ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2016» атты XI Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XI Международной научной конференции студентов и молодых ученых «НАУКА И ОБРАЗОВАНИЕ - 2016»

PROCEEDINGS of the XI International Scientific Conference for students and young scholars «SCIENCE AND EDUCATION - 2016»

2016 жыл 14 сәуір
Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2016» атты XI Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XI Международной научной конференции студентов и молодых ученых «Наука и образование - 2016»

PROCEEDINGS of the XI International Scientific Conference for students and young scholars «Science and education - 2016»

2016 жыл 14 сәуір

Астана

ӘӨЖ 001:37(063)
КБЖ 72:74
Ғ 96

Ғ96 «Ғылым және білім – 2016» атты студенттер мен жас ғалымдардың XI Халық. ғыл. конф. = XI Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2016» = The XI International Scientific Conference for students and young scholars «Science and education - 2016» . – Астана: http://www.enu.kz/ru/nauka/ nauka-i-obrazovanie/, 2016. – .... б. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-764-4

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

ӘОЖ 001:37(063)
КБЖ 72:74

ISBN 978-9965-31-764-4

©Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2016

УДК 004.056.5

ИССЛЕДОВАНИЕ АЛГОРИТМА ПОТОКОВОГО ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ КОДА, КОРРЕКТИРУЮЩЕГО ОШИБКИ

Акбалинов Алиби Кайратович
Магистрант 1-го курса факультета информационных технологий ЕНУ им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – Сатыбалдина Д.Ж.

Целью настоящей работы является реализация методов обеспечения конфиденциальности и целостности данных на основе совместного применения криптографических алгоритмов и помехоустойчивого кодирования. Разработано приложение «Кодирование и шифрование», реализующее последовательную систему из синхронного потового шифратора, сверточного кодера и декодера сверточных кодов. Для создания приложения использовалась технология визуального и объектно-ориентированного программирования на платформе .NET Framework (Microsoft Visual Studio Professional 2013). Исходный код написан на языке высокого уровня C#.

В качестве генератора гаммы в потоковой криптосистеме использован регистр сдвига с обратной связью [1]. Сдвиговые регистров используются также для реализации сверточного кодера [2] и многопорогового декодера двоичных и символьных данных [3, 4].

После запуска исполняемого файла появится главное окно приложения, представленное на рисунке 1.

