Лекция 13. Схемы разделения секрета. Визуальная криптография

Косолапов Ю.В.

ЮФУ

2 декабря 2020 г.

Содержание

Постановка задачи

Постановка задачи

- Имеется черно-белое **секретное** изображение размера $K \times N$, которое требуется разделить среди n участников.

Постановка задачи

- Имеется черно-белое **секретное** изображение размера $K \times N$, которое требуется разделить среди n участников.
- Каждый участник не должен получить какой-либо информации о секрете по своей доле (доли участников еще называются **тенями**).

Постановка задачи

- Имеется черно-белое **секретное** изображение размера $K \times N$, которое требуется разделить среди n участников.
- Каждый участник не должен получить какой-либо информации о секрете по своей доле (доли участников еще называются **тенями**).
- Любые k участников должны восстановить секрет.

Постановка задачи

- Имеется черно-белое **секретное** изображение размера $K \times N$, которое требуется разделить среди n участников.
- Каждый участник не должен получить какой-либо информации о секрете по своей доле (доли участников еще называются **тенями**).
- Любые k участников должны восстановить секрет.
- Восстановление секрета должно производиться без вычислений: визуально.

Постановка задачи

- Имеется черно-белое **секретное** изображение размера $K \times N$, которое требуется разделить среди n участников.
- Каждый участник не должен получить какой-либо информации о секрете по своей доле (доли участников еще называются **тенями**).
- Любые k участников должны восстановить секрет.
- Восстановление секрета должно производиться без вычислений: визуально.

Возможный протокол Recon

Совместить тени, распечатанные на просвечивающейся пленке, и посмотреть результат на просвет (около источника света).

Постановка задачи

- Имеется черно-белое **секретное** изображение размера $K \times N$, которое требуется разделить среди n участников.
- Каждый участник не должен получить какой-либо информации о секрете по своей доле (доли участников еще называются **тенями**).
- Любые k участников должны восстановить секрет.
- Восстановление секрета должно производиться без вычислений: визуально.

Возможный протокол Recon

Совместить тени, распечатанные на просвечивающейся пленке, и посмотреть результат на просвет (около источника света).

Возможные области применения:

Постановка задачи

- Имеется черно-белое **секретное** изображение размера $K \times N$, которое требуется разделить среди n участников.
- Каждый участник не должен получить какой-либо информации о секрете по своей доле (доли участников еще называются **тенями**).
- Любые k участников должны восстановить секрет.
- Восстановление секрета должно производиться без вычислений: визуально.

Возможный протокол Recon

Совместить тени, распечатанные на просвечивающейся пленке, и посмотреть результат на просвет (около источника света).

Возможные области применения:

- Цифровые водяные знаки (защита авторских прав).

Постановка задачи

- Имеется черно-белое **секретное** изображение размера $K \times N$, которое требуется разделить среди n участников.
- Каждый участник не должен получить какой-либо информации о секрете по своей доле (доли участников еще называются **тенями**).
- Любые k участников должны восстановить секрет.
- Восстановление секрета должно производиться без вычислений: визуально.

Возможный протокол RECON

Совместить тени, распечатанные на просвечивающейся пленке, и посмотреть результат на просвет (около источника света).

Возможные области применения:

- Цифровые водяные знаки (защита авторских прав).
- Возможно: аутентификация, CAPTCHA (тест Тьюринга).

(n, n)-схема: способ М. Наор и А. Шамира (Visual cryptography, Naor& Shamir, 1994).

(n, n)-схема: способ М. Наор и А. Шамира (Visual cryptography, Naor& Shamir, 1994).

- Черно белое изображение представляется в виде $K \times N$-матрицы из нулей и единиц: 0 — белый пиксель, 1 — черный пиксель.

$$\begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,N} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,N} \\ \vdots & \cdots & \ddots & \vdots \\ b_{K,1} & b_{K,2} & \cdots & b_{K,N} \end{pmatrix}$$

(n, n)-схема: способ М. Наор и А. Шамира (Visual cryptography, Naor& Shamir, 1994).

