Лабораторная работа № 11
Скрытая передача информации с помощью программы Mathcad

1. Цель работы

Изучить методы скрытой передачи информации с помощью программы Mathcad.

2. Общие сведения

Математическая система **Mathcad** естественно вписалась в операционную систему MS Windows. Система имеет удобный интерфейс, хорошо развитые средства помощи и обширную справочную базу. Программа Mathcad позволяет проводить численные расчёты и аналитические преобразования, строить многоцветные двух- и трёхмерные графики.

Отличительной особенностью системы является использование в ней общепринятых в математике символов для обозначения операций интегрирования, дифференцирования, вычисления рядов, пределов и т. д. Возможность использования латинских, греческих букв, верхних и нижних индексов позволяет записывать формулы в привычном виде. С помощью кириллицы можно делать комментарии на русском языке.

Очень просты в реализации многие численные методы: решение линейных и нелинейных уравнений, вычисление определённых интегралов, оптимизация, решение дифференциальных уравнений, сплайн-интерполяция, аппроксимация и т. д.

С помощью математической системы Mathcad удобно осуществлять исследование и изучение методов криптографии и стеганографии, так как система позволяет использовать не только встроенные функции, но осуществлять программирование.

Для внедрения в графический файл в данной работе использован метод LSB. Для внедрения информации в текстовый контейнер использована ещё одна идея. Она состоит в том, что делают разное число пробелов в конце каждого предложения текстового документа. Причём для внедрения нуля вставляют два пробела, а для внедрения единицы – один пробел.

3. Задания на выполнение лабораторной работы

3.1. Задание 1. Сокрытие информации в младших битах графического контейнера

В соответствии с номером варианта необходимо с помощью математической системы Mathcad скрыть текст в цветном рисунке формата BMP. Рисунки находятся в папке Container. Текст перед внедрением должен быть зашифрован методом Виженера. Ключ для шифрования выбирается в соответствии с табл. 3.1.1. Шифруемый текст указан в табл. 3.1.2.

Таблица 3.1.1

Вариант	Ключ	Вариант	Ключ
1	Mgp2CqP	9	77FDQpy
2	LJy573D	10	RqMn765
3	29bNSar2	11	ECCxz3G
4	GRwq62	12	MCZ871ha
5	Dmv91FF	13	917BVt3S
6	Tsz63LH	14	HAqp55C
7	Ffw175Jj	15	nwYY51J
8	gvBNM99	16	tLDa441

Таблица 3.1.2

Вар	Текст
1	Иногда нежелание уступить место в транспорте делает мужчину начитаннее. *В. Колечицкий*
2	Всегда глупым не бывает никто, иногда – бывает каждый. *Г. Уэллс*
3	Границы рая и ада подвижны, но всегда проходят через нас. *С. Лец*
4	Хочешь обнять весь мир – купи глобус. *М. Генин*
5	Для того, чтобы носить очки, мало быть умным, надо ещё плохо видеть. *В. Дубинский*
6	В математике нет символов для неясных мыслей. *А. Пуанкаре*
7	Рыба, которая в каждом червяке видит крючок, долго не проживёт. *З. Холодюк*
8	Многие мужчины, влюбившись в ямочку на щеке, по ошибке женятся на всей девушке. *С. Ликок*
9	В настоящей бомбе с часовым механизмом взрывчатым веществом является время. *С. Лец*
10	Сколько человека не воспитывай, он всё равно хочет жить хорошо. *Б. Замятин*
11	Телеграфный столб никогда не поймёт принцип действия телеграфа. *Л .Собеский*
12	Столбу много прощается за его прямоту. *Ц. Меламед*
13	Тот, кто не разбирается ни в чём, может взяться за что угодно. *С. Лец*
14	В практической жизни от гения проку не более, чем от телескопа в театре. *А. Шопенгауэр*
15	Дни такие длинные, а годы такие короткие. *А. Доде*
16	Если хочешь выглядеть молодой и стройной, держись поближе к старым и толстым. *Д. Исон*

3.2. Задание 2. Исследование графического контейнера

В соответствии с номером варианта определить десятичные значения цветовых составляющих пустого (исходного) контейнера (R, G, B) для пикселя, координаты которого указаны в таблице 3.2.1.

