УДК 004 DOI: 10.30748/soi.2017.148.21

И.И. Маракова, Л.А. Кузнецова, М.Д. Ташева

Одесский национальный политехнический университет, Одесса

ИССЛЕДОВАНИЕ МЕТОДОВ РЕВЕРСИВНЫХ ЦИФРОВЫХ ЗНАКОВ (ЦВЗ) ДЛЯ ВЕРИФИКАЦИИ МЕДИЦИНСКИХ ИЗОБРАЖЕНИЙ

Рассмотрен метод идентификации и верификации медицинских диагностических изображений, основанный на реверсивных ЦВЗ. Разработанный метод был реализован и протестирован с использованием реальных данных. На основании метода разработана система, реализующая преимущества описанного метода, и позволяющая проводить дальнейшие исследования с целью его дальнейшего развития и оптимизации.

Ключевые слова: *медицинская информация, цифровой водяной знак, стегосигнал, стегообраз, стегосообщение.*

Вступление

Конфиденциальность и целостность медицинской информации, как правило, регламентируется законодательными, как впрочем, и этическими нормами. В настоящее время темпы развития информационных технологий, медицинского диагностического оборудования явно опережают разработку соответствующих законодательных норм. Вышесказанное обусловило необходимость развития технологий защиты медицинской информации, представленной в цифровом виде.

После определения подоптимальной структуры системы, выработки требований к основным параметрам, обеспечивающих достижение заданных значений вероятностей ошибок детектирования ЦВЗ и надежности восприятия стегосигнала в условиях простейших преобразований стегосигнала, представляется возможным адаптировать систему относительно более сложных и характерных для конкретного практического применения преобразований стегосигнала в канале обработки и/или несанкционированного пользователя. Но даже для простейших преобразований стегосообщения необходимо с учетом отклонения от принципа Кергоффа с точки зрения теоретико-игрового подхода рассматривать различные режимы работы системы с ЦВЗ, динамику изменения показателей системы при достижении баланса между двумя сторонами (разработчик системы и несанкционированный пользователь), либо временного преимущества какой-либо из сторон [1]. Адаптации подоптимальных систем с ЦВЗ для практического использования в условиях более сложных преобразований канала обработки подразумевает коррекцию структуры системы или ее отдельных составляющих, изменение параметров, вероятностных мер ЦВЗ, позволяющих не снизить показатели системы, полученные при оценке в условиях простейших преобразований.

Цель статьи. Рассмотреть метод идентификации и верификации медицинских диагностических изображений, основанный на реверсивных ЦВЗ. Реализовать и протестировать метод с использованием реальных данных.

Основная часть

При решении задач верификации технологии ЦВЗ в отличие от решающих аналогичные задачи криптографических методов, а именно, формирования цифровая подпись (ЦП), не увеличивают размер сообщения, не могут быть просто отброшены без ухудшения надежности восприятия стегосообщения. С другой стороны, в качестве ЦВЗ можно использовать ЦП некоторого сообщения при выполнении требований по надежности восприятия стегосообщения и устойчивости к преобразованиям стегосигнала, определяемыми особенностями практического использования.

Основная проблема верификации на основе ЦП, заключающаяся в несанкционированном удалении ЦП, для ЦВЗ не актуальна. Однако возникает другая проблема: ЦВЗ должны быть инвертируемы, т.е. необходимо точное восстановление исходного основного покрывающего сообщения (ОПС) после детектирования.

При использовании технологий ЦВЗ для контроля над копированием, предотвращения несанкционированного копирования, мониторинга рекламного вещания и т.д. полагается, что некоторые изменения ОПС в результате погружения ЦВЗ являются допустимыми и на приемной части восстановление ОПС не требуется. Однако для подтверждения целостности, в частности, в медицинском менеджменте, криминалистике, требуется точное вос-

становление исходного ОПС. Например, если ОПС содержит N бит и после процедуры сжатия останется только L бит, то в N–L бит ОПС допустимо погружать ЦВЗ, которые будут утрачены при сжатии (полухрупкие системы с ЦВЗ). Практическое применение такого подхода ограничено [1].

