# Видеозаписи Обработка и защита Лекция 3. Защита видео

аспирант кафедры 42
Гусев Павел
pg@cnpo.ru

# Защита информации

- Конфиденциальность

*шифрование , …*

- Целостность

*контрольные суммы, …*

- Доступность

*механизмы аутентификации, …*

# Защита авторских прав

- Регулируется частью 4 Гражданского Кодекса Российской Федерации.
- Статья 1259. Объекты авторских прав:

*1. Объектами авторских прав являются произведения науки, литературы и искусства независимо от достоинств и назначения произведения, а также от способа его выражения:*

*…*

***аудиовизуальные произведения;***

*…*

# Цифровой водяной знак

- ЦВЗ - специальная метка, незаметно внедряемая в изображение или другой сигнал с целью тем или иным образом контролировать его использование; реквизит защищенного изображения, свидетельствующий о наличии авторских прав на данное изображение.
- *накоплен большой опыт в применении;*
- *чувствителен к изменению формата видео;*
- *бесполезен в случае, если видео было распространено до внедрения ЦВЗ.*

# Цифровой отпечаток

- Цифровой отпечаток (digital video fingerprint) - набор бит, представляющий какие-то уникальные характеристики видеопоследовательности, отражающие уникальное содержимое видео-файла; применяется в задачах обнаружения копирования на основе содержимого видео-потока.
- *зависит от содержания видео;*
- *незначительное количество исследований до настоящего времени;*
- *отсутствие реализаций в открытом доступе.*


Обнаружение копирования на основе содержимого видео-потока
Алгоритм извлечения
Алгоритм принятия решения
Извлечение характерстик
Построение цифрового отпечатка
Сравнение цифровых отпечатков
Решение
На основе сцен
На основе ключевых кадров

# Виды цифровых отпечатков

- Основанные на глобальных дескрипторах – используют все пиксели в кадре.

- Основанные на локальных дескрипторах – используют только значимые точки или POI (points of interest)

# Глобальные дескрипторы

- Границы сцен;
- Цветность, яркость и интенсивность;
- Изменения в кадре и между кадрами;
- Порядковые измерения;
- Преобразования.

# Границы сцен

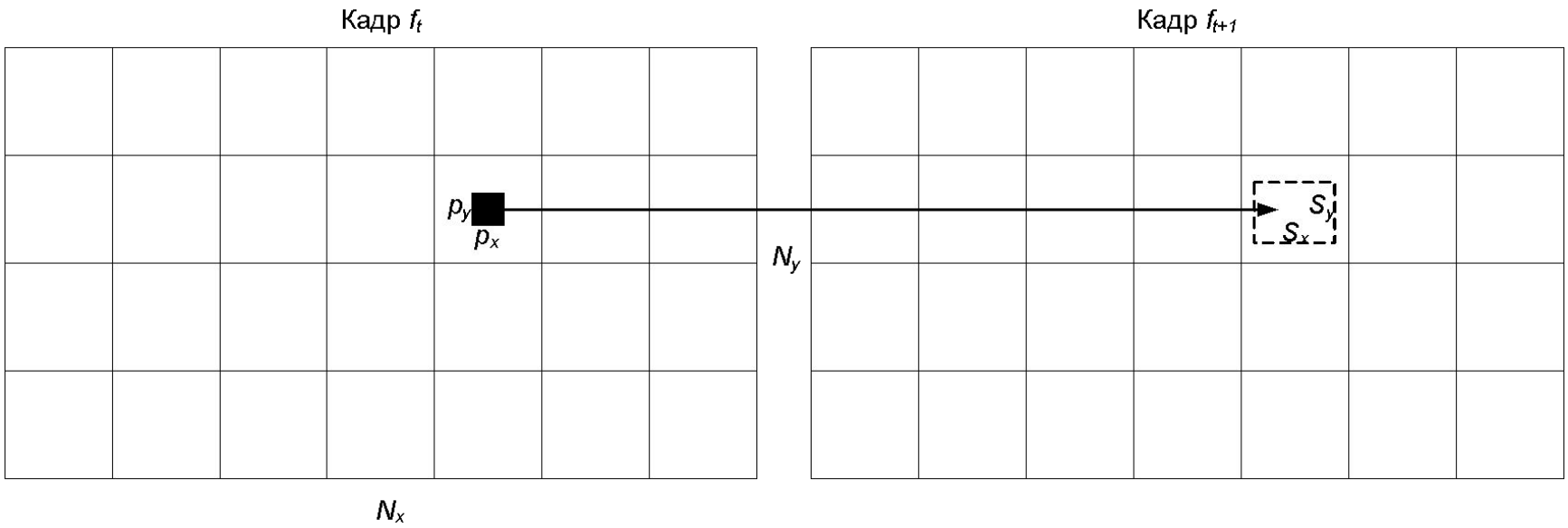
- Сцена - последовательность кадров, в которой каждый следующий кадр незначительно отличается от предыдущего.
- В качестве цифрового отпечатка используется по сути временная длительность сцен.

