СПИИРАН

Методы обеспечения безопасности видеоданных с различной степенью конфиденциальности

05.13.19 – Методы и системы защиты информации, информационная безопасность

Фахрутдинов Роман Шафкатович

Научный руководитель - д.т.н., профессор Молдовян Н.А.

Санкт-Петербург - 2012

Цель диссертационного исследования

Снижение затрат на реализацию защищенных систем передачи видеоинформации

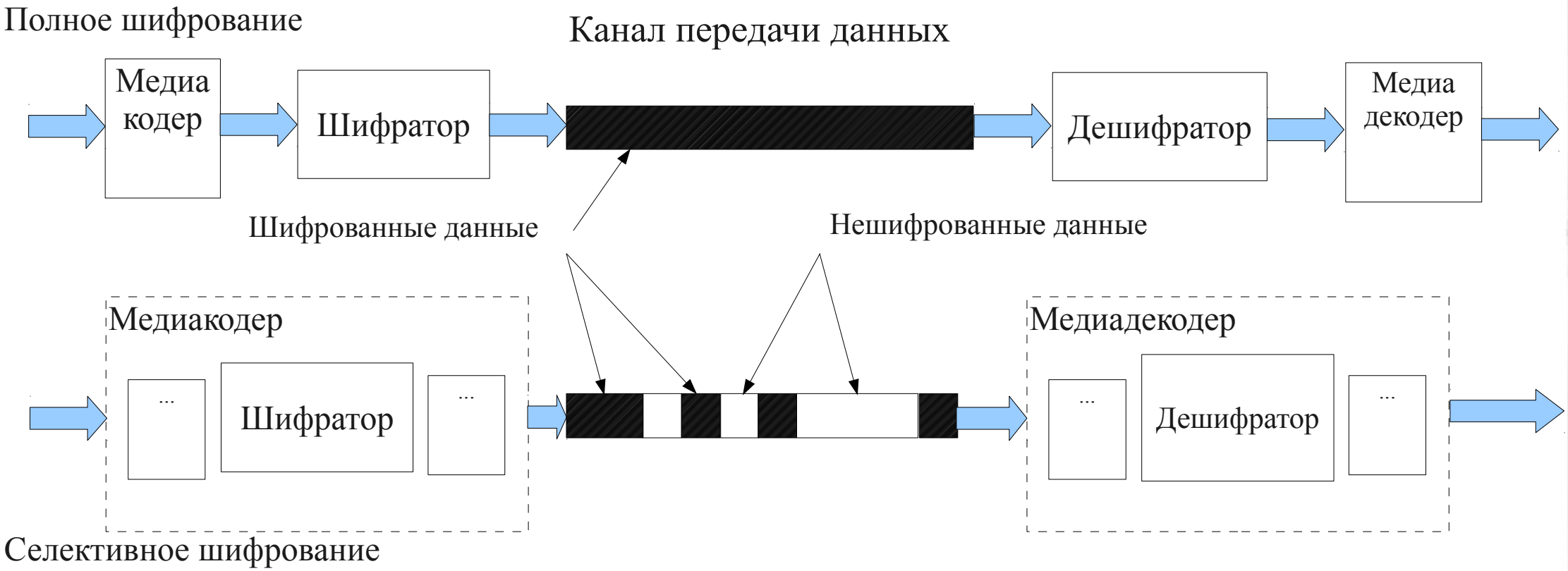
Задача исследования

Разработка технических решений, обеспечивающих возможность построения системы защиты видеоинформации в зависимости от требуемого уровня конфиденциальности

Актуальность

- широкое использование видеоинформации
- мобильные устройства
- GPRS, WiFi, WCDMA, LTE
- мобильный интернет
- видеотелефония
- видеонаблюдение
- цифровое наземное, кабельное и спутниковое ТВ

Два основных подхода к шифрованию видеоданных : селективный и полный



Селективные методы

Преимущества:

✔ сохранение структуры видеопотока
✔ высокая скорость работы
✔ устойчивость к ошибкам передачи данных
✔ сложность в получении сжатой и незащищённой копии
✔ сильная искажение изображения при просмотре без ключа
✔ простая реализация при интеграции в видеокодек

Недостатки:

✗ негарантированная стойкость
✗ ухудшение коэффициента сжатия
✗ отсутствие механизмов использования уникальной ключевой информации в каждом кадре
✗ низкая стойкость к атаке известного контекста
✗ существенный объём данных, подлежащий шифрованию

Методы полного закрытия

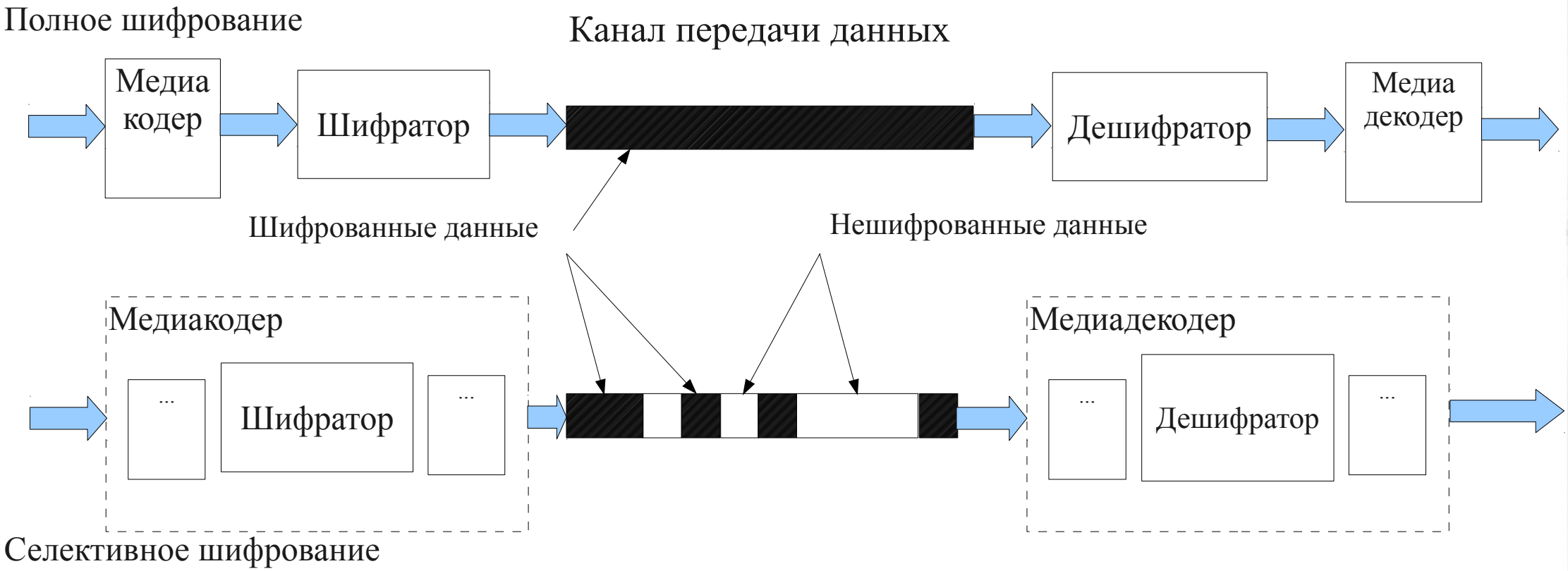
Преимущества:

✔ гарантированная стойкость при использовании соответствующей криптографии
✔ отсутствия влияния на коэффициент сжатия
✔ нет необходимости модифицировать видеокодек

Недостатки:

✗ наличие фазы «открытых сжатых данных»
✗ криптографической обработке подлежит вся видеоинформация
✗ при ошибках в канале связи происходит размножение ошибок
✗ необходимость совместимой инфраструктуры передачи данных
✗ отсутствие возможности совместить в одном потоке и закрытые и незакрытые данные