- Черно белое изображение представляется в виде $K \times N$-матрицы из нулей и единиц: 0 — белый пиксель, 1 — черный пиксель.

$$\begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,N} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,N} \\ \vdots & \cdots & \ddots & \vdots \\ b_{K,1} & b_{K,2} & \cdots & b_{K,N} \end{pmatrix}$$

- Пример (буква «А»):

$$\begin{array}{ccccccccc} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

(n, n)-схема: способ М. Наор и А. Шамира (Visual cryptography, Naor& Shamir, 1994).

- Черно белое изображение представляется в виде $K \times N$-матрицы из нулей и единиц: 0 — белый пиксель, 1 — черный пиксель.

$$\begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,N} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,N} \\ \vdots & \cdots & \ddots & \vdots \\ b_{K,1} & b_{K,2} & \cdots & b_{K,N} \end{pmatrix}$$

- Пример (буква «А»):

$$\begin{array}{ccccccccc} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

- В протоколе SHARE каждый пиксель обрабатывается отдельно.

Протокол SHARE. Подготовка

Протокол SHARE. Подготовка

- Строится матрица S размера $n \times 2^n$ (строк столько, сколько участников)

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 1 & 1 & \dots & 1 \\ 0 & 1 & 0 & 1 & \dots & 1 \end{pmatrix}$$

Протокол SHARE. Подготовка

- Строится матрица S размера $n \times 2^n$ (строк столько, сколько участников)

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 1 & 1 & \dots & 1 \\ 0 & 1 & 0 & 1 & \dots & 1 \end{pmatrix}$$

- Из столбцов четного веса формируется матрица S_0 (**для белых пикселей**), а из столбцов нечетного – матрица S_1 (**для черных пикселей**)

$$S_0 = \begin{pmatrix} 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 1 & 1 & \dots \end{pmatrix}, S_1 = \begin{pmatrix} 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ 0 & 1 & 1 & \dots \\ 1 & 0 & 1 & \dots \end{pmatrix}$$

Протокол SHARE

Протокол SHARE для **одного** пикселя

Протокол SHARE

Протокол SHARE для **одного** пикселя

- Пусть $b \in \{0, 1\}$ — очередной пиксель секретного изображения

Протокол SHARE

Протокол SHARE для **одного** пикселя

- Пусть $b \in \{0, 1\}$ — очередной пиксель секретного изображения
- В матрице S_b случайным образом переставляются **столбцы**: $\sigma(S_b)$.

Протокол SHARE

Протокол SHARE для **одного** пикселя

- Пусть $b \in \{0, 1\}$ — очередной пиксель секретного изображения
- В матрице S_b случайным образом переставляются **столбцы**: $\sigma(S_b)$.
- Для одного бита b долей i-итого участника ($i \in \{1, ..., n\}$) является i-ая строка $\sigma(S_b)[i]$ матрицы $\sigma(S_b)$.

Итог: секретное изображение преобразуется в долю i-ого участника по схеме

$$\begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,N} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,N} \\ \vdots & \cdots & \ddots & \vdots \\ b_{K,1} & b_{K,2} & \cdots & b_{K,N} \end{pmatrix} \to \begin{pmatrix} \sigma_{1,1}(S_{b_{1,1}})[i] & \sigma_{1,2}(S_{b_{1,2}})[i] & \cdots & \sigma_{1,N}(S_{b_{1,N}})[i] \\ \sigma_{2,1}(S_{b_{2,1}})[i] & \sigma_{2,2}(S_{b_{2,2}})[i] & \cdots & \sigma_{2,N}(S_{b_{2,N}})[i] \\ \vdots & \cdots & \ddots & \vdots \\ \sigma_{K,1}(S_{b_{K,1}})[i] & \sigma_{K,2}(S_{b_{K,2}})[i] & \cdots & \sigma_{K,N}(S_{b_{K,N}})[i] \end{pmatrix}$$

Протокол SHARE. Замечание

Протокол SHARE. Замечание

- В доле i-ого участника строк столько же, сколько и в исходном изображении, но столбцов в 2^{n-1} раз больше (картинка растягивается в ширину).

