УДК 004.056.5

Борисенко И.И. (ОНПУ, Одесса)

ПОВЫШЕНИЕ ПОМЕХОУСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА

Введение

Одной из актуальных, но нерешенных на сегодняшний день в полном объеме проблем является защита авторских прав, прав интеллектуальной собственности и конфиденциальных данных, имеющих цифровой формат. Важным направлением в решении этой проблемы является разработка методов сокрытия информации, в частности, методов цифровой стеганографии [1].

Общей чертой всех стеганографических методов является то, что скрываемое сообщение, или дополнительная информация (ДИ), встраивается в некоторый объект, или контейнер, не привлекающий внимания, который затем открыто пересылается адресату по каналу связи. Контейнер с погруженным в него ДИ будем называть стегосообщением. Система, которая выполняет задачу встраивания и выделения сообщений из другой информации называется стегосистемой.

В [2] был предложен новый стеганографический алгоритм (назовем его Stego_Graph) организации пересылки и декодирования секретного сообщения, основанный на применении теорий графов. Представленный алгоритм разрабатывался для таких информационно-скрывающих систем, где максимизируется пропускная способность (ПС) при обеспечении требуемой секретности стегоканала, а к помехоустойчивости предъявляются минимальные требования.

Целью настоящей работы является повышение помехоустойчивости алгоритма Stego_Graph, обеспечение возможности его применения в системах, где присутствуют помехи.

Поскольку в качестве контейнера используется цифровое изображение, математической моделью которого является матрица, то в качестве инструмента для повышения помехоустойчивости был выбран недавно разработанный общий подход к анализу информационных систем, основанный на теории возмущений и теории матриц [3]. В силу этого, для достижении поставленной цели, необходимо решить *задачи:*

-Детального анализа алгоритма Stego_Graph, позволяющего выявить резервы повышения его помехоустойчивости;

-Анализа возмущений сингулярных векторов матрицы контейнера при погружении ДИ с использованием Stego_Graph;

-Модификации процедуры погружения ДИ в контейнер для изменения области локализации возмущений сингулярных векторов;

-Практического подтверждения повышения помехоустойчивости стегоалгоритма путем вычислительного эксперимента и сравнительного анализа результатов работы его различных модификаций.

1. Краткий обзор алгоритма Stego_Graph

В основе алгоритма погружения секретного сообщения лежит изменение яркости некоторых пикселей исходного изображения – $f(x,y)$. Практические эксперименты показали, что для того, чтобы обеспечить надежность восприятия стегосообщения, вычисленная яркость пикселя $f'(x,y)$ должна находится в заданных пределах

$$f(x,y)-\delta \le f'(x,y) \le f(x,y)+\delta, \qquad (1)$$

где δ - максимально допустимая величина отклонения яркости пикселя от исходного значения.

В [2] предлагается итерационный алгоритм – Алгоритм 1 для разбивки изображения на подобласти и определяются пороговые значения каждой подобласти.

В качестве иллюстрации работы алгоритма рассмотрим третий блок изображения Pout.tif размерности 8x8. Положим δ=15. Это значение установлено экспериментально для данного изображения. В результате работы Алгоритма 1, изображение будет сегментировано на четыре подобласти со следующей градацией яркости 214-184, 183-153, 152-122, 121-106 с соответствующими значениями порогов T_1=199, T_2=168, T_3=137, T_4=114. При вычислении T_4 была применена операция округления. Далее проведем пороговое преобразование изображения с адаптивным порогом. Матрица исходного изображения и результаты обработки с адаптивным порогом представлены на рис.2(а),(б) соответственно. Различными оттенками серого выделены четыре указанные подобласти.

Таким образом, в результате пороговой обработки получаем бинарную матрицу и, в дальнейшем, будем использовать ее для погружения секретного сообщения.

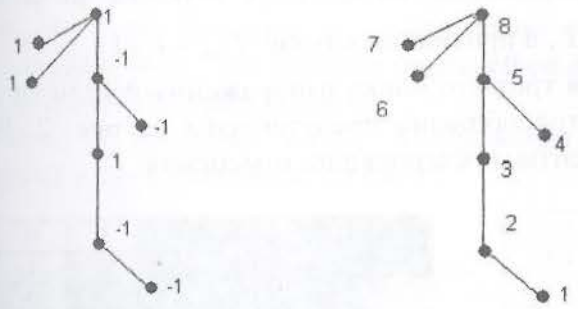
Для подготовки ДИ к погружению в контейнер используется теория графов. Базовые сведения и определения по теории графов можно найти, например, в [4].