Два основных подхода к шифрованию видеоданных : селективный и полный



Методы полного закрытия

Преимущества:

✔ гарантированная стойкость при использовании соответствующей криптографии
✔ отсутствия влияния на коэффициент сжатия
✔ нет необходимости модифицировать видеокодек

Недостатки:

✗ наличие фазы «открытых сжатых данных»
✗ криптографической обработке подлежит вся видеоинформация
✗ при ошибках в канале связи происходит размножение ошибок
✗ необходимость совместимой инфраструктуры передачи данных
✗ отсутствие возможности совместить в одном потоке и закрытые и незакрытые данные

Преимущества разрабатываемого селективного метода

✔ закрытие каждого кадра с использованием уникальной ключевой информации
✔ существенная стойкость к атаке известного контекста
✔ получение сжатой, но незащищённой копии видеоинформации затруднено
✔ управление степенью деградации изображения при просмотре без ключа
✔ высокая скорость работы
✔ сильное искажение изображения при просмотре без ключа
✔ устойчивость к ошибкам передачи данных
✔ несущественное изменение коэффициента сжатия
✔ сохранение структуры видеопотока,простая интеграция в видеокодек

Перестановка блоков при сжатии

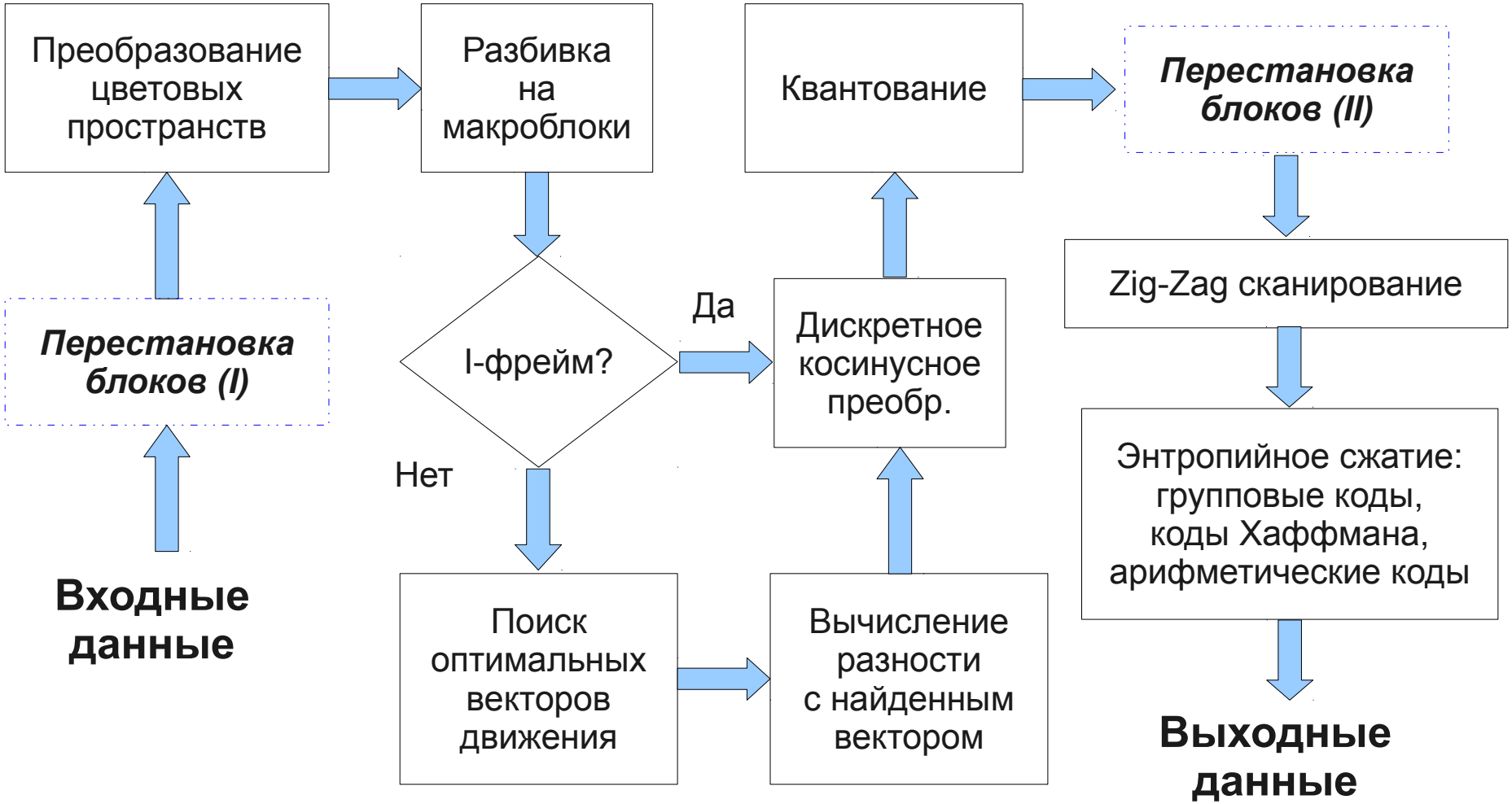


Таблица перестановок

Перестановкой по таблице P называется такое преобразование исходного массива B, что элементы результирующего массива R равны :

$$R_i = B_j, \text{ где } j = P_i$$

Обратной перестановкой по таблице P называется такое преобразование массива R, что элементы результирующего массива B' равны :

$$B'_j = R_i, \text{ где } j = P_i$$

Отметим, что преобразования $B \rightarrow R$ и $R \rightarrow B'$ обладает свойствами биективного отображения, а процедура перестановки является биекцией.

Безопасные методы получения псевдослучайных данных

Метод Фибоначчи с запаздываниями

$x_k=(x_{k-a} * x_{k-b}) mod\ 2^{64}$, где

x_k — числа из диапазона $[0,2^{64}-1]$

a и *b* — задержки, выбираются различные пары, например (17,5),(55,24),(71,65),(97,33)

$2^{61}*(2^r-1)$ - период такого генератора, где $r = max\ a,b$

Метод запуска блочного шифра в режиме счётчика

1.Присваиваем начальное значение счётчика c_1

2. Блок данных, подлежащий зашифровке, заполняется значениями счётчика $C(c_1,c_2,c_3...c_n)$, где $c_{i+1}=c_i+1$, *n* — размер блока блочного шифра

3.Блок шифруется на секретном ключе *k* алгоритмом *E* : $C'=E_k(C)$

4. *C'* используется как блок псевдослучайных данных для заполнения таблицы P с проверкой на уникальность значений и с выборкой по модулю равному размеру таблицы перестановок

Уникальная ключевая информация для каждого кадра

Последовательность кадров

Индивидуальные таблицы перестановок

501	48	614	1593	694	1499
903	545	451	643	878	641
815	1013	797	49	78	1523
12	1452	809	1117	1195	197
292	386	58	435	721	629
1188	1367	1236	929	1137	1139
198	1502	985	750	971	1371
1538	609	832	1440	1506	410
987	303	623	1305	1420	554
323	774	1398	213	656	1014

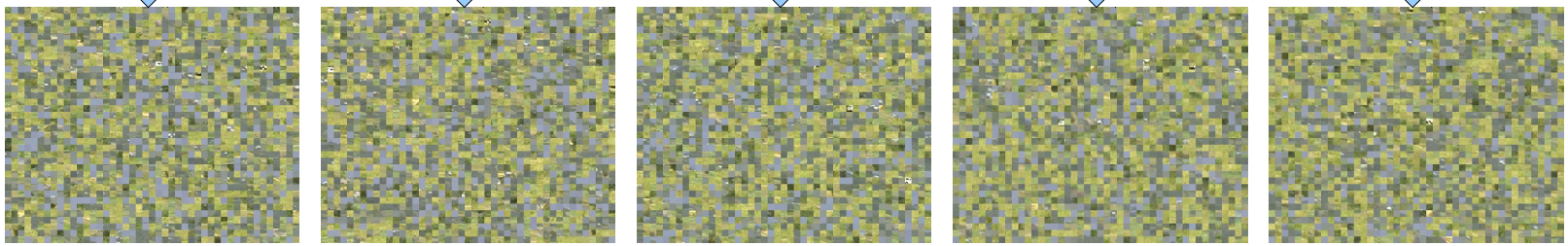
626	1522	1214	1317	1084	337
64	32	1599	711	29	1249
52	146	1259	1068	1466	275
124	1097	1411	1133	272	1329
768	477	661	747	960	175
673	1283	470	1434	1247	1569
808	1406	473	1129	1007	374
290	1320	1089	285	1081	585
950	171	993	211	476	1063
1200	21	1456	551	1257	1349