# Цветность, яркость и интенсивность

- Методы этого типа используют в качестве цифрового отпечатка пространственную информацию ключевых кадров

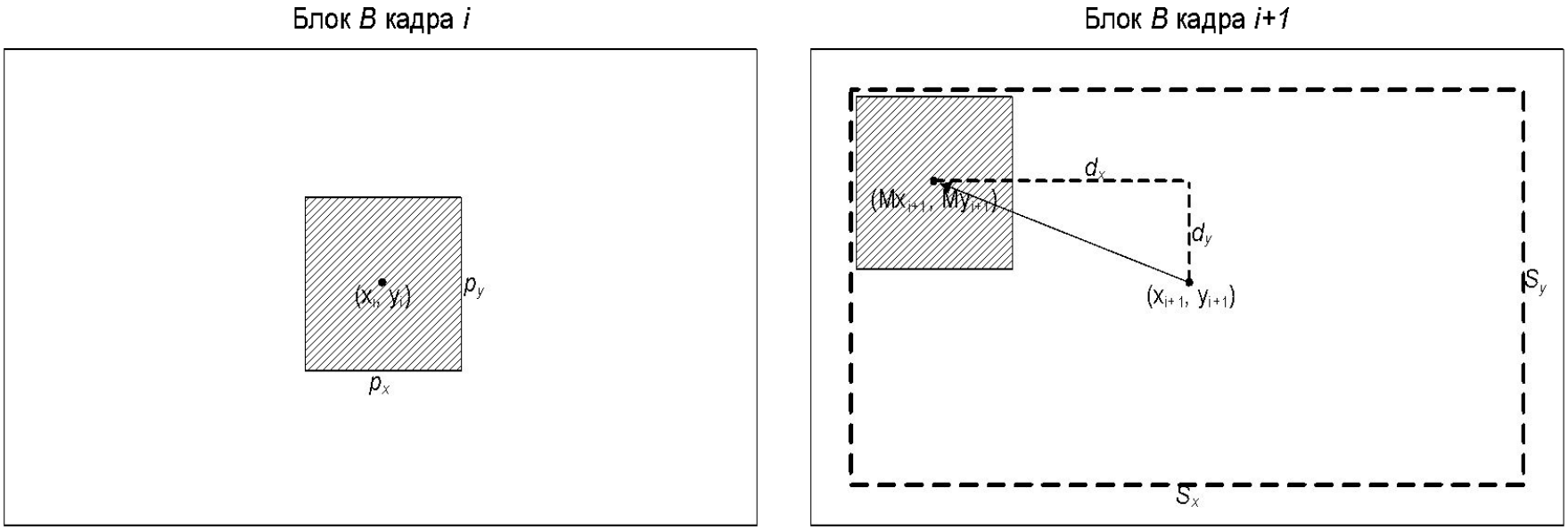
- Яркостная компонента несет в себе достаточно информации для однозначной идентификации изображения

# Изменения в кадре и между кадрами




$N = N_x \, x \, N_y$ - число блоков;
$(p_x, p_y)$ – размер сравниваемого участка;
$(S_x, S_y)$ – размер окрестности поиска.

# Направление движения




$(p_x, p_y)$ – размер сравниваемой области;
$(S_x, S_y)$ – размер окрестности поиска;
$(x_i, y_i)$ – координаты центра блока в кадре i;
$(x_{i+1}, y_{i+1})$ – координаты центра блока в кадре i+1;
$(Mx_{i+1}, My_{i+1})$ – координаты центра подходящей области;
$d = (d_x, d_y)$ – вектор направления движения.

# Порядковые измерения

- Каждый кадр делится на блоки
- В каждом блоке высчитывается характеристика (цветность, яркость, пр.)
- Блоки выстраиваются по возрастанию (убыванию) этой характеристики
- Цифровой отпечаток – порядок следования этих блоков.

# Порядковые измерения

# Преобразования

- ДКП
- ДПФ
- КПФМ
- И прочие

# Локальные дескрипторы

- Используют не все пиксели в кадре
- Точнее алгоритмов, основанных на глобальных дескрипторах
- Требуют детектирования points of interest например детектором Харриса
- Значительно медленнее

# Требования к цифровому отпечатку

- Время построения цифрового отпечатка – требования не предъявляются, желательно – соизмеримо с длительностью видео.
- Время сравнения – минимизировать.
- При этом, чем меньше цифровой отпечаток – тем быстрее сравнение, но возрастает корреляция!

# Требования к цифровому отпечатку

- Цифровой отпечаток должен строиться ***для каждой сцены*** видеопоследовательности;
- Цифровой отпечаток должен ***зависеть от всех пикселей*** кадра;
- Цифровой отпечаток должен ***учитывать зависимость*** между кадрами.

# Алгоритм построения цифрового отпечатка vs. Хэш-функции

- Цифровой отпечаток может быть переменной длины в рамках одного алгоритма.