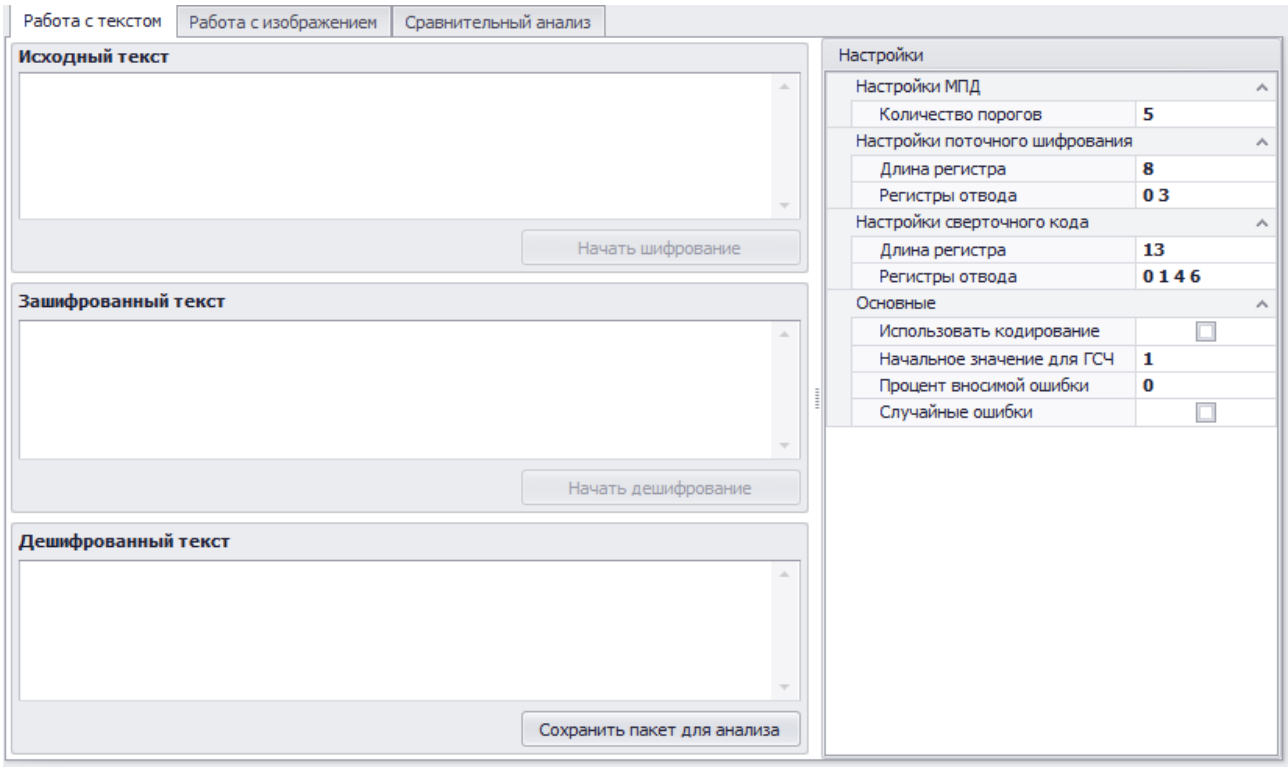

Рисунок 1 – Интерфейс приложения «Кодирование и шифрование».

Основные шаги при работе с приложением «Использование декодирования при шифровании данных»:

– выбирается вкладка соответствующая типу данных, которые будут шифроваться (текстовой блок или графический файл);

– настраиваются основные компоненты (использование кодирования или без кодирования, процент вносимой ошибки, случайные ошибки и т.д.); в случае, если

используется кодирование, то в качестве кодирующего алгоритма будет выступать сверточный кодер (ConvolutionEncoder), настройки для которого включает в себя длину регистра сдвига и точки съема); в качестве декодирующего алгоритма выступает многопороговый декодер (МПД), пример настройки всех компонентов показан на рисунке 2;

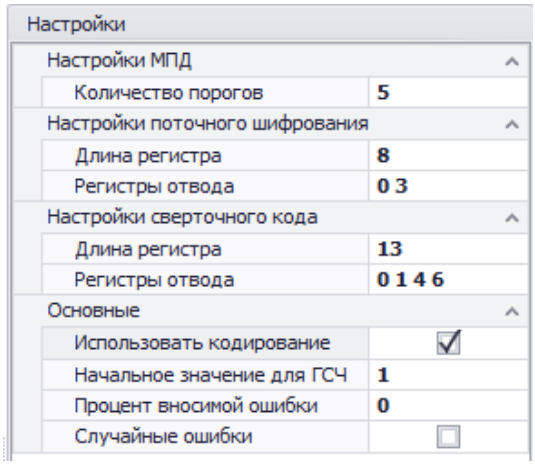

Рисунок 2 – Пример настройки кодера, декодера и шифратора.

– после выбора всех параметров кнопка «Начать шифрование» становится активной, после её нажатия данные переводятся в битовый формат, кодируются сверточным кодом (если было выбрано «Использовать кодирование») с заданными настройками; затем в полученное сообщение вносятся случайные ошибки, в соответствии с указанными настройками, производится зашифрование информации (см. рис. 3).

