«Национальный исследовательский ядерный университет
«МИФИ»

На правах рукописи

ШИФРИНА АННА ВЛАДИМИРОВНА

ОПТИКО-ЦИФРОВЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ СТРУКТУРИРОВАННЫХ АМПЛИТУДНЫХ МАСОК И АСИММЕТРИЧНОГО КОДИРОВАНИЯ

Специальность 01.04.21 — Лазерная физика

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2021

Работа выполнена в Национальном исследовательском ядерном университете «МИФИ»

Научный руководитель	**Стариков Ростислав Сергеевич** д.ф.-м.н., профессор отделения лазерных и плазменных технологий офиса образовательных программ (412) НИЯУ МИФИ

Официальные оппоненты:

Колючкин Василий Яковлевич	
д.т.н., доцент	профессор кафедры «Лазерные и оптико-электронные системы» МГТУ им. Н.Э. Баумана
Павлов Александр Владимирович	
д.ф.-м.н., с.н.с.	доцент факультета фотоники НИУ ИТМО
Быковский Алексей Юрьевич	
к.ф.-м.н.	высококвалифицированный ведущий научный сотрудник лаборатории оптоэлектронных процессоров ФИАН

Защита состоится «25» мая 2022 г. в 15:00 часов на заседании диссертационного совета МИФИ.01.04 федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ» (115409, г. Москва, Каширское шоссе, 31).

С диссертацией можно ознакомиться в библиотеке НИЯУ МИФИ и на сайте https//ds.mephi.ru/ федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»

Автореферат разослан «__» _____ 20__ г.

Учёный секретарь диссертационного совета _____ к.ф.-м.н. Краснов В.В.

Общая характеристика работы

Актуальность темы

В настоящее время оптические методы кодирования информации получают всё большее развитие и становятся полноправной альтернативой традиционным цифровым методам. К недостаткам цифровых методов стоит отнести относительно небольшую длину ключей кодирования (порядка сотен бит) и высокие требования к вычислительным мощностям и быстродействию устройств, на которых данные методы реализованы — и, как следствие, высокие энергетические затраты. Перспективным для создания альтернативного класса криптографических систем является использование оптических принципов. Оптические методы кодирования информации позволяют использовать двумерные ключи кодирования, что увеличивает их эффективную длину до десятков и сотен тысяч бит, а также позволяют сократить энергетические затраты. Дополнительным уникальным преимуществом является возможность кодирования визуальной информации непосредственно в процессе её регистрации (что принципиально, например, для создания систем защищённой видеосвязи). Потенциальные преимущества оптических криптографических схем определили не ослабевающий интерес к ним на протяжении последних 25 лет. Наиболее распространённые оптические криптографические схемы из разрабатываемых в настоящее время используют пространственно-когерентное освещение. Однако данные исследования носят перспективный характер и ориентированы на элементную базу следующего поколения. Затруднения в переходе к практической реализации связаны с низким качеством декодированных изображений, обусловленным возникновением спекл-шума из-за использования в качестве освещения когерентного излучения, а также с высокой сложностью аппаратной реализации. Более перспективным для практической реализации является использование пространственно-некогерентного квазимонохроматического освещения, которое не приводит к возникновению спекл-шума и позволяет использовать в качестве регистрирующих устройств матричные фотосенсоры. Недостатками такой схемы кодирования являются узкий фурье-спектр

кодированного изображения, упрощающий задачу нелегитимного декодирования, низкое качество декодированных изображений при использовании ключей кодирования, обеспечивающих высокую криптографическую стойкость, и невозможность создания асимметричной криптографической схемы на основе тех же принципов, что и для кодирования с когерентным освещением. Существование данных недостатков определяет актуальность данной работы, нацеленной на их устранение и создание полноценной асимметричной оптической криптографической системы с пространственно-некогерентным освещением.

Целью работы является разработка и исследование асимметричной оптико-цифровой криптографической схемы с использованием пространственно-некогерентного освещения и структурированных амплитудных масок.

Для достижения этой цели были поставлены следующие **задачи**:

1. Построение и апробация численной модели процесса оптического кодирования с пространственно-некогерентным освещением, учитывающей влияние как аппаратного комплекса, так и параметров используемых элементов (в первую очередь, ключей кодирования).
2. Разработка и апробация методов повышения качества декодированных изображений и криптографической стойкости кодированных изображений, основанных на использовании структурированных амплитудных масок.
3. Разработка и апробация контейнера цифровых данных на основе кодов с коррекцией ошибок, специализированного для оптических криптографических систем и используемого для предотвращения искажения данных в процессах кодирования и декодирования.
4. Разработка и экспериментальная реализация асимметричной оптической криптографической схемы с использованием пространственно-некогерентного освещения.

Научная новизна

Научная новизна работы определяется тем, что в ней:

1. Впервые разработана численная модель процесса оптического кодирования с пространственно-некогерентным освещением, учитывающая

влияние аппаратного комплекса и параметров используемых ключей кодирования на качество декодированных изображений.

2. Разработаны и экспериментально апробированы методы использования амплитудных структурированных масок для повышения отношения сигнал/шум декодированных изображений и криптографической стойкости кодированных изображений.

3. Разработан и экспериментально апробирован новый контейнер цифровых данных на основе битовых кодов с коррекцией ошибок, обладающий широким диапазоном доступных пользователю параметров и специализированный для оптических криптографических систем.

4. Впервые разработана оптико-цифровая асимметричная криптографическая схема с использованием пространственно-некогерентного освещения.

Практическая значимость

Практическая значимость работы обусловлена тем, что:

1. Разработана методика анализа влияния элементной базы на параметры оптической криптографической системы с пространственно-некогерентным освещением, осуществляемого на этапе её моделирования.

2. Разработана методика повышения криптографической стойкости оптических систем кодирования с пространственно-некогерентным освещением до уровня, соответствующего когерентным системам, с сохранением высокого отношения сигнал/шум.