- Незначительное изменение входных данных (шум, удаление кадров) не должно существенно влиять на итоговый цифровой отпечаток.

# Актуальность

- **Задача поиска и обнаружения видеофайлов на накопителях**
  Например, Videntifier Forensic, VideoScanner от AmpedSoftware.

- **Задача обнаружения фактов копирования и распространения видео-материалов, защищенных авторским правом**
  Например, ContentID от Youtube.

# Основная проблема цифровых отпечатков

- Основная задача – найти баланс между вычислительной и временной сложностью алгоритмов и точностью сравнения
- Чем меньше будет цифровой отпечаток, тем быстрее будет проходить сравнение, но тем больше будет корреляция.

# Копии и похожие видео

(a) The similar videos which are not copies (different games)

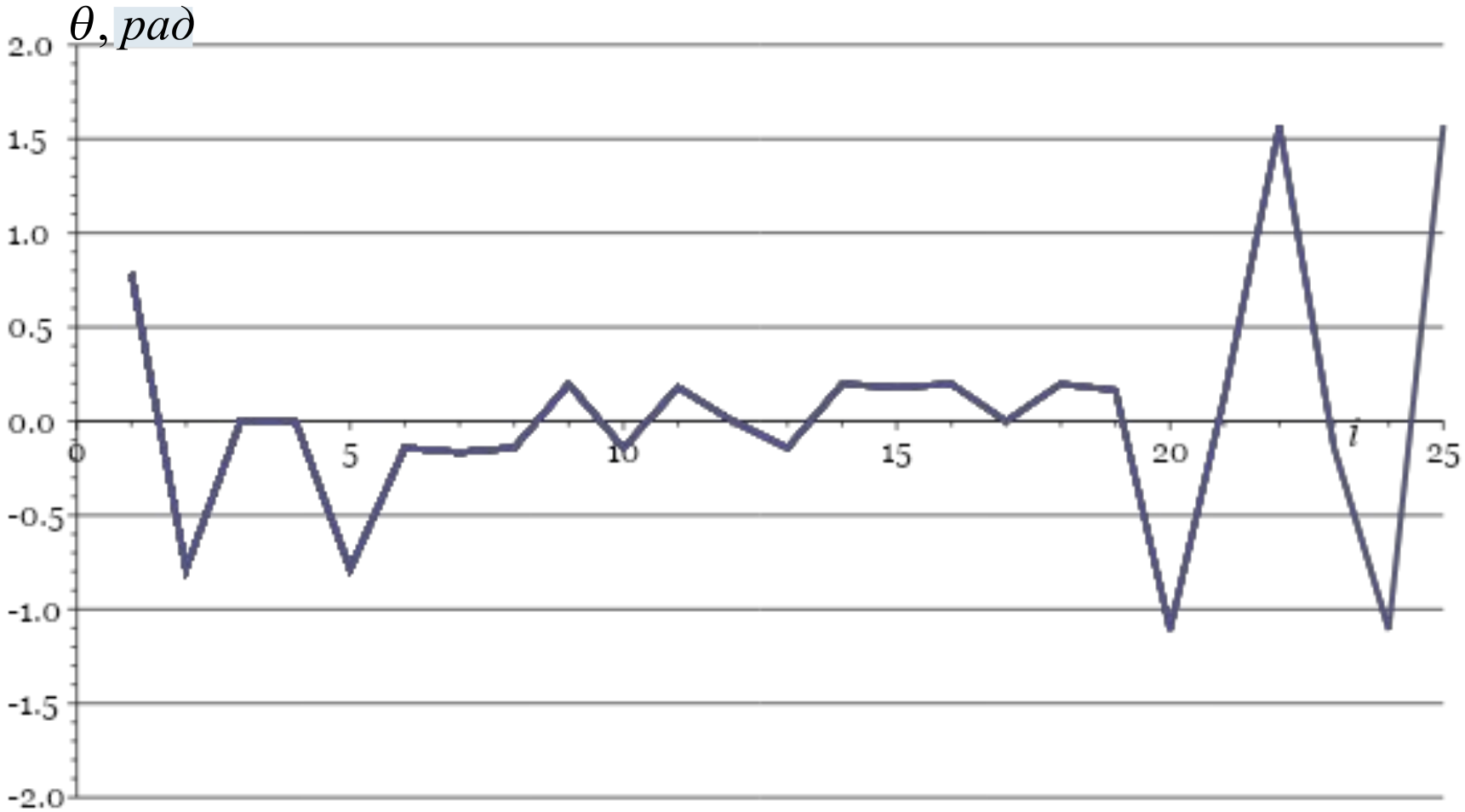

(b) Two videos which are copies (one is used to make the other)

# Атаки, которым надо противостоять

- Удаление/вставка единичных кадров;
- Искажение цветовой гаммы;
- Добавление искажений и шумов;
- Вставка логотипа;
- Изменение видео-формата;
- Изменение размера или разрешения видеоизображения;
- Прочие атаки…