Секретное сообщение представляется в виде помеченного графа-дерева, а затем строится матрица S полученного дерева по правилу

$$s_{ij} = \begin{cases} 0, \textit{ если вершина } v_i \textit{ не смежна с вершиной } v_j, \\ 1, \textit{ если вершина } v_i \textit{ смежна с вершиной } v_j \end{cases} \quad (2)$$

Алгоритм формирования матрицы ДИ – Алгоритм 2 представлен в [2].

Пусть задано некоторое сообщение длиною 8 бит: {1 ,1, 1,-1, -1,1, -1,-1},тогда построение графа такого сообщения и его матрицы демонстрирует рисунок 1.



а) б)

1	1	0	0	0	0	0	0
1	2	1	0	0	0	0	0
0	1	3	0	1	0	0	0
0	0	0	4	1	0	0	0
0	0	1	1	5	0	0	1
0	0	0	0	0	6	0	1
0	0	0	0	0	0	7	1
0	0	0	0	1	1	1	8

в)

Рис.1. Дерево сообщения и его матрица
а – дерево исходного сообщения; б – помеченное дерево исходного сообщения;
в – матрица дерева сообщения

Элементы главной диагонали не используются алгоритмом сокрытия информации, поэтому на рис.1 (в), который представляет матрицу S, на диагонали матрицы проставлены номера вершин графа. Поскольку S – симметрична, то можно использовать одну из ее треугольных подматриц – нижнюю или верхнюю. Анализируя структуру нижней подматрицы матрицы S (для определенности) замечаем, что первых 7 бит секретного сообщения вписались в элементы s_{ij} $j=\overline{1,n-1}$, $i=\overline{j+1,n}$, начиная с элемента s_{87}.

Таким образом, двигаясь снизу вверх вдоль диагонали, которая находится ниже главной, можно восстановить всю исходную последовательность, пользуясь признаком наличия единицы в ячейках матрицы как переключателем знака. Для восьмого бита можно определить любую ячейку подматрицы, лежащую ниже второй диагонали, скажем для определенности - s_{81}.

В общем случае ДИ, которая представлена последовательностью 1 и -1, может начинаться с любого знака, поэтому эту информацию также нужно отобразить в матрице,

например, следующим образом. Если $s_{87}=1$, то последовательность начинается с плюса, если $s_{87}=0$, то - с минуса.

Процесс погружения ДИ в контейнер состоит в следующем. Матрицу исходного изображения F разобьем на блоки размерности 8x8 стандартным образом, так, что объединение всех блоков составят матрицу F.

Информация погружается в каждый выделенный блок, поэтому ограничимся описанием погружения ДИ в один из них, в нижний его треугольник.

Для выделенного блока контейнера проводится пороговое преобразование по Алгоритму 1, в результате получаем матрицу, обозначим ее G. Из сообщения, которое нужно погрузить в контейнер, выделяется подпоследовательность длиною 8 бит и для выделенной подпоследовательности строится матрица S по Алгоритму 2.

Погружение информации в блок контейнера будет происходить в результате корректировки яркости пикселей контейнера (Алгоритм 3 [2]), которая будет происходить только в том случае, если обнаружится несовпадение значений элементов $g_{i,i-1}$ и $s_{i,i-1}$, $i=\overline{2,8}$ и элементов g_{81} и s_{81} матриц G и S. Если $g_{i,i-1}\neq s_{i,i-1}$, $i=\overline{2,8}$, то значение яркости пикселя $f_{i,i-1}$ матрицы F следует увеличить или уменьшить в зависимости от того, какое значение принимает $s_{i,i-1}$. Например, если $s_{i,i-1}=0$, то это означает, что $g_{i,i-1}=1$ и, следовательно, $f_{i,i-1}$ следует уменьшить. Новое значение $f_{i,i-1}$ зависит от порогового значения T подобласти, к которой принадлежит $f_{i,i-1}$, и будет определяться следующим образом. Если $s_{i,i-1}=0$, то новое значение яркости $f_{i,i-1}$ будет $f_{i,i-1}=T$, в противном случае $f_{i,i-1}=T+1$.

Проиллюстрируем все сказанное для третьего блока изображения Pout.tif и ДИ={1, 1, 1, -1, -1, 1, -1, -1}. Этапы создания стегосообщения представлены на рис. 2. В матрице стегосообщения – рис.2 г) выделены элементы, претерпевшие изменения.