300	411	819	513	1067	93
1567	162	1037	284	99	341
770	510	715	1242	225	1505
394	682	1150	660	139	571
377	1159	1074	927	928	617
1272	360	1386	1461	1520	840
1602	732	1328	1442	218	538
1211	271	714	1511	1568	1077
627	931	1118	131	945	700
1432	14	1202	748	366	896

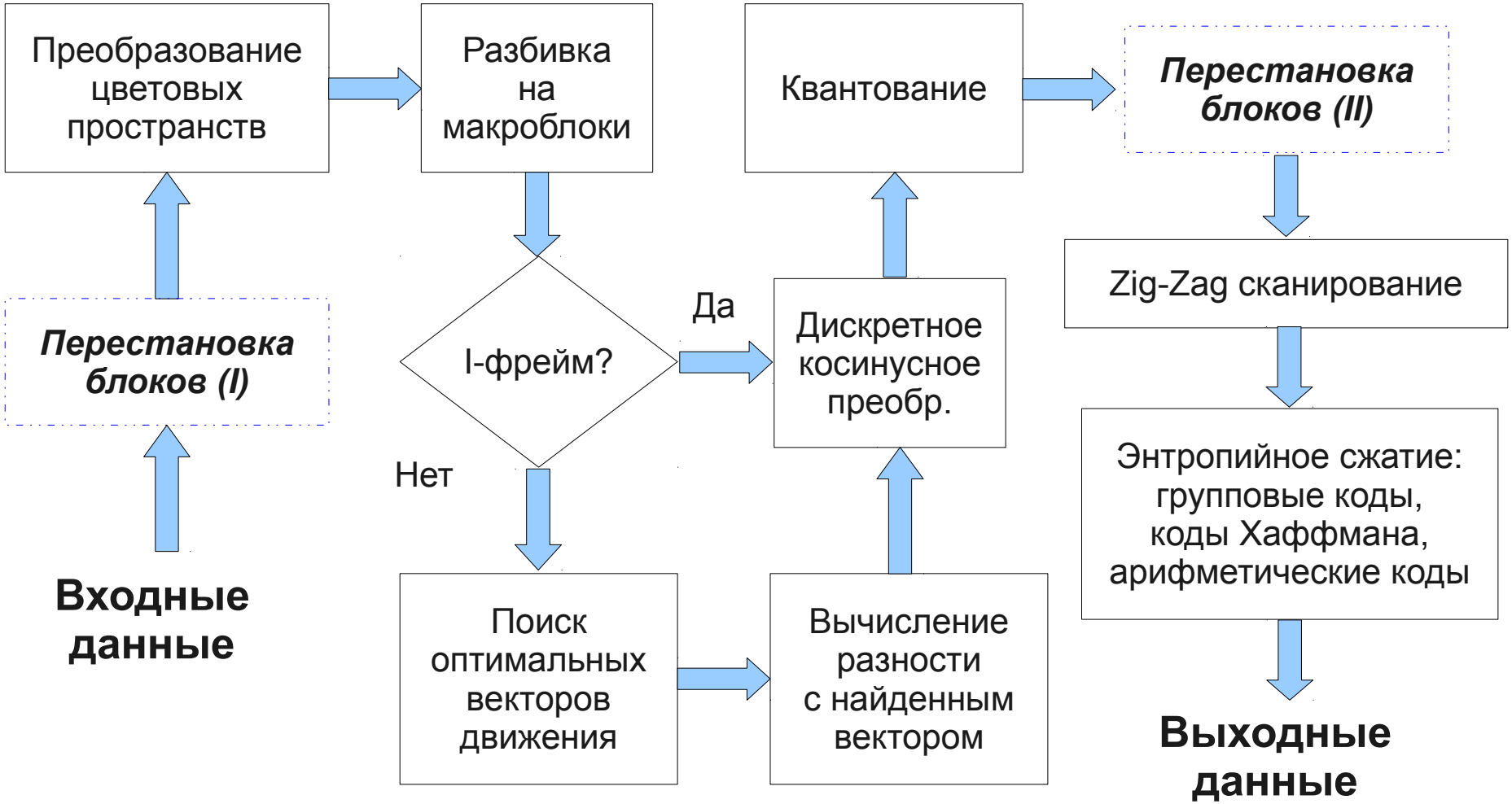
780	1362	336	1557	79	365
670	426	674	1512	1065	38
132	465	771	25	243	440
550	1390	1474	1310	1295	1168
297	875	472	1334	851	215
460	521	148	511	1064	1488
1124	135	177	1009	267	701
988	1500	299	999	1219	937
1004	849	462	1592	1385	170
1416	657	973	1443	565	1424

1237	332	842	947	1292	1017
602	1331	972	699	44	1058
1453	1044	1082	1582	1162	1304
786	1119	759	1548	205	415
1193	1559	826	1597	1428	1109
1025	122	1370	936	566	1071
1472	1545	975	1070	92	1374
1391	321	620	324	293	958
994	831	835	817	1396	639
1160	9	1478	189	823	136