Таблица 3.2.1

Вариант	Строка	Столбец
1	9	30
2	10	31
3	11	32
4	12	33
5	13	34
6	14	35
7	15	36
8	16	37
9	17	38
10	18	39
11	19	40
12	20	10
13	21	11
14	22	12
15	23	13
16	24	14

3.3. Задание 3. Внедрение информации в текстовые документы

Необходимо в текстовом документе с помощью Mathcad скрыть указанную в табл. 3.3.1 букву. Для выполнения этого задания следует подготовить контейнер – текстовый документ, который содержит более восьми предложений, разделённых точками. Основу контейнера должны составлять немецкие пословицы, указанные в таблице 3.3.1. Указанный фрагмент текста следует дополнить цифрами, которые разделены точками.

Таблица 3.3.1

Вар.	Внедряемая буква	Фрагмент текстового контейнера
1	A	Besser ein kleiner Fisch als gar nichts auf dem Tisch
2	B	Besser heut ein Ei als morgen ein Kuechlein
3	C	Besser zweimal messen, als einmall vergessen
4	D	Alt Holz brennt besser als junges
5	E	Der Gast ist wie der Fisch, er bleibt nicht lange frisch
6	F	Der Kranke und der Gesunde haben ungleiche Stunde
7	G	Anderer Fehler sind gute Lehrer
8	H	Einem geschenkten Gaul schaut man nicht ins Maul
9	I	Ein gutter Plan ist halb getan
10	J	Jedes Tierchen hat sein Plaesierchen
11	K	Keine Antwort ist auch eine Antwort
12	L	Kraft, die nicht wirkt, erschlafft
13	M	Liebe und Verstand gehen selten Hand in Hand
14	N	Man lernt, solange man lebt
15	O	Voller Magen lernt mit Unbehagen
16	P	Ein Erfahrener ist besser als zehn Gelehrte

4. Порядок выполнения лабораторной работы

4.1. Методические указания к заданию 3.1

Основная идея сокрытия информации в графическом файле, которая использована в этом задании, заключается в том, что каждый внедряемый символ сообщения преобразуют в двоичную систему счисления и побитно внедряют в графический контейнер, путём замены последних (младших) битов цветовых составляющих изображения.

Программа, с помощью которой осуществляется сокрытие информации в рисунках формата BMP, находится в папке Задание_1. Имя файла grafika.xmcd (Mathcad 15). Скрываемое сообщение следует поместить в текстовый документ M.txt. Демонстрационный незаполненный графический контейнер имеет имя quadr.bmp. Контейнеры для каждого варианта находятся в папке Container. Рисунок с внедрённым текстом сохраняется в графическом файле с именем S_LSB.bmp. Извлечённый на приёме из рисунка текст помещается в текстовый файл m_dec.txt.

Если не делать изменений в программе, то все перечисленные документы должны быть размещены на диске D, в папках Stego_Math\Grafika_Lab. Очевидно, что при использовании дисков, файлов и папок с другими именами необходимо сделать соответствующие изменения в тексте программы (указать правильный путь).

Текст программы снабжён подробными комментариями, которые позволяют детально разобраться в алгоритмах шифрования и сокрытия информации.