213	214	212	197	137	112	110	109
189	210	213	210	165	119	110	108
159	204	210	212	189	137	119	107
133	186	200	209	194	153	128	107
137	175	201	210	195	145	126	107
189	164	175	199	175	131	121	108
214	186	164	154	142	121	113	107
215	200	177	131	119	113	112	106

а)

1	1	1	1	0	0	0	0
0	1	1	1	0	1	0	0
0	1	1	1	0	0	1	0
0	0	1	1	0	0	0	0
0	1	1	1	0	1	0	0
0	0	1	0	1	0	1	0
1	0	0	0	1	1	0	0
1	1	1	0	1	0	0	0

б)

1	0	0	0	0	0	0	0
1	2	0	0	0	0	0	0
0	1	3	0	0	0	0	0
0	0	0	4	0	0	0	0
0	0	0	1	5	0	0	0
0	0	0	0	0	6	0	0
0	0	0	0	0	0	7	0
0	0	0	0	0	0	1	8

в)

213	214	212	197	137	112	110	109
200	210	213	210	165	119	110	108
159	204	210	212	189	137	119	107
133	186	199	209	194	153	128	107
137	175	201	210	195	145	126	107
189	164	175	199	168	131	121	108
214	186	164	154	142	114	113	107
199	200	177	131	119	113	115	106

г)

Рис.2. Этапы погружения ДИ в контейнер
а – матрица F исходного изображения; б – матрица G порогового преобразования F;
в – матрица сообщения S; г – матрица F' стегосообщения.

Аналогично погружаются последующие 8 бит информации в верхнюю треугольную подматрицу матрицы F. Таким образом, в один блок контейнера погружается 16 бит информации.

Процедура извлечения ДИ из контейнера очень проста и сводится к определению знака элементов ДИ. Если элемент матрицы G' порогового преобразования контейнера, в который погружался бит информации, равен 1, то знак элемента ДИ следует изменить на противоположный по отношению к предыдущему элементу.

2. Модификация базового алгоритма. Разработка алгоритмов Stego_Graph_1 и Stego_Graph_2

Алгоритм Stego_Graph обладает высокой надежностью восприятия, поскольку матрица контейнера претерпевает малые изменения при погружении в нее секретного сообщения, хорошей пропускной способностью - 0.25 бит/пиксель, а объем правильно восстановленной информации достигает 100%, но Stego_Graph может применяться только в условиях идеального канала связи. При появлении незначительных помех объем правильно восстановленной информации снижается до 65%. Детальный анализ Stego_Graph позволил выявить скрытые резервы повышения его помехоустойчивости.

Напомним, что следуя Алгоритму 3 погружения ДИ в контейнер, пикселю контейнера присваивается значение $T+1$, если 0 характеристической матрицы контейнера надо преобразовать в 1, и T в противном случае, где T- значение порога. Таким образом, полученное значение либо вовсе не отличается от порогового, либо на единицу больше. Наложение незначительного шума, что эквивалентно, например, ± 2 градациям яркости приводит к тому, что пиксель может оказаться в прежней подобласти. Чтобы придать пикселю большую устойчивость логично присвоить ему такое значение, которое будет соответствовать середине требуемой подобласти, но это может повлечь корректировку яркости на значение большее δ, что в свою очередь неминуемо повлечет нарушение надежности восприятия. Это касается пикселей со значениями, близкими к значениям границ области, к которой они принадлежат.

Вернемся к третьему блоку изображения Pout.tif и рассмотрим его пороговое преобразование, представленное на Рис. 3.

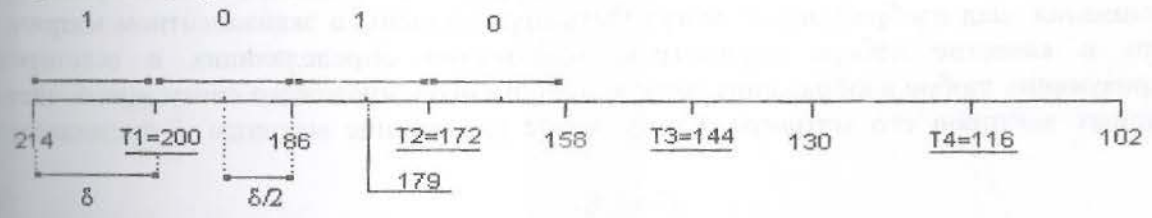


Рис. 3. Шкала порогового преобразования 3-го блока Pout.tif

Установим некоторые соглашения: правая граница не принадлежит текущей области (кроме последней), δ выбираем четной (для определенности 14), последнюю область, если она меньше 2δ доопределяем до 2δ. Все эти соглашения обеспечат целочисленное значение порога во всех областях, что немаловажно для обеспечения надежности восприятия стего, если δ достигает предельно-допустимых значений.