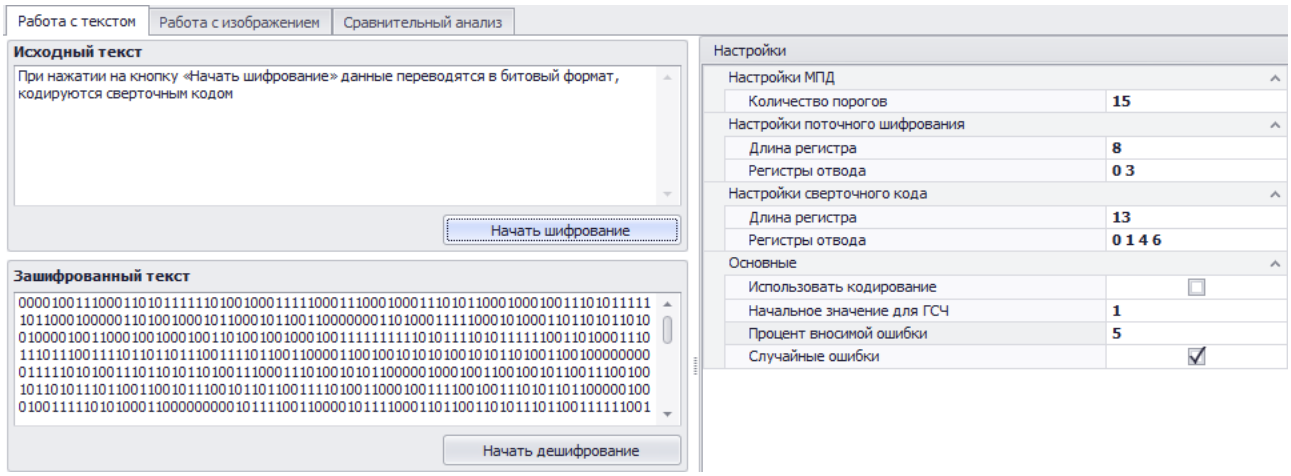

Рисунок 3 – Пример зашифрования текста без использования помехоустойчивого кодирования с внесенными случайными ошибками.

При нажатии кнопки «Начать дешифрование», битовая последовательность шифртекста (с внесенными ошибками в канале связи) гаммируется с битами гаммы потокового синхронного генератора. Видно, что без использования методов коррекции ошибок происходит расшифрование данных с ошибками (см. рис. 4).

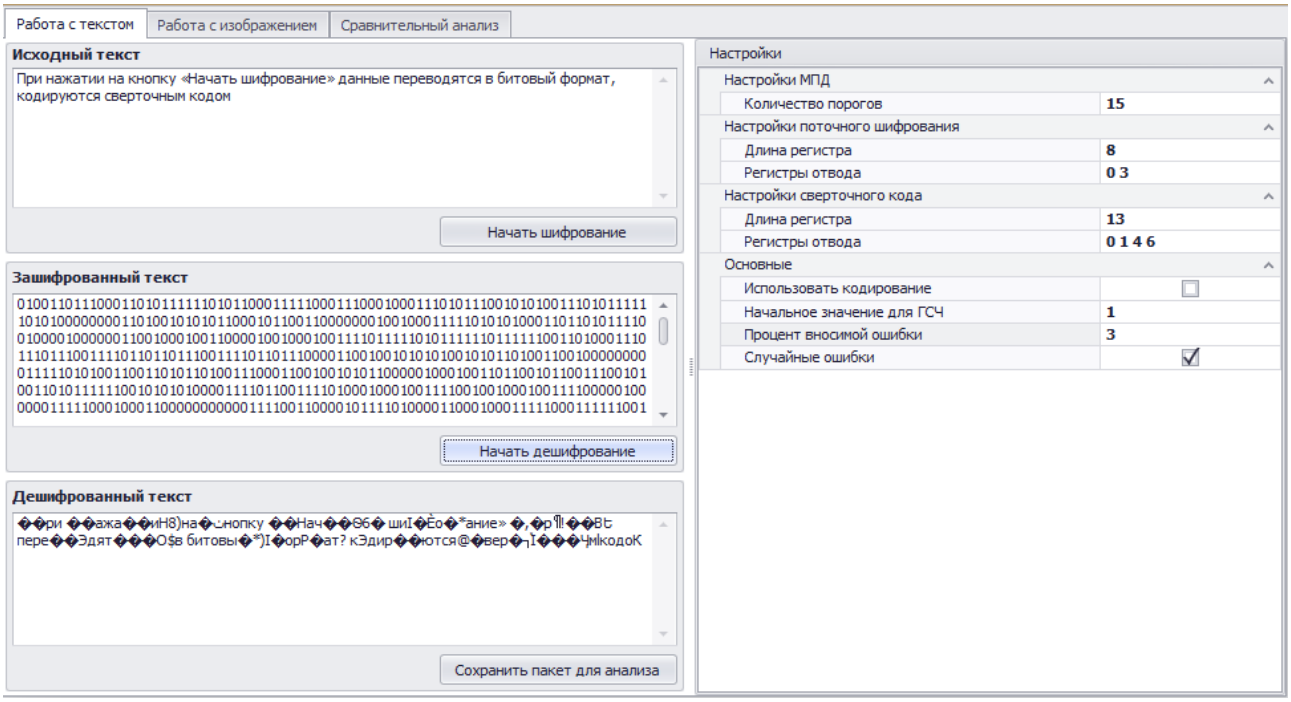

Рисунок 4 – Пример расшифрования текста без использования помехоустойчивого кодирования с 3% случайных ошибок

Аналогичный результат получен также при шифровании файла изображения: из рисунка 5 видно, что без использования кодирования и декодирования внесенные ошибки повлияли на качество изображения после расшифрования.