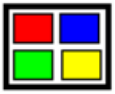
Передающая сторона

Mathcad 15

ORIGIN := 1

Контейнером. является рисунок формата BMP (глубина цвета 24 бита)

Внешний вид графического контейнера



"D:\Stego_Math\Grafika_Lab\quadr.bmp"

Считывание матрицы цветовых компонент

C := READRGB("D:\Stego_Math\Grafika_Lab\quadr.bmp")

Матрица цветовых составляющих RGB контейнера

C =

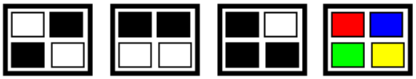
	1	2	3	4	5	6	7	8	9
1	255	255	255	255	255	255	255	255	255
2	255	255	255	255	255	255	255	255	255
3	255	255	255	255	255	255	255	255	255
4	255	255	255	255	255	255	255	255	255
5	255	255	255	255	255	0	0	0	0
6	255	255	255	255	255	0	0	0	0
7	255	255	255	255	255	0	0	0	...

Грфическое представление цветовых составляющих контейнера

Следует обратить внимание на строки D:\Stego_Math\Grafika_Lab\quadr.bmp они указывают путь к контейнеру. При выполнении работы в каждом конкретном случае нужно выполнить коррекцию подобных строк.

Грфическое представление цветовых составляющих контейнера

R G B Исходный рисунок



C "D:\Stego_Math\Grafika_Lab\quadr.bmp"

Белый цвет на предыдущем рисунке - соответствующая составляющая есть, черный цвет - данной составляющей нет.

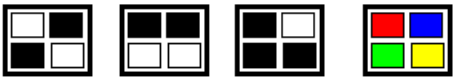
Желтый цвет представляет собой смесь красного и зеленого цветов.

Ниже осуществляется выделение каждой из трех цветовых составляющих:

R := READ_RED("D:\Stego_Math\Grafika_Lab\quadr.bmp")

G := READ_GREEN("D:\Stego_Math\Grafika_Lab\quadr.bmp")

B := READ_BLUE("D:\Stego_Math\Grafika_Lab\quadr.bmp")



R G B "D:\Stego_Math\Grafika_Lab\quadr.bmp"

Представление открытого текста в десятичной и двоичной СС

Открытый текст находится в файле с именем M.txt

M := READBIN("M.txt" ,"byte")

M =

	1
1	207
2	240
3	238
4	225
5	224
6	32
7	32
8	207
9	240
10	238
11	225
12	224
13	32
14	32
15	207
16	...

M =

	1
1	11001111b
2	11110000b
3	11101110b
4	11100001b
5	11100000b
6	100000b
7	100000b
8	11001111b
9	11110000b
10	11101110b
11	11100001b
12	11100000b
13	100000b
14	100000b
15	11001111b
16	...

Число символов в открытом тексте

Nm := rows(M) Nm = 56

Формирование алфавита источника сообщения

i := 1.. 256

$A_i := i - 1$ $A_1 = 0$ $A_{256} = 255$

$Na := rows(A)$ $Na = 256$

Секретный ключ

$K := "SeCrE"$

Количество символов в ключе

$Nk := strlen(K)$

$Nk = 5$

Ключ в десятичной СС

$$str2vec(K) = \begin{pmatrix} 83 \\ 101 \\ 67 \\ 114 \\ 69 \end{pmatrix}$$

Увеличение ключа до длины открытого текста
за счета циклического повторения ключа.

$$K' := \left| \begin{array}{l} K \leftarrow str2vec(K) \\ \text{for } i \in 1..Nm \\ \quad \left| \begin{array}{l} r \leftarrow mod(i, Nk) \\ K'_i \leftarrow K_r \text{ if } r > 0 \\ K'_i \leftarrow K_{Nk} \text{ if } r = 0 \end{array} \right. \\ K' \end{array} \right.$$

K' =

	1
1	83
2	101
3	67
4	114
5	69
6	83
7	101
8	67
9	114
10	69
11	83
12	101
13	67
14	114
15	69
16	...