Пороговое преобразование предписывает превращение значений яркости пикселей в 0 или 1. Если обратиться к Рис.3, то легко заметить, что нули и единицы различных областей чередуются. Для пикселя, характеристическое значение которого равно 1 (кроме первой подобласти), не имеет значения, в какую подобласть он будет переведен, главное при этом сохранить надежность восприятия стегосообщения. Например, рассмотрим область с значениями границ 186-158 и порогом $T=172$. Если пиксель со значением яркости, которое удовлетворяет условию $179=186-\delta/2\le f(x,y)\le 186$ следует уменьшить так, чтобы его характеристическое значение равнялось нулю, то ему следует присвоить значение $T1-\delta/2=200-7=193$ если же пиксель имеет яркость, удовлетворяющую условию $T2<f(x,y)<T2+\delta/2$, то ему следует присвоить значение $T2-\delta/2=172-7=165$ при этом

разность между исходным и новым значением будет удовлетворять условию (1), то есть находиться в пределах $\pm\delta$.

Алгоритм 3. Корректирование яркости пикселя контейнера в Stego_Graph_1

Шаг 1. Определить границы $L(z)$ и $L(z+1)$ области, к которой принадлежит $f_{i,j}$. Определить значение порога T_k

Шаг 2. Если $g_{i,j} \neq s_{i,j}$ и $s_{i,j} = 0$, то

Если $k \neq 1$(не первая область) и $L(z) - f_{i,j} \leq \delta/2$; то $f_{i,j} = T_{k-1} - \delta/2$,

в противном случае $f_{i,j} = T_k - \delta/2$.

Если $g_{i,j} \neq s_{i,j}$ и $s_{i,j} = 1$, то

Если $k \neq n$(не последняя область) и $f_{i,j} - L(z+1) \leq \delta/2$, то $f_{i,j} = T_{k+1} + \delta/2$,

в противном случае $f_{i,j} = T_k + \delta/2$.

Для первой и последней области текущего блока погружение информации осуществляется так же, как и в алгоритме Stego_Graph.

При погружении ДИ в алгоритме Stego_Graph_2 используется информационная избыточность, каждое значение ДИ записывается трижды, то есть создаются блоки вида 000 и 111, а при декодировании знак определяется по большинству однотипных символов в блоке.

3.Оценка чувствительности стегосообщения к помехам в канале связи

При решении задачи повышения помехоустойчивости базового алгоритма был использован общий подход к анализу информационных систем, основанный на теории возмущений и теории матриц, который представлен в [3]. Изложим вкратце основные его концепции, которые использовались при разработке алгоритмов Stego_Graph_1 и Stego_Graph_2.

Поскольку математической моделью контейнера-изображения является матрица, а все преобразования над изображением могут быть представлены в эквивалентном матричном виде, то в качестве набора параметров, однозначно определяющих и всесторонне характеризующих любое изображение, можно использовать множество сингулярных чисел и сингулярных векторов его матрицы. Сингулярное разложение матрицы F представимо в виде:

$$F = U\Sigma V^T, \qquad (3)$$

где U и V матрицы левых и правых сингулярных векторов соответственно (СНВ), а Σ-матрица сингулярных чисел (СНЧ). В общем случае сингулярное разложение матрицы определяется неоднозначно, но можно выполнить нормальное сингулярное разложение, которое является единственным.