Протокол SHARE. Замечание

- В доле i-ого участника строк столько же, сколько и в исходном изображении, но столбцов в 2^{n-1} раз больше (картинка растягивается в ширину).
- При восстановлении (методом «на просвет») изображение будет растянутым в ширину (это нехорошо).

Протокол SHARE. Замечание

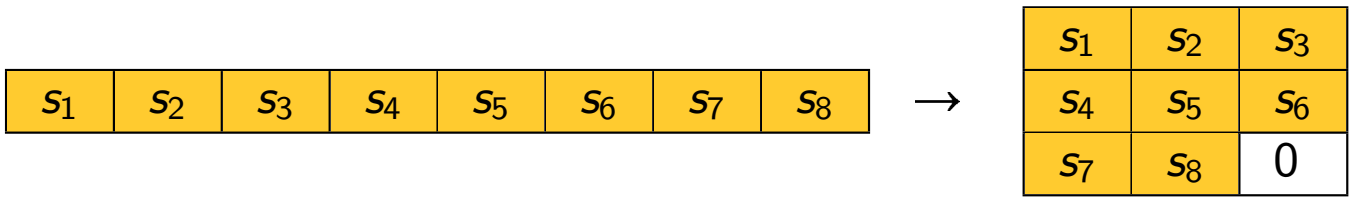
- В доле i-ого участника строк столько же, сколько и в исходном изображении, но столбцов в 2^{n-1} раз больше (картинка растягивается в ширину).
- При восстановлении (методом «на просвет») изображение будет растянутым в ширину (это нехорошо).
- Для (почти) пропорционального растяжения в ширину и в высоту, вместо строки $\sigma_{l,m}(S_{b_{l,m}})[i]$ в долю можно записывать представление этой строки в виде прямоугольной (а если получается, квадратной) матрицы.

Протокол SHARE. Замечание

- В доле i-ого участника строк столько же, сколько и в исходном изображении, но столбцов в 2^{n-1} раз больше (картинка растягивается в ширину).
- При восстановлении (методом «на просвет») изображение будет растянутым в ширину (это нехорошо).
- Для (почти) пропорционального растяжения в ширину и в высоту, вместо строки $\sigma_{l,m}(S_{b_{l,m}})[i]$ в долю можно записывать представление этой строки в виде прямоугольной (а если получается, квадратной) матрицы.
- Если для полного заполнения такой матрицы не хватает данных из $\sigma_{l,m}(S_{b_{l,m}})[i]$, то незаполненные ячейки следует заполнить нулями (либо единицами, но не случайным образом):

Протокол SHARE. Замечание

- В доле i-ого участника строк столько же, сколько и в исходном изображении, но столбцов в 2^{n-1} раз больше (картинка растягивается в ширину).
- При восстановлении (методом «на просвет») изображение будет растянутым в ширину (это нехорошо).
- Для (почти) пропорционального растяжения в ширину и в высоту, вместо строки $\sigma_{l,m}(S_{b_{l,m}})[i]$ в долю можно записывать представление этой строки в виде прямоугольной (а если получается, квадратной) матрицы.
- Если для полного заполнения такой матрицы не хватает данных из $\sigma_{l,m}(S_{b_{l,m}})[i]$, то незаполненные ячейки следует заполнить нулями (либо единицами, но не случайным образом):



Полнота протокола Recon

Почему все n участников могут восстановить секрет?

Полнота протокола Recon

Почему все n участников могут восстановить секрет?

- Доли (тени) для белых пикселей формируются на основе матрицы S_0, а доли черных пикселей – на основе матрицы S_1.

Полнота протокола Recon

Почему все n участников могут восстановить секрет?

- Доли (тени) для белых пикселей формируются на основе матрицы S_0, а доли черных пикселей – на основе матрицы S_1.
- В протоколе Recon доли накладываются друг на друга.

