УДК 004.056.5: 519.17

Кобозева А.А., Маракова И.И.

ФОРМАЛИЗАЦИЯ ПОСТРОЕНИЯ СТЕГАНОГРАФИЧЕСКОГО СООБЩЕНИЯ НА ОСНОВЕ ТЕОРИИ ГРАФОВ

Введение

Одним из наиболее ценных богатств современной жизни является информация. Широкое распространение мультимедийных технологий в последнее десятилетие привело к упрощению доступа к информации, а значит, к угрозе ее несанкционированного использования. Задача защиты информации от неавторизованного доступа является на сегодняшний день актуальнейшей и до сих пор неразрешенной. Это привело к повышению интереса й расширению исследований в области разработки методов по защите информации, среди которых одно из ведущих мест занимают методы стеганографии, в частности компьютерной стеганографии [1].

Общей чертой всех стеганографических методов является то, что скрываемое сообщение, или дополнительная информация (ДИ), встраивается в некоторый объект, или основное сообщение (ОС), не привлекающий внимания, который затем открыто пересылается адресату по каналу связи. В качестве ОС может использоваться изображение, аудио-, видеосигнал и т.д.

Эффективность любого стеганографического метода оценивается, исходя из совокупности требований надежности восприятия после погружения скрываемого сообщения, эффективности декодирования ДИ при заданных помехах, устойчивости декодирования к возмущающим воздействиям в канале связи.

Целью настоящей работы является формализация процесса построения стеганографического сообщения, обеспечивающего требование надежности восприятия заполненного контейнера. Математическая модель ОС и выделяемой для погружения ДИ подобласти строится на основе теории графов.

1. Достаточное условие надежности восприятия стегосообщения

Не ограничивая общности рассуждений, для простоты дальнейшего изложения в качестве ОС будем рассматривать изображение.

Любое изображение в градациях серого можно представить как некоторую вещественную функцию f двух вещественных переменных x и y, областью определения которой, не ограничивая общности рассуждений, можно считать $[0,1]\times[0,1]\subset R^2$:

$$f(x,y):[0,1]\cdot[0,1]\to R^+. \qquad (1)$$

Если $f(x,y)$ является основным сообщением, или контейнером, используемым для встраивания в него некоторой дополнительной информации с целью ее скрытой передачи, также рассматриваемой как функция $z(x,y)$ вида (1), тогда погружение ДИ в контейнер равносильно получению нового изображения, т.е. построению новой функции $s(x,y)$ вида (1), которую далее будем называть стегосообщением. Процесс погружения дополнительной информации в основное сообщение будем называть стеганографическим преобразованием ОС. Способы формирования стегосообщения могут быть различными, например, аддитивный способ в предложенных выше обозначениях определяется соотношением

$$s(x,y)=f(x,y)+z(x,y). \qquad (2)$$

Для приложений цифровой стеганографии необходимо формализовать переход к цифровому изображению.

Пусть непрерывная область $[0,1]\times[0,1]$ подвергается равномерной дискретизации прямыми $x = ih,\ y = jh$. Не ограничивая общности рассуждений, будем считать, что $i, j = \overline{1, n-1},\ h = 1/n$, где n – количество частичных сегментов, на которые разбиваются отрезки $[0,1]$ по осям Ox и Oy. Это количество выбирается одинаковым для обеих сторон исходного квадрата-изображения. Такая дискретизация приведет к появлению n^2 одинаковых прямоугольных подобластей со стороной, равной h, которые в дальнейшем будем называть элементарными подобластями (ЭП). В каждой из полученных ЭП выбирается срединная точка (центр квадрата), координаты которой обозначим $(x_i, y_j),\ i, j = \overline{1, n}$. Определим новую функцию $f_{цр}(x, y)$, значение которой в точках отдельной элементарной подобласти, являющейся окрестностью (x_i, y_j), считается постоянным и равным значению $f(x_i, y_j),\ i, j = \overline{1, n}$. Таким образом, после дискретизации изображения исходная функция $f(x, y)$ заменяется на интерполирующую ее функцию $f_{цр}(x, y)$, являющуюся интерполяционным сплайном нулевой степени [2]. Теперь в качестве ОС рассматривается $f_{цр}(x, y)$.