# Эффективный алгоритм, предлагаемый в дипломной работе

# Извлечение характеристик



# Цифровой отпечаток

$$T_{scene},$$

$$№_{block},$$

$$\theta_{\max} = \left(\theta_{\max_1}, \theta_{\max_2}, \ldots, \theta_{\max_n}\right),$$

$$\theta_{\min} = \left(\theta_{\min_1}, \theta_{\min_2}, \ldots, \theta_{\min_m}\right),$$

$$\Delta\theta_{inc} = \left(\Delta\theta_{inc_1}, \Delta\theta_{inc_2}, \ldots, \Delta\theta_{inc_k}\right),$$

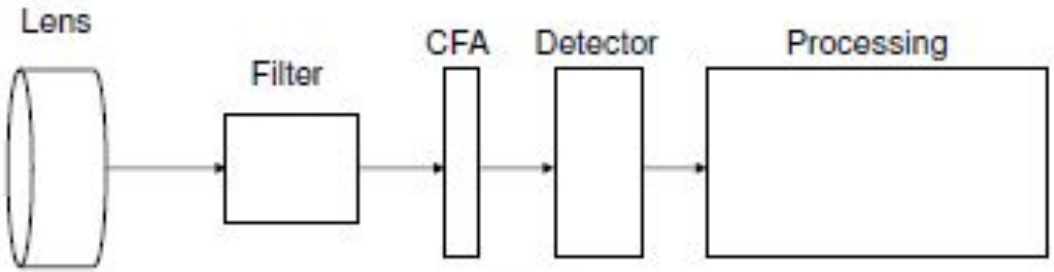
$$\Delta\theta_{dec} = \left(\Delta\theta_{dec_1}, \Delta\theta_{dec_2}, \ldots, \Delta\theta_{dec_p}\right).$$

# Размер цифрового отпечатка

| **Число блоков** | **Интенсивность движения в видео** | | |
|---|---|---|---|
| | *низкая* | *средняя* | *высокая* |
| *1* | **400 байт** | **612 байт** | **603 байт** |
| *10* | **2,6 Кбайт** | **3,7 Кбайт** | **6,5 Кбайт** |
| *100* | **17,7 Кбайт** | **33,8 Кбайт** | **50 Кбайт** |
| *1000* | **157 Кбайт** | **210 Кбайт** | **484 Кбайт** |
| *10000* | **774 Кбайт** | **1,6 Мбайт** | **3,6 Мбайт** |

# Время построения цифрового отпечатка

| **Размер блока *P*** | **Размер блока *S*** | | | | |
|---|---|---|---|---|---|
| | *4x4* | *12x12* | *20x20* | *28x28* | *36x36* |
| *3x3* | **3** | **4** | **14** | **26** | **30** |
| *9x9* | **–** | **8** | **44** | **145** | **165** |
| *15x15* | **–** | **–** | **37** | **224** | **296** |
| *21x21* | **–** | **–** | **–** | **118** | **305** |
| *27x27* | **–** | **–** | **–** | **15** | **205** |




(a)

| | | | | | |
|---|---|---|---|---|---|
| G | R | G | R | G | R |
| B | G | B | G | B | G |
| G | R | G | R | G | R |
| B | G | B | G | B | G |
| G | R | G | R | G | R |
| B | G | B | G | B | G |

(b)

| | | | | | |
|---|---|---|---|---|---|
| M | G | M | G | M | G |
| C | Y | C | Y | C | Y |
| M | G | M | G | M | G |
| C | Y | C | Y | C | Y |
| M | G | M | G | M | G |
| C | Y | C | Y | C | Y |

(c)

**Fig. 1**. (a) Major stages of processing in a camera pipeline. (b) CFA pattern using RGB values. (c) CFA pattern using YMCA values

В работе [2] также описывается математическая модель процесса получения изображения. Поступающий на вход сенсора свет можно обозначить, как $x=(x_{ij}),\ i=1,\ldots,m,\ j=1,\ldots,n$, где $m\times n$ - разрешение сенсора. Обозначив шум съемки за $\eta=(\eta_{ij})$, аддитивный случайный шум за $\varepsilon=(\varepsilon_{ij})$ и темновой ток за $c=(c_{ij})$, сигнал на выходе сенсора $y=(y_{ij})$ можно представить следующим образом:

$$y_{ij}=f_{ij}(x_{ij}+\eta_{ij})+c_{ij}+\varepsilon_{ij}. \qquad (1)$$

После этого сигнал $y$ проходит множественную обработку. Некоторые операции, применяемые к сигналу, могут быть нелинейными. Таким образом, окончательные значения пикселей $p_{ij}$, которые принимают значение в пределах $0\le p_{ij}\le 255$ можно выразить следующим выражением:

$$p_{ij}=P(y_{ij},N(y_{ij}),i,j), \qquad (2)$$

где $P$ – нелинейная функция, зависящая от $y_{ij}$, расположения пикселя $i$, $j$ и значений $y$ локальной окрестности $N(y_{ij})$.