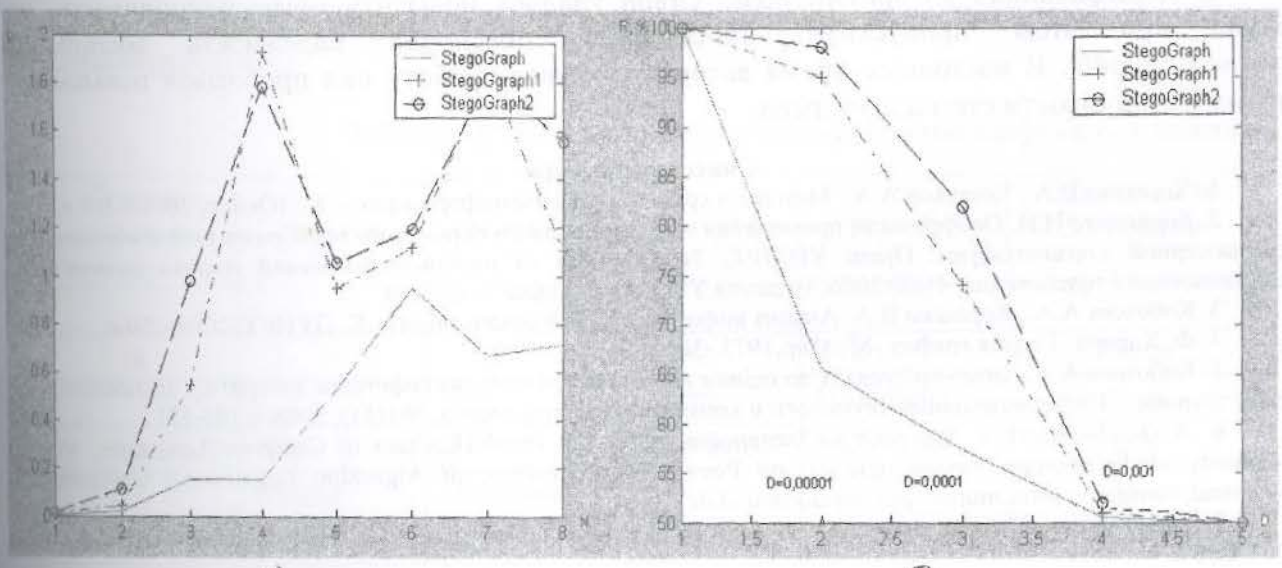
Любое стегопреобразование возмутит матрицу контейнера F, а значит, определенным образом возмутит соответствующие СНЧ и СНВ, что позволяет свести задачу анализа стегопреобразования к анализу возмущений СНЧ и СНВ. Далее, нам понадобится два важных утверждения, обоснованных в [5]. Во-первых, СНВ, отвечающие малым СНЧ, получают значительные возмущения даже при малых возмущениях контейнера, напротив СНВ, отвечающие наибольшим СНЧ отличаются большой помехоустойчивостью. Во-вторых, возмущения СНЧ сравнимы с возмущением данных - ΔF, т.е. СНЧ матрицы контейнера являются нечувствительными к возмущающим воздействиям, независимо от того, чувствительным или нет окажется стегосообщение к возмущающим воздействиям, поэтому имеет смысл анализировать лишь СНВ а совокупное их возмущение использовать как меру чувствительности стегосообщения к возмущающим воздействиям. На основании первого утверждения был сделан вывод, что алгоритм Stego_Graph следует модифицировать таким образом, чтобы матрица контейнера, при внесении в нее ДИ, получила такое

возмущение, что привело бы к возмущению не только СНВ, отвечающим малым СНЧ, но и СНВ, которые более устойчивы к помехам. Второе утверждение использовалось для оценки помехоустойчивости Stego_Graph и его модификаций.

В среде MATLAB был проведен вычислительный эксперимент, в ходе которого практически были реализованы новые стегометоды и проведена оценка их помехоустойчивости. Для демонстрации результатов далее используется третий блок Pout.tif, что является характерной картиной для других блоков Pout.tif, а также других изображений.

В силу особенностей погружения ДИ по алгоритму Stego_Graph матрица контейнера получает достаточно малые возмущения и в первую очередь возмущаются СНВ, отвечающие малым СНЧ – рис.4.а) (это 6,7,8 СНВ – ДИ находится в основном в этих векторах и при малейшей помехе информация искажается). При погружении ДИ по алгоритмам Stego_Graph_1 и Stego_Graph_2 значительному возмущению подвергаются также СНВ, отвечающие 5, 4 и 3 СНЧ, т.е больше информации переносится в те вектора, которые являются более устойчивыми к дополнительным воздействиям. Анализируя поведение СНВ (их совокупное возмущение) матрицы контейнера, можно сделать вывод, что самым устойчивым стегосообщением к дополнительным помехам является алгоритм Stego_Graph_2, что и подтверждает рис.4. б).

Возмущения в канале связи моделировались при помощи аддитивного гауссовского шума, наложение которого осуществлялось стандартной процедурой *imnoise*, с математическим ожиданием равным нулю и дисперсиями D=0.00001, D=0.0001 и D=0.001. Как и ожидалось, самый большой объем правильно восстановленной информации был получен по алгоритму Stego_Graph_2.