Совершенно аналогично строим приближающую функцию $z_{цр}(x, y)$, отвечающую ДИ. На рассматриваемой стадии процесса дискретизации формирование стегосообщения заключается в построении интерполяционного сплайна нулевой степени $s_{цр}(x, y)$ для функции $s(x, y)$. При аддитивном способе (2) формирования стеганографического преобразования дискретизированного исходного изображения

$$s_{цр}(x, y) = f_{цр}(x, y) + z_{цр}(x, y). \qquad (3)$$

$f_{цр}(x, y)$ как сплайн нулевой степени на линях, являющихся границами ЭП ($x = ih,\ y = jh,\ i, j = \overline{1, n-1}$), может либо оказаться непрерывной функцией, либо претерпевает скачки [2], [3]. Очевидно, что преобразование (3) изменяет эти скачки и даже может сделать нулевыми на каких-то линиях или порождает их там, где $f_{цр}(x, y)$ была непрерывной.

Одним из требований, выдвигаемых к стеганографическому преобразованию ОС, является его надежное восприятие после погружения ДИ. Рассматривая ОС и ДИ как сплайны нулевой степени, приходим к истинности следующего утверждения:

У т в е р ж д е н и е 1. Стеганографическое преобразование ОС $f_{цр}(x, y)$ удовлетворяет требованию надежности восприятия, если погружение (3) ДИ $z_{цр}(x, y)$ происходит в те элементарные подобласти дискретизированной исходной области, на границах которых функция $f_{цр}(x, y)$ имеет максимальные или достаточно большие скачки.

По функции $f_{цр}(x, y)$ определим новую функцию:

$$F_{цр}(x, y) = \left[f_{цр}(x, y) \right].$$

Здесь $[\bullet]$ означает функцию целой части. Значения $F_{цр}(x, y)$ могут быть только целыми. На практике для изображений в градациях серого используют:

$$F_{цр}(x, y) : [0,1]\times[0,1] \to \{0,1,\text{K},255\}.$$

$F_{pr}(x,y)$ соответствует ОС. Совершенно аналогично строим приближающую функцию $Z_{pr}(x,y)$, отвечающую ДИ. Очевидно, если в утверждении 1 заменить $f_{np}(x,y)$ и $z_{np}(x,y)$ на $F_{pr}(x,y)$ и $Z_{pr}(x,y)$ соответственно, то утверждение останется истинным.

2. Граф изображения

Для численного представления полученной функции $F_{pr}(x,y)$ на практике до сих пор традиционно применялась матрица F, размерность которой $n \times n$, а элементы $F(i,j)$ определяются в соответствии с формулой:

$$F(i,j) = F_{pr}(x_i, y_j), \quad i,j = \overline{1,n}.$$

Из всего вышесказанного вытекает, что каждый элемент матрицы $F(i,j)$, $i,j = \overline{1,n}$ отвечает ЭП, являющейся окрестностью (x_i, y_j), исходной дискретизированной области. Скачки функции $F_{pr}(x,y)$ на границах подобластей отвечают разности значений соседних элементов в матрице F. Соседними для элемента $F(i,j)$ в матрице F будем называть элементы $F(i,j-1)$, $F(i,j+1)$, $F(i-1,j)$, $F(i+1,j)$, $i,j = \overline{1,n}$. При этом, если $j-1<1$, $i-1<1$, $j+1>n$, $i+1>n$, то соответствующих соседей у элемента $F(i,j)$ нет. Выделение ЭП исходного ОС для погружения в него ДИ, о которой идет речь в утверждении 1, теперь сводится к поиску элементов $F(i,j)$ матрицы изображения, имеющих таких соседей $F(i_1, j_1)$, для которых

$$|F(i,j) - F(i_1, j_1)| > M,$$

где M – наименьшее допустимое значение скачка функции для погружения ДИ в рамках заданных ограничений. Назовем *M предельным допустимым скачком функции.*

Для решения этой задачи в качестве математической модели исходного изображения рассмотрим не матрицу F, как это традиционно делалось ранее, а построенный определенным образом неориентированный граф $G_F(X,E)$.