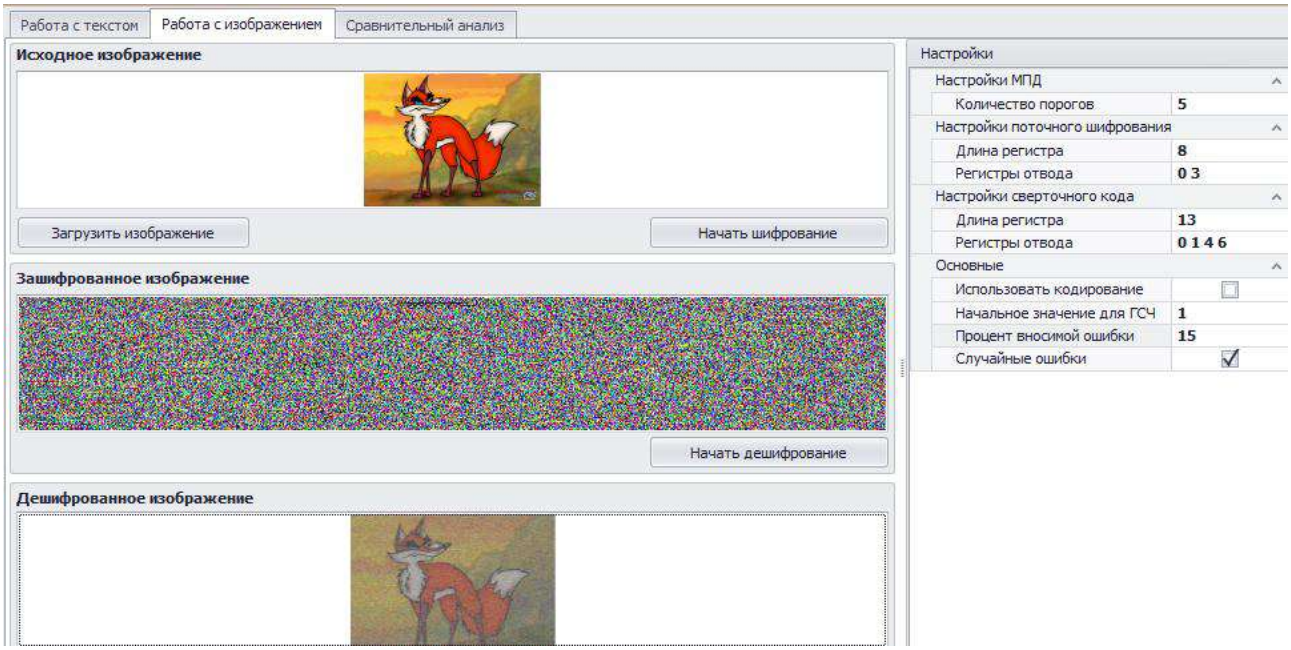

Рисунок 5 – Пример расшифрования графического файла без использования помехоустойчивого кодирования с 3% случайных ошибок

Результат эксперимента можно сохранить в пакет для более детального анализа. Пакет содержит всю информацию об исходном и полученном изображении или текста, что позволит оценить различия. Чтобы сохранить пакеты анализа, нужно нажать на кнопку «Сохранить пакет для анализа», которая станет активной после расшифрования данных (см. рисунок 6).