Шифрование модифицированным методом Виженера

```
M_cod := | for j ∈ 1..Nm
         |   for i ∈ 1..Na
         |     m ← i if M_j = A_i
         |     n ← i if K'_j = A_i
         |   r ← mod(m + n,Na)
         |   M_cod_j ← A_r if r > 0
         |   M_cod_j ← A_Na if r = 0
         | M_cod
```

Текст

M =

	1
1	207
2	240
3	238
4	225
5	224
6	32
7	32
8	207
9	240
10	238
11	225
12	224
13	32
14	32
15	207
16	...

Ключ

K' =

	1
1	83
2	101
3	67
4	114
5	69
6	83
7	101
8	67
9	114
10	69
11	83
12	101
13	67
14	114
15	69
16	...

Криптограмма

M_cod =

	1
1	35
2	86
3	50
4	84
5	38
6	116
7	134
8	19
9	99
10	52
11	53
12	70
13	100
14	147
15	21
16	...

M_cod=M+K`+1(mod256)

Ключ = SeCrE

Метки начала и конца мест внедрения текста в контейнер.
Метки должны представлять собой комбинации символов,
вероятность появления которых в тексте мала.

μs := "@start@"

μe := "@endnd@"

Добавление меток к зашифрованному тексту

$$sMe := stack(str2vec(\mu s), M\_cod, str2vec(\mu e))$$

Число символов в скрываемом сообщениии (включая метки начала и конца вложения)

$$rows(sMe) = 70$$

Количество необходимых битов (НЗБ) для сокрытия сообщения и меток

$$8 \cdot rows(sMe) = 560$$

Число имеющихся НЗБ в выбранном графическом контейнере

$$rows(C) \cdot cols(C) = 1.065 \times 10^4$$

В данном контейнере можно скрыть текст, состоящий из

$$rows(C) \cdot \frac{cols(C)}{8} = 1.332 \times 10^3 \quad \text{букв}$$

Полученное значение говорит о том, что текст с запасом умещается в контейнере.

Функция преобразования десятичного числа в двоичное число

$$D2B(x) := \left| \begin{array}{l} \text{for } i \in 1..8 \\ \quad \left| \begin{array}{l} V_i \leftarrow mod(x, 2) \\ x \leftarrow floor\left(\frac{x}{2}\right) \end{array} \right. \\ V \end{array} \right.$$

Преобразование матрицы C в вектор Cv и изменение порядка следования цветовых матриц с R-G-B на B-G-R.
Перестановка цветовых составляющих сделана для повышения криптостойкости.

```
Cv := | C' ← augment(B, G, R)
      | Cv ← C'^⟨1⟩
      | for i ∈ 2.. cols(C')
      |   Cv ← stack(Cv, C'^⟨i⟩)
```

Cv =

	1
1	255
2	255
3	255
4	255
5	255
6	255
7	...

Вложение сообщения в контейнер

```
Sv := | for μ ∈ 1.. rows(sMe)
      |   b ← D2B(sMe_μ)
      |   for i ∈ 1.. 8
      |     P ← D2B[Cv_{i+8·(μ−1)}]
      |     P_1 ← b_i
      |     Sv_{i+8·(μ−1)} ← B2D(P)
      | for j ∈ rows(Sv) + 1.. rows(Cv)
      |   P ← D2B(Cv_j)
      |   P_1 ← round(rnd(1))
      |   Sv_j ← B2D(P)
      | Sv
```

Результат вложения в векторной форме:

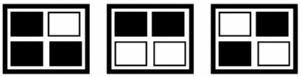
Sv =

	1
1	254
2	254
3	254
4	254
5	254
6	...

