

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Томский государственный университет систем управления и
радиоэлектроники»

Алгоритмы встраивания информации в цифровые данные с повышенной робастностью

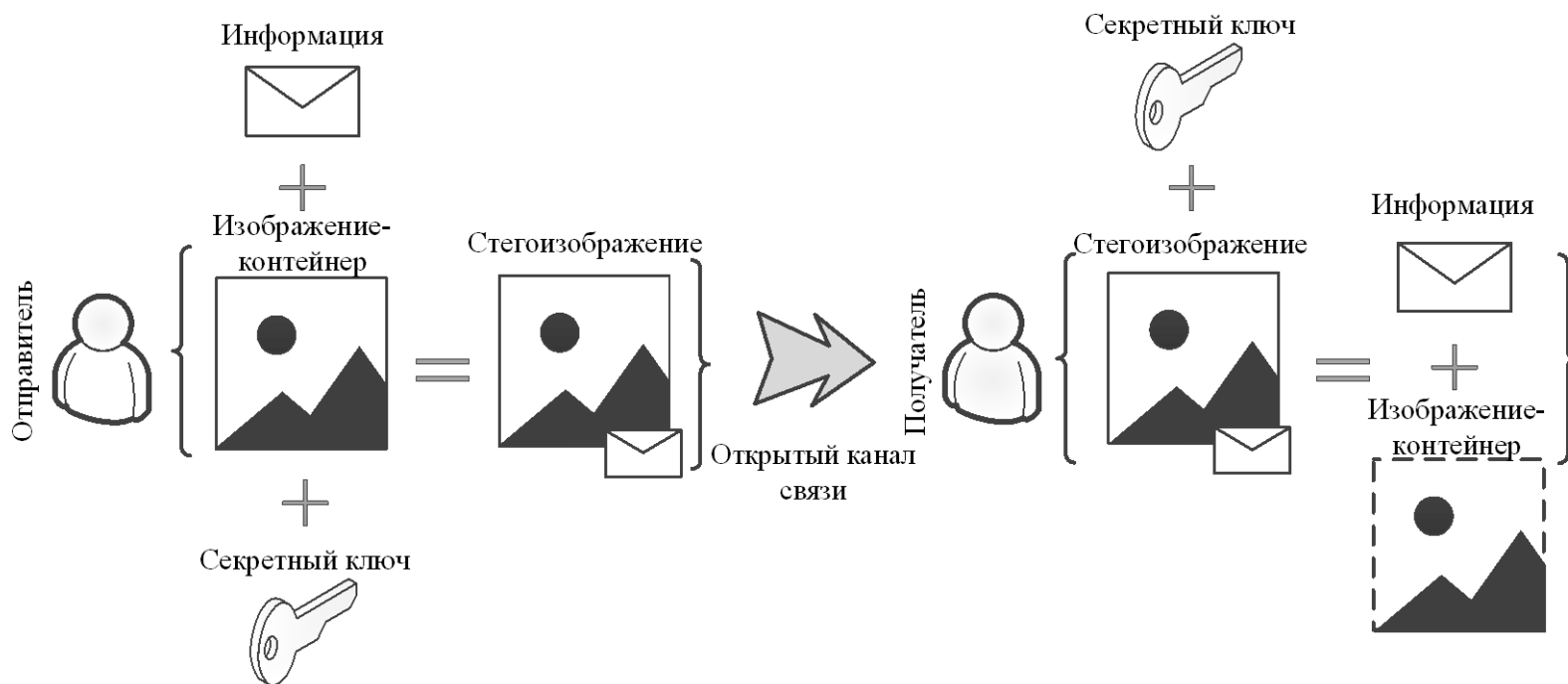
Доклад Мельман А.С., аспирантки 2-го года обучения

Руководитель:

Шелупанов А.А., д.т.н., заведующий каф. КИБЭВС

Введение

- Стеганография направлена на защиту конфиденциальности информации. Стеганография скрывает сам факт наличия какого-либо секретного сообщения.
- Цифровые водяные знаки (ЦВЗ) предназначены для обеспечения защиты авторства либо целостности самого объекта-контейнера, в который встраивается дополнительная информация – водяной знак.



Цель работы

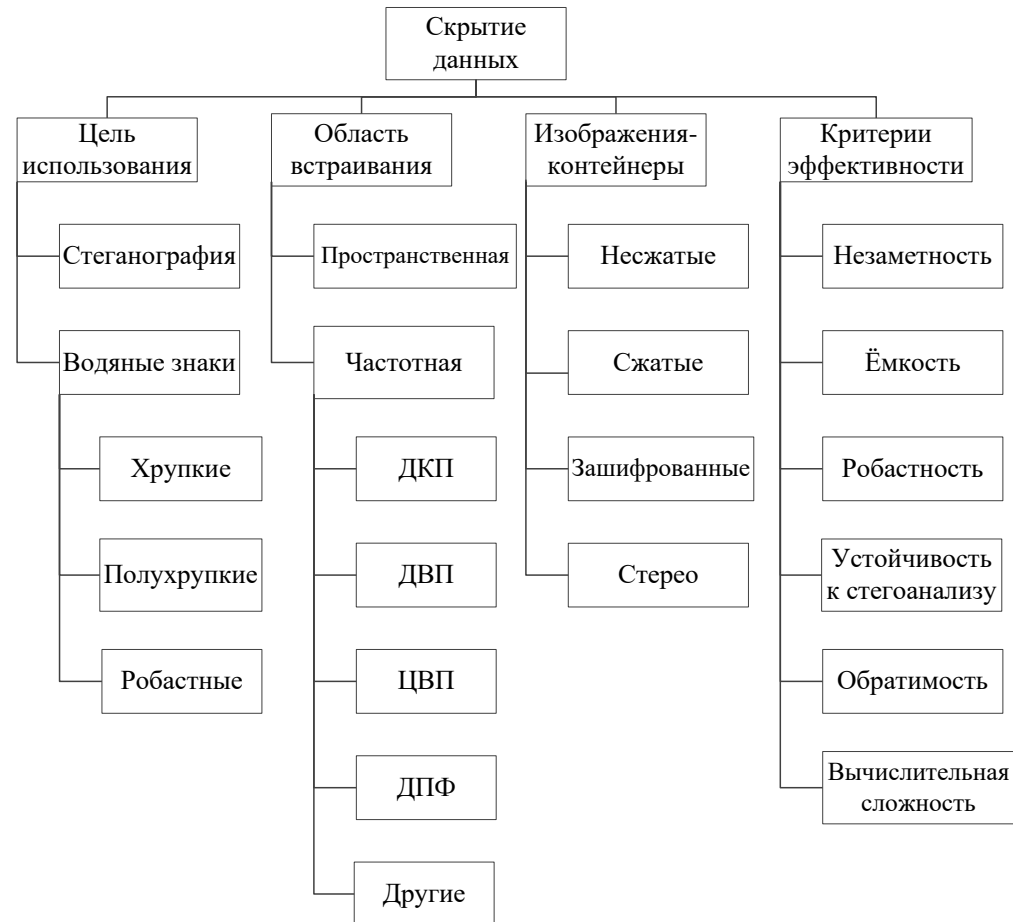
- Повышение эффективности встраивания дополнительных информационных последовательностей в цифровые изображения по критерию робастности за счет разработки комплекса новых более эффективных алгоритмов.