3. Разработанный контейнер цифровых данных может быть использован не только в криптографических системах, но и в иных оптических информационных системах, где необходима корректировка ошибок, возникающих вследствие шумов и прочих искажений.

4. Разработанная асимметричная оптическая криптографическая схема может быть использована для шифрования потоков данных в режиме реального времени с криптографической стойкостью, превышающей стойкость существующих цифровых алгоритмов на 2-3 порядка.

Основные научные положения, выносимые на защиту

1. Численная модель оптической криптографической схемы с пространственно-некогерентным освещением, которая позволяет оценить влияние аппаратного комплекса и параметров используемых элементов на отношение сигнал/шум с точностью не хуже 70%.

2. Методика использования структурированных амплитудных масок в схеме оптического кодирования с пространственно-некогерентным освещением, обеспечивающая увеличение криптографической стойкости в 2,7 раза.

3. Контейнер цифровых данных, основанный на битовых кодах с коррекцией ошибок и специализированный для задач оптического кодирования, обладающий широким диапазоном доступных параметров: размер от 64 до 8192 отсчётов по одной стороне с произвольным соотношением сторон, плотность записи данных до 0,86, максимальный процент корректируемых ошибок 16%, что в 22 раза превышает соответствующее значение для QR-кода.

4. Оптико-цифровая асимметричная криптографическая схема с пространственно-некогерентным освещением, обеспечивающая значение отношения сигнал/шум, аналогичное симметричной схеме, но не имеющая уязвимости в виде необходимости предварительной передачи ключа кодирования.

Личный вклад автора

Все результаты получены лично автором работы или в соавторстве при его непосредственном участии.

Апробация работы

Основные результаты работы прошли апробацию на следующих международных и российских конференциях:

- VI, VII, VII, IX и X Международная конференция по фотонике и информационной оптике (Москва, 2017-2021);

- XIV Всероссийский молодёжный Самарский конкурс-конференция научных работ по оптике и лазерной физике (Самара, 2017);
- XIV и XVIII Международная конференция «ГОЛОЭКСПО» (Звенигород, 2017; Геленджик, 2021);
- X и XI Международная конференция «Фундаментальные проблемы оптики» (Санкт-Петербург, 2018-2019).

Публикации по теме

По теме диссертации опубликовано 25 печатных работ, среди них:

- 5 статей в изданиях, индексируемых в базах данных WoS и Scopus и/или включённых в Перечень ВАК РФ,
- 20 — в трудах международных и всероссийских конференций.

Структура диссертации

Диссертация состоит из введения, четырёх глав, заключения и списка цитированной литературы, включающего 114 наименований. Общий объём диссертации 163 страницы, включая 80 рисунков и 3 таблицы.

Содержание работы

Во введении кратко обосновывается актуальность задачи создания асимметричной оптической криптографической системы с пространственно-некогерентным освещением, сформулированы цели и задачи исследования, обоснованы новизна и практическая значимость результатов исследований. Излагаются основные положения, выносимые автором на защиту.

Первая глава содержит детальный литературный обзор существующих оптических криптографических схем и математическое описание процесса оптического кодирования с пространственно-некогерентным освещением.

В Разделе 1.1 обсуждаются работы, посвящённые различным методам оптического кодирования на основе преобразования световых полей. Детально рассматривается наиболее популярный метод оптического кодирования с пространственно-когерентным освещением: кодирование с двумя случайными фазовыми масками (DRPE, Double random phase encoding). Отмечено, что задача

экспериментальной реализации разработанных DRPE методов во многом остаётся не реализованной, большинство исследований опирается на результаты численного моделирования. Сложность оптической реализации связана с высокими требованиями к точности позиционирования оптических элементов и низким качеством декодированных изображений из-за наличия спекл-шума. Один из способов упрощения оптической криптографической схемы — изменение типа освещения с когерентного на некогерентное.

Раздел 1.2 посвящён описанию процесса оптического кодирования с пространственно-некогерентным освещением. Принципиальная схема кодирования приведена на рисунке 1.

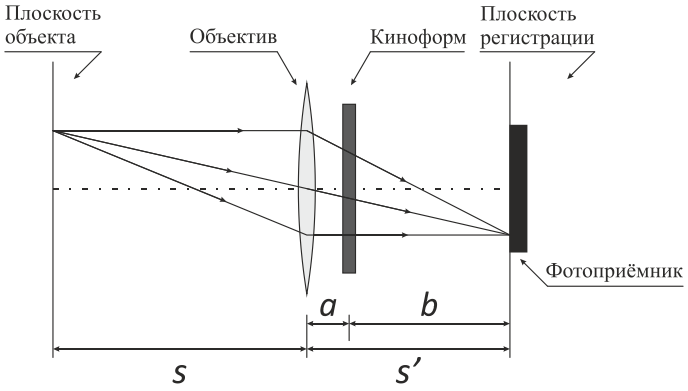


Рисунок 1 — Принципиальная схема оптического кодирования с использованием дифракционного оптического элемента (киноформа)

В данной схеме ключ кодирования формируется дифракционным оптическим элементом (ДОЭ), в качестве которого используется киноформ. Кодированное изображение представляет собой свёртку распределения интенсивностей кодируемого изображения и импульсного отклика ключа кодирования — его функции рассеянии точки (ФРТ) Достоинствами метода являются высокое быстродействие, отсутствие спекл-шума и простота реализации.

Процесс оптического кодирования можно приближённо описать уравнением:

$$g(i,j) = f(i,j) \otimes h(i,j) + n(i,j), \qquad (1)$$

где g — кодированное изображение, f — исходное изображение, h — ФРТ, n — аддитивный шум, i, j — индексы, соответствующие координатам отсчетов изображений, ⊗ — операция свёртки.