# Темновой ток

- В физике и электронике темновым током называют малый электрический ток, который протекает через фоточувствительный детектор, например, фотодиод, фотоэлектронный умножитель, полупроводниковый детектор гамма-квантов и др. при отсутствии поглощенных фотонов.
- Физической причиной существования темнового тока являются тепловые генерации электронов и дырок в p-n слое полупроводникового прибора или в толще полупроводника, которые затем начинают упорядоченно двигаться за счет сильного электрического поля.

Упрощенная модель сигнала на выходе сенсора выглядит следующим образом. Пусть $I[i,j]$- сигнал в одной цветовой полосе в пикселе $(i,j)$, $i = 1, \ldots, m$, $j = 1, \ldots, n$ для одного кадра до применения операции демозаикинга, а $Y[i,j]$ – интенсивность света в пикселе $[i,j]$. Отбросив индексы пикселей для удобочитаемости, модель сигнала на выходе сенсора имеет вид:

$$I = g^{\gamma} \cdot \left[ (1+K)Y + \Lambda + \Theta_s + \Theta_r \right]^{\gamma} + \Theta_q, \qquad (6)$$

где $g$ – усиление цветового канала, $\gamma$ - фактор гамма-коррекции, $K$ – нулевое среднее значение, отвечающее за шумовой портрет, а $\Lambda$, $\Theta_s$, $\Theta_r$ и $\Theta_q$ обозначают следующие виды шумов: темновой ток, дробовой шум, шум считывания и шум квантования соответственно. Упрощая это выражение, используя только первый член разложения в ряд Тейлора, получается

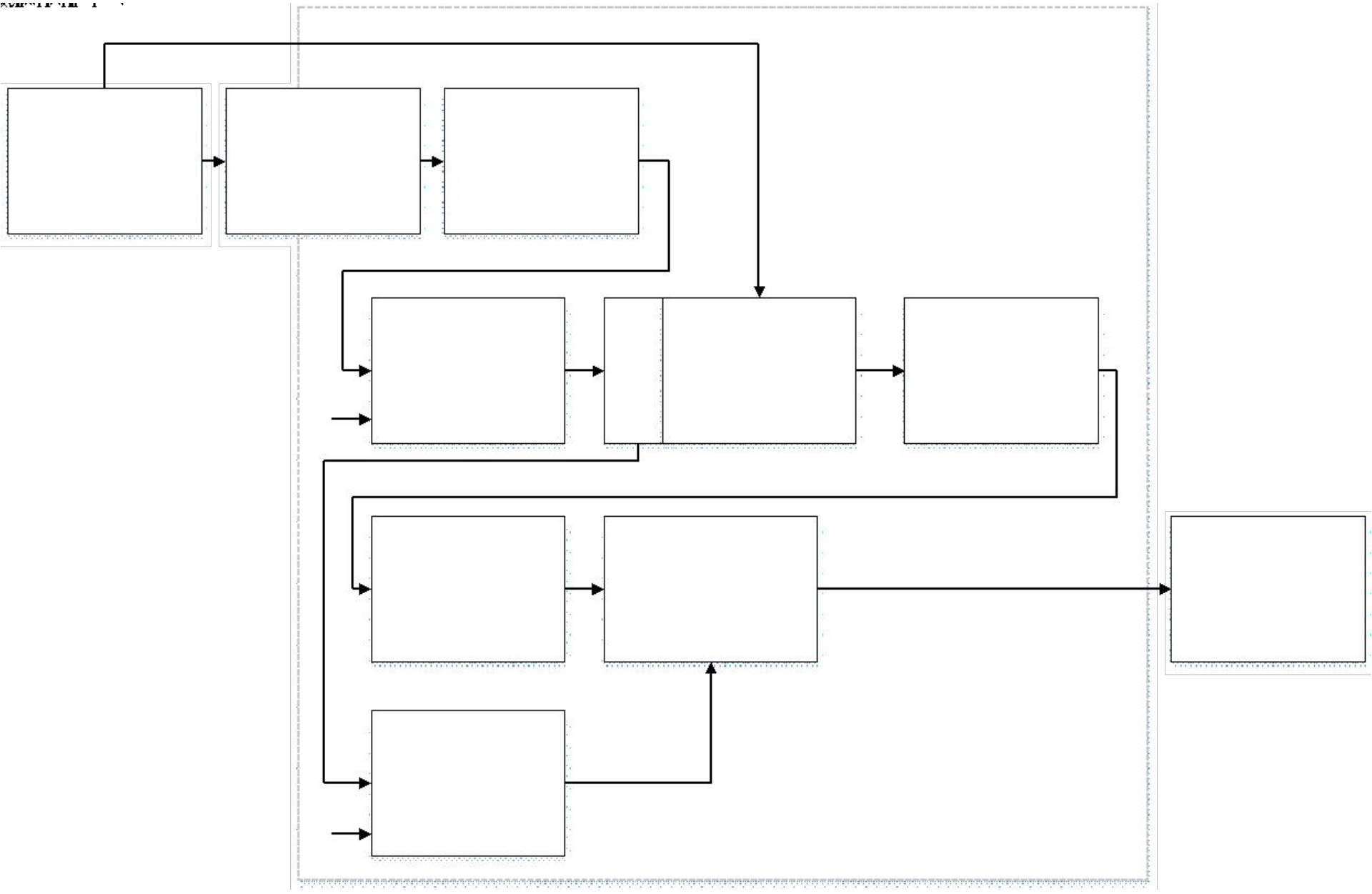
$$I = I^{(0)} + \gamma I^{(0)} K + \Theta, \qquad (7)$$