Основные результаты за 2-й год обучения

- Существенно расширен обзор предметной области.
- Разработана новая версия адаптивного алгоритма встраивания информации в коэффициенты дискретного косинусного преобразования (ДКП) цифровых изображений с безошибочным извлечением.
- Проведены дополнительные эксперименты по выбору наилучших параметров алгоритма и анализу эффективности.

Обзор предметной области

- Расширен и актуализирован обзор предметной области (по состоянию на осень 2020).
- Проведена классификация, обзор и анализ наиболее актуальных направлений исследований в области стеганографии и ЦВЗ.



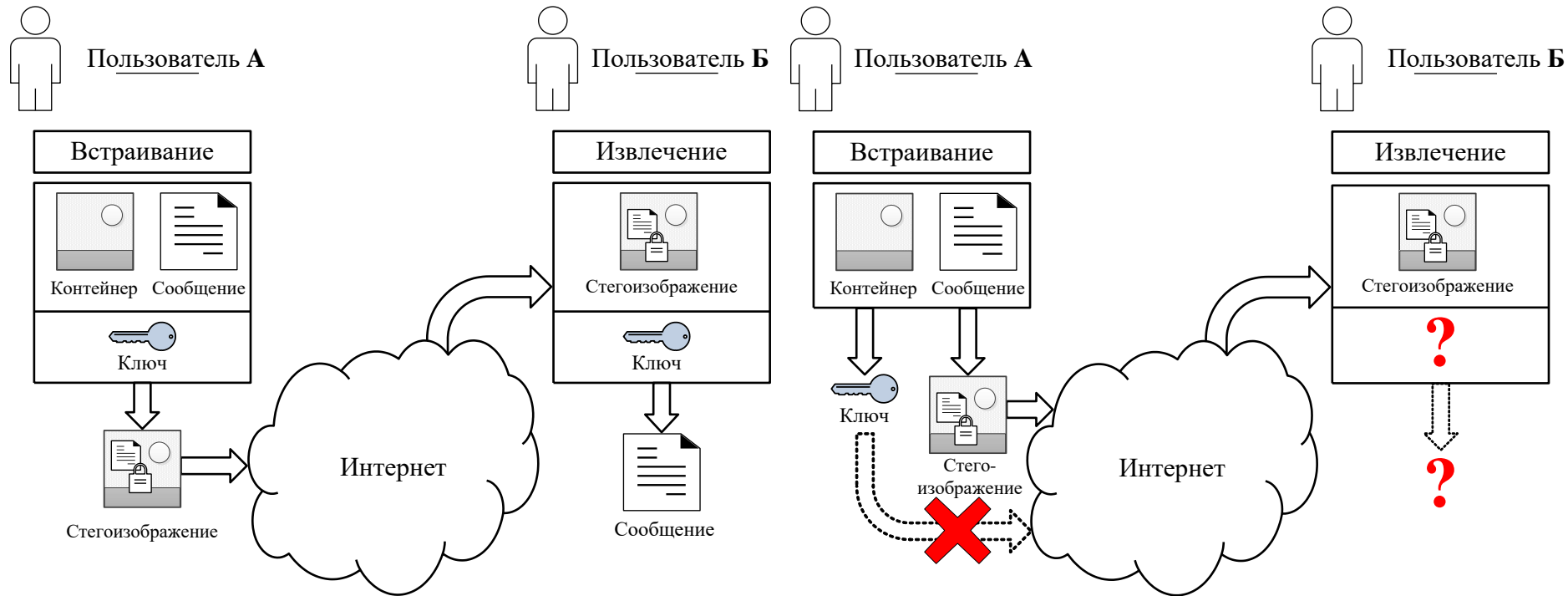
Актуальные проблемы предметной области

- Уязвимость перед стегоанализом либо отсутствие данных об устойчивости к нему.
- Проблема возникновения ошибок при извлечении информации.
- Отсутствие анализа устойчивости к внешним воздействиям либо низкая устойчивость к ним.
- Проблема передачи дополнительной информации, уникальной для каждой пары контейнер-вложение.