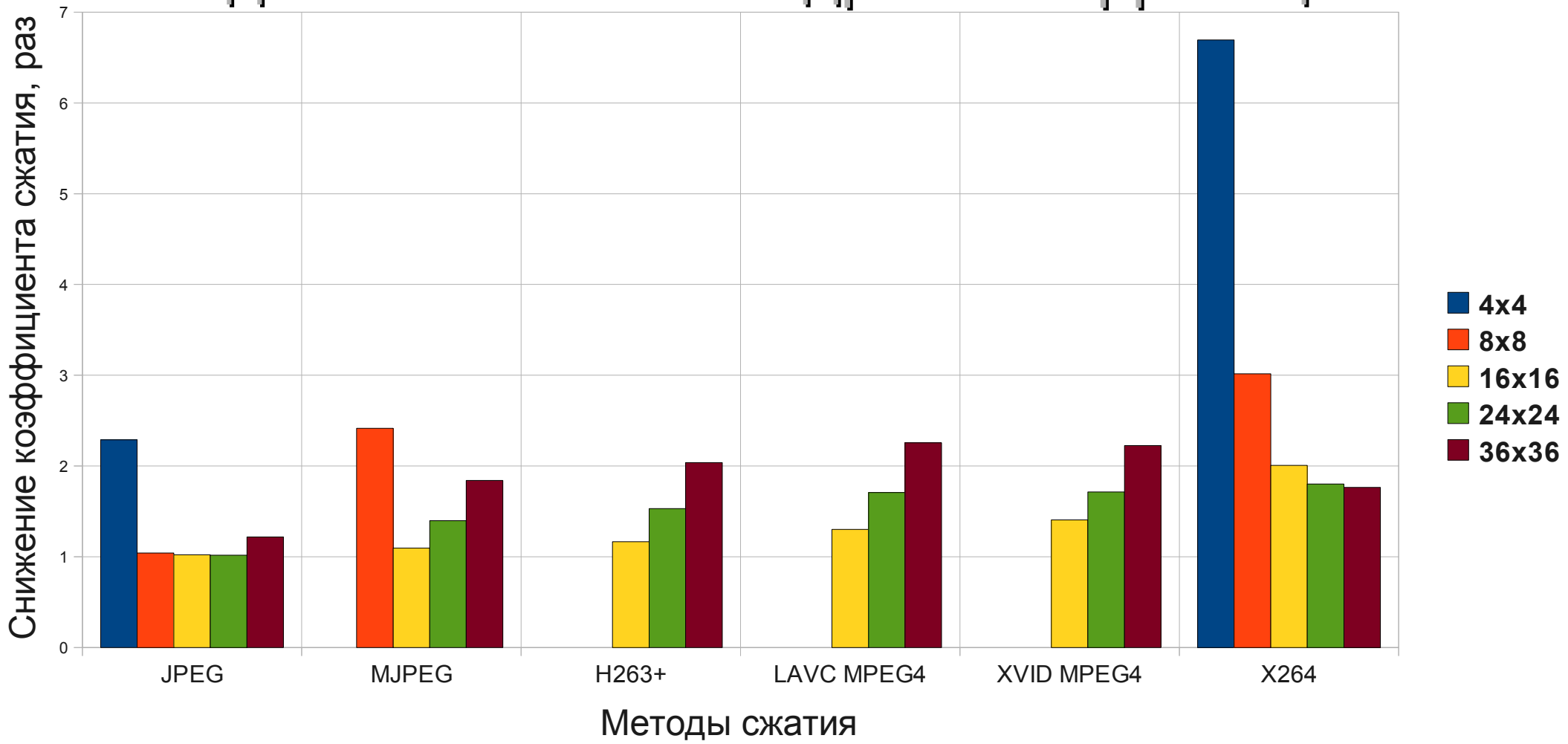
Перестановленные кадры



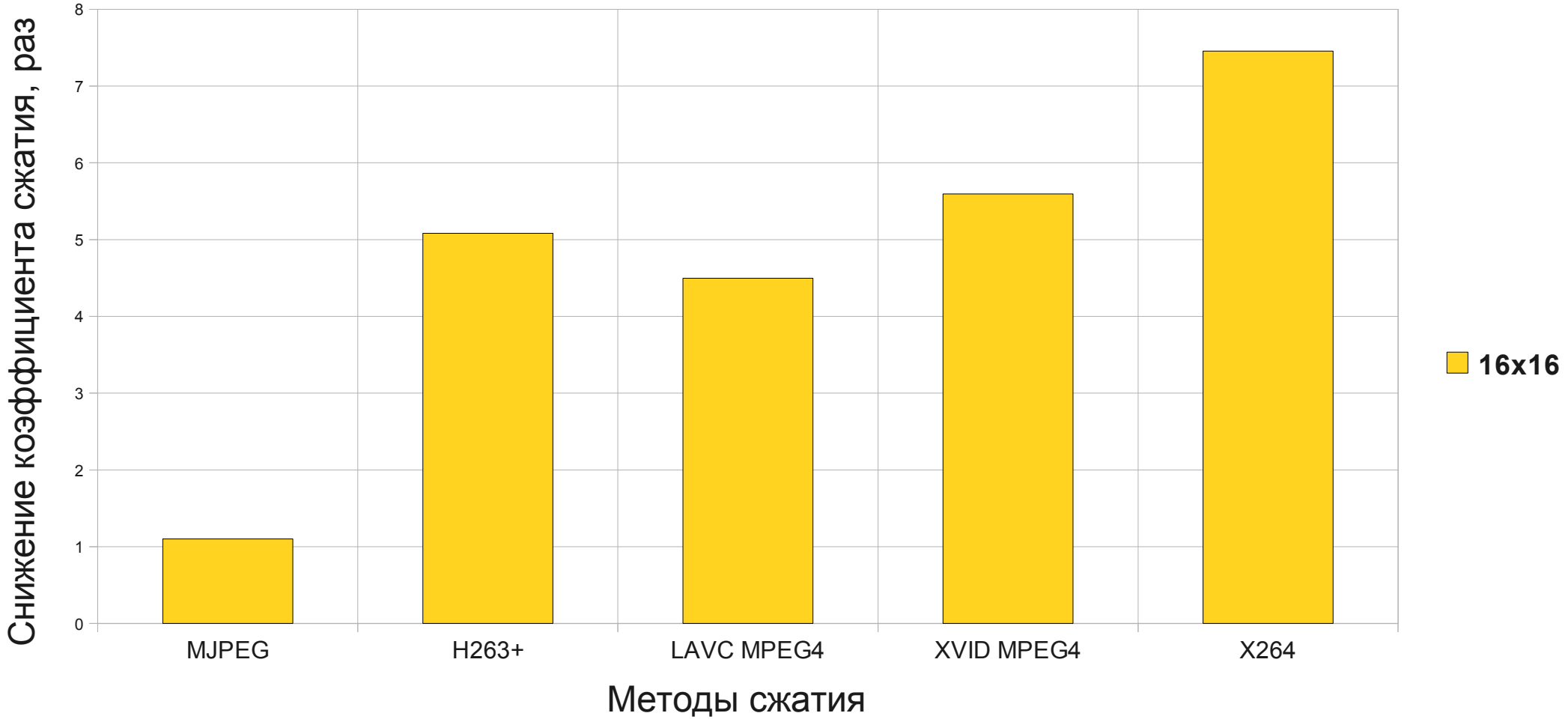
Перестановка блоков при сжатии



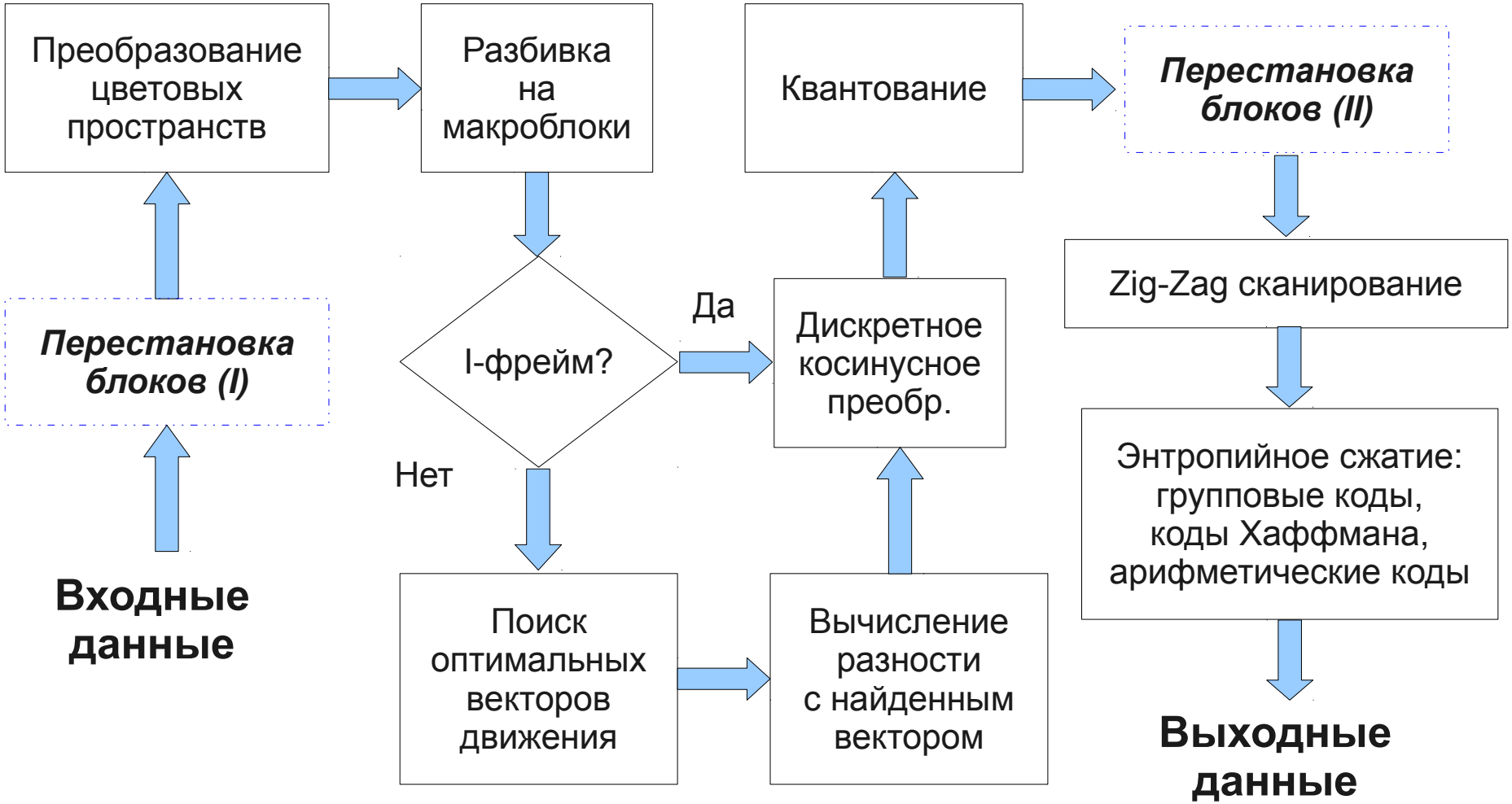
Перестановка блоков перед сжатием видео с низкой межкадровой корреляцией