В фурье-плоскости уравнение (1) имеет вид:

$$G(u,v) = F(u,v) \cdot H(u,v) + N(u,v), \qquad (2)$$

где G, F, H и N — фурье-спектры функций g, f, h и n; u,v — индексы, соответствующие координатам в Фурье-плоскости.

В отсутствие шума ($N(u,v) = 0$) и нулевых значений у функции $\mathrm{H}(u,v)$, фурье-спектр F’ декодированного изображения f’ находится как:

$$F'(u,v) = \frac{G(u,v)}{H(u,v)} = G(u,v) \cdot Y(u,v), \qquad (3)$$

где $Y(u,v) = {}^{1}/_{\mathrm{H}(u,v)}$ — декодирующий инверсный фильтр. В данной работе для декодирования применялся инверсный фильтр с регуляризацией А.Н. Тихонова. В качестве сглаживающей функции использовалась константа — максимум спектра мощности ФРТ:

$$Y(u,v,\alpha) = \frac{|H(u,v)|}{|H(u,v)|^2 + \alpha \cdot max(|H(u,v)|^2)}, \qquad (4)$$

где α — параметр регуляризации.

В Разделе 1.3 приводится описание разработанной многофакторной модели оптического кодирования с пространственно-некогерентным освещением. Разработанная численная модель учитывает следующие факторы, влияющие на качество декодированного изображения:

- нормированная средняя энергия (НСЭ) ключа кодирования — отношение средней величины энергии в импульсном отклике ключа кодирования к максимальному по ключу значению энергии;
- шумовые характеристики регистрирующего фотосенсора;
- преобразование растров отклика кодирующего ДОЭ и исходного изображения при их регистрации фотосенсором;
- шум синтеза ДОЭ (синтез ДОЭ осуществляется итерационным методом Герчберга-Сэкстона с локализацией шума);

- оптические аберрации, возникающие при аппаратной реализации криптографической системы;
- фоновая засветка, вызванная взаимодействием оптического излучения с различными оптическими элементами системы и искажением ДОЭ при его отображении на фазовом жидкокристаллическом пространственно-временном модуляторе света (ЖК ПВМС) из-за флуктуаций фазового сдвига.

Была проведена апробация разработанной модели, заключавшаяся в сравнении результатов, предсказанных моделью и полученных в оптических экспериментах (в первую очередь значений нормированного среднеквадратичного отклонения качества декодированного изображения от кодируемого (НСКО)). Для апробации была выбрана симметричная схема оптического кодирования с пространственно-некогерентным освещением (рисунок 2), в качестве кодируемых объектов выступали полутоновые изображения.

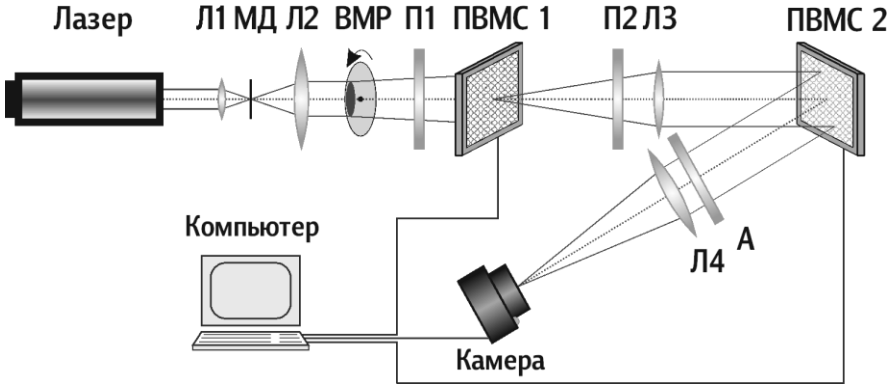
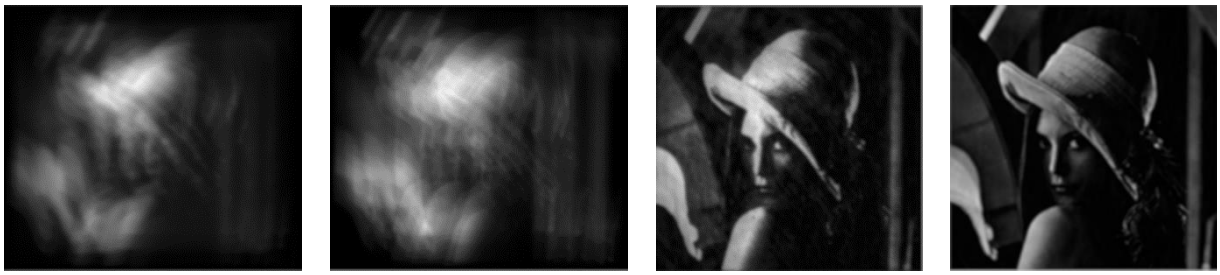


Рисунок 2 — Схема аппаратной реализации оптической криптографической системы с пространственно-некогерентным освещением

В качестве источника освещения использовался волоконный лазер IPG Photonics VLM-561-5 с длиной волны 561 нм и максимальной оптической мощностью 5 Вт. Линзы Л1 и Л2 формировали коллимированный пучок излучения, который проходил через микродиафрагму МД. Вращающийся матовый рассеиватель ВМР разрушал пространственную когерентность излучения. Кодируемое изображение отображались амплитудным ЖК ПВМС1 HoloEye LC2002, с разрешением 800x600 пикселей. Поляризаторы П1, П2 и

анализатор А обеспечивали правильное функционирование ЖК ПВМС HoloEye PLUTO VIS с разрешением 1920x1080 пикселей. На фазовый ЖК ПВМС2 выводился кодирующий фазовый ДОЭ. Фотосенсор камеры Vieworks VA-29MG2 с разрешением 6576x4384 пикселей регистрировал кодированное изображение, после чего оно передавалось на компьютер.