Преобразование вектора Sv в матрицу
S

$$S' := \text{for } i \in 1,2..\text{cols}(C)$$
$$S^{\langle i \rangle} \leftarrow \text{submatrix}[Sv,(i-1)\cdot\text{rows}(C)+1,i\cdot\text{rows}(C),1,1]$$

Результат преобразования в матрицу



S'

Исходная матрица цветов

C

Из сравнения матриц видно, что в полученной матрице S` две составляющие переставлены (R и B)

Расстановка цветовых матриц в правильном порядке

$$BM := \text{submatrix}\left(S',1,\text{rows}(C),1,\frac{\text{cols}(C)}{3}\right)$$

$$GM := \text{submatrix}\left(S',1,\text{rows}(C),\frac{\text{cols}(C)}{3}+1,2\cdot\frac{\text{cols}(C)}{3}\right)$$

$$RM := \text{submatrix}\left(S',1,\text{rows}(C),2\cdot\frac{\text{cols}(C)}{3}+1,\text{cols}(C)\right)$$

$$S := \text{augment}(RM,GM,BM)$$

Результат восстановления

S

Исходные матрицы

C

Из сравнения последних рисунков видно, что цветовые составляющие пустого контейнера и заполненного расставлены в одинаковом порядке

$$\text{WRITERGB}(\text{"S\_LSB.bmp"}) := S$$

Контейнер S-LSB.bmp содержит секретное и вложение и этот рисунок следует переслать на приемную сторону

Приемная сторона

Выдение цветовых составляющих

RP := READ_RED("S_LSB.bmp")

RP

GP := READ_GREEN("S_LSB.bmp")

GP

BP := READ_BLUE("S_LSB.bmp")

GP

Преобразование матрицы в вектор

$$SvP := \left| \begin{array}{l} S' \leftarrow \text{augment}(BP, GP, RP) \\ SvP \leftarrow S'^{\langle 1 \rangle} \\ \text{for } i \in 2..\text{cols}(S') \\ \quad SvP \leftarrow \text{stack}\left(SvP, S'^{\langle i \rangle}\right) \end{array} \right.$$

SvP =

	1
1	254
2	254
3	254
4	254
5	254
6	254
7	...

$$MfP := \left| \begin{array}{l} \text{for } \mu \in 1..\dfrac{\text{rows}(SvP)}{8} \\ \quad \text{for } i \in 1..8 \\ \quad\quad P \leftarrow D2B\left[SvP_{i+8\cdot(\mu-1)}\right] \\ \quad\quad b_i \leftarrow P_1 \\ \quad MfP_\mu \leftarrow B2D(b) \\ \quad MfP_\mu \leftarrow MfP_\mu + 32.5 \text{ if } MfP_\mu < 32 \\ MfP \end{array} \right.$$

MfP =

	1
1	64
2	115
3	116
4	97
5	114
6	...

$\text{rows}(\text{MfP}) = 1.331 \times 10^3$

```
N := | for s ∈ 0,1..31
     |   i ← 1
     |   for μ ∈ 1..rows(MfP)
     |     if MfP_μ = s + 32.5
     |       N_{i,s+1} ← μ
     |       i ← i + 1
     | N
```

```
M_codP := | s ← 0
          | e ← 0
          | βs ← strlen(μs)
          | βe ← strlen(μe)
          | MfP ← vec2str(MfP)
          | for μ ∈ 1..strlen(MfP)
          |   s ← μ + βs if substr(MfP,μ,βs) = μs ∧ s = 0
          |   e ← μ − 1 if substr(MfP,μ,βe) = μe ∧ e = 0
          |   break if s ≠ 0 ∧ e ≠ 0
          | MfP ← substr(MfP,s,e − βs)
          | M_codP ← str2vec(MfP)
          | for n ∈ 1..cols(N)
          |   for i ∈ 1..rows(N)
          |     break if N_{i,n} = 0
          |     M_codP_{(N_{i,n})−βs} ← n − 1 if 0 < N_{i,n} ≤ rows(M_codP) + βs
          | M_codP
```