Перестановка блоков перед сжатием видео с высокой межкадровой корреляцией



Перестановка блоков при сжатии

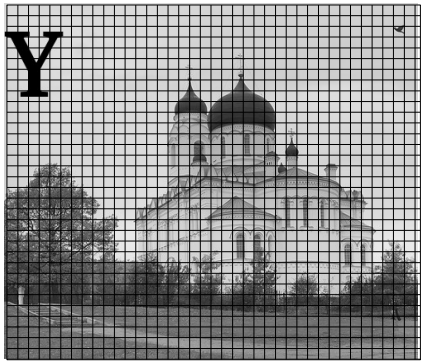


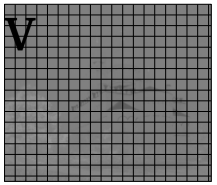
Операции над блоками в процессе обработки

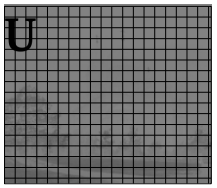
1

2

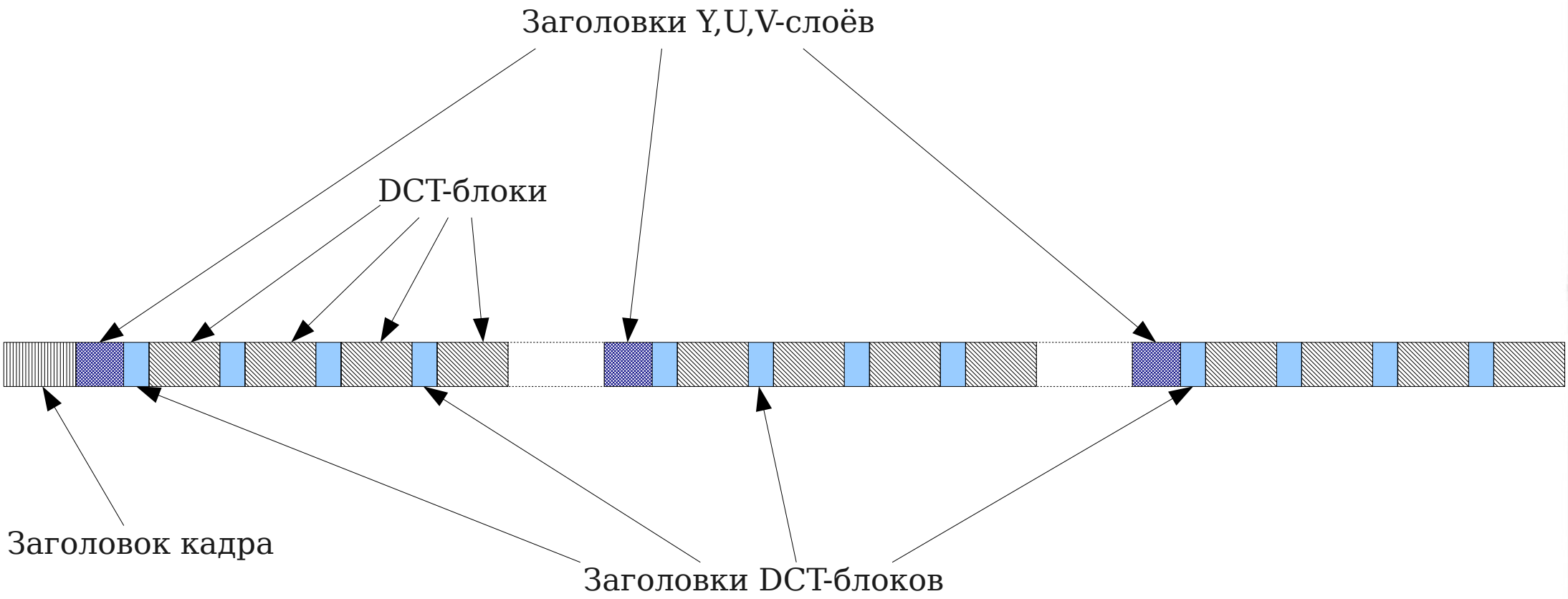
3



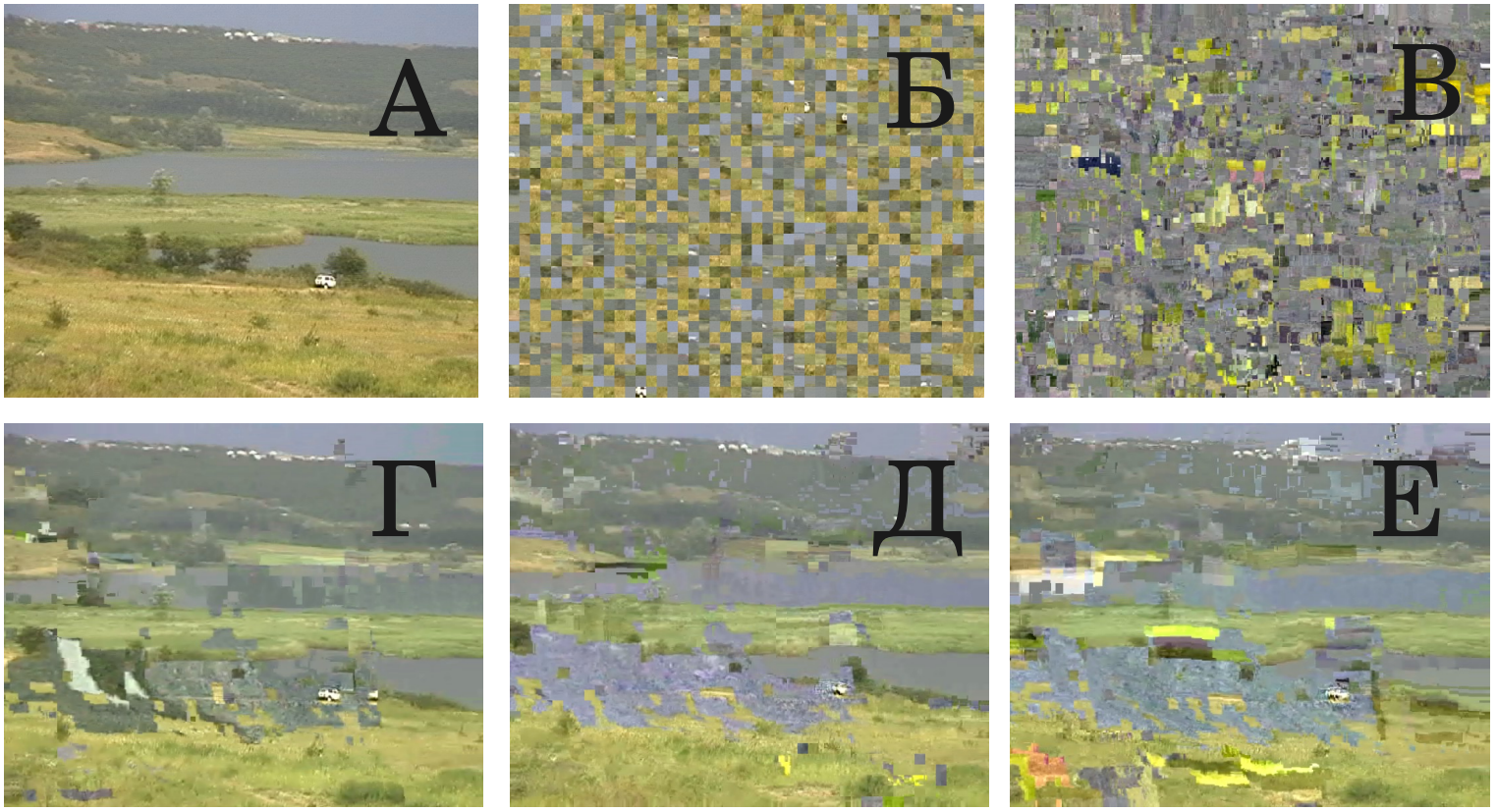


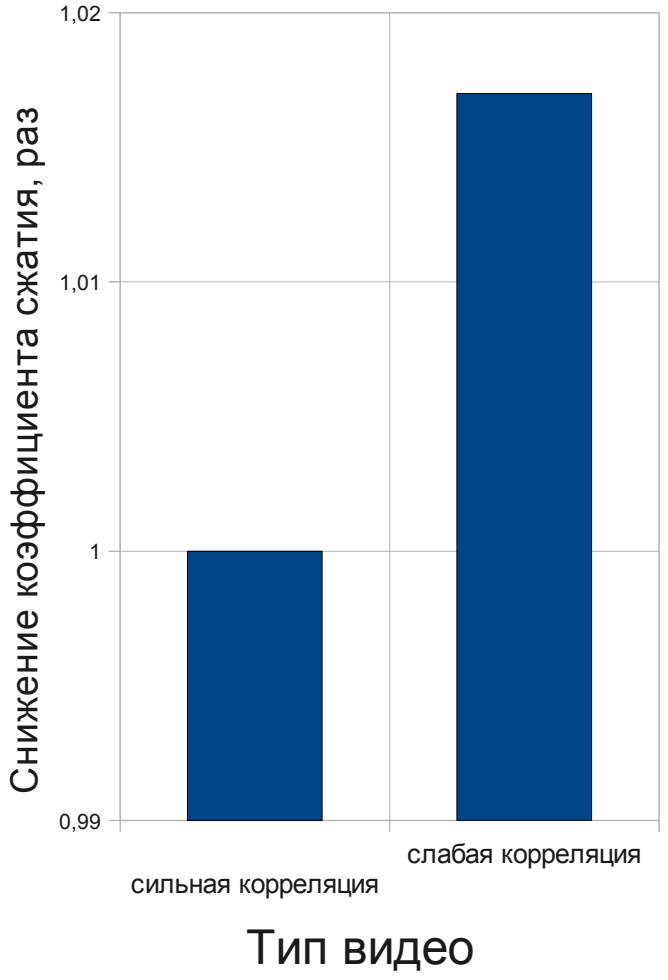


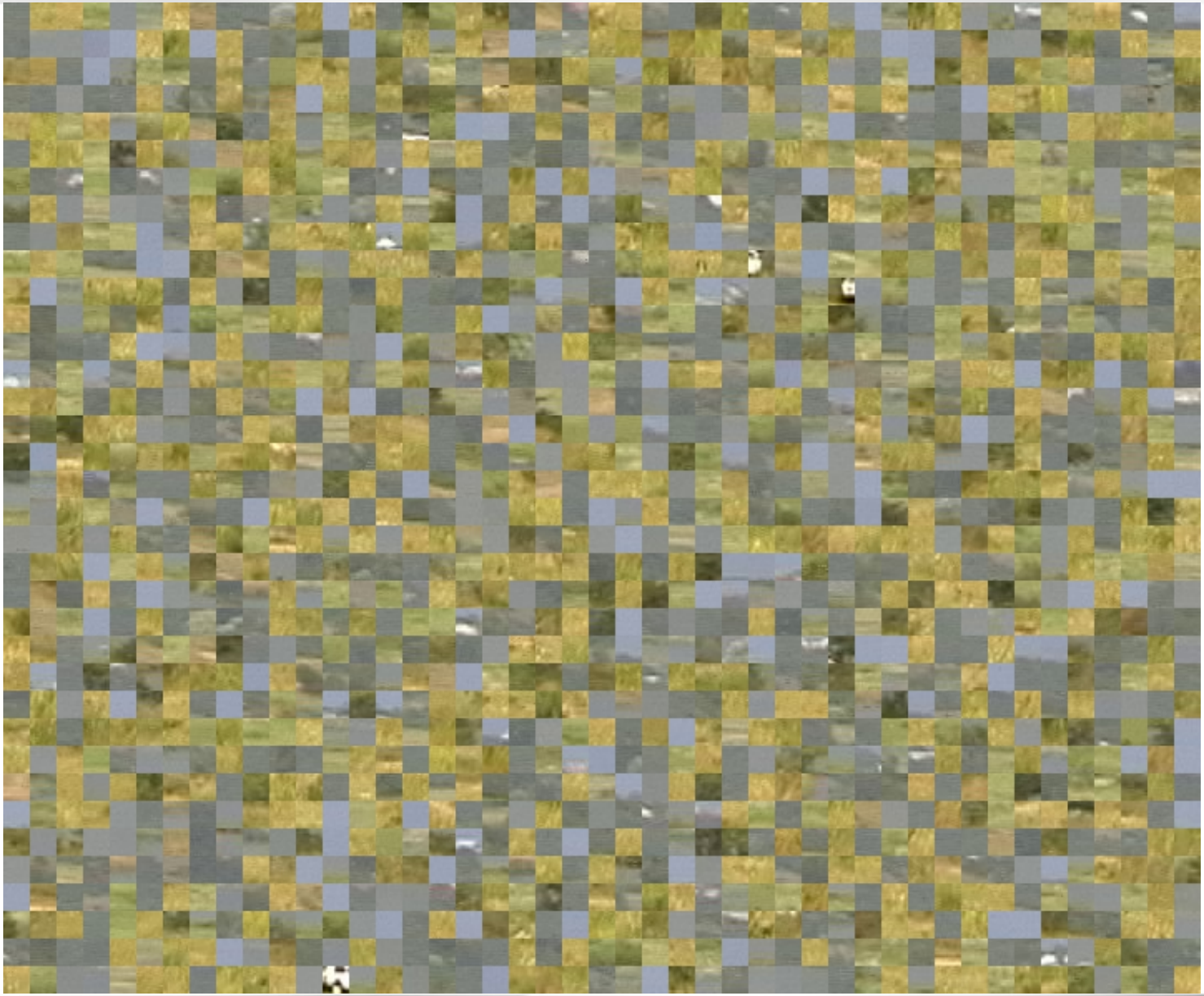
Структура данных перед энтропийным сжатием