Сравнение результатов оптического эксперимента и полученных с использованием многофакторной модели продемонстрировано на рисунке 3.



(а) (б) (в) (г)

Рисунок 3 — Кодированные и декодированные изображения, полученные при использовании идентичных ключей кодирования: в оптическом эксперименте (а, в), в результате использования многофакторной модели (б, г)

Для декодированного изображения, полученного в результате использования многофакторной модели, значение НСКО составило 0,13 (в то время как для модели, учитывающей только шумы фотосенсора — 0,05), что значительно ближе к результатам оптического эксперимента — 0,19.

Во второй главе представлены результаты разработки и апробации метода использования структурированных амплитудных масок (САМ) в оптической криптографической системе с пространственно-некогерентным освещением.

В Разделе 2.1 описано применение САМ для повышения качества декодированного изображения. Предложено использование прямоугольных разрежающих масок в виде решёток, накладываемых на кодируемое изображение, и приводящее к мультиплицированию его спектра.

В Разделе 2.2 описано применение САМ для повышения криптографической стойкости кодированных изображений, оцениваемой как значение коэффициента демаскировки. Предложен метод на основе двукратной реализации операции оптического кодирования: вначале с изображением, на которое наложена

случайная маска, а затем с изображением, на которое наложен её негатив. Итоговое кодированное изображение получается вычитанием промежуточных друг из друга. Наложение случайной маски приводит к уширению спектра изображения, а операция вычитания позволяет получить знакопеременное кодированное изображение (со значениями фазы половины отсчётов π).

В Разделе 2.3 осуществлено численное моделирование использования САМ в оптической криптографической системе с пространственно-некогерентным освещением. На выборке из 10 полутоновых тестовых изображений и 185 ключей кодирования получены зависимости значения НСКО от значения НСЭ ключей кодирования для обоих типов используемых САМ (рисунок 4).

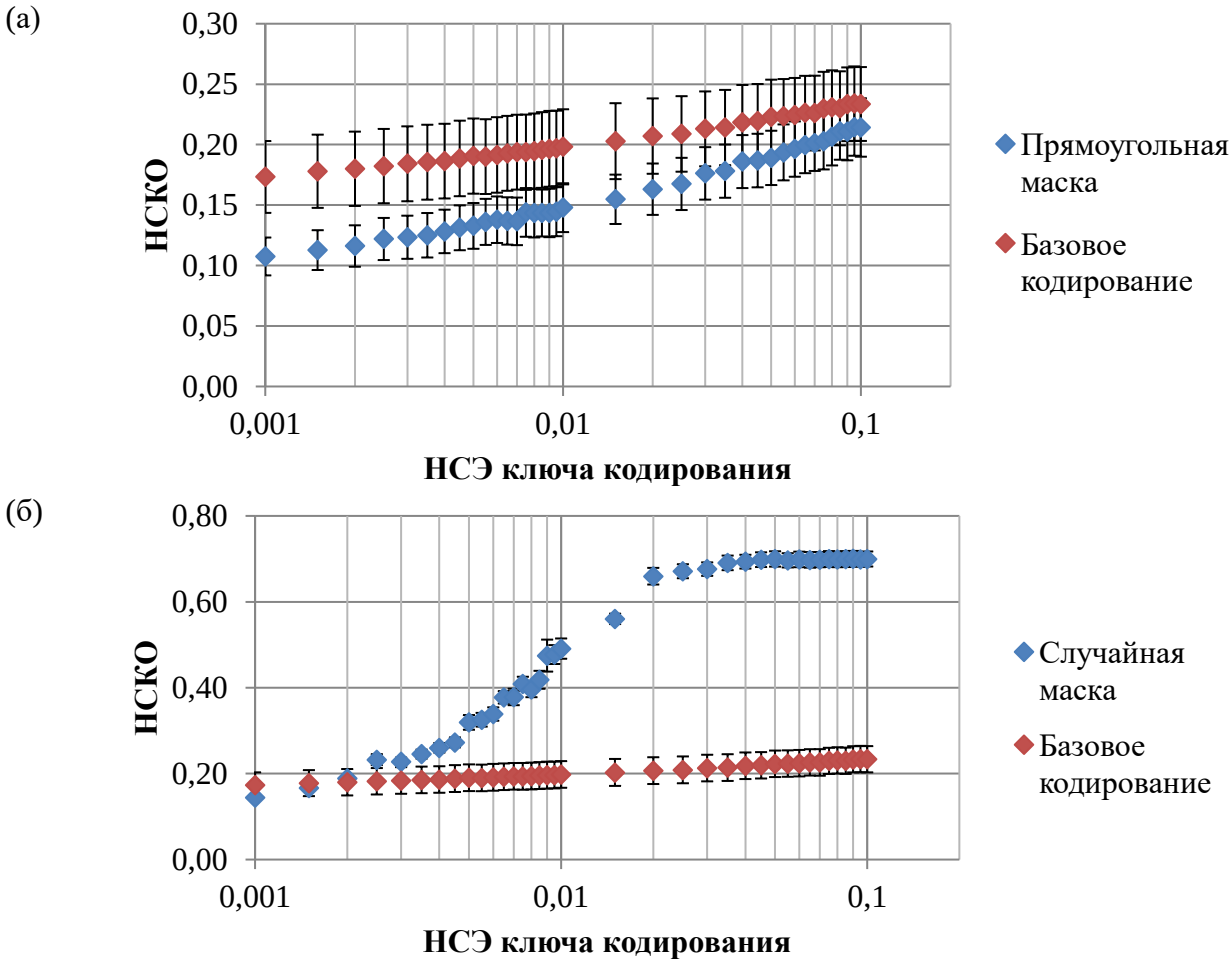


Рисунок 4 — Зависимость значения НСКО от значения НСЭ ключа кодирования: для кодирования с использованием прямоугольных разрежающих масок (а) и с использованием взаимодополняющих случайных масок (б)

Показано, что для ключей кодирования, имеющих практическое значение (со значением НСЭ меньше 0,01) использование прямоугольной разрежающей маски приводит к уменьшению значения НСКО (увеличению значения отношения сигнал/шум (ОСШ)) в 1,32-1,56 раза. Использование взаимодополняющих случайных масок в том же диапазоне значений НСЭ приводит к ухудшению качества декодированного изображения, однако они обеспечивают значительно более высокую криптографическую стойкость кодированного изображения (благодаря чему возможно использование ключей с малым значением НСЭ). На рисунке 5 показана зависимость коэффициента демаскировки кодированного изображения от значения НСЭ ключа кодирования для кодирования со случайными масками и для базового оптического кодирования.