Алфавит на приеме

$i := 1..256$

$AP_i := i - 1$

Число символов

$NaP := rows(AP)$

$NaP = 256$

Секретный ключ

$KP := "SeCrE"$

$NkP := strlen(KP)$

Длина ключа

$NkP = 5$

Объем принятого сообщения

$NmP := rows(M\_codP)$

$rows(sMe) = 70$

Расширение секретного ключа до длины секретного сообщения M_codP

$$K'P := \left| \begin{array}{l} KP \leftarrow str2vec(KP) \\ \text{for } i \in 1..NmP \\ \quad r \leftarrow mod(i, NkP) \\ \quad K'P_i \leftarrow KP_r \text{ if } r > 0 \\ \quad K'P_i \leftarrow KP_{NkP} \text{ if } r = 0 \\ K'P \end{array} \right.$$

$K'P =$

	1
1	83
2	101
3	67
4	114
5	69
6	83
7	101
8	67
9	114
10	69
11	83
12	...

```
MP := | for j ∈ 1..NmP
      |   for i ∈ 1..NaP
      |     m ← i if M_codP_j = AP_i
      |     n ← i if KP_j = AP_i
      |   r ← mod(NaP + m − n, NaP)
      |   MP_j ← AP_r if r > 0
      |   MP_j ← AP_NaP if r = 0
      | MP
```

WRITEBIN("m_dec.txt","byte",0) := MP

Отправленный открытый текст находится в файле M.txt
Принятый текст находится в файле m_dec.txt

Переданный текст

M =

	1
1	207
2	240
3	238
4	225
5	224
6	32
7	32
8	207
9	240
10	238
11	225
12	224
13	32
14	32
15	207
16	...

Принятый текст

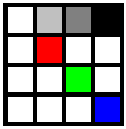
MP =

	1
1	207
2	240
3	238
4	225
5	224
6	32
7	32
8	207
9	240
10	238
11	225
12	224
13	32
14	32
15	207
16	...

4.2. Методические указания к заданию 3.2

Рассмотрим, как располагаются цветовые компоненты в матрице цветовых составляющих.

Пусть рисунок представляет собой небольшой квадрат со стороной 4 пикселя. В верхней строке квадрата расположены белый, два серых и чёрный пиксели. Во второй строке - три белых и красный пиксели. Третья строка состоит из трёх белых и одного зелёного пикселя. В последней строке рисунка располагаются три белых и синий пиксели. Первый столбец состоит из четырёх белых пикселей.



Матрица цветовых составляющих, которая описывает этот рисунок, содержит 4 строки и 12 столбцов. Число строк в матрице совпадает с числом строк на рисунке. Число столбцов в матрице в три раза больше, чем число пикселей в строке рисунка. Это объясняется тем, что для каждого пикселя необходимо указать три цветовые составляющие: красную, зелёную и синюю (R, G и B). В данном случае используется 24-х битная модель цветного рисунка.

	1	2	3	4	5	6	7	8	9	10	11	12
1	255	192	128	0	255	192	128	0	255	192	128	0
2	255	255	255	255	255	0	255	255	255	0	255	255
3	255	255	0	255	255	255	255	255	255	255	0	255
4	255	255	255	0	255	255	255	0	255	255	255	255
5	R	R	R	R	G	G	G	G	B	B	B	B

Первая строка матрицы цветовых составляющих описывает первую строку рисунка. При этом компоненты, расположенные в столбцах 1, 5 и 9 (255, 255, 255) соответствуют белому пикселю, который находится в левом верхнем углу рис.1. Чёрный пиксель в правом верхнем углу рисунка описывается составляющими 0, 0, 0, которые расположены в первой строке, в столбцах 4, 8 и 12. Красный пиксель (составляющие 255, 0, 0) описывается элементами, находящимися во второй строке (столбцы 2, 6 и 10).

Анализируя рисунок и матрицу, несложно разобраться с описанием остальных пикселей.