Определение 1. Пусть F - $n \times n$-матрица изображения $f(x,y)$. Граф $G_F(X,E)$ будем называть *графом изображения*, если:

1) $|X| = n^2$, причем каждая вершина соответствует одному и только одному элементу матрицы F;
2) ребро $< i, j >$ принадлежит множеству E тогда и только тогда, когда вершины i и j графа $G_F(X,E)$ соответствуют таким соседним элементам $F(k_i, m_i)$ и $F(k_j, m_j)$ матрицы F, для которых

$$|F(k_i, m_i) - F(k_j, m_j)| > M,$$

где M – предельный допустимый скачок функции.

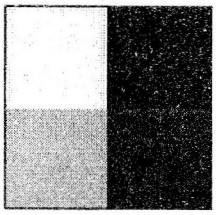


Рис. 1

Для иллюстрации определения 1 рассмотрим пример. На рис. 1 представлено изображение в градациях серого. Не ограничивая общности, для простоты предположим, что размерность изображения 10 х 10 пикселей (n=10). Матрица, отвечающая этому изображению, имеет вид:

$$F = \begin{pmatrix} 240 & 240 & 240 & 240 & 240 & 4 & 4 & 4 & 4 & 4 \\ 240 & 240 & 240 & 240 & 240 & 4 & 4 & 4 & 4 & 4 \\ 240 & 240 & 240 & 240 & 240 & 4 & 4 & 4 & 4 & 4 \\ 240 & 240 & 240 & 240 & 240 & 4 & 4 & 4 & 4 & 4 \\ 240 & 240 & 240 & 240 & 240 & 4 & 4 & 4 & 4 & 4 \\ 200 & 200 & 200 & 200 & 200 & 98 & 98 & 98 & 98 & 98 \\ 200 & 200 & 200 & 200 & 200 & 98 & 98 & 98 & 98 & 98 \\ 200 & 200 & 200 & 200 & 200 & 98 & 98 & 98 & 98 & 98 \\ 200 & 200 & 200 & 200 & 200 & 98 & 98 & 98 & 98 & 98 \\ 200 & 200 & 200 & 200 & 200 & 98 & 98 & 98 & 98 & 98 \end{pmatrix}.$$

Нумерацию графа проведем следующим образом: элементу $F(i,j)$ матрицы будет соответствовать узел графа с номером $(i\text{-}1)n+j$. Такое помечивание сохраняет наглядность соответствия между матрицей и графом. Граф, отвечающий изображению на рис. 1, при $M = 30$ представлен на рис. 2, при $M = 100$ - на рис. 3 (выбор M для произвольной $f(x,y)$ определяется в зависимости от вида самого изображения, от характера заданных ограничений либо экспериментально).