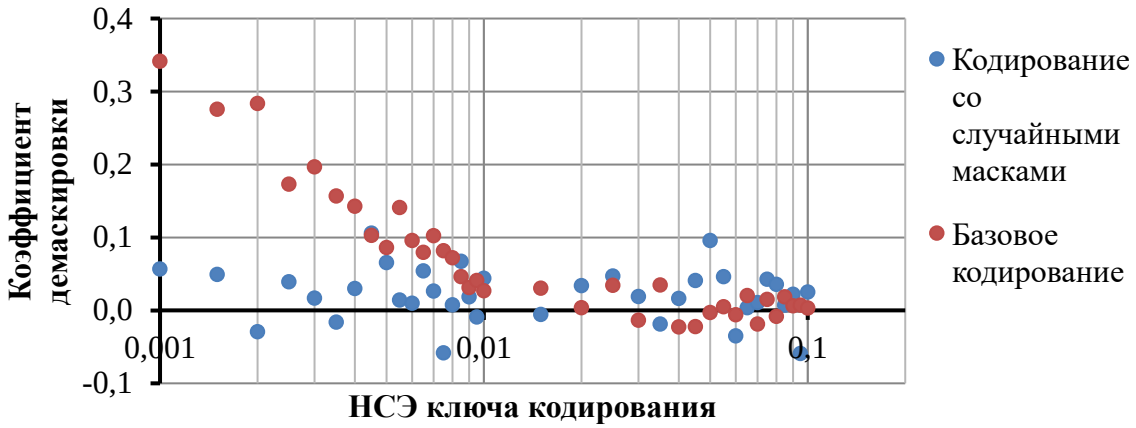


Рисунок 5 — Зависимость коэффициента демаскировки кодированного изображения от значения НСЭ ключа кодирования

Для ключей со значениями НСЭ в диапазоне 0,001-0,01 была рассчитана степень уменьшения коэффициента демаскировки, которая составила 2,2-8,1 раза. Данных значений достаточно, чтобы кодированное изображение, полученное при использовании даже весьма разреженных ключей, уже не содержало визуально различимых элементов исходного изображения.

В Разделе 2.4 представлены результаты использования САМ в оптических экспериментах. Получено, что использование взаимодополняющих случайных масок понижает значение коэффициента демаскировки по сравнению с базовым оптическим кодированием в 2,7 раза, что согласуется с результатами численного моделирования. Для разрежающей маски в виде бинарной решётки степень

увеличения значения ОСШ декодированного изображения составила 1,06 раза (значение ОСШ для базового оптического кодирования — 5,21, для кодирования с использованием маски — 5,54). Меньшая степень увлечения значения ОСШ по сравнению с результатами численного моделирования связана с затруднениями, возникающими при устранении разрежения с декодированного изображения: искажения спектра в процессах кодирования и декодирования не позволяют осуществить эффективную частотную фильтрацию. Примеры кодированных и декодированных изображений, полученных в ходе оптических экспериментов, представлены на рисунке 6.

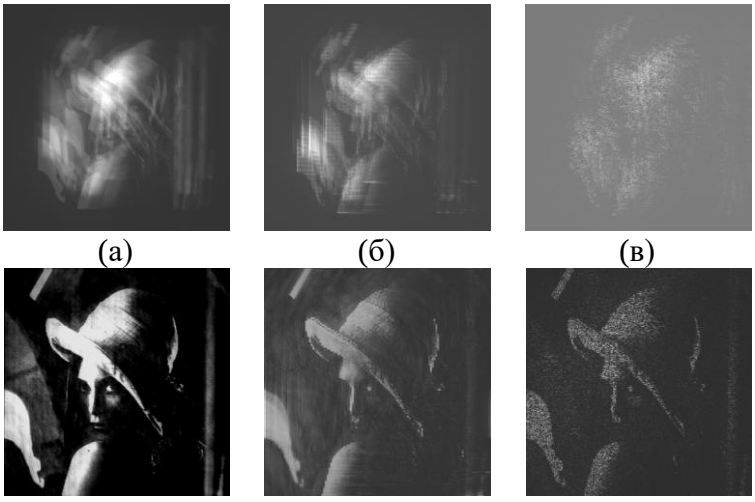


Рисунок 6 — Кодированные (а-в) и декодированные (г-е) изображения, полученные в ходе оптического эксперимента. Кодирование без использования масок (а, г), с использованием разрежающей маски в виде решётки (б, д), с использованием взаимодополняющих случайных масок (в, е)

В третьей главе описан разработанный в ходе данной работы матричный контейнер цифровых данных (МКЦД), специализированный для оптических криптографических систем и основанный на использовании кодов с коррекцией ошибок.

В Разделе 3.1 описаны существующие способы графического представления цифровых данных в оптических информационных системах: прямое представление, представление с использованием кодировки и упаковка информации в контейнер. Среди контейнеров данных наиболее популярными являются QR-коды. Их основным преимуществом является возможность

компенсации возникающих искажений за счёт использования кодов с коррекцией ошибок. Однако QR-коды не специализированы для оптических криптографических систем и обладают существенными недостатками. Во-первых, они основаны на байтовых кодах, хотя имеют битовое (бинарное) графическое представление — т.е. уязвимы к искажениям в виде шумов. Во-вторых, QR-коды содержат набор служебных элементов для их точного позиционирования, избыточный для оптических криптографических систем, т.к. возникающие в них искажения не связаны со значительными сдвигами или поворотами.