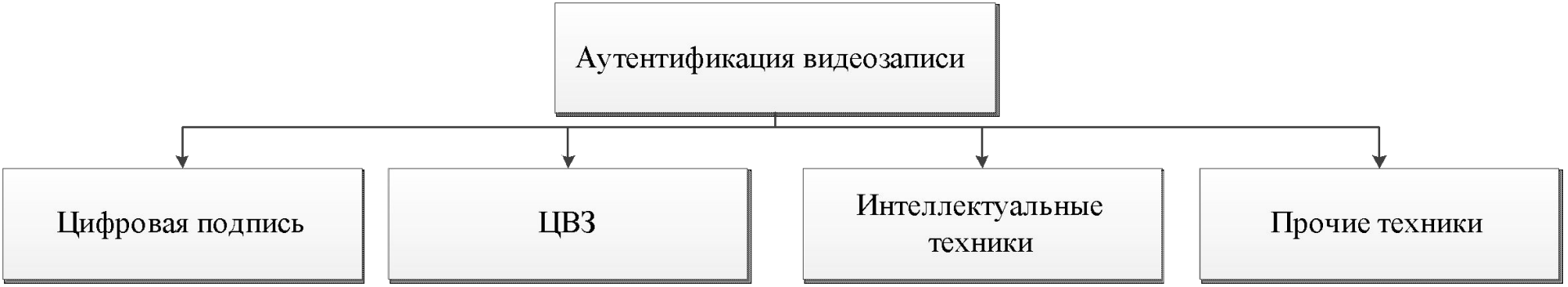
где $I^{(0)} = (gY)^{\gamma}$ - выходной сигнал сенсора в отсутствии шума или потерь при сжатии; $\Theta$ - комплекс независимых шумовых компонент.

# Идеи по аутентификации видеозаписей, используя техники для изображений

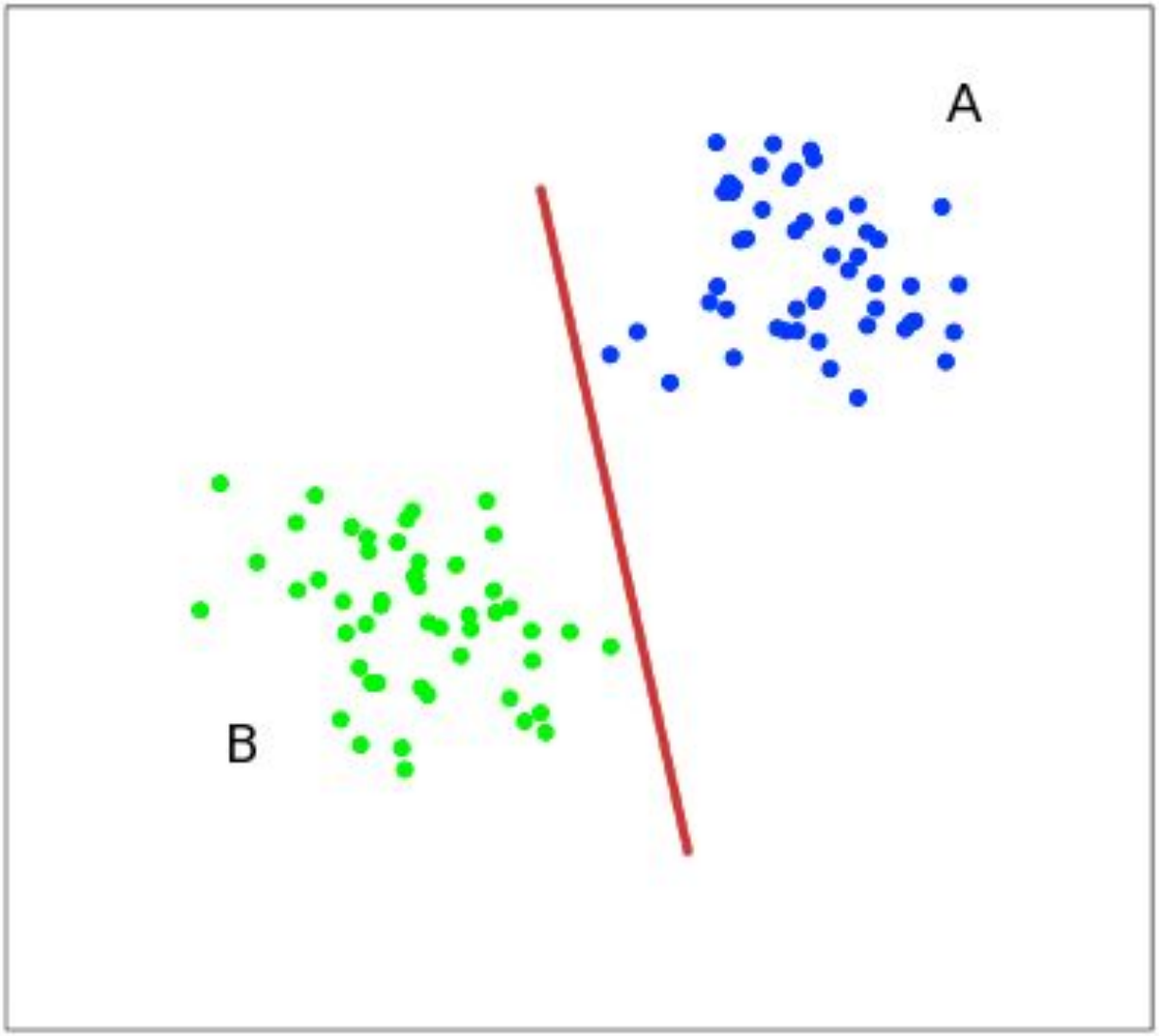
- Матрицы квантования
  - Свои у каждого производителя оборудования;
  - I-кадры кодируются при помощи JPEG