4.3. Методические указания к заданию 3.3

Основная идея сокрытия информации с помощью рассматриваемого способа состоит в том, что делают разное число пробелов в конце каждого предложения контейнера. Причём для внедрения 0 делают два пробела, а для внедрения 1 – один пробел. Очевидно, что пропускная способность такой стеганосистемы низкая. С помощью одного предложения открытого текста можно передать лишь один бит. Если принять, что среднее предложение состоит из восьми слов по семь букв, то пропускная способность составит 0,002.

Программа для сокрытия информации в текстовых документах находится в папке Задание_3 (имя файла – Probely_Lab.xmcd). Пустой контейнер сохранен с именем cont.txt. Контейнер с внедрённой информацией имеет имя m_per.txt. Принятое сообщение хранится в текстовом документе с именем m_prm.txt.

По заданию требуется скрыть в контейнере одну букву (то есть 8 бит информации). Это означает, что пустой контейнер должен содержать не менее восьми предложения. Признаком предложения является сочетание двух символом: точки и пробела.

Таким образом, для выполнения задания необходимо создать текстовый документ, в который нужно вписать заданную немецкую пословицу. Очевидно, что пословица не позволит скрытно передать 8 бит информации. Поэтому текст пословицы должен быть дополнен несколькими предложениями.

Рассмотрим, как это можно сделать.

Пример.

Пусть задан текст, в котором нужно скрытно передать 1 байт информации:

Er ist das fünfte Rad am Wagen.

Дополним его символами, среди которых чаще всего встречаются точки и пробелы (они имитируют предложения).

Er ist das fünfte Rad am Wagen. 1. 2. 3. 4. 5. 6. 7. 8.

Такой (или подобный) контейнер можно использовать для скрытой передачи информации.

Указанные дополнения пословиц цифрами сделаны для уменьшения объёма набираемого текста и для большей концентрации на идее сокрытия информации.

Далее приведён текст программы.

Передающая сторона

Mathcad 11

Кодирование осуществляется путем изменения числа пробелов в конце предложения. Два пробела - логический 0, один пробел - логическая 1.

ORIGIN := 1

Считывание контейнера с жесткого диска.

Контейнер на кириллице воспроизводится непечатаемыми символами. По этой причине целесообразно использовать текст, использующий латинские буквы.

C := READBIN("c16.txt" ,"byte")

$Ct := C^T$

Ct =

	1	2	3	4	5	6	7	8	9	10
1	80	114	111	98	97	46	32	82	111	...

Вввод секретного сообщения.
Здесь можно использовать и латиницу и кириллицу.

M := "F"

Десятичный код вложения

str2vec(M) = (70)

Формирование метки окончания предложения (точка пробел).

π := ". "

Десятичные коды метки окончания предложения

$\text{str2vec}(\pi)^{T} = (46 \quad 32)$

Определение числа битов в скрываемом сообщении.

$L := 8 \cdot \text{strlen}(M) \qquad L = 8$

Определение объема контейнера

$$N\pi := \left| \begin{array}{l} N\pi \leftarrow 0 \\ \text{for } i \in 1..\text{rows}(C) \\ \quad \left| \begin{array}{l} II \leftarrow \text{submatrix}(C, i, i+1, 1, 1) \text{ if } i < \text{rows}(C) \\ N\pi \leftarrow N\pi + 1 \text{ if } II = \text{str2vec}(\pi) \end{array} \right. \\ N\pi \end{array} \right.$$

В выбранном контейнере можно скрыть Nπ бит

$N\pi = 8$

Функции преобразования чисел из одной СС в другую

$$D2B(x) := \left| \begin{array}{l} \text{for } i \in 1..8 \\ \quad \left| \begin{array}{l} V_i \leftarrow \text{mod}(x, 2) \\ x \leftarrow \text{floor}\left(\frac{x}{2}\right) \end{array} \right. \\ V \end{array} \right.$$