В Разделе 3.2 приведено описание МКЦД, основанного на использовании битовых кодов с коррекцией ошибок. МКЦД представляет собой последовательность из нескольких сообщений, вся необходимая служебная информация расположена в центре первого сообщения (рисунок 7).

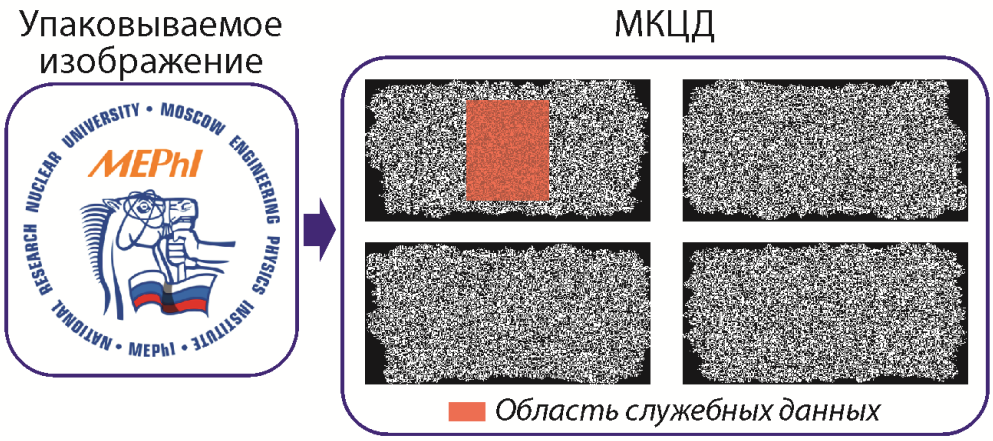


Рисунок 7 — Упаковка графического файла в МКЦД, представляющий собой последовательность из четырёх связанных между собой сообщений

В таблице 1 представлено сравнение параметров МКЦД и QR-кодов.

Таблица 1 — Сравнение параметров МКЦД и QR-кода

Параметр	**QR-код**	**МКЦД**
Доступные размеры	40 значений в диапазоне 21-177 с шагом 4 модуля	Все значения в диапазоне 64-8192 модуля
Соотношение сторон	1:1	Произвольное
Доступные расчётные значения процента корректируемых ошибок	7, 15, 25 или 30%	Диапазон 1-21,7%
Максимальное количество связанных сообщений в последовательности	16	8192
Скремблирование данных	Нет	Да
Наличие демаскирующих служебных блоков	Да	Нет
Количество градаций яркости	2	Произвольное значение
Границы	Прямые	Контур произвольной формы

Было определено соотношение между расчётным и экспериментальным значениями степени избыточности (максимального процента корректируемых ошибок). Для этого было численно промоделировано зашумление сообщений контейнера шумом типа «соль и перец» с постепенно нарастающей плотностью. При этом использовалось графическое представление «один модуль — один пиксель». Показано, что для МКЦД зависимость может быть с высокой точностью линейно аппроксимирована уравнением $СИ_{МКЦД} = 0,78*СИ_{БЧХ}-0,012$, где $СИ_{МКЦД}$, $СИ_{БЧХ}$ — экспериментальная и расчётная степени избыточности. Диапазон экспериментальных значений составил 0,5-16,3%. Подобная зависимость была рассчитана и для QR-кодов. Для всех расчётных значений степени избыточности экспериментальное значение составило приблизительно 0,7%.

В Разделе 3.3 представлены результаты численного моделирования использования МКЦД в оптической криптографической системе с пространственно-некогерентным освещением. Определено экспериментальное значение степени избыточности, соответствующее параметрам моделировавшейся системы и использованного МКЦД. Экспериментальное значение составило 7,3%, в то время как расчётное значение было 12,0%. Аналогичное моделирование было осуществлено и для QR-кодов. Для них экспериментальное значение составило 1,1% (расчётное — 7%).

В Разделе 3.4 описаны эксперименты по кодированию МКЦД в оптической криптографической системе с пространственно-некогерентным освещением. Схема аппаратной реализации системы представлена на рисунке 8.

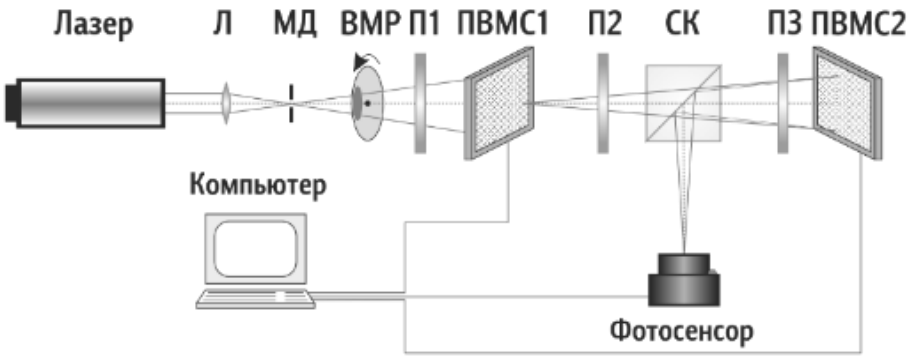


Рисунок 8 – Схема аппаратной реализации оптической криптографической системы с пространственно-некогерентным освещением

От изначальной схемы, представленной на рисунке 2, данная схема отличается тем, что является безлинзовой. Это позволило повысить эффективность процесса кодирования за счёт уменьшения оптических потерь.