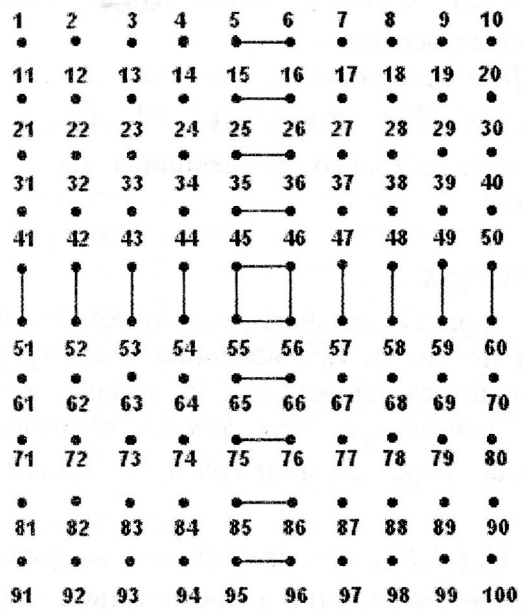


Рис. 2

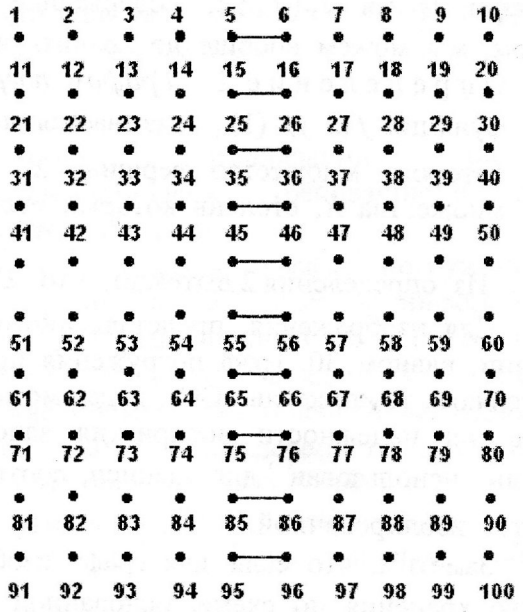


Рис. 3

При такой математической модели изображения область скачков функции $F_{pr}(x, y)$, пригодная для погружения ДИ, становится очевидной. Погружение имеет смысл осуществлять в те пиксели ОС, которым в графе изображения отвечают узлы, степень которых [4] не равна нулю, т.е. узлы, не являющиеся изолированными.

На практике удобно после задействования очередного пикселя, при выполнении погружения ДИ, узлы графа, один из которых отвечает рассматриваемому пикселю, а второй – смежный с ним, сделать изолированными.

Любой машинный алгоритм, оперирующий с графами, обычно очень чувствителен к способу их представления. Одним из наиболее экономичных в смысле памяти и позволяющих легко устанавливать свойства смежности в графе является способ хранения,

основанный на структуре смежности графа $G(X,E)$ [5]. Эта схема представления использует два массива, общая длина которых равна

$$|X|+2|E|+1. \qquad (4)$$

Очевидно, для большого количества изображений граф изображения будет иметь большое число изолированных вершин (если только в изображении не происходит резкого изменения тона в окрестностях большого, т.е. сравнимого с общим количеством, числа пикселей). Их количество зависит от значения M и может варьироваться при помощи подбора M. Это приведет к тому, что мощность множества E будет небольшой по сравнению с $|X|$, а значит, для хранения массивов, представляющих граф изображения, потребуется примерно столько же памяти, сколько и для матрицы изображения. Но граф, в отличие от матрицы, не требует уже никаких дополнительных исследований для выделения области погружения ДИ.

3. Граф погружения дополнительной информации в изображение

Преимуществом графа, соответствующего определению 1, является то, что он полностью отражает структуру матрицы изображения, однако для наших целей выделения подобласти для погружения ДИ эта информация даже избыточна. Действительно, мы никак не используем изолированные вершины, не изменяем подграфы графа $G_F(X,E)$, содержащие узлы, степень которых равна нулю. Таким образом, мы можем вообще не хранить изолированные вершины.

Определение 2. *Графом погружения ДИ в изображение*, отвечающее функции $f(x, y)$ (1), называется подграф $G_{FP}(X_P,E_P)$ графа $G_F(X,E)$, для которого множество вершин X_P содержит те и только те вершины из множества X, степень которых отлична от нуля.

Из определения 2 вытекает, что $E_P = E$, а $X_P \subseteq X$.

Для изображения, представленного на рис.1 при предельном допустимом скачке функции, равном 30, граф погружения представлен на рис. 4. Все вершины этого графа определяют те пиксели ОС, куда может производиться запись ДИ с соблюдением требования надежности восприятия заполненного контейнера. Как только очередной пиксель использован для записи, соответствующая пара вершин графа $G_{FP}(X_P,E_P)$ делается изолированной.

Заметим, что если для графа изображения $G_F(X,E)$, представленного на рис. 1, для его хранения по схеме, основанной на структуре смежности, в соответствии с (4) потребуются два массива суммарной длины 141, то для графа погружения $G_{FP}(X_P,E_P)$ суммарная длина массивов в той же схеме хранения составит всего лишь 77, что гораздо меньше количества элементов в соответствующей матрице F.