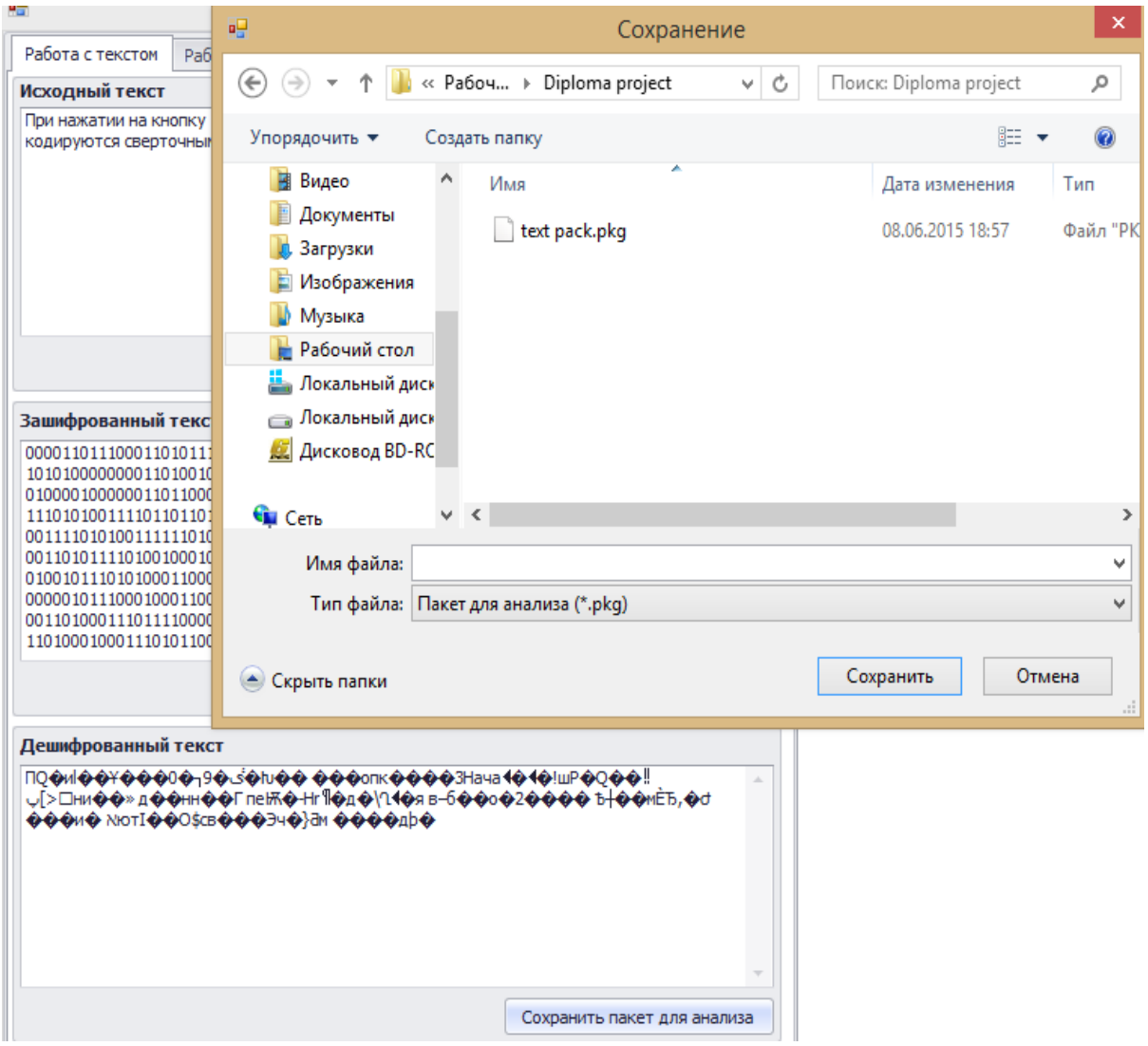

Рисунок 6 – Сохранение пакета для анализа текста

Загрузить сохраненные пакеты можно, выбрав вкладку «Сравнительный анализ» приложения «Кодирование и шифрование» (см. рисунок 1). При загрузке пакетов все количественные данные из пакетов автоматически встраиваются в общую таблицу (см. рис.6).

Таким образом, можно оценить при каких настройках результаты декодирования и соответственно восстановления данных наиболее эффективные.

Заключение. Разработанное приложение реализации комбинированной системы из синхронного шифратора, кодера и многопорогового декодера имеет следующие возможности:

– задание настроек потокового шифратора, сверточного кодера и многопорогового декодера (длина регистра сдвига, точки съема, начальное состояние регистра);

– использование мультимедийной информации для кодирования и шифрования;

– возможность повторного использования созданных схем;

– хранение и воспроизведение результатов работы схем для анализа эффективности;

– анализ и сравнение эффективности схем с предварительным кодированием и без кодирования, их скорости работы.