Результаты проведённого обзора

- Подготовлена первая версия обзорной главы диссертации.
- Результаты обзора опубликованы в журнале IEEE Access (Q1 WoS и Scopus): Evsutin O.O. Digital steganography and watermarking for digital images: a review of current research directions / O.O. Evsutin, A.S. Melman, R.V. Meshcheryakov // IEEE Access. – 2020. – Vol. 8. – P. 166589 - 166611. DOI: 10.1109/ACCESS.2020.3022779

Проблема передачи дополнительной информации, уникальной для каждой пары контейнер-вложение



Стеганографическая передача информации с использованием ключа

Стеганографическая передача информации с использованием дополнительной информации

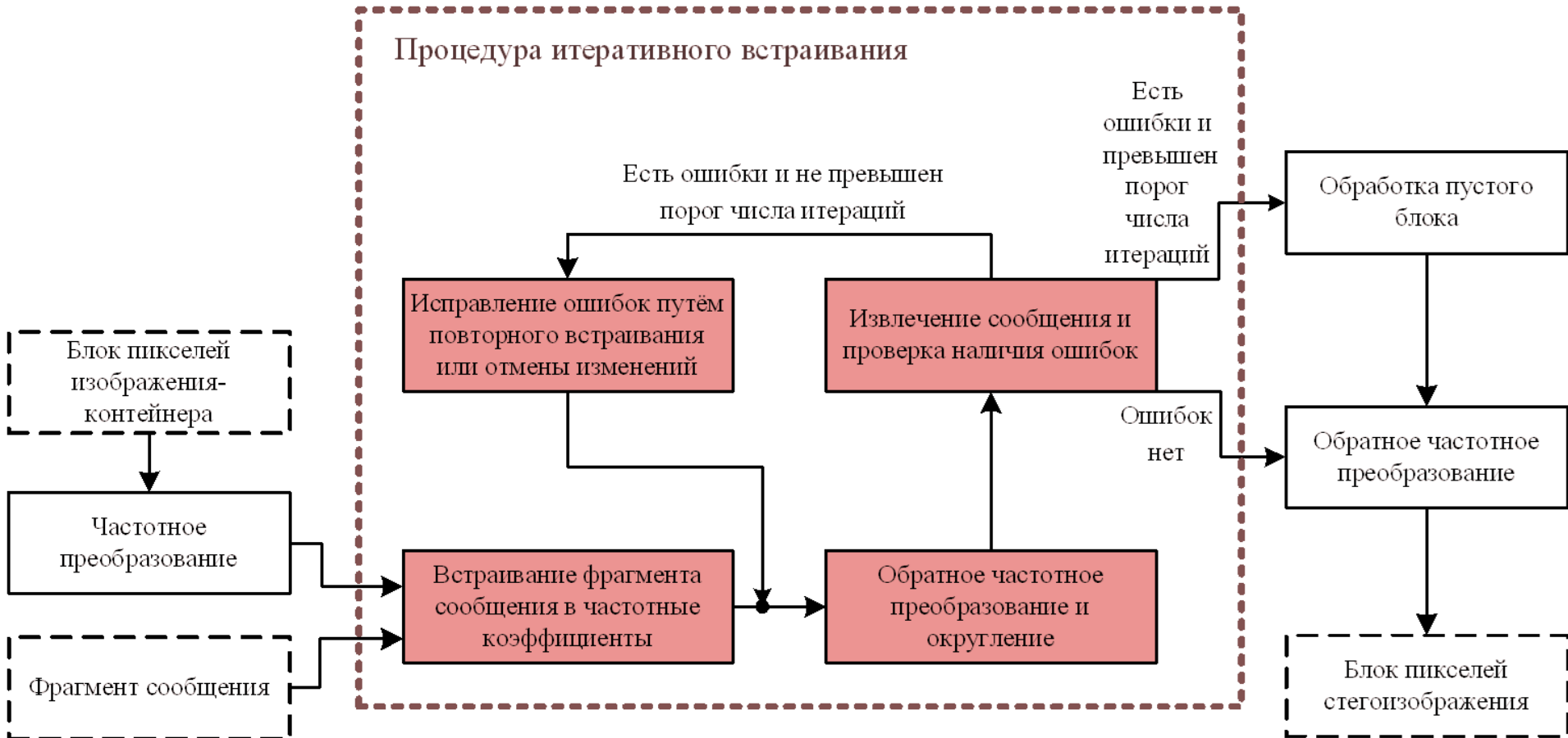
Проблема возникновения ошибок при извлечении информации



Решение обозначенных проблем

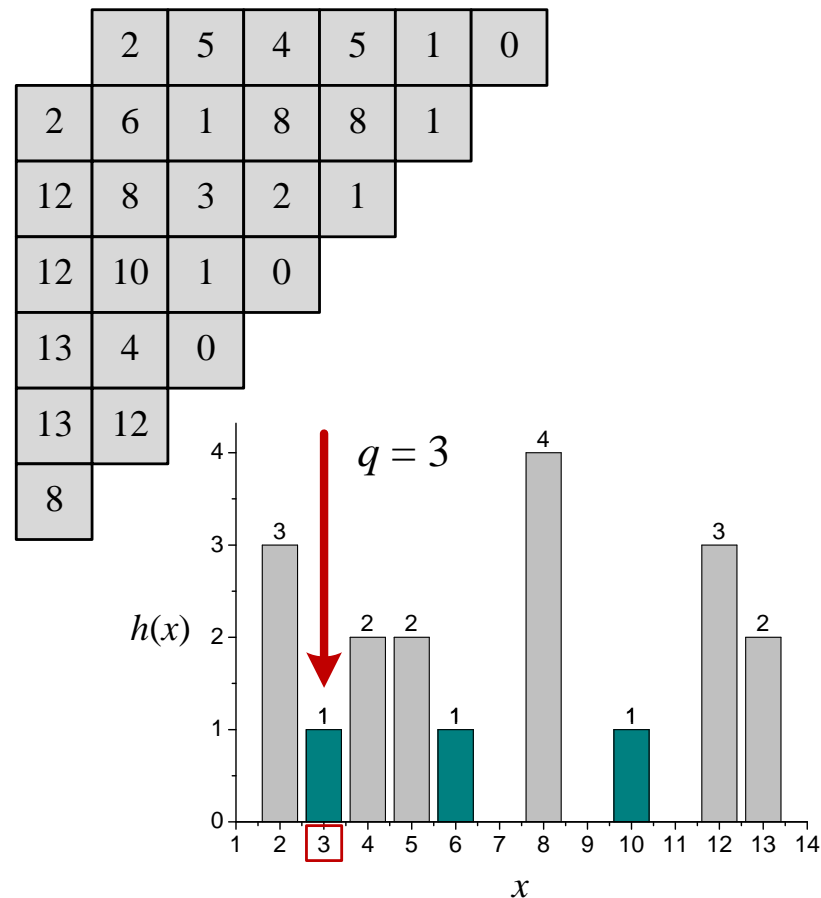
- Итеративная процедура встраивания информации.
- Адаптивный выбор параметра встраивания – шага квантования.
- Инвариантность выбора параметров встраивания к процедуре встраивания.

