УДК [621.391 + 512.6] : 004.9

Новый метод внедрения водяного знака в аудиосигнал

А.А. Жарких, В.Ю. Пластунов
Судоводительский факультет МА МГТУ, кафедра радиотехники и радиотелекоммуникационных систем

Аннотация. Представлен новый метод внедрения водяного знака в аудиосигнал в виде аудиосигнала на основе преобразований конформной алгебры единичного круга. Рассматриваются результаты моделирования метода во временной области и дается оценка вычислительной сложности. Приведены интересные результаты внедрения и извлечения водяного знака с пренебрежимо малыми искажениями.

Abstract. This paper presents a novel method of an audio signal digital watermarking by an audio signal. The method is based on the conformal algebra transformations of a unit disk. The paper examines the results of modeling method in time domain and estimates computational complexity. Encouraging results have been presented showing digital watermark embedding and extraction with negligibly small distortions.

Ключевые слова: водяной знак, ЦВЗ, аудиосигнал, конформная алгебра
Key words: watermark, DWM, audio signal, conformal algebra

1. Введение

Цель работы – представление нового метода внедрения в аудиосигнал водяного знака в виде аудиосигнала. Методы защиты информации, при которых сам факт ее передачи скрывается, исследует отрасль знаний под названием "стеганография". Большинство методов в этой отрасли знаний основаны на внедрении передаваемого сообщения в некоторое другое сообщение, называемое контейнером. В работе (*Грибунин и др.*, 2002) выделяются 4 основных направления в стеганографии: внедрение сообщения с целью его скрытой передачи (covert communication), внедрение цифровых водяных знаков (watermarking), внедрение идентификационной информации (fingerprinting), внедрение заголовков (captioning). Если судить по объему существующих работ, самым главным направлением является внедрение цифровых водяных знаков (ЦВЗ). О качественно новом уровне разработок в области ЦВЗ в последние годы говорит созданный в 2006 году 15-тью крупнейшими компаниями альянс разработчиков методов ЦВЗ "Digital Watermarking Alliance" (http://www.digitalwatermarkingalliance.org).

В большинстве современных работ часто понятие "watermarking" (в него входят вопросы, связанные с авторскими правами и защитой контента) смешивается с понятием "fingerprinting" (внедрение идентификационной информации в мультимедийный контент, без рассмотрения вопросов, связанных с авторскими правами). Немного перефразировав определение из (*Cox et al.*, 2007), внедрение цифрового водяного знака можно определить как совокупность методов обработки сигналов для изменения (незаметного или заметного) объекта авторского права с целью внедрения информации об объекте авторского права.

ЦВЗ широко применяется для различных задач:

- для мониторинга ТВ/радио/интернет вещания (управление правами на вещание, обнаружение "воровства" сигнала, подтверждение присутствия в программе спонсированного контента);
- для идентификации и отслеживания источника утечки копии пререлизного контента;
- для борьбы с распространением экранных копий видеофильмов, например, при помощи принудительного внедрения идентификационного номера в видео и аудио ряды;
- для улучшения взаимодействия систем (устройств) управления, создания и распространения (фильтрации и классификации) различного мультимедийного контента (фотографий, аудиосигналов, видеоизображений и т.д.), например, в сетях P2P.

Все методы внедрения ЦВЗ можно разделить по методу внедрения на 6 основных групп (*Cvejic*, 2004):

- методы внедрения информации в наименее значимые биты;
- методы внедрения информации в фазу сигнала;
- методы с использованием сигнала-эхо;
- методы с прямым расширением спектра;
- "лоскутные" (статистические) методы;
- методы, ориентированные на характеристики сигнала-контента или контент-адаптивные методы.

Более детально ознакомиться с каждой группой методов можно в монографии (*Cvejic, Seppänen*, 2007). Предлагаемый же в данной работе метод мы бы отнесли к контент-адаптивной группе методов.