Результаты экспериментов представлены на рисунке 9. Среднее количество ошибок на одно сообщение МКЦД составило 289±31. Полученные значения заметно ниже степени избыточности использовавшихся МКЦД, благодаря чему все данные были извлечены безошибочно.

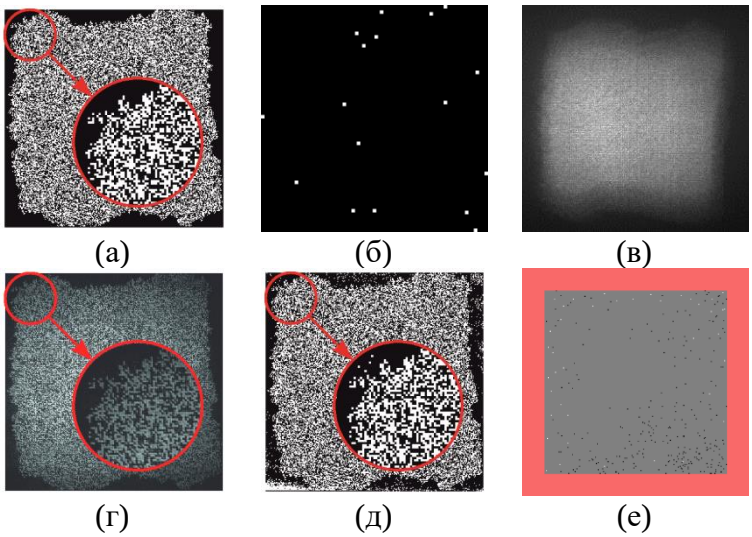


Рисунок 9 — Результаты оптического кодирования МКЦД: сообщение МКЦД с увеличенным фрагментом (а), ключ кодирования (б), кодированное изображение (в), декодированное изображение с увеличенным фрагментом до (г) и после (д) постобработки, карта распределения ошибок (е)

В четвёртой главе описана разработанная асимметричная оптическая криптографическая схема с пространственно-некогерентным освещением на основе двукратной реализации операции кодирования.

В Разделах 4.1 и 4.2 дано описание асимметричных криптографических систем и принципов их построения в случае оптического кодирования с пространственно-когерентным освещением.

В разделе 4.3 представлен разработанный метод асимметричного оптического кодирования с пространственно-некогерентным освещением. Процессы кодирования и декодирования описываются следующим образом:

1. Отправитель кодирует исходное изображение I ключом кодирования k_1 и отправляет однократно кодированное изображение E_1 Получателю.

2. Получатель кодирует полученное однократно кодированное изображение E_1 ключом кодирования k_2 и возвращает двукратно кодированное изображение E_{12} Отправителю.

3. Отправитель декодирует двукратно кодированное изображение E_{12} с помощью инверсного фильтра k_1^{-1}, основанного на ключе кодирования k_1 и отправляет однократно декодированное изображение E_2 Получателю.

4. Получатель декодирует кодированное изображение E_2 с помощью инверсного фильтра k_2^{-1}, основанного на ключе кодирования k_2 и получает исходное изображение I.

Таким образом, по незащищённым каналам связи передаются только кодированные изображения E_1, E_{12} и E_2, но не ключи k_1 и k_2.

Наиболее перспективными для практического применения являются две реализации предложенного метода: двукратно оптическое асимметричное кодирование, в котором операции кодирования реализованы оптически (выше быстродействие, однако из-за накопления шумов может значительно снижаться качество декодированных изображений), и оптико-цифровое асимметричное кодирование, где первая операция реализована оптически, а вторая численно (быстродействие ниже, но выше качество декодированных сообщений).

Далее описан метод аутентификации пользователей криптографической схемы на основе расчёта хэш-сумм от фрагментов фурье-спектров кодированных изображений для устранения её уязвимости к атакам типа «Man in the Middle». Показано, что попытка подмены выбранного фрагмента приводит к ухудшению качества декодированных изображений в 2-10 раз, что наглядно демонстрирует наличие вмешательства.

В Разделе 4.4 представлены результаты численного моделирования разработанной асимметричной оптической криптографической схемы. Показано, что для двукратно оптической реализации для всех использовавшихся значений НСЭ ключей кодирования значения НСКО декодированных изображений лежат в диапазоне 0,45-0,47, что соответствует крайне высокой степени зашумлённости на пороге визуального распознавания элементов изображения и связано как с накоплением шумов, так и с ограниченным динамическим диапазоном фотосенсора регистрирующей камеры. Для оптико-цифровой реализации показано, что добавление второй операции кодирования не оказывает влияния на качество декодированного изображения.

Полученные результаты проведения оптических экспериментов представлены в Разделе 4.5. В экспериментах (рисунок 10) значения НСЭ обоих ключей кодирования — 0,005. Значение НСКО декодированного изображения составило 0,189, что соответствует достаточно высокому качеству и аналогично симметричному оптическому кодированию (0,191).