Итеративное встраивание



Адаптивный выбор шага квантования

DC	2.22	4.89	3.93	-4.88	0.87	-0.27	0.4
-1.77	6.30	0.88	7.93	-8.36	-1.02	2.59	3.71
-12.19	7.93	2.65	-1.96	1.42	5.68	-0.02	2.03
-11.71	9.56	0.99	0.38	-3.21	-3.14	-3.23	-2.18
-12.63	4.43	0.22	-0.8	2.38	3.45	0.86	2.09
-13.25	11.88	-1.91	-2.92	2.48	0.87	2.39	1.42
-7.54	4.65	-2.27	-3.62	-3.43	5.17	0.35	-2.08
-3.15	2.43	0.53	0.66	3.34	-0.76	-1.75	0.96



Адаптивный алгоритм встраивания информации в коэффициенты ДКП с безошибочным извлечением

Вход: изображение-контейнер, сообщение, порог итераций τ , координаты флага. **Выход:** стегоизображение.

Шаг 1: Разбить изображение-контейнер на неперекрывающиеся блоки размером 8×8 , выполнить ДКП каждого блока.

Шаг 2: По всем блокам изображения выполнять:

Шаг 2.1: Вычислить значение шага квантования q .

Шаг 2.2: Проверить необходимость выравнивания гистограммы $h(q)$ и при положительном исходе уточнить значение q .

Шаг 2.3: Встроить фрагмент сообщения и бит-флаг = 1.

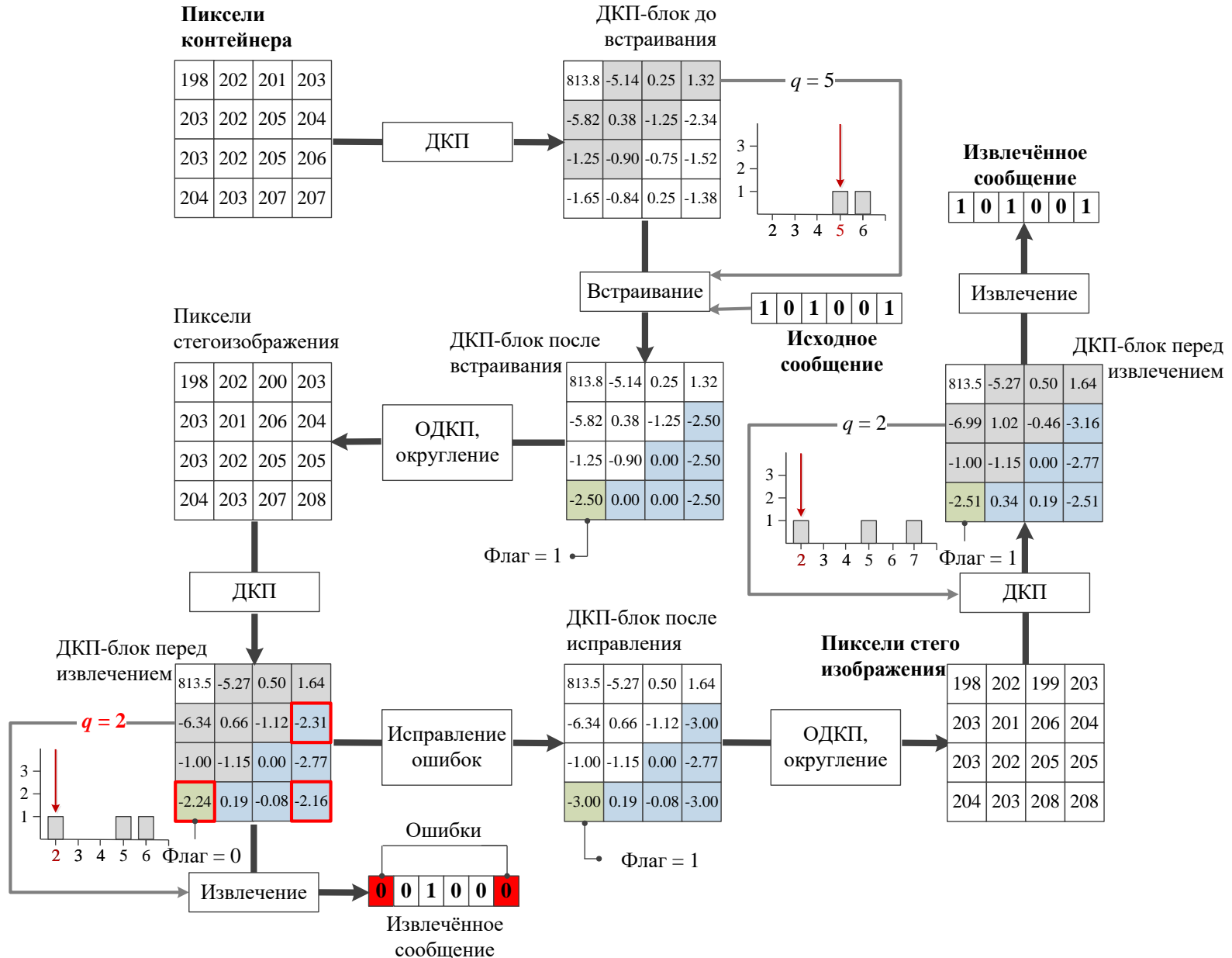
Шаг 2.4: Выполнить ОДКП, округление, ДКП.

Шаг 2.5: Извлечь встроенную строку и проверить её на наличие ошибок. Если ошибок нет, перейти к следующему блоку, иначе – скорректировать ошибки и перейти к шагу 2.4. Если превышен порог итераций τ , перейти к шагу 2.6.

Шаг 2.6: Обработать пустой блок.