В работах (*Жарких*, 1999a; 1999b; 2001) анонсировалась возможность использования алгебры преобразований единичного круга (*Лаврентьев, Шабат*, 1987) в задачах защиты информации. Как показали теоретические расчеты и программная реализация, алгебраические операции алгебры преобразований единичного круга могут быть использованы для защиты аудиосигналов (*Жарких*, 2003; 2005a; 2005c; *Zharkikh, Plastunov*, 2008).

В (*Жарких*, 2005b) показано, что математические операции, используемые в (*Жарких*, 2003; 2005a; 2005c) и настоящей работе, являются следствием ограничения преобразований единичного круга до преобразований интервала (-1;1) вещественной оси. Сумма двух чисел из интервала (-1;1) определяется выражениями (1) и (2). Произведение вещественного числа из интервала от минус бесконечности до плюс бесконечности на число из интервала (-1;1) со значениями в интервале (-1;1) определяется выражениями (3) и (4). Произведение, определенное выражениями (3) и (4), в общем случае нелинейно по обоим аргументам. Для натуральных значений r выражение (4) может быть получено путем применения к выражению (2) метода математической индукции. Для целых, рациональных и вещественных значений r выражение (4) обобщается тривиально.

$$\oplus : (-1;1)^2 \Rightarrow (-1;1), \tag{1}$$

$$\forall X, Y \in (-1;1)\ \ Z = X \oplus Y = \frac{X+Y}{1+XY} \in (-1;1), \tag{2}$$

$$\otimes : (-1;1) \times (-\infty;+\infty) \Rightarrow (-1;1), \tag{3}$$

$$\begin{gathered} \forall X \in (-1;1) \,\&\, \forall r \in (-\infty;+\infty) \\ Z = X \otimes r = \frac{(1+X)^r - (1-X)^r}{(1+X)^r + (1-X)^r} \in (-1;1). \end{gathered} \tag{4}$$

В (*Zharkikh, Plastunov*, 2008) были рассмотрены методы внедрения аудиосигнала в аудиосигнал в контексте общего подхода к задачам стеганографии. В данной работе мы адаптируем один из методов работы (*Zharkikh, Plastunov*, 2008) для задач внедрения в аудиосигнал водяного знака в виде аудиосигнала.

Перечислим характерные требования к методам внедрения цифрового водяного знака в контент (*Грибунин и др.*, 2002):

- необходимо обеспечить минимально низкую вероятность ложного обнаружения водяного знака в контенте (при ложном обнаружении ЦВЗ может возникнуть отказ к воспроизведению контента, не содержащего ЦВЗ);
- метод должен обеспечивать внедрение водяного знака заданного размера;
- метод должен реализовываться минимально возможным числом операций;
- извлечение водяного знака должно быть максимально простым и быстрым для авторизированного пользователя;
- метод должен обеспечивать заданную стойкость к преднамеренным и случайным воздействиям на сигнал с внедренным ЦВЗ;
- возможность добавления или изменения ЦВЗ в контенте с уже внедренным водяным знаком.

В (*Жарких*, 2003; 2005a) был предложен метод стеганографии, который обладал следующей особенностью: для извлечения сообщения на приемной стороне необходимо было наличие пустого контейнера.

Метод из (*Zharkikh, Plastunov*, 2008), в отличие от метода из (*Жарких*, 2003; 2005a), позволяет решить задачу внедрения цифрового водяного знака, так как в (*Zharkikh, Plastunov*, 2008) нет необходимости использования пустого контейнера на приемной стороне. Требование наличия пустого контейнера (контента), делает бессмысленным внедрение цифрового водяного знака – контент уже присутствует на приемной стороне.

2. Одноканальный метод

Напомним кратко метод стеганографии, предложенный в (*Жарких*, 2003; 2005a).

Обозначим через $X_C(t)$ и $X_M(t)$ сообщение-контейнер и внедряемое сообщение соответственно. Здесь, традиционно, через t обозначается время.