- Шумовой портрет
  - Возникает за счет неоднородности фотосенсора;
  - Соответственно можно расширить на видеозаписи.

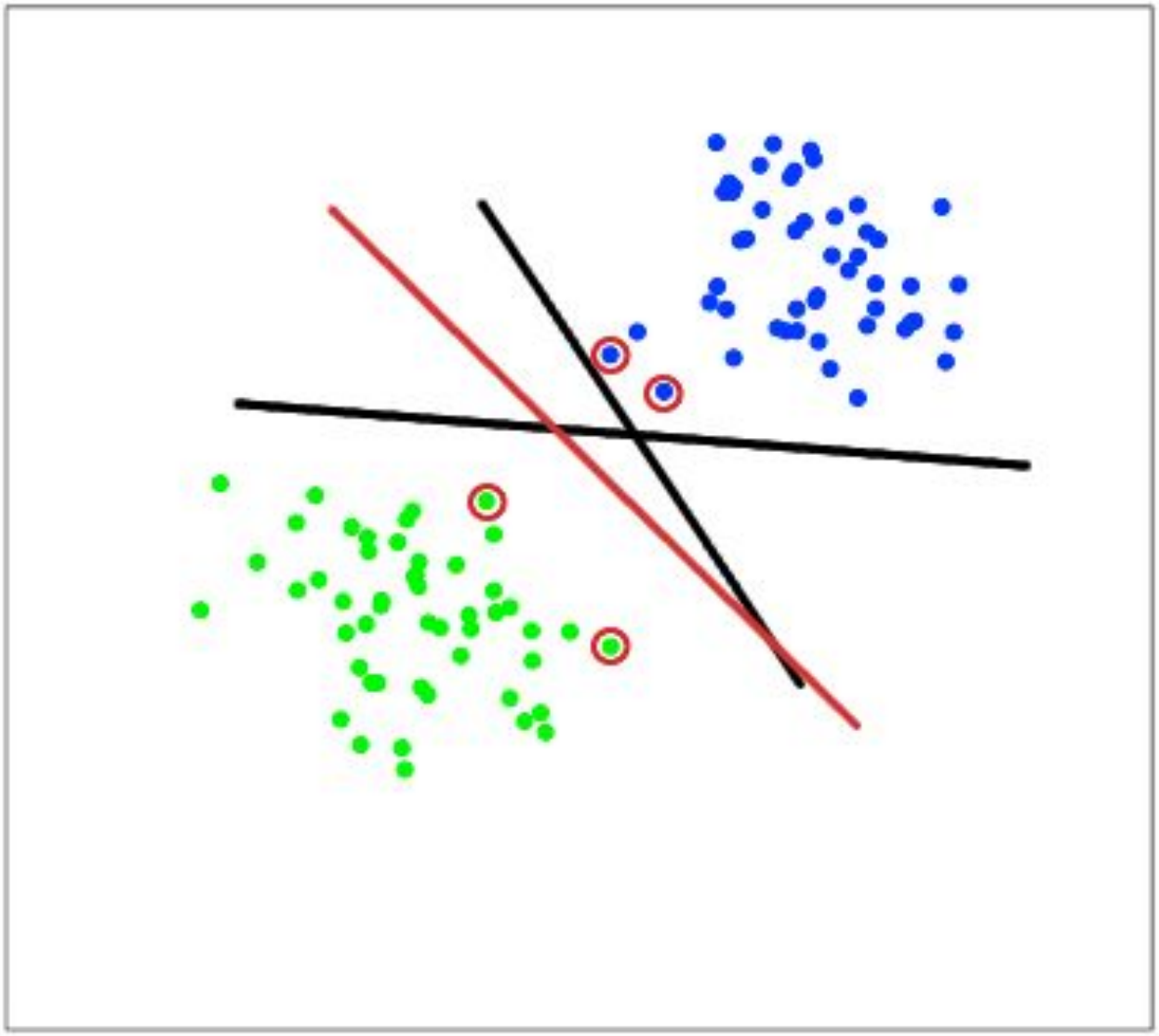



Аутентификация видеозаписи
Цифровая подпись
ЦВЗ
Интеллектуальные техники
Прочие техники