Шаг 3: Сформировать стегоизображение и завершить алгоритм. 13

Адаптивный алгоритм встраивания информации в коэффициенты ДКП с безошибочным извлечением



Исследование зависимости эффективности встраивания от выбора областей встраивания и невстраивания

0	2	3	9	10	20	21	35
1	4	8	11	19	22	34	36
5	7	12	18	23	33	37	48
6	13	17	24	32	38	47	49
14	16	25	31	39	46	50	57
15	26	30	40	45	51	56	58
27	29	41	44	52	55	59	62
28	42	43	53	54	60	61	63

Низкочастотные (НЧ) коэффициенты
 Среднечастотные (СЧ) коэффициенты
 Высокочастотные (ВЧ) коэффициенты

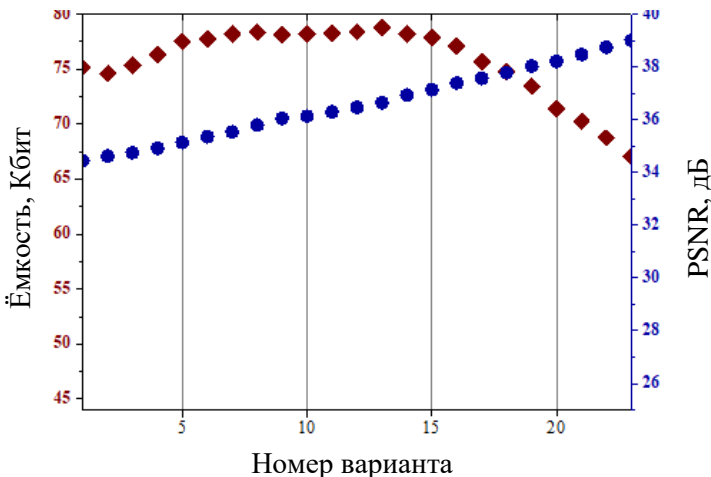
Рассмотрено 4 случая соотношений между областями встраивания и невстраивания:

- ВЧ коэффициенты и часть СЧ коэффициентов;
- НЧ коэффициенты и часть СЧ коэффициентов;
- СЧ коэффициенты, часть ВЧ коэффициентов и часть НЧ коэффициентов;
- НЧ коэффициенты и ВЧ коэффициенты.

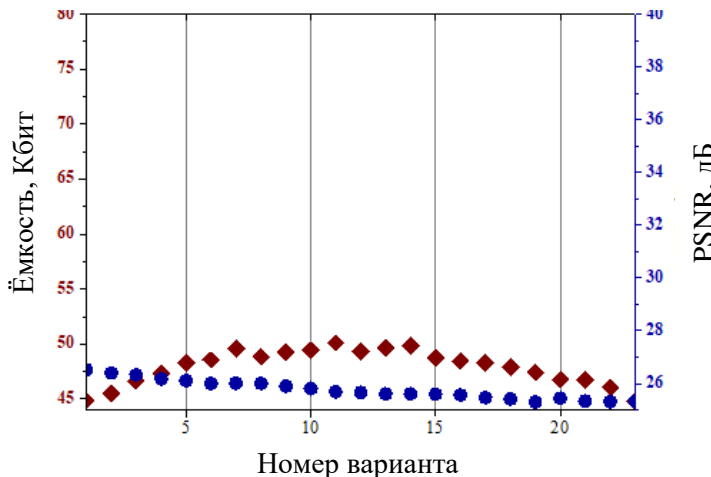
Номер варианта	Размер области встраив.	Состав области встраивания					
		НЧ коэффициенты		СЧ коэффициенты		ВЧ коэффициенты	
		Начальный	Конечный	Начальный	Конечный	Начальный	Конечный
Случай 1 (ВЧ + СЧ)							
1	43	—	—	21	42	43	63
2	42	—	—	22	42	43	63
...
23	21	—	—	—	—	43	63
Случай 2 (НЧ + СЧ)							
1	20	1	20	—	—	—	—
2	21	1	20	21	21	—	—
...
23	42	1	20	21	42	—	—

Исследование зависимости эффективности встраивания от выбора областей встраивания и невстраивания

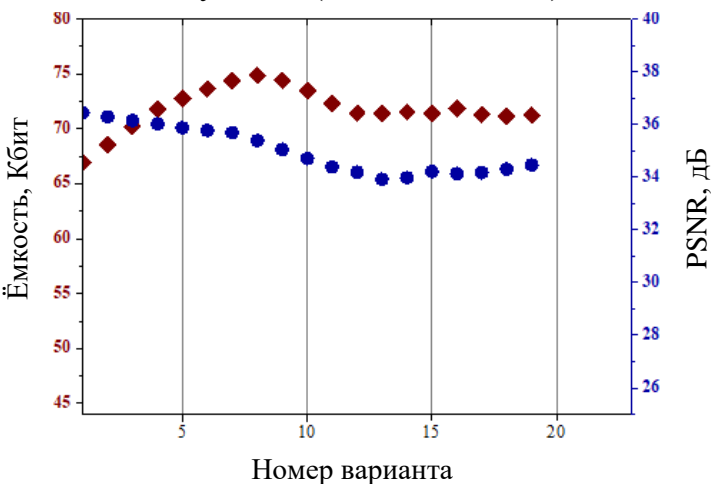
Случай 1 (ВЧ + СЧ)



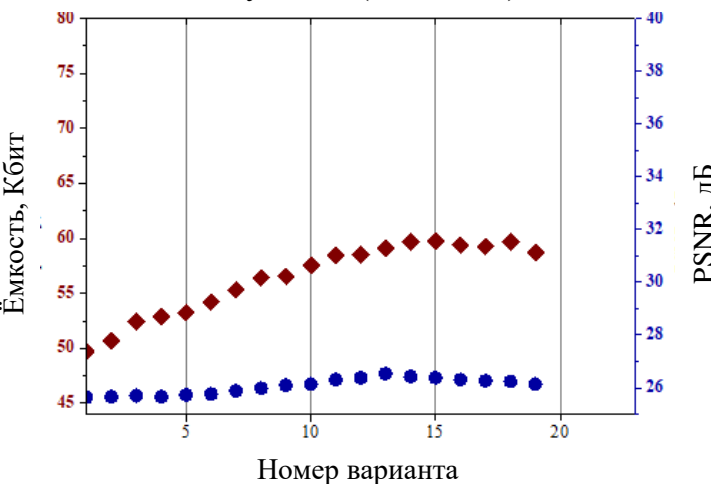
Случай 2 (НЧ + СЧ)



