В то же время встраивание скрываемого элемента на старшую позицию в числе исключает влияние его оснований на реконструкцию элементов исходной видеопоследовательности. Действительно, рассмотрим данное свойство на примере i-го элемента j-й видеопоследовательности, т.е

$$a'''_{i,j} = [N(j)''' / V'_{i,j}] - [N(j)''' / \psi_{i.j} V'_{i,j}]\psi_{i.j} =$$

$$= [N(j)''' / \prod_{\xi=i+1}^{m+1} \psi_{\xi,j}] - [N(j)''' / \psi_{i.j} \cdot (\prod_{\xi=i+1}^{m+1} \psi_{\xi,j})]\psi_{i.j} \quad \text{для } i = \overline{2, m+1}.$$

Из анализа данного выражения видно, что значения весовых коэффициентов $V'_{i,j}$ для $i = \overline{2, m+1}$ не содержат основание встроенного элемента $\psi_{1,j}$.

Отсюда, при стеганографическом кодировании неравновесного позиционного числа с имплантированным битом на позицию старшего элемента будет обеспечиваться устойчивость встроенных данных одновременно с минимизацией влияния при реконструкции остальных элементов.

3.Выводы

Разработана стеганографическая система на основе прямого и обратного функционального преобразования для неравновесного позиционного числа с имплантированным элементом, обеспечивающая встраивание и изъятие скрываемой информации на основе соответственно структурного стеганографического кодирования и декодирования.

Обосновано наличие структурной стеганографической избыточности в кодовом представлении стеганокода, образуемой на основе имплантации скрываемой информации в неравновесное позиционное число. Это создает дополнительную возможность для злоумышленника относительно установления факта наличия встроенной информации.

Создано правило встраивания информации для структурного стеганографического кодирования, заключающееся в том, что:

1) один бит скрываемого сообщения встраивается на старшую позицию неравновесного позиционного числа;

2) локализация стеганографической избыточности достигается на основе отсечения младшего бита стеганограммы.

Научная новизна. Впервые спроектирована стеганографическая система на основе непосредственного встраивания скрываемого элемента в видеопоследовательность. В отличие от других стеганосистем обеспечивается одновременное встраивание и изъятие скрываемой информации соответственно в процессе формирования и реконструкции кода-контейнера в неравновесном позиционном базисе оснований. Это обеспечивает встраивание скрываемой информации на основе учета количества структурной избыточности фрагментов видеоизображений.

Список литературы: 1. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с. **2.** *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288с. **3.** *Тарасов Д.О., Мельник А.С., Голобородько М.М.* Класифікація та аналіз безкоштовних програмних засобів стеганографії // Інформаційні системи та мережі. Вісник НУ "Львівська політехніка" 2010. № 673.С. 365-374. **4.** *Баранник В.В.* Метод формування функціонала стеганографічного кодування, стійкого до стегано-атак / *В.В. Бараннік, А.Е. Бекіров* //АСУ та прилади автоматики. 2013. Вип. 165. С. 34 – 43.