Перестановка во время сжатия







Возможность восстановления изображения при перестановке перед сжатием

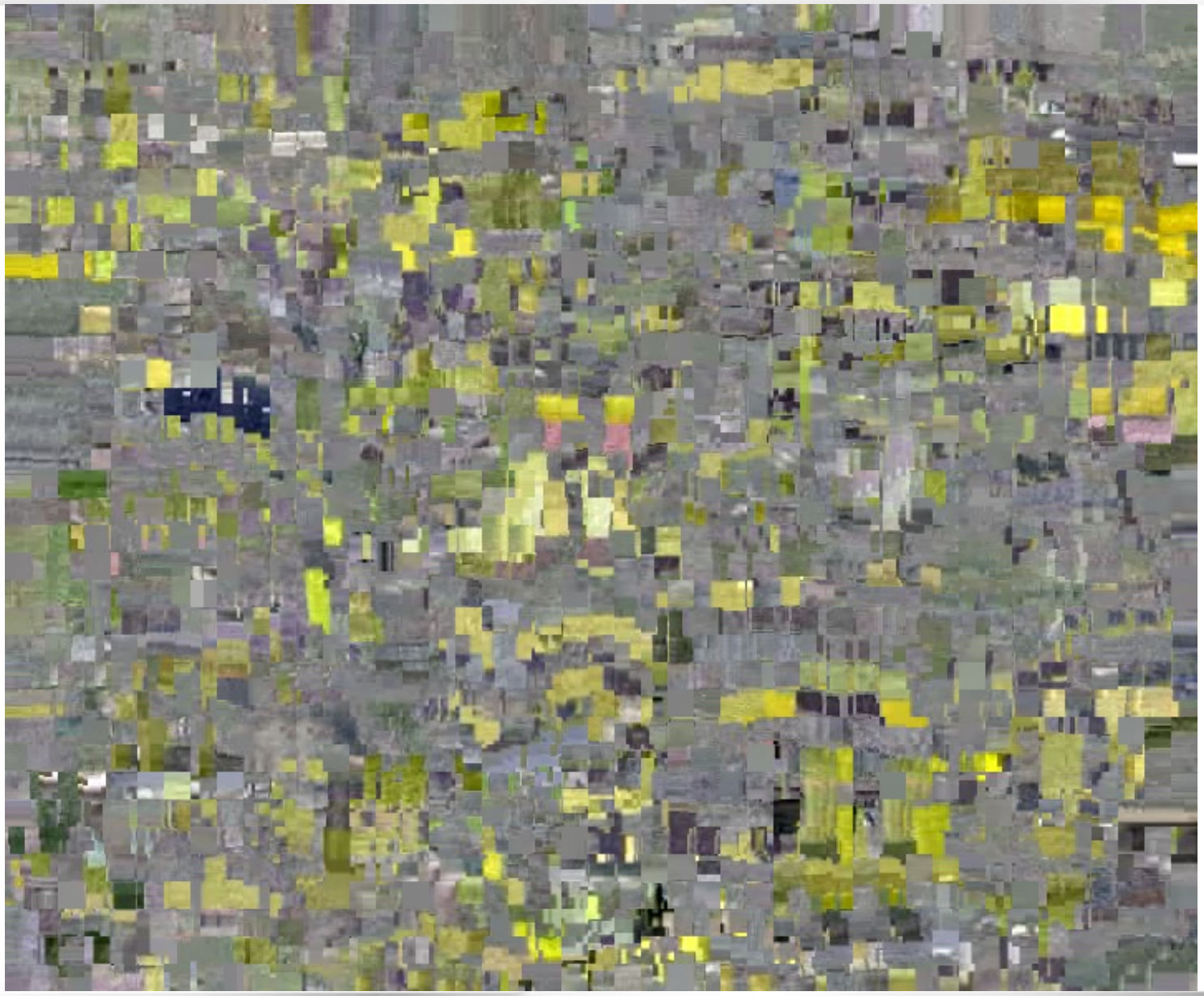
Оптимальным решением будет минимизация суммы

$$\sum_{i=1}^{r}\sum_{j=1}^{c-1}\left|G[i,j,3]-G[i,j+1,1]\right|+\sum_{i=1}^{r-1}\sum_{j=1}^{c}\left|G[i,j,4]-G[i+1,j,2]\right|$$

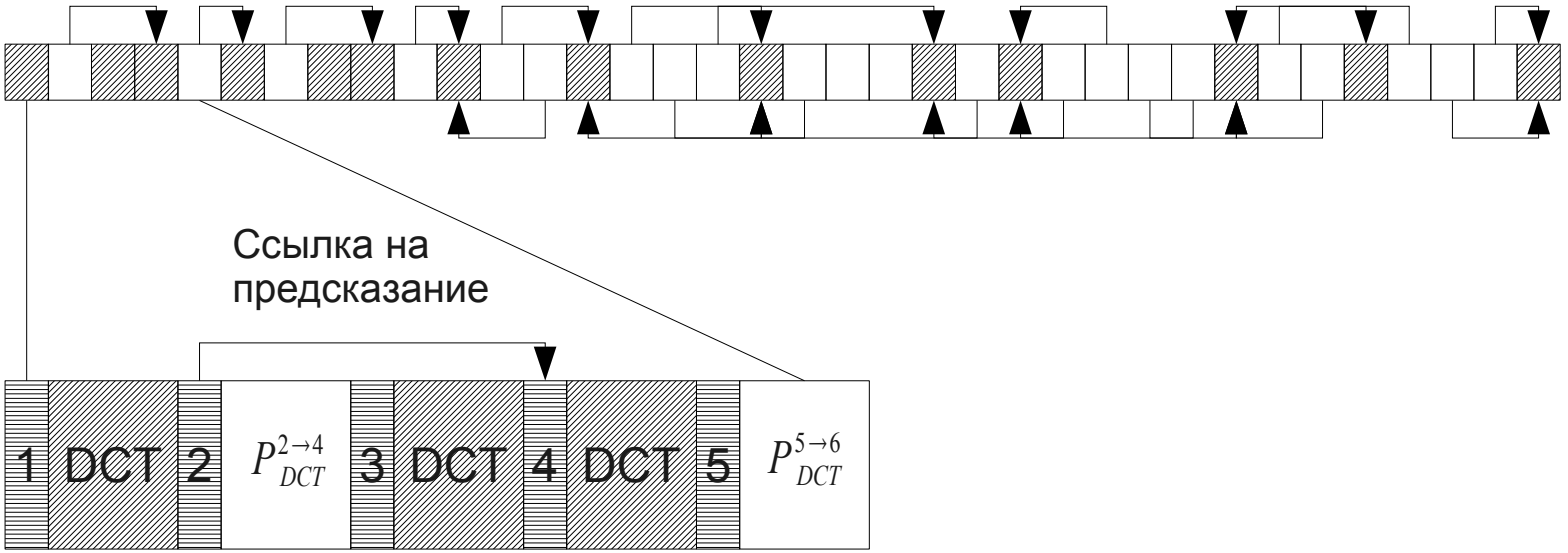
где *G(i,j,k)* - одна из граней *k* (1-левая, 2-верх, 3-правая,4-низ) блока *i,j*

Задача восстановления перестановленного изображения является NP-C сложной. Её решение ***можно проверить за полиномиальное время***, ***но время полного решения слишком велико***, так как общее число вариантов перестановок при количестве блоков *r* в ширину и *c* в высоту = *(r*c)!*. Поэтому для решения применяют различные ***эвристические*** методы:

- **Методы целочисленного и линейного программирования**
- **Эволюционные или генетические алгоритмы**
- **Метод имитации отжига**
- **Алгоритм поиска табу**
- **Метод удовлетворения ограничений**