Случай 3 (СЧ + НЧ + ВЧ)

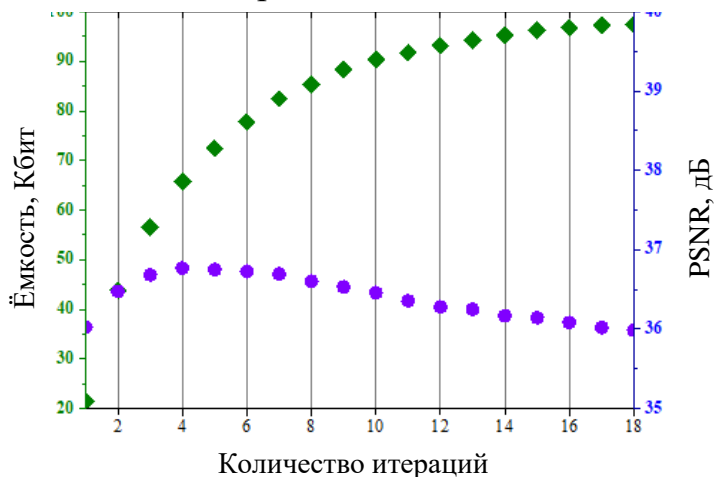


Случай 4 (НЧ + ВЧ)

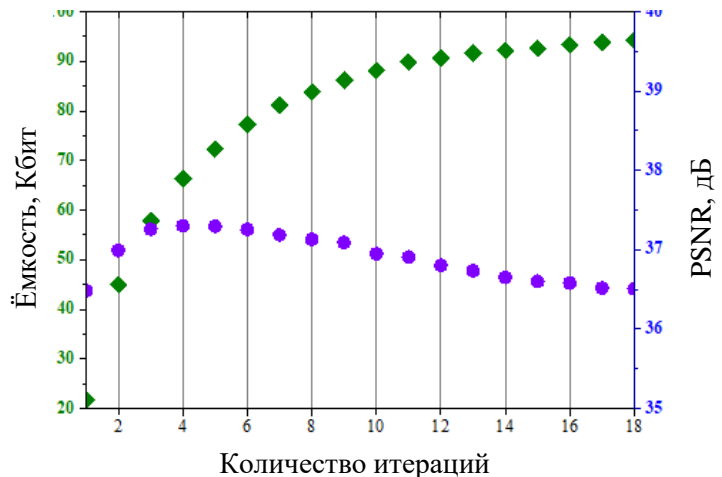


Исследование зависимости эффективности встраивания от количества итераций τ для областей встраивания разного размера (ВЧ + СЧ)