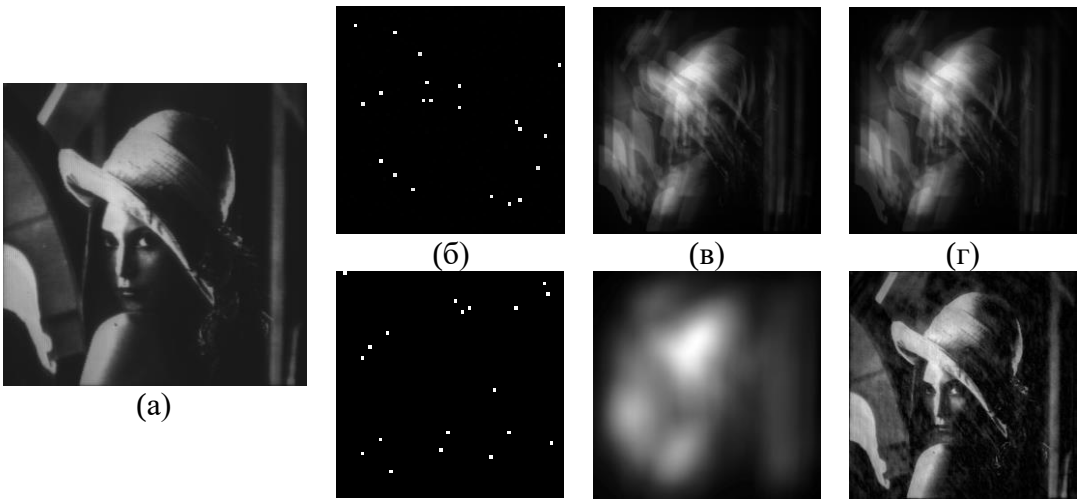


Рисунок 10 — Результаты оптического эксперимента по аппаратной реализации оптико-цифровой версии асимметричной криптографической схемы: кодируемое изображение (а), ключи кодирования (б, д), однократно (в) и двукратно (е) кодированные изображения, однократно (г) и двукратно (ж) декодированные изображения

Таким образом результаты оптических экспериментов подтвердили выводы, сделанные на основе численного моделирования, и демонстрируют эффективность и работоспособность разработанной асимметричной оптической криптографической схемы.

Основные выводы работы

Основные результаты работы можно сформулировать следующим образом:

1. Разработана и экспериментально апробирована многофакторная модель оптической криптографической схемы с пространственно-некогерентным освещением, позволяющая оценить влияние аппаратного комплекса и параметров используемых элементов на отношение сигнал/шум системы с точностью не хуже 70%.
2. Разработаны методы использования структурированных амплитудных масок в оптической криптографической системе с пространственно-некогерентным освещением для повышения качества декодированных изображений (разрежающие маски в виде решёток) и криптографической стойкости системы (взаимодополняющие случайные маски).

3. По результатам экспериментальной апробации получено, что: в численных экспериментах — применение разрежающей маски повышает значение отношения сигнал/шум (ОСШ) на 30-60%, использование взаимодополняющих случайных масок увеличивает криптографическую стойкость в 2-8 раз; в оптическом эксперименте — увеличивает криптографическую стойкость в 2,7 раза.

4. Разработан матричный контейнер цифровых данных (МКЦД), специализированный для задач оптического кодирования и обладающий широким диапазоном параметров: размер от 64 до 8192 отсчётов по одной стороне с произвольным соотношением сторон, максимальный процент корректируемых ошибок до 21,7%, до 8192 изображений может быть объединено в последовательность, содержащую один файл. МКЦД не чувствителен к локализации шумов и может быть окружён контуром произвольной формы.

5. Анализ устойчивости МКЦД к искажениям и его сравнение с QR-кодом показали, что экспериментальные значения уровня коррекции ошибок МКЦД лежат в диапазоне 0,5-16,3%, в то время как для QR-кода возможно единственное значение 0,7%; плотность записи данных на 15% превышает возможности QR-кода.

6. Предложены две реализации асимметричной оптической криптографической схемы с пространственно-некогерентным освещением. Двукратно оптическая реализация обладает максимальным быстродействием, но низким значением ОСШ декодированного изображения, гибридная оптико-цифровая — меньшим быстродействием, но значением ОСШ, сравнимым с симметричной системой.

7. Разработан метод аутентификации пользователей оптической криптографической схемы на основе расчёта хэш-сумм от фрагментов фурье-спектров кодированных изображений. Показано, что метод устраняет уязвимость разработанной асимметричной оптической криптографической

схемы к атакам типа «Man in the Middle» как в случае кодирования полутоновых изображений, так и при использовании МКЦД.

8. Численные и оптические эксперименты показали, что разработанная асимметричная оптическая криптографическая схема не уступает симметричной по качеству декодированных изображений, однако лишена уязвимости в виде необходимости предварительного обмена ключами кодирования.

Статьи в журналах, индексированных в базах данных WOS и SCOPUS и/или включённых в Перечень ВАК РФ

1. Cheremkhin P.A., Evtikhiev N.N., **Shifrina A.V.** et al. New customizable digital data container for optical cryptosystems // J. Opt., 2021. 23, № 11. P. 115701.
2. Cheremkhin P.A., Evtikhiev N.N., **Shifrina A.V.** et al Lensless optical encryption with speckle-noise suppression and QR codes // Appl. Opt., 2021. 60, № 24. P. 7336-7345
3. Evtikhiev N.N., Krasnov V.V., **Shifrina A.V.** et al. Multi-Factor Model of an Optical Encryption System with Spatially Incoherent Illumination // Optoelectron. Instrum. Data Process. Pleiades journals, 2020. 56, № 2. P. 176–182. (Евтихиев Н.Н., Краснов В.В., **Шифрина А.В.**, и др. Многофакторная модель системы оптического кодирования с пространственно-некогерентным освещением // Автометрия. 2020. 56, № 2. С. 84-91).
4. Cheremkhin P.A., Evtikhiev N.N., **Shifrina A.V.** et al. Asymmetric image optical encryption under spatially incoherent illumination // Laser Phys. Lett. Institute of Physics Publishing, 2020. 17, № 2. P. 025204.
5. Евтихиев Н.Н., Краснов В.В., **Шифрина А.В.**, и др. Применение дополнительных входных амплитудных масок в системах оптического кодирования с пространственно-некогерентным освещением // Компьютерная оптика. 2017. 41, № 3. С. 391–398.

Шифрина Анна Владимировна

Оптико-цифровые криптографические системы с использованием структурированных амплитудных масок и асимметричного кодирования.

Автореферат дис. на соискание учёной степени кандидата физико-математических наук

Подписано к печати _____ Заказ № _____

Формат 60×90/16. Усл. Печ. Л. 1. Тираж 100 экз.

Типография _____