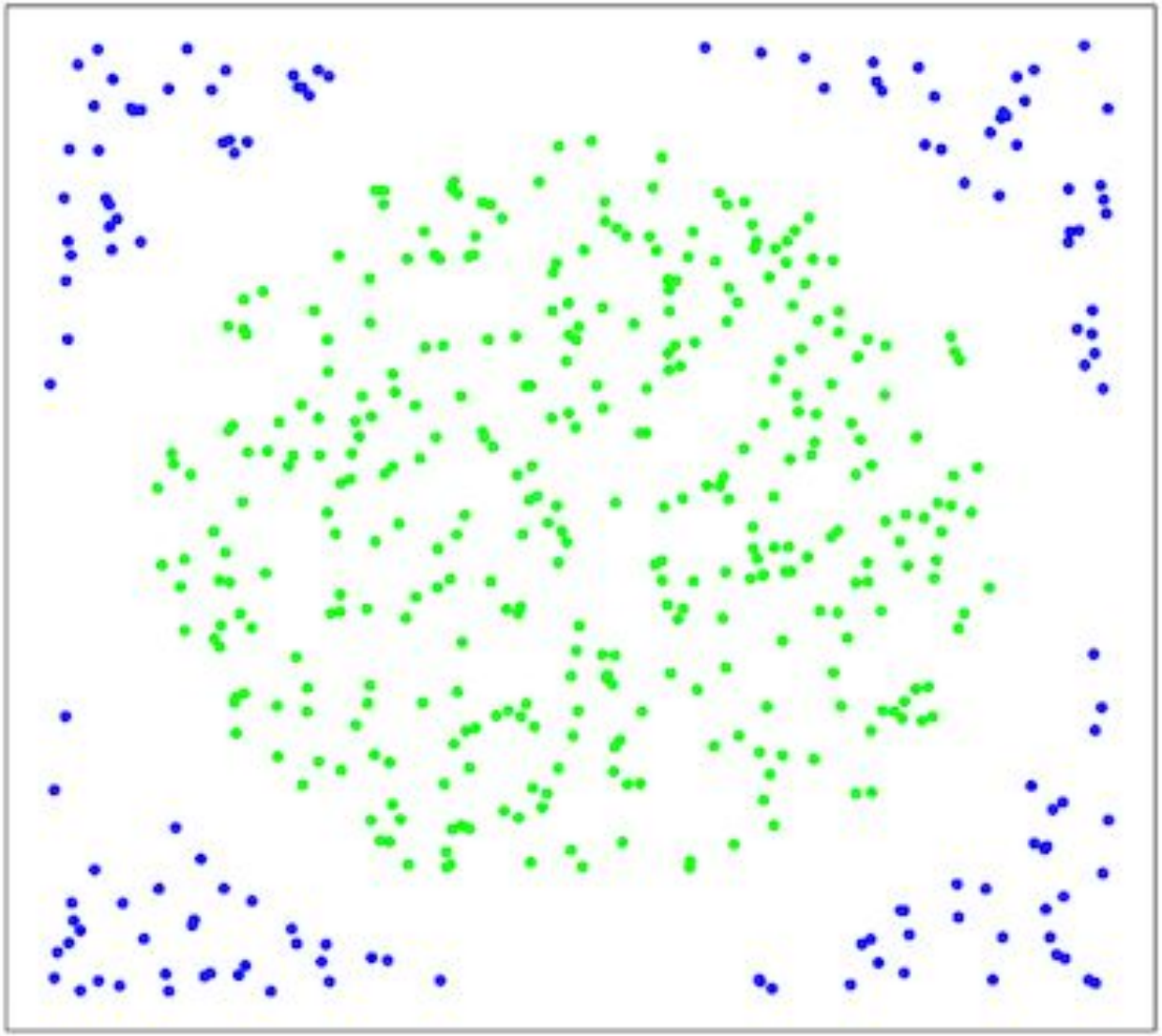
# Метод опорных векторов



# Метод опорных векторов



# Метод опорных векторов



# Метод опорных векторов

В этом случае поступают так: все элементы обучающей выборки вкладываются в пространство **X** более высокой размерности с помощью специального отображения $\varphi : \mathbb{R}^n \to X$. При этом отображение $\varphi$ выбирается так, чтобы в новом пространстве **X** выборка была *линейно* разделима.