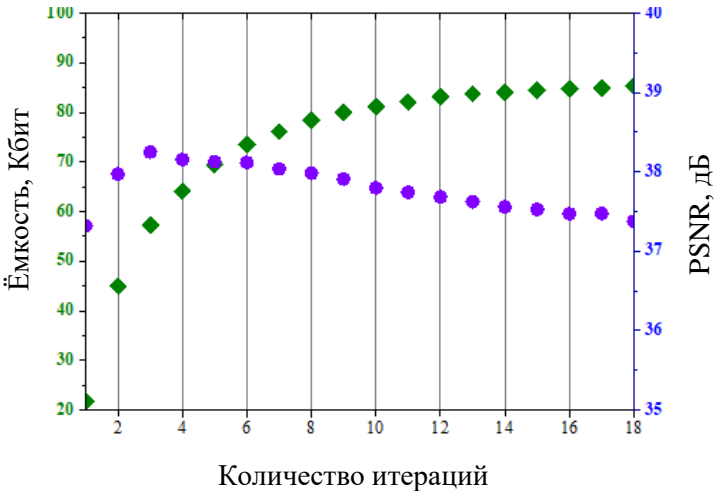
Область встраивания из 31 элемента



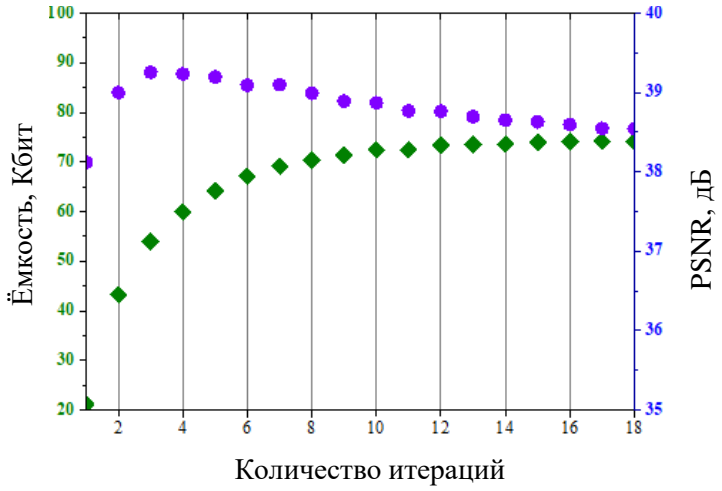
Область встраивания из 29 элементов



Область встраивания из 25 элементов



Область встраивания из 21 элемента

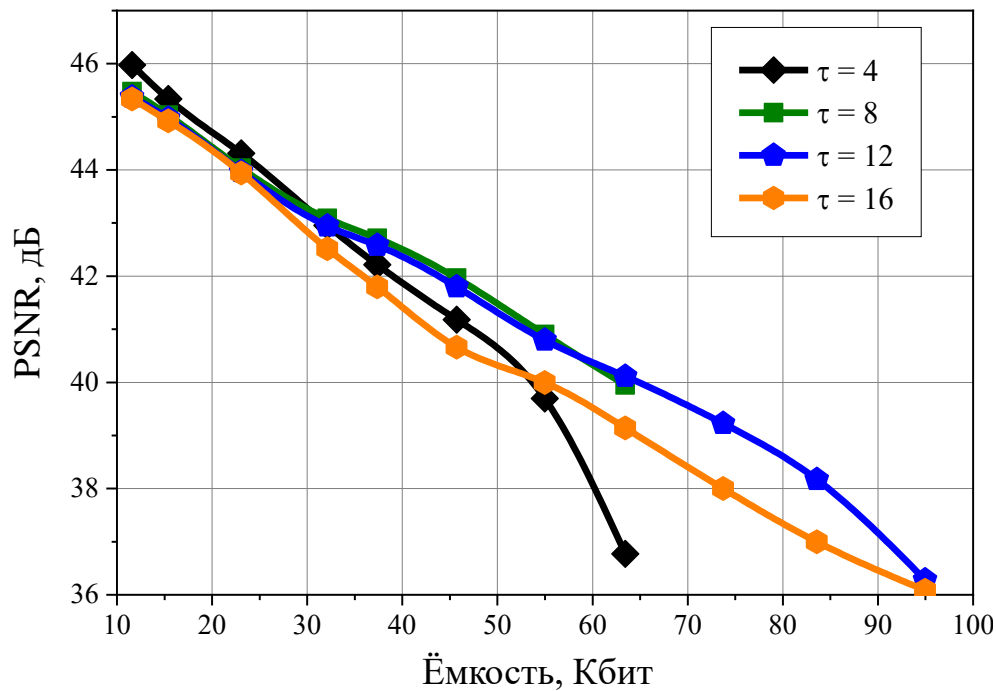


Незаметность встраивания

Изображение-контейнер



Стегоизображение

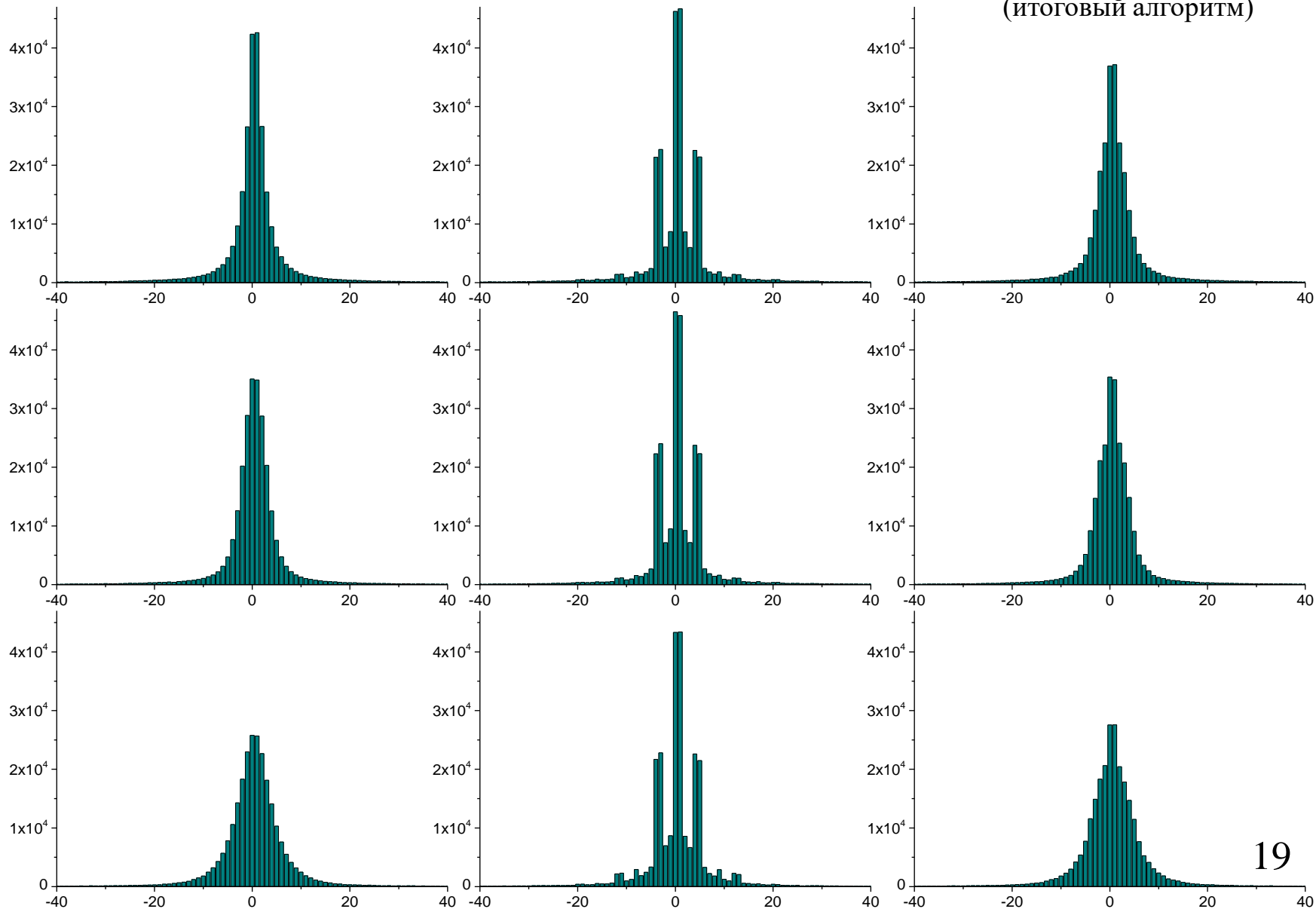


Стегоанализ (анализ гистограмм)