Предлагается метод погружения реверсивных ЦВЗ для идентификации и верификации изображений в формате BMP, позволяющий восстановить исходное изображение с точностью до одного бита. При этом возможно погружать каждый бит идентификатора как в отдельно взятый пиксель, так и в группу пикселей. Предложенная система ЦВЗ несекретна, т.е. не требуется знание секретного ключа. Другими словами, в системе не реализуется принцип Керкгоффса [5]. При извлечении ЦВЗ не требуется знание исходного изображения, т.е. детектор ЦВЗ является неинформированным.

На основе данного метода была реализована программная версия системы верификации и идентификации медицинских изображений. Программа разработана на платформе Microsoft .NET. В программе реализовано внедрение в изображение его hash-значения SHA1. Система апробирована для базы данных изображений диагностики мозга. Для арифметического кодирования вектора R использовалась программа адаптивного арифметического кодирования.

С точки зрения надежности восприятия изображения с погруженным идентификатором рассматривались амплитуды преобразования уровней $A = 2, 4, 8$ и размеры групп $N = 4, 16, 64$.

Пропускная способность системы верификации и аутентификации зависит от значений параметров предварительного преобразования $L, L_1, L_2, A.N1, N2$, которые, в свою очередь, определяются гистограммой яркости изображения. Для светлых изображений верификация при обеспечении незаметности ЦВЗ возможна при $N = 64$, $A = 4$. Однако, для темных изображений верификация выполнима при $N \le 16$, $A \ge 6$ и для обеспечения незаметности ЦВЗ могут потребоваться дополнительные усилия.

Очевидна зависимость обеспечения незаметности ЦВЗ от параметра преобразования ЦВЗ A и размера матрицы N1N2. Для каждого изображения существует оптимальное соотношение данных параметров.

Разработанный в разделе метод верификации изображения может быть применен как в секретном режиме, т.е. при использовании секретного ключа и соответствующих криптографических алгоритмов, так и в открытом.

Однако, в ряде случаев вполне достаточным может быть проведение процедуры верификации без применения криптографических стандартов. Действительно, ранее указывалось, что после арифметического сжатия разница $\Delta L = L = L_1$ соответствует числу бит, которые могут быть использованы для записи идентификатора изображения, длина которого L_2. Если $L_2 < \Delta L$, то возникает возможность погружения дополнительной информации. Однако, для открытой системы верификации возможно использовать все $\Delta L = L = L_1$ для сокрытого хранения конфиденциальной медицинской информации.

Выводы

В результате работы было установлено: Для верификации изображений на основе погружения ЦВЗ, представляющего собой ЦП данного изображения, использование алгоритма погружения на основе модульного сложения позволяет выполнять восстановление ОПС после детектирования ЦВЗ, но приводит к ухудшению эффективности детектирования ЦВЗ. Полученные аналитические выражения оценки вероятности ошибочного декодирования одного бита ЦВЗ при использовании трех типов детекторов: ЛКД и предлагаемых адаптивных (ПД, МД) позволили формализовать процедуру оптимизации. Выявлено важное свойство модульного аддитивного погружения, заключающееся в том, что вероятность ошибки не является монотонной функцией интенсивности ЦВЗ и существует некоторое оптимальное значение параметра α, которому соответствует минимальное значение вероятности ошибки. Для всех типов детекторов ОПС в виде изображений с плоской гистограммой яркости не подлежат верификации без специальных мер предварительной обработки.

Важным выводом является то, что уже на этапе погружения ЦВЗ в виде ЦП представляется возможным оценить возможность верификации ОПС. Разработчик системы может изменять значение параметра α, реализацию ЦВЗ, изменять гистограмму ОПС, если это необходимо и возможно [5]. Однако данные преобразования ОПС должны быть обратимыми и известными на приемной части системы. Чтобы не передавать дополнительную информацию, возможно на приемной части использовать некоторую «кодовую книгу», задающую типы преобразований, значения параметров. При этом процедура верификации потребует проведения тестов до получения наилучшего результата.

Предложен метод идентификации и верификации медицинских диагностических изображений, основанный на реверсивных ЦВЗ. Параметры преобразования, такие как размер группы преобразования N и параметр преобразования A, могут быть адаптивно настроены, что позволяет обеспечить необходимый уровень гибкости для достижения

баланса между емкостью внедряемой в изображение информации и незаметностью внедрения. Метод был реализован и протестирован с использованием реальных данных. Результаты теста показывают, что он может быть использован в распределенной базе данных медицинских изображений, где критерии целостности изображений и незаметности водяного знака являются определяющими.