Предположим, что одно и то же ОС используется для пересылки ДИ многократно. Тогда выделение и хранение графа погружения, очевидно, обладает рядом преимуществ по сравнению с традиционными методами хранения и подготовки ОС для погружения в него секретной информации:

1) хранение в виде графа подобласти, используемой непосредственно для погружения, часто потребует сравнительно небольших объемов памяти;

2) задача обеспечения требования надежности восприятия путем выделения подобласти ОС, наиболее пригодной с этой точки зрения для погружения ДИ, решается однократно, не требуя исследования матрицы изображения каждый раз при выборе его в качестве контейнера.

Предположим, что у нас имеется некоторый банк изображений, используемых в качестве ОС для пересылки информации. Требуется осуществить выбор основного сообщения для данной ДИ таким образом, чтобы гарантировать, что пересылаемый объем информации поместится в выбранном контейнере. Такой выбор можно производить, используя только графы погружения , которые хранятся вместе с соответствующими изображениями, что значительно сократит время поиска нужного ОС по сравнению с выбором, осуществляемым по матрицам изображений (в том случае, конечно, если мощности X_P значительно меньше мощностей X множеств вершин соответствующих графов). Такой выигрыш, очевидно, будет не для любого изображения.

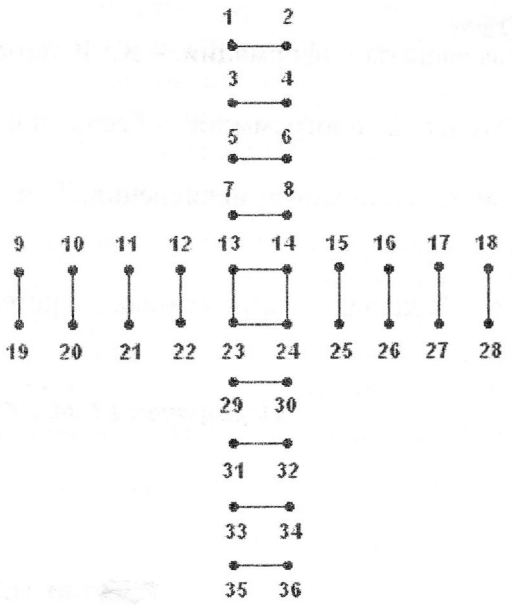


Рис.4

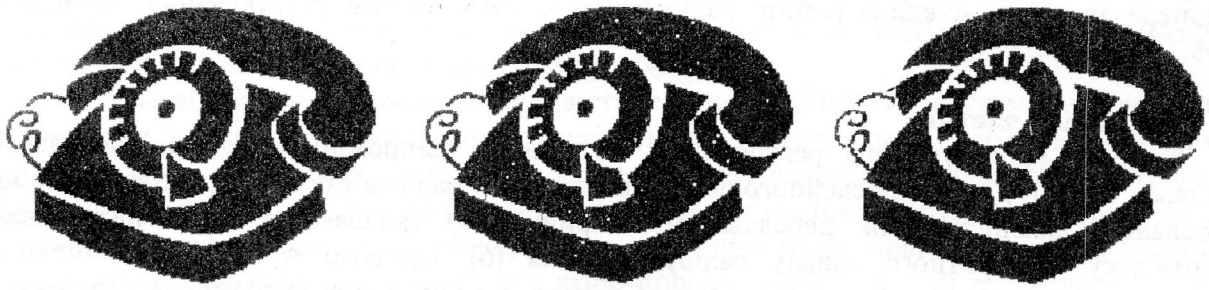
Поскольку в качестве ОС, вообще говоря, может использоваться произвольное изображение, кроме того, возможен выбор различных значений предельно допустимого скачка функции, принципиально невозможно получение точных оценок для сравнения запросов к памяти при использовании графа погружения и матрицы изображения.

4. Заключение

В настоящей работе предложен метод формализации построения стеганографического сообщения с учетом удовлетворения требованию надежности восприятия заполненного контейнера на основе теории графов.