$$B2D(x) := \sum_{i=1}^{8} \left(x_i \cdot 2^{i-1}\right)$$

Вложение сообщения в контейнер

```
S := Mvec ← str2vec(M)
     Mvec_bin ← D2B(Mvec_1)
     for j ∈ 2 .. strlen(M)
       Mvec_bin ← stack(Mvec_bin, D2B(Mvec_j))  if strlen(M) > 1
     C' ← C
     for μ ∈ 1 .. 8·strlen(M)
       for i ∈ 1 .. rows(C')
         S_(rows(S)+1) ← C'_i
         II ← submatrix(C', i, i + 1, 1, 1)  if i < rows(C')
         if II = str2vec(π)
           if Mvec_bin_μ = 1
             C' ← submatrix(C', i + 2, rows(C'), 1, 1)
             S_(rows(S)+1) ← 32
             while (C'_1) = 32
               C' ← submatrix(C', 2, rows(C'), 1, 1)
             break
           if Mvec_bin_μ = 0
             if II = str2vec(π)
               C' ← submatrix(C', i + 2, rows(C'), 1, 1)
               S_(rows(S)+1) ← 32
               S_(rows(S)+1) ← 32
               while C'_1 = 32
                 C' ← submatrix(C', 2, rows(C'), 1, 1)
             break
     stack(S, C')
```

Десятичные коды заполненного контейнера

S =

	1
1	80
2	114
3	111
4	98
5	97
6	46
7	32
8	...

$St := S^T$

+

St =

	1	2	3	4	5	6	7	8	9	10
1	80	114	111	98	97	46	32	32	82	...

F(01000110)

$D2B(70)^T = (0\ 1\ 1\ 0\ 0\ 0\ 1\ 0)$ Здесь старший разряд справа.

Исходный текст

vec2str(C) = "Proba. Roba. Boba. Eins. Zwei. Drei. Vier. Fuenf. Ja"

Шифрограмма

vec2str(S) = "Proba. Roba. Boba. Eins. Zwei. Drei. Vier. Fuenf. Ja"

Приемная сторона

Извлечение вложения

$S' := S$

$P := \pi$

$$M' := \left| \begin{array}{l} \mu \leftarrow 1 \\ \text{for } i \in 1..\text{rows}(S') \\ \quad \left| \begin{array}{l} II \leftarrow \text{submatrix}(S', i, i+1, 1, 1) \text{ if } i < \text{rows}(S') \\ \text{if } II = \text{str2vec}(P) \\ \quad \left| \begin{array}{l} M'bin_{\mu} \leftarrow 0 \text{ if } S'_{i+1} = S'_{i+2} = 32 \\ M'bin_{\mu} \leftarrow 1 \text{ if } S'_{i+1} \neq S'_{i+2} \\ \mu \leftarrow \mu + 1 \end{array} \right. \end{array} \right. \\ \text{for } j \in 1..\text{rows}(M'bin) \div 8 \\ \quad M'vec_j \leftarrow B2D(\text{submatrix}(M'bin, 8 \cdot j - 7, 8 \cdot j, 1, 1)) \\ \text{vec2str}(M'vec) \end{array} \right.$$

Результат извлечения скрытого в пробелах текста (символа)

$M' = "F"$

Отправленный и принятый символы совпали.

5. Требования к отчёту

Отчёт подготавливается в электронном виде. Он должен содержать рисунок, содержащий указанный в задании текст, десятичные значения цветовых составляющих указанных пикселей, текстовый документ с внедрённым символом, листинги использованных программ.

6. Контрольные вопросы

6.1. Какие математические системы Вы знаете?

6.2. Что означает аббревиатура LSB?

6.3. Как с помощью матрицы цветовых составляющих определить значения компонент R, G, B для заданного пикселя?

6.4. Как по известному размеру графического контейнера формата BMP определить максимальный объем внедряемого сообщения методом LSB?

6.5. Перечислите методы внедрения информации в текстовые документы

6.6. Перечислите форматы графических файлов.

6.7. Перечислите цветовые модели.

7. Список литературы

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. — 288 с. — ISBN: 966-8806-06-9