Особенности восстановления изображения при перестановке в процессе сжатия

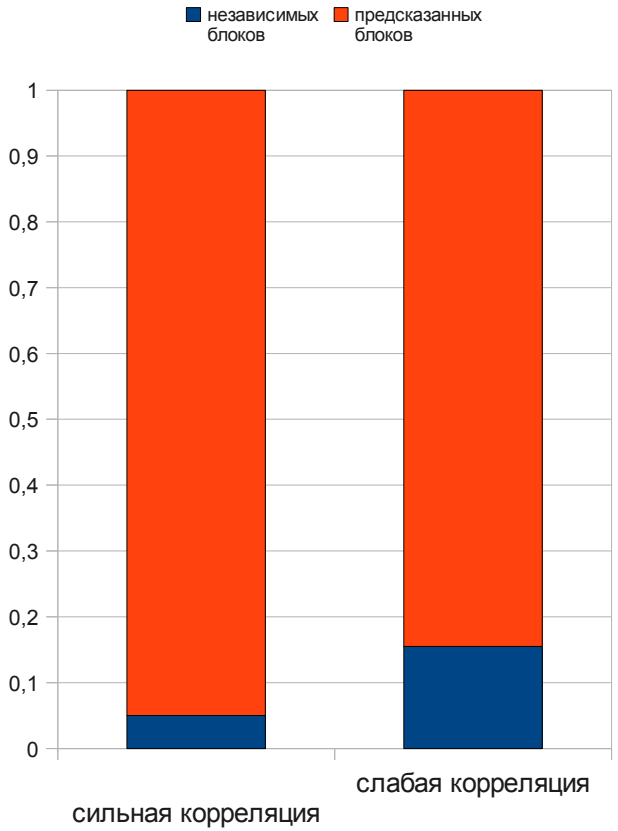


2 Заголовок макроблока

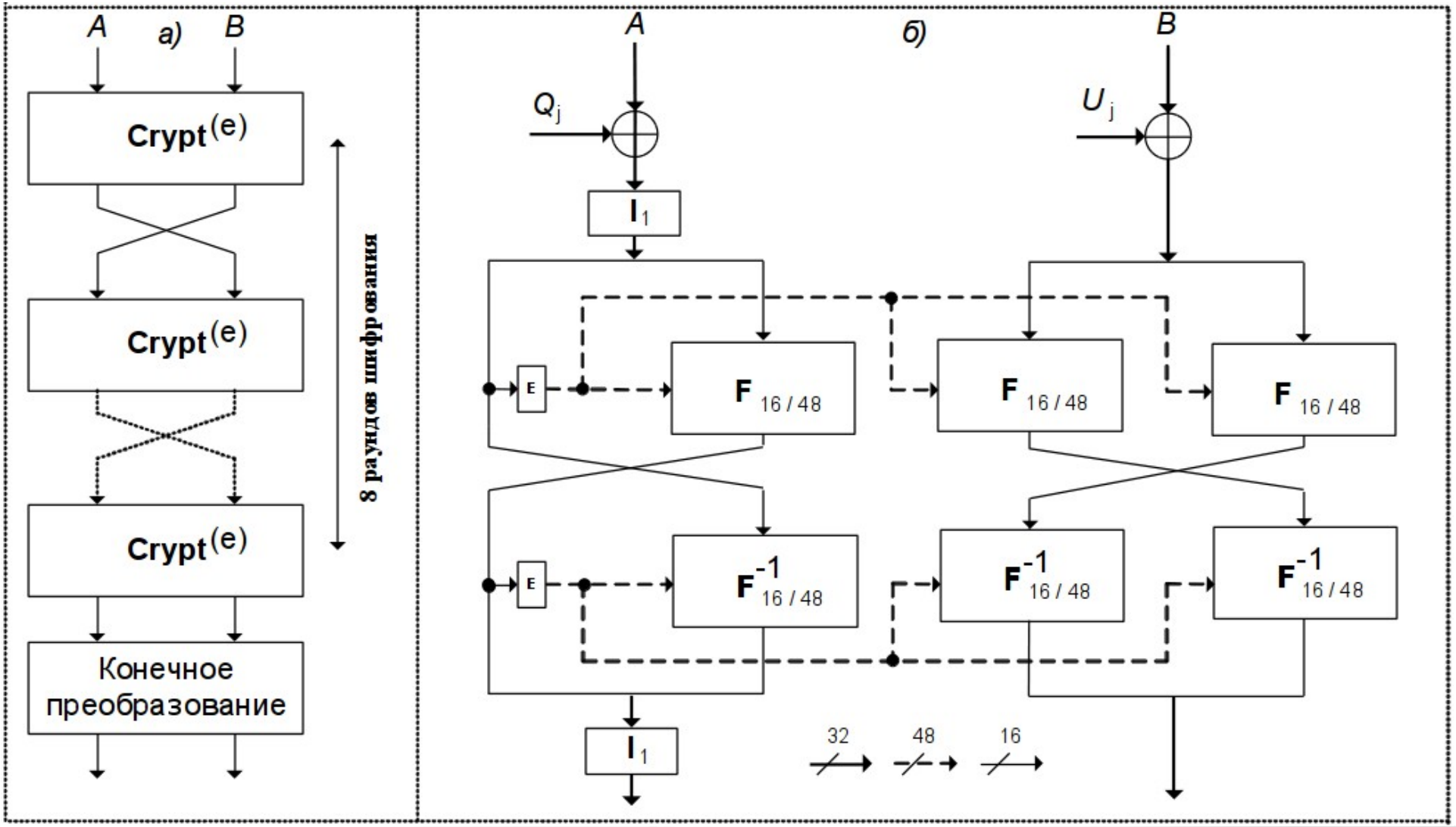
DCT Независимо-кодированный макроблок

$P^{2\to4}_{DCT}$ Макроблок, закодированный с предсказанием

Соотношение блоков



Шифр Video-64u



Число раундов	*Влияние битов входного текста*				*Влияния битов входного ключа*			
	d_1	d_c	d_a	d_{sa}	d_1	d_c	d_a	d_{sa}
1	10.8906	0.4561	0.3403	0.3230	5.7094	0.2358	0.1784	0.1595
2	27.9137	0.9687	0.8722	0.8695	18.8532	0.7124	0.5891	0.5821
3	31.9145	1.0000	0.9967	0.9904	29.5780	0.9844	0.9240	0.9174
4	**32.0001**	**1.0000**	**0.9990**	**0.9920**	31.9288	1.0000	0.9971	0.9906
5	**31.9900**	**1.0000**	**0.9992**	**0.9920**	**31.9999**	**1.0000**	**0.9991**	**0.9921**
6	**32.0047**	**1.0000**	**0.9992**	**0.9920**	**32.0000**	**1.0000**	**0.9992**	**0.9910**
7	**31.9994**	**1.0000**	**0.9992**	**0.9922**	**32.0017**	**1.0000**	**0.9992**	**0.9922**
8	**31.9997**	**1.0000**	**0.9993**	**0.9921**	**31.9997**	**1.0000**	**0.9993**	**0.9921**

Шифр	Число раундов	*N*	#CLB (configurable logic blocks)	Частота, МГц	Скорость, Мбит/с (Mbps)	Показатель эффективности Mbps/#CLB
Video-64u	8	1	56	380.6	3044	51
AES	10	1	200	339.087	4350	21.7

Результаты

✔ закрытие каждого кадра с использованием уникальной ключевой информации
✔ существенная стойкость к атаке известного контекста
✔ получение сжатой, но незащищённой копии видеоинформации затруднено
✔ высокая скорость работы
✔ сильное искажение изображения при просмотре без ключа
✔ сохранение структуры видеопотока,простая интеграция в видеокодек
✔ устойчивость к ошибкам передачи данных
✔ несущественное изменение коэффициента сжатия
✔ скоростной гарантированный метод шифрования видеоданных
✔ метод шифрования отдельных изображений, совместимый с наиболее общеупотребительным алгоритмом сжатия JPEG

✗ затруднено управление степенью деградации изображения при просмотре без ключа
✗ точно неизвестно, сколько именно вычислительных ресурсов требуется злоумышленнику для восстановления перестановленных видеокадров, с учётом разработки новых методов восстановления перестановленных изображений
✗ для практической проверки использовался видеокодек предыдущего поколения
✗ не использовались возможности дополнительного искажения DCT-блоков с помощью вращения относительно главной диагонали
✗ отсутствует механизм согласования параметров шифрования через видеоконтейнер (при отсутствии обратной связи между видеошифратором и видеодешифратором)

Спасибо за внимание