Определим алгоритм формирования заполненного контейнера следующим выражением:

$$S(\alpha, m, t) = X_C(t) \oplus \left(X_M\left(\frac{t}{m}\right) \otimes \alpha \right), \tag{5}$$

где α – это параметр преднамеренного ослабления, m – параметр преднамеренного растяжения сигнала во времени.

Заполненный контейнер передается через канал, в котором могут появиться ошибки $N_{CH}(t)$. После прохождения через канал аудиосигнал с внедренным ЦВЗ преобразуется следующим образом:

$$U_C(\alpha,m,t) = S(\alpha,m,t) * N_{CH}(t), \tag{6}$$

где * – операция взаимодействия сообщения и помехи в канале передачи.

Мы не моделируем изменение заполненного контейнера в канале передачи. Мы отражаем только тот факт, что ошибки существуют, но являются достаточно малыми.

Алгоритм выделения скрытого сообщения из заполненного контейнера можно представить следующими формулами

$$D_1(t) = U_C(\alpha,m,t) \oplus \left(X_C(t) \otimes (-1)\right), \tag{7}$$

$$D_2(t) = D_1(t) \otimes \frac{1}{\alpha}, \tag{8}$$

$$D(\alpha,m,t) = D_2(mt). \tag{9}$$

В случае малости канальных ошибок $D(\alpha,m,t)$ практически совпадает с $X_M(t)$. Если канальные ошибки не являются малыми, то выражение (9) должно быть изменено с учетом возможной компенсации этих ошибок. Упрощенные структурные схемы преобразований одноканального алгоритма представлены на рис. 1 и 2. Во всех приведенных схемах 1) и 2) обозначают входы для уменьшаемого и вычитаемого, 3) и 4) обозначают входы для основания и показателя степени, 5) и 6) обозначают входы для числителя и знаменателя, соответственно.

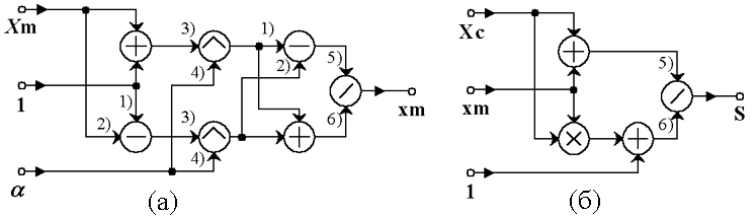

Рис. 1. Нелинейное ослабление сообщения (а) и внедрение сообщения в контейнер (б)

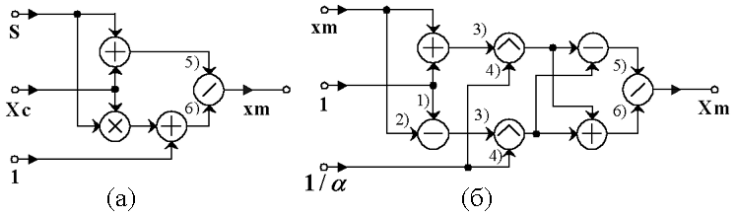

Рис. 2. Извлечение ослабленного сообщения из контейнера (а) и нелинейное усиление ослабленного сообщения (б)

3. Двуканальный метод

Для двухканального метода через $X_C(t)$ и $X_M(t)$ обозначены защищаемый аудиосигнал (контент) и внедряемый аудиосигнал (ЦВЗ), соответственно. Организуется два канала: канал суммирования (10) и канал вычитания (11).

$$S^{(+)}(\alpha,m,t) = X_C(t) \oplus \left(X_M\left(\frac{t}{m}\right) \otimes (+\alpha) \right), \tag{10}$$

$$S^{(-)}(\alpha,m,t) = X_C(t) \oplus \left(X_M\left(\frac{t}{m}\right) \otimes (-\alpha) \right). \tag{11}$$