а) б)

Рис. 4. Представление погруженной и восстановленной информации алгоритмами StegoGraph, StegoGraph1, StegoGraph2: а) – представление погруженной информации возмущенными СНВ (P- норма разности СНВ матрицы контейнера и матрицы стегосообщения, N – номер СНВ); б) – объем правильно восстановленной информации (R,%) при различных значения D.

Заключение

В работе рассмотрены алгоритмы для стегосистем, задачей которых является скрытая передача конфиденциальной информации. Отличительной особенностью таких систем является сокрытие самого факта передачи сообщений, поэтому одной из важнейших характеристик является надежность восприятия стегосообщения. Логично заключить, что чем меньше мы вносим возмущения в контейнер, тем надежней стегоканал, именно по этому принципу был построен алгоритм Stego_Graph, а также алгоритм, например, представленный

в [6], в котором пиксели контейнера, как правило, заменяются найденными необходимыми по значению пикселями, а не корректируются. Все подобные алгоритмы, основанные на малых возмущениях кодирования, очень чувствительны к помехам, поскольку, как показано в четвертом разделе, малые возмущения контейнера при стегопреобразовании приводят к возмущениям лишь малоустойчивых СНВ, отвечающим малым СНЧ. Под влиянием внешних воздействий такие вектора получают дополнительные возмущения и значительная часть ДИ, которая в них находится, теряется.

Для создания помехоустойчивых алгоритмов следует стремиться к тому, чтобы возмущению подвергались вектора, отвечающие большим СНЧ. СНВ, отвечающие самым большим СНЧ самые устойчивые. Даже при сильных помехах, когда изображение претерпевает серьезные искажения, можно извлечь информацию из этих векторов почти без потерь. Но, к сожалению, мы не можем погружать информацию в эти вектора, поскольку нарушается надежность восприятия стегосообщения. Это оъясняется тем, что СНВ, отвечающие наибольшим СНЧ матрицы изображения соответствуют низкочастотным, а наименьшим – высокочастотным составляющим исходного контейнера. Частотная чувствительность системы человеческого зрения проявляется в том, что человек гораздо более восприимчив к низкочастотной, чем к высокочастотной составляющей сигнала. В силу сказанного выше задача разработки помехоустойчивого алгоритма представляет собой поиск компромисса между его характеристиками, так как улучшение одного его параметра, например, величину пропускной способности, приходится обеспечивать за счет других параметров, таких как скрытность передачи информации или устойчивость к возмущающим воздействиям.

В модификациях алгоритма Stego_Graph удалось повысить помехоустойчивость, не меняя при этом пропускную способность, обеспечив надежность восприятия стегосообщения. В настоящее время автор продолжает работу над проблемой повышения помехоустойчивости стегоалгоритмов.

Список літератури

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

2. Борисенко И.И. Особенности применения многоуровневого порогового преобразования изображения в компьютерной стеганографии. Праці УНДІРТ. Теоретичний та науково-практичний журнал радіозв'язку, радіомовлення і телебачення, 4(48) 2006. Видання УНДІРТ м. Одеса – с.53-59.

3. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности.-К.:ДУИКТ, 2009.-250 с.

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

5. Кобозєва А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснованого на теорії збурень. - Информационные технологи и компьютерная инженерия, №1(11), 2008, с.164-171.

6. A Graph-Theoretic Approach to Steganography. Stefan Hetzl (Institute of Computer Languages, Vienna University of Technology, hetzl@logic.at) and Petra Mutzel (Institute of Algorithm Engineering, University of Dortmund, Germany, petra.mutzel@cs.uni-dortmund.de).

7. Б.Н. Иванов. Дискретная математика. Алгоритмы и программы. –М: Лаборатория Базовых Знаний, 2001.-288 с.

Областю наукових досліджень є комп'ютерна стеганографія, а саме стегосистеми, які забезпечують таємну передачу конфіденціальної інформації. В статті розглядається питання підвищення стійкості до завад алгоритму, який був розроблений для створення стегоповідомлень в умовах ідеального каналу зв'язку.

Ключові слова: стеганографія, алгоритм, стійкість до завад.

В статье рассматривается вопрос повышения стойкости к помехам алгоритма, разработанного для создания стегосообщений в условиях идеального канала связи.

Ключевые слова: стеганография, алгоритм, стойкость з помехам.

The task of improvement of noise stability of the algorithm, that was developed for creating steganomessages in the ideal communication channel.

Key words: steganography, algorithm, noise stability.

Поступила 18.11.2009