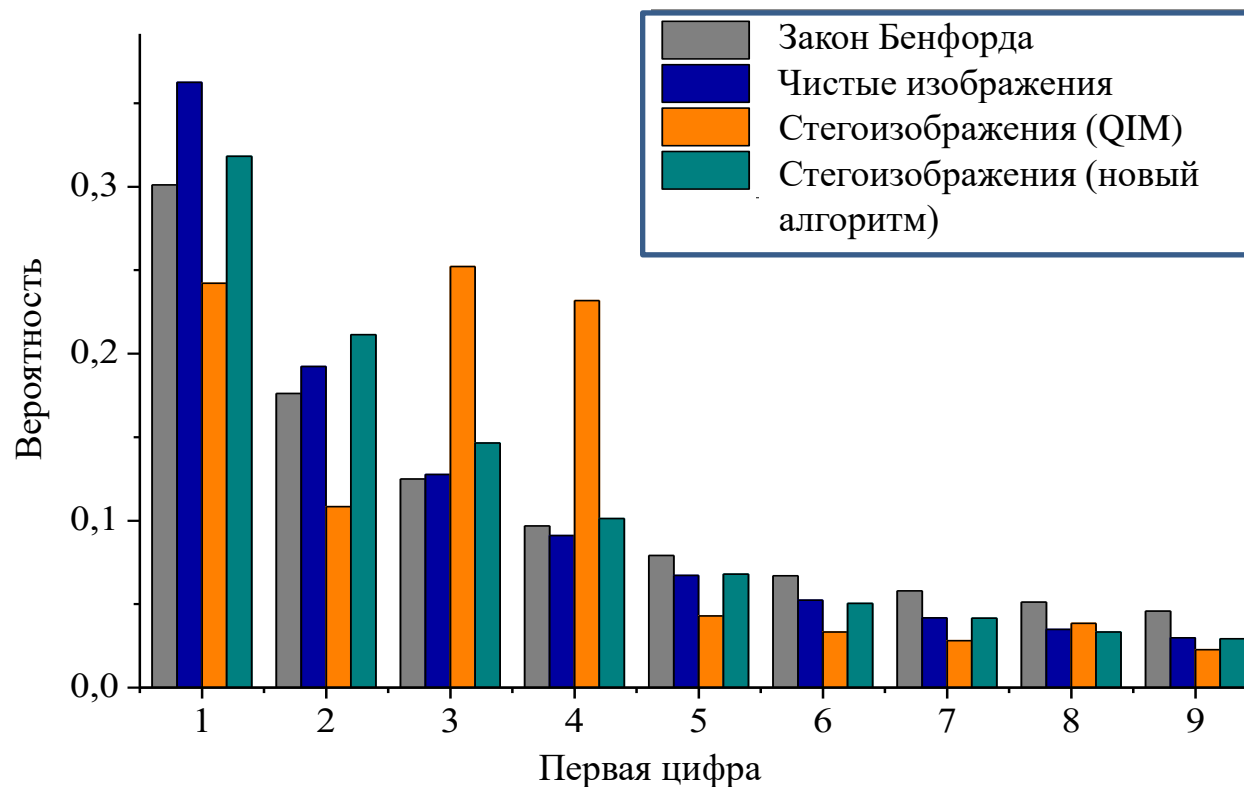
Изображение-контейнер

Без корректировки гистограммы

С корректировкой гистограммы
(итоговый алгоритм)



Стегоанализ на основе закона Бенфорда



Согласно закону Бенфорда, для реальных величин вероятность того, что цифра будет стоять на первом месте в числе тем выше, чем меньше эта цифра. При этом вероятность того, что x будет первой цифрой числа, вычисляется по формуле

$$P(x) = \log_{10} \left(1 + \frac{1}{x} \right), \quad x = 1, \dots, 9$$

Сравнение с аналогами

Алгоритм	Емкость	PSNR , dB	Доля ошибок в извлеч. сообщении, %	Необходимость доп. инф-ции для извлечения	Маск-ка искажений
Rabie and Kamel (2017)	512×512 пикселей	32.20– 28.75	>> 0	Да	Нет
Arunkumar et al. (2019)	256×256 пикселей	49.72	0.18	Да	Нет
Lin (2014)	455,306 бит	43.99	0	Да	Нет
Chen et al. (2016)	2,048–16,384 бит	44,90– 44,20	> 0	Нет	Нет
Fakhredanesh et al. (2019)	300–1,500 бит	72.28– 70.24	10–33	Нет	Да
Chen (2008)	196.608	37.06	>> 0	Нет	Нет
Evsutin et al. (2018)	4,096–40,960 бит	47.39– 36.87	0	Нет	Нет
Новый алгоритм	300–100,000 бит	57.69– 36.29	0	Нет	Да

Полученные результаты

Разработанный алгоритм:

- обеспечивает безошибочное извлечение встроенной информации за счёт итеративной процедуры встраивания;
- маскирует искажения естественной модели цифрового изображения в частотной области за счёт адаптивного выбора шага квантования;
- не требует передачи дополнительной информации, уникальной для каждой пары «контейнер-вложение» для извлечения данных;
- обеспечивает хорошее соотношение ёмкости и незаметности встраивания.

Результаты опубликованы в журнале Signal Processing (Q1 WoS и Scopus): Evsutin O.O Algorithm of error-free information embedding into the DCT domain of digital images based on the QIM method using adaptive masking of distortions / O.O. Evsutin, A.S. Melman, R.V. Meshcheryakov // Signal Processing. – 2020. DOI: <https://doi.org/10.1016/j.sigpro.2020.107811>

Ближайшие планы

- Повышение эффективности алгоритма итеративного встраивания в фазовый спектр коэффициентов дискретного преобразования Фурье.
- Исследование применимости технологии ЦВЗ для защиты электронных документов.

Формальные признаки (за 2-й год обучения)

- Преподавание: практики по КМЗИ, ТОКБ, руководство проектом ГПО.
- Публикации: 3 публикации Scopus и WoS, 5 публикаций РИНЦ.
- 2 свидетельства о регистрации программ для ЭВМ.
- Руководство грантом РФФИ.

Заключение

За отчётный период были получены следующие результаты:

- Существенно расширен обзор предметной области.
- Разработана новая версия адаптивного алгоритма встраивания информации в коэффициенты ДКП цифровых изображений с безошибочным извлечением.
- Проведены обширные дополнительные эксперименты по выбору наилучших параметров алгоритма и анализу эффективности.
- Результаты исследований опубликованы в высокорейтинговых научных журналах.

Спасибо за внимание.