Рис. 5 иллюстрирует преимущества использования графа погружения при выделении подобласти основного сообщения для встраивания секретной информации по сравнению с рассеянным погружением той же ДИ: заполненный контейнер (рис. 5, *в*) визуально практически не отличается от изображения, отвечающего ОС (рис. 5, *а*). Монохромное изображение приводится в качестве примера для большей наглядности.

Предлагаемый в работе метод может быть использован и для цветных изображений. Как известно, зрительная система человека является наименее чувствительной к синему цвету, поэтому встраивать ДИ в изображение, имеющее RGB-кодирование, целесообразно в канал синего цвета. Пусть основное сообщение



а *б* *в*

Рис. 5. Основное сообщение (*а*); стегосообщение, сформированное методом случайного интервала (*б*); стегосообщение с ДИ, погруженной в область, определяемую графом погружения (*в*)

$F = \{R, G, B\}$, тогда граф погружения для такого изображения строится в соответствии с матрицей B, в подматрицу которой и происходит встраивание скрываемого сообщения.

Список литературы

1. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации. – К.: Юниор, 2003. – 501 с.

2. *Каханер Д., Моулер К., Нэш С.* Численные методы и программное обеспечение. - М.: Мир, 2001. – 575 с.

3. *Фихтенгольц Г.М.* Курс дифференциального и интегрального исчисления. Том 1. - М.: Наука, 1969. – 608 с.

4. *Харари Ф.* Теория графов.-М.: Мир, 1973.- 300 с.

5. *Джордж А., Лю Дж.* Численное решение больших разреженных систем уравнений. – М.: Мир, 1984.- 333 с.

Поступила 12.04.2006

УДК 62-55:681.515

Купах Н.І.

КЛАСИФІКАЦІЯ СИСТЕМ АВТОМАТИЧНОГО РЕГУЛЮВАННЯ ПОТУЖНОСТІ ПЕРЕДАВАЧА В АДАПТИВНИХ КАНАЛАХ РАДІОЗВ'ЯЗКУ

1. Вступ

Радіозв'язок є потужним інструментом рішення прикладних задач як державного, так і побутового рівня. Він дозволяє реалізувати повний спектр інформаційних послуг: передачу телефонних повідомлень, обмін даними, підключення до глобальних інформаційних мереж, одержання й передачу відеозображень, телебачення й т.д. Роль радіозв'язку в суспільстві й техніці постійно зростає. Радіозв'язок, здійснюючи обмін інформацією, доповнює й значно розширює можливості проводного зв'язку. Для створення якісних систем радіозв'язку необхідно вирішувати цілий ряд проблем. Так, для систем радіорелейного зв'язку і особливо тропосферного радіозв'язку істотною проблемою є боротьба із завмираннями. Ефективним засобом рішення цієї проблеми є розробка адаптивних каналів радіозв'язку з системи автоматичного регулювання потужності випромінювання радіопередавачів. Регулювання потужності випромінювання радіопередавачів надто важливе і потрібне для радіосистем мобільного зв'язку. Наприклад, без точного регулювання потужності випромінювання радіопередавачів неможлива робота радіосистем CDMA на базі устаткування стандарту IS-95.

2. Основна частина

Система автоматичного регулювання потужності випромінювання радіопередавача (система АРПП) для радіорелейного або тропосферного радіозв'язку (як правило, система з фіксованою дальністю між передавачем і приймачем) складається з прямого каналу радіозв'язку і зворотного каналу радіоуправління [6]. Система АРПП для мобільного радіозв'язку (система зі змінною дальністю між передавачем і приймачем) також складається з прямого (базова станція – мобільна станція) і зворотного (мобільна станція – базова станція) каналів радіозв'язку. Кожний канал радіозв'язку систем АРПП включає радіоланку: радіопередавальний пристрій – середовище розповсюдження радіохвиль – радіоприймальний пристрій. Система АРПП, на відміну від інших радіотехнічних систем, практично завжди піддана специфічним впливам – завмиранням сигналу в середовищі розповсюдження