На основании метода разработана система, реализующая преимущества описанного метода, и позволяющая проводить дальнейшие исследования с целью его дальнейшего развития и оптимизации. Представляется интересным рассмотрение возможности реализации различных режимов секретности процедуры верификации изображения.

Полученные в данной работе результаты имеют практическое значение [3; 4]. Использование алгоритма погружения на основе модульного сложения позволяет выполнять восстановление ОПС после детектирования ЦВЗ, но приводит к ухудшению эффективности детектирования ЦВЗ. Посредством аналитических исследований теоретически обоснована и проверена экспериментально оптимизация системы верификации ОПС на основе модульного способа погружения ЦВЗ, представляющего собой ЦП ОПС. Важным выводом является то, что уже на этапе погружения ЦВЗ в виде ЦП представляется возможным оптимизировать верификацию конкретного ОПС, уменьшить вероятности ошибок детектирования ЦВЗ более чем на два порядка (оптимизация α, обратимые модификации гистограммы ОПС, выбор типа детектора). Выявлено важное свойство модульного аддитивного погружения, заключающееся в том, что вероятность ошибки не является монотонной функцией интенсивности ЦВЗ.

Предложен метод идентификации и верификации медицинских диагностических изображений, основанный на реверсивных ЦВЗ. Параметры преобразования, такие как размер группы преобразования N и параметр преобразования A, могут быть адаптивно настроены, что позволяет обеспечить необходимый уровень гибкости для достижения баланса между емкостью внедряемой в изображение информации и незаметностью внедрения. Метод был реализован и протестирован с использованием реальных данных. Результаты теста показывают, что он может быть использован в распределенной базе данных медицинских изображений, где критерии целостности изображений и незаметности водяного знака являются определяющими.

Рассмотрена возможность реализации секретного и открытого режимов верификации медицинских изображений.

Список литературы

*1. Blobel, B. (2006). Advanced and secure architectural * Encyclopedia of Healthcare Information Systems MEDICAL INFORMATION SCIENCE REFERENCE New York 2008. – 231 p.*

2. Idris F. Review of Image and Video Indexing Techniques / F. Idris, S. Panchanathan // Journal of Visual Communication and Image Representation, 1997. – v.8. – P .53-73.

3. Маракова І.І. Технологія цифрових водяних меток з головними покриваючими повідомленнями в нагляду бінарних зображень / І.І. Маракова // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: Науково-технічний збірник. – К.: НДЦ „Тезис" НТУУ „КПІ". – 2003. – Вип. 7. – С.5 3-58.

4. Moulin P., O'Sullivan. Information-theoretic Analysis of Watermarking // Proc. of the International Conference on Acoustic, Speech and Signal Processing. – 2000. – Vol. 6. – P. 3630-3633.

5. Маракова И.И. Синтез и исследование методов верификации объектов электронного документооборота / И.И. Маракова, Л.А. Кузнецова, А.А. Сыропятов // Захист інформації. – 2008 . – № 2. – С. 50-65.

Поступила в редколлегию 23.02.2017

Рецензент: д-р техн. наук проф. В.В. Скачков, Военная академия, Одесса.

ДОСЛІДЖЕННЯ МЕТОДІВ РЕВЕРСИВНИХ ЦИФРОВИХ ЗНАКІВ ДЛЯ ВЕРИФІКАЦІЇ МЕДИЧНИХ ЗОБРАЖЕНЬ

І.І. Маракова, Л.А. Кузнецова, М.Д. Ташева

В роботі розглянуто метод ідентифікації і верифікації медичних діагностичних зображень, заснований на реверсивних ЦВЗ. Розроблений метод був реалізований і протестований з використанням реальних даних.

***Ключові слова**: медична інформація, цифровий водяний знак, стегосигнал, стегообраз, стегоповідомлення.*

RESEARCH METHODS REVERSAL OF DIGITAL MARKS FOR VERIFICATION OF MEDICAL IMAGES

I. Maracova, L. Kuznecova, M. Tasheva

This paper focuses the method of authentication and verification of medical diagnostic images, based on reversible digital watermarking. A method was realized and tested with the use of the real data. Basis on the method is the system which worked out allowing to do further researches.

***Keywords**: Medical information, The digital water mark, steganographic signal, steganographic image, steganographic message.*