Здесь $S^{(+)}(\alpha,m,t)$ – суммарный аудиосигнал с ЦВЗ, $S^{(-)}(\alpha,m,t)$ – разностный аудиосигнал с ЦВЗ. Физически эти каналы могут быть организованы различными способами. Важно лишь то, что значение исходного аудиосигнала входит в них идентичным образом с точностью до знака. После прохождения канала связи каналы аудиосигнала с ЦВЗ преобразуются следующим образом:

$$U_C^{(+)}(\alpha,m,t) = S^{(+)}(\alpha,m,t) * N_{CH}^{(+)}(t), \tag{12}$$

$$U_C^{(-)}(\alpha,m,t) = S^{(-)}(\alpha,m,t) * N_{CH}^{(-)}(t), \tag{13}$$

где $N^{(+)}{}_{CH}(t)$ и $N^{(-)}{}_{CH}(t)$ – помехи при передаче по суммарному и разностному каналам, соответственно, * – операция взаимодействия помех и сигнала в канале передачи. Как и ранее, считаем ошибки достаточно малыми. Алгоритм извлечения контента и ЦВЗ из суммарного и разностного сигналов описывается следующими формулами:

$$R_1(t) = U_C^{(+)}(\alpha, m, t) \oplus \left(U_C^{(-)}(\alpha, m, t) \otimes (-1)\right), \tag{14}$$

$$R_2(t) = R_1(t) \otimes \frac{1}{2\alpha}, \tag{15}$$

$$R(\alpha, m, t) = R_2(mt), \tag{16}$$

$$Q_1(t) = U_c^{(+)}(\alpha, m, t) \oplus U_c^{(+)}(\alpha, m, t), \tag{17}$$

$$Q_2(t) = Q_1(t) \otimes \frac{1}{2}, \tag{18}$$

$$Q(\alpha, m, t) = Q_2(t). \tag{19}$$

В отсутствие ошибок канала передачи $R(\alpha,m,t)$ практически совпадает с $X_M(t)$, а $Q(\alpha,m,t)$ совпадает с $X_C(t)$. Если ошибки не малы и необходимо их компенсировать, то в метод может вводиться растяжение. Упрощенные структурные схемы внедрения ЦВЗ в два канала аудиосигнала и извлечения ослабленного ЦВЗ и усиленного контента 2-канального алгоритма представлены на рис. 3. Если на второй вход схемы, представленной на рис. 3б, подается разностный сигнал с ЦВЗ (-S2), то на выходе схемы появляется ослабленный сигнал ЦВЗ. В случае же если на второй вход схемы, представленной на рис. 3б, подается суммарный сигнал (S2), то на выходе схемы появляется усиленный сигнал контента. Операции нелинейного ослабления и усиления сообщения в одно- и двуканальном методах выполняются по идентичным схемам (рис. 1а и 2б, соответственно).

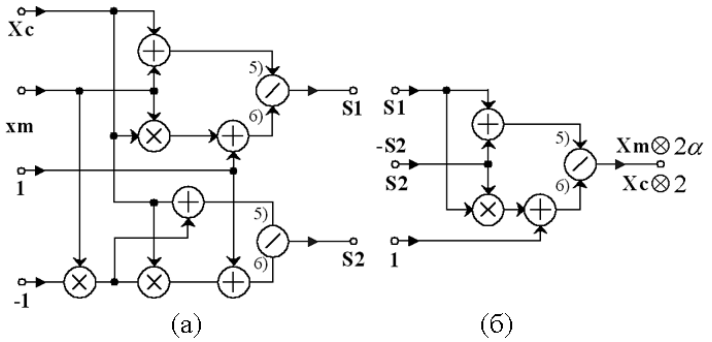

Рис. 3. Формирование суммарного и разностного сигналов на основе сигнала контента и ослабленного ЦВЗ (а) и извлечение усиленного контента и ослабленного ЦВЗ из суммарного и разностного сигналов (б)