Полнота протокола Recon

Почему все n участников могут восстановить секрет?

- Доли (тени) для белых пикселей формируются на основе матрицы S_0, а доли черных пикселей – на основе матрицы S_1.
- В протоколе Recon доли накладываются друг на друга.
- Такое наложение можно представить, как операцию логического OR, примененную к строкам-долям.

Полнота протокола Recon

Почему все n участников могут восстановить секрет?

- Доли (тени) для белых пикселей формируются на основе матрицы S_0, а доли черных пикселей – на основе матрицы S_1.
- В протоколе Recon доли накладываются друг на друга.
- Такое наложение можно представить, как операцию логического OR, примененную к строкам-долям.
- В матрице S_0 есть один нулевой столбец, а в матрице S_1 такого столбца нет.

Полнота протокола Recon

Почему все n участников могут восстановить секрет?

- Доли (тени) для белых пикселей формируются на основе матрицы S_0, а доли черных пикселей – на основе матрицы S_1.
- В протоколе Recon доли накладываются друг на друга.
- Такое наложение можно представить, как операцию логического OR, примененную к строкам-долям.
- В матрице S_0 есть один нулевой столбец, а в матрице S_1 такого столбца нет.
- Поэтому операция OR для долей, соответствующих **черному** пикселю, даст вектор длины 2^{n-1}, состоящий из **всех единиц** (пример для $n = 4$):

1	1	1
1	1	1
1	1	0

Полнота протокола Recon

Почему все n участников могут восстановить секрет?

- Доли (тени) для белых пикселей формируются на основе матрицы S_0, а доли черных пикселей – на основе матрицы S_1.
- В протоколе Recon доли накладываются друг на друга.
- Такое наложение можно представить, как операцию логического OR, примененную к строкам-долям.
- В матрице S_0 есть один нулевой столбец, а в матрице S_1 такого столбца нет.
- Поэтому операция OR для долей, соответствующих **черному** пикселю, даст вектор длины 2^{n-1}, состоящий из **всех единиц** (пример для $n = 4$):

1	1	1
1	1	1
1	1	0

- А для долей, соответствующих **белому** пикселю, эта операция даст вектор длины 2^{n-1}, состоящий из $2^{n-1} - 1$ единиц (пример для $n = 4$):

0	1	1
1	1	1
1	1	0

,

1	0	1
1	1	1
1	1	0

,...,

1	1	1
1	1	1
1	0	0

Корректность протокола SHARE

Почему все каждый участник не может по свойе доле узнать секрет?

Корректность протокола SHARE

Почему все каждый участник не может по свойе доле узнать секрет?

- Потому что в матрицах S_0 и S_1 строки имеют одинаковый вес (хотя и разную структуру).

Корректность протокола SHARE

Почему все каждый участник не может по свойе доле узнать секрет?

- Потому что в матрицах S_0 и S_1 строки имеют одинаковый вес (хотя и разную структуру).
- Пример для $n = 3$:

$$S_0 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, S_1 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Корректность протокола SHARE

Почему все каждый участник не может по свойе доле узнать секрет?

- Потому что в матрицах S_0 и S_1 строки имеют одинаковый вес (хотя и разную структуру).
- Пример для $n = 3$:

$$S_0 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, S_1 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

- Поэтому, за счет случайной перестановки наблюдаемая в доле строка длины 2^{n-1} может соответствовать как белому пикселю, так и черному.

Корректность протокола SHARE

Почему все каждый участник не может по свойе доле узнать секрет?

- Потому что в матрицах S_0 и S_1 строки имеют одинаковый вес (хотя и разную структуру).
- Пример для $n = 3$:

$$S_0 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, S_1 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

- Поэтому, за счет случайной перестановки наблюдаемая в доле строка длины 2^{n-1} может соответствовать как белому пикселю, так и черному.
- Аналогично можно показать, что любые $n - 1$ участников не смогут восстановить секрет (упражние в качестве домашнего задания).

Заключение

Спасибо за внимание!