МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

МЕТОДЫ ОПТИЧЕСКОГО ШИФРОВАНИЯ КОМПОЗИЦИИ ИЗОБРАЖЕНИЙ

Беркович Павел Александрович

Научный руководитель:
заведующий кафедры ММАД,
кандидат физико-математических наук
Бодягин Игорь Александрович

МИНСК 2022

РЭФЕРАТ

Дыпломная праца, 79 старонак, 7 табліц, 44 малюнка, 24 крыніцы, 3 дадатка.

Ключевые слова: ВІЗУАЛЬНАЯ КРЫПТАГРАФІЯ, ЭЛЕКТРОННЫ ЛІЧБАВЫ ПОДПІС, АПТЫЧНАЕ ШЫФРАВАННЕ, СІНУСОІДНАЕ КАДАВАНЬНЕ ПРЫВАТНАГА МУЛЬТЫПЛЕКСАВАННЯ, ШЫФРАВАННЕ З ПАДВОЙНАЙ ВЫЯВАЙ, РАСШЫФРОЎКА, КРЫПТАГРАФІЧНЫ АНАЛІЗ, АТАКА КЛЮЧА, АТАКА АКЛЮЗІІ, СКРАМБЛЯВАННЕ ПІКСЕЛЯЎ, ПЕРАЎТВАРЭННЕ ГІРАТАРА.

Аб'ект даследавання – схема шыфравання з падвойнай выявай.

Мэта працы – удасканаліць алгарытм гіраторнага пераўтварэння малюнкаў шляхам ужывання аперацый скрамблявання пікселяў паміж выявамі. Атрыманы ў выніку распрацоўкі новы метад шыфравання неабходна праверыць на бяспеку, а менавіта прааналізаваць яго ўстойлівасць да нападаў ключа, аклюзіі і шумавым абурэнням.

Вынікам з'яўляецца атрыманы алгарытм, а таксама яго крыптаграфічны аналіз.

Вобласцю прымянення з'яўляюцца ўсе сферы, якія прымяняюць у сваіх тэхналогіях візуальную крыптаграфію і аптычнае шыфраванне.

ABSTRACT

Diploma work, 79 pages, 7 tables, 44 drawings, 24 sources, 3 annexes.

Keywords: VISUAL CRYPTOGRAPHY, ELECTRONIC DIGITAL SIGNATURE, OPTICAL ENCRYPTION, SINUSOIDAL CODING OF PRIVATE MULTIPLEXING, DOUBLE-IMAGE ENCRYPTION, DECODING, CRYPTOGRAPHIC ANALYSIS, KEY ATTACK, OCCLUSION ATTACKS, BOMBING PIXELS, GYRO TRANSFORMATION.

The object of study is a double-image encryption scheme.

The purpose of the work is to improve the gyratory image transformation algorithm by applying pixel scrambling operations between images. The new encryption method obtained as a result of development needs to be checked for security, namely, to analyze its resistance to key attacks, occlusion, and noise disturbances.

The result is the resulting algorithm, as well as its cryptographic analysis.

The scope is all areas that use visual cryptography and optical encryption in their technologies.

РЕФЕРАТ

Дипломная работа, 79 страниц, 7 таблиц, 44 рисунка, 24 источника, 3 приложения.

Ключевые слова: ВИЗУАЛЬНАЯ КРИПТОГРАФИЯ, ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ, ОПТИЧЕСКОЕ ШИФРОВАНИЕ, СИНУСОИДАЛЬНОЕ КОДИРОВАНИЕ ЧАСТНОГО МУЛЬТИПЛЕКСИРОВАНИЯ, ШИФРОВАНИЕ С ДВОЙНЫМ ИЗОБРАЖЕНИЕМ, РАСШИФРОВКА, КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ, АТАКА КЛЮЧА, АТАКА ОККЛЮЗИИ, СКРЕМБЛИРОВАНИЕ ПИКСЕЛЕЙ, ПРЕОБРАЗОВАНИЕ ГИРАТОРА.

Объект исследования – схема шифрования с двойным изображением.

Цель работы – усовершенствовать алгоритм гираторного преобразования изображений путем применения операций скремблирования пикселей между изображениями. Полученный в результате разработки новый метод шифрования необходимо проверить на безопасность, а именно проанализировать его устойчивость к атакам ключа, окклюзии и шумовым возмущениям.

Результатом является полученный алгоритм, а также его криптографический анализ.

Областью применения являются все сферы, применяющие в своих технологиях визуальную криптографию и оптическое шифрование.

Введение

Благодаря бурному развитию сферы информационных технологий, в нашу жизнь вошли и стали уже привычными технологии, без которых современный мир трудно себе представить. Каждый день повсеместно совершаются миллионы самых разнообразных компьютерных операций. С активным развитием и распространением информационных технологий человечество столкнулось с одной из самых насущных на сегодняшний день проблемой – безопасностью хранения, передачи и получения информации в цифровом пространстве.

Существует множество самых различных технологий, которые стоят на страже безопасности совершаемых в сети операций. Например, в основе традиционных систем бумажного документооборота лежит принцип заверки документов подписью и печатью ответственного лица. Достоверность такого документа определяется визуально при его предъявлении. Степень защиты бумажных документов от различного рода угроз (подделка, дублирование и пр.) достаточна мала. В системах электронного документооборота для решения такого рода задач используются технологии Электронной Цифровой Подписи (ЭЦП).

Отдельно стоит вопрос зашифровки и передачи изображений. Эти возможности особенно важны для таких интернет-разработок, как социальные сети, фотостоки, электронная почта и т.д. Для осуществления операций шифрования изображений существует отдельная ветвь криптографии – визуальная криптография.

Визуальная криптография — это криптографический метод, который позволяет шифровать визуальную информацию (изображения, текст и т. д.) таким образом, чтобы расшифрованная информация отображалась как визуальное изображение, то есть использует характеристики человеческого зрения.

Благодаря визуальной криптографии, многие документы – паспорта, избирательные бюллетени, завещания, договора аренды – теперь могут существовать в электронной форме (это особенно важно в период пандемии),

а любая бумажная версия будет в этом случае только копией электронного оригинала.

В данной работе будут рассмотрены разнообразные схемы визуальной и оптической криптографии. Сначала будет рассмотрен предмет визуальной криптографии, ее достоинства и недостатки, а также будут разобраны примеры ее методов. Затем будут изучены алгоритмы оптического шифрования. Более подробно будет разобран принцип работы алгоритма шифрования нескольких изображений методом синусоидального кодирования частотного мультиплексирования. Данный метод будет проверен на криптостойкость, а именно будут проанализированы безопасность ключа и устойчивость к атакам окклюзии. Также будут проведены корреляционный анализ и анализ гистограммы.

Цель работы – усовершенствовать алгоритм путем применения операций скремблирования пикселей между изображениями и гираторного преобразования. Полученный в результате разработки новый метод шифрования необходимо проверить на безопасность, а именно проанализировать его устойчивость к атакам ключа, окклюзии и шумовым возмущениям.