4. Результаты моделирования

Для практического использования приведенного метода необходимо согласованно выбирать сигналы контента, ЦВЗ, и параметр α. Задача такого согласования и выбора является очень сложной и требует дальнейшего исследования. Тем не менее, для заданного класса сигналов можно использовать сигнал ЦВЗ и параметр α, найденные методом простого подбора. При фиксированных сигналах контента и ЦВЗ формируемые сигналы на передающей и приемной стороне существенно зависят от параметра α. Для практики важны такие значения параметра α, при которых сигнал ЦВЗ хорошо прячется, извлекается, внедрение ЦВЗ происходит без искажения сигнала контента. Если параметр α выбран относительно малым, то сигнал ЦВЗ хорошо скрывается, не искажает сигнала контента, но извлекается с артефактами. Если параметр α выбран относительно большим, то сигнал ЦВЗ плохо скрывается в контенте, искажает сигнал контента, но извлекается с высоким качеством и без артефактов. Таким образом, выбор значений параметра α ограничен как сверху, так и снизу требованиями к реальным системам внедрения ЦВЗ.

Параметр α, отвечающий за ослабление внедряемого ЦВЗ, не должен превышать единицу. В случае α=1 сигнал ЦВЗ остается неизменным, а если α>1, то происходит нелинейное усиление сигнала ЦВЗ: низкие по уровню отсчеты изменяются пропорционально α, а отсчеты ЦВЗ, близкие по уровню к 1, приближаются к 1 еще больше. Поэтому параметр α необходимо выбирать в интервале от 0 до 1.

Если параметр α выбран оптимальным образом, то сигнал ЦВЗ хорошо прячется, т.е. в суммарном и разностном сигналах его невозможно обнаружить путем прослушивания или измерения. Это также означает, что суммарный и разностный сигналы практически совпадают с исходным сигналом контента, т.е. внедрение ЦВЗ не искажает сигнала контента, и этом случае сигнал ЦВЗ также будет извлекаться с хорошим качеством. Для фиксированных сигналов контента и ЦВЗ всегда можно указать некоторый интервал оптимальных значений параметра α.

Для примера приведем некоторые графики временных представлений сигналов, полученных в результате моделирования алгоритмов внедрения и извлечения. На всех графиках по оси абсцисс отложено время t в миллисекундах, по оси ординат L – нормированные на единицу значения отсчетов сигналов из wav-файлов.

В качестве аудиосигнала контента был выбран музыкальный фрагмент (рис. 4), а в качестве аудиосигнала ЦВЗ – фрагмент фонемы речи (рис. 5а). Для данных фрагментов оптимальными являются значения параметра α в диапазоне от 0.01 до 0.04. При указанных значениях параметра α суммарный и разностный сигналы практически совпадают с исходным сигналом контента (рис. 4), а извлеченный ЦВЗ – с исходным сигналом ЦВЗ (рис. 5а). На рисунках 5б, 6а, 6б показаны временные представления сигналов для случаев неоптимального выбора параметра α. На рис. 5б представлен извлеченный сигнал ЦВЗ при α равном 0.0001. На рисунке видно, что при данном значении параметра α, извлеченный сигнал ЦВЗ сильно отличается от исходного (рис. 5а), тогда как суммарный и разностный сигналы практически совпадают с исходным сигналом контента (рис. 4).

На рис. 6а и 6б представлены соответственно суммарный и разностный сигналы при $\alpha = 0.9$. Из рисунков видно, что суммарный и разностный сигналы существенно отличаются как между собой, так и от сигнала контента. При параметре α, равном 0.9, сигнал ЦВЗ извлекается с высоким качеством и практически совпадает с исходным сигналом ЦВЗ (рис. 5а). Если параметр α выбран оптимально, то в качестве сигнала принятого контента можно использовать либо суммарный, либо разностный сигналы.

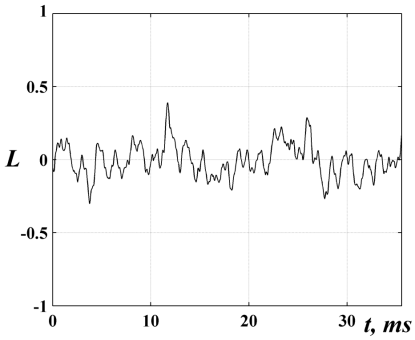

Рис. 4. Временное представление защищаемого сигнала (контента)