Научная новизна данного подхода заключается в том, что впервые в криптосистеме использован многопороговый декодер, обладающий высокой скоростью декодирования и

низкой сложности реализации на регистрах сдвига [3]. Многопороговый декодер одинаково быстро может производить действия, как над битовыми данными символами, так и над байтовыми символами [4]. Поэтому многопороговый декодер и системы защиты информации на его основе могут применяться в высокоскоростных системах передачи и хранения больших объемов информации.

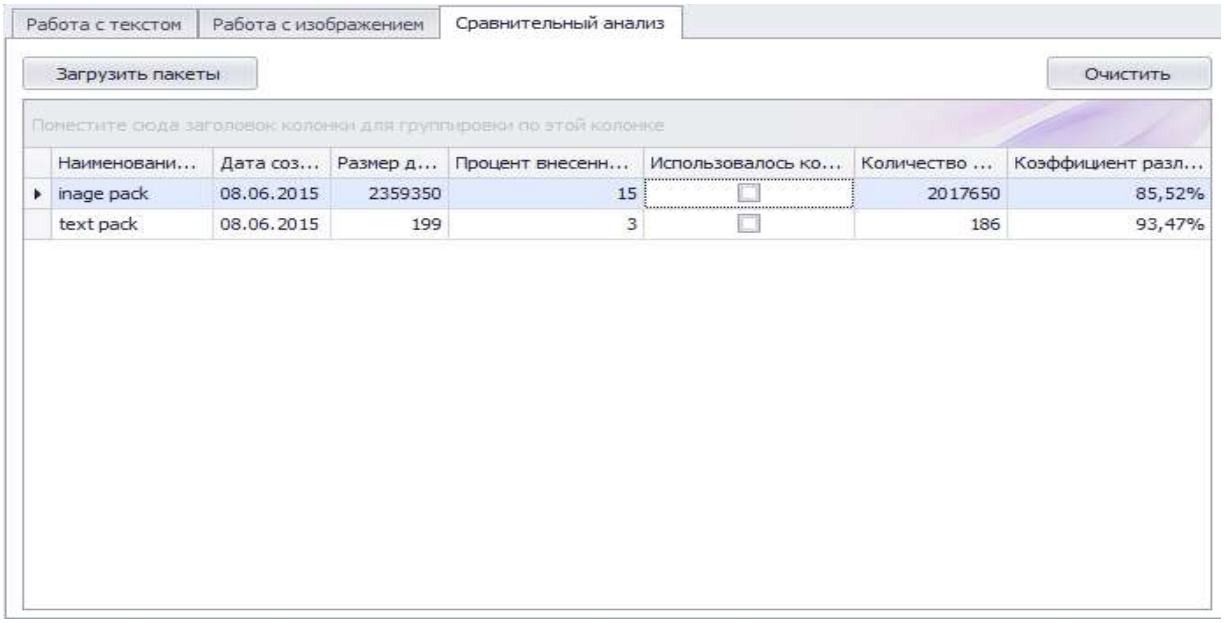

Рисунок 6 – Сравнительный анализ данных из пакетов
с указанием коэффициентов различия файлов до шифрования и после расшифрования.

Список использованных источников

1 Мао Венбо. Современная криптография: теория и практика/ Перевод с англ.- М.: Издательский дом «Вильямс», 2005 – 768 с.

2Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение.– М.: Техносфера.– 2005. – 320 стр.

3 Золотарёв В.В., Сатыбалдина Д.Ж., Ташатов Н.Н., Адамова А.Д. Оценка сложности реализации декодеров сверточных кодов // Вестник КазНТУ им. К. Сатпаева. – 2015. – №3. – С.361-368.

4 Zolotarev V., Ovechkin G., Satybaldina D., Tashatov N., Adamova A., Mishin V. Efficiency multithreshold decoders for self-orthogonal block codes for optical channels. // International Journal of Circuits, Systems and Signal Processing – 2014.- Volume 8. – Pp.487-495.

УДК 004.942

МЕТОДЫ КОМАНДНОЙ РАЗРАБОТКИ WEB ПРОЕКТОВ НА ПЛАТФОРМЕ TEAM FOUNDATION SERVER

Аманжолов Арнай Нурұлы
Магистрант кафедры «Вычислительная техника» факультета информационных технологий ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Джузбаева Б.Г.

Современные разработки программного продукта требуют участия в реализации проекта кроме профессионалов – программистов, но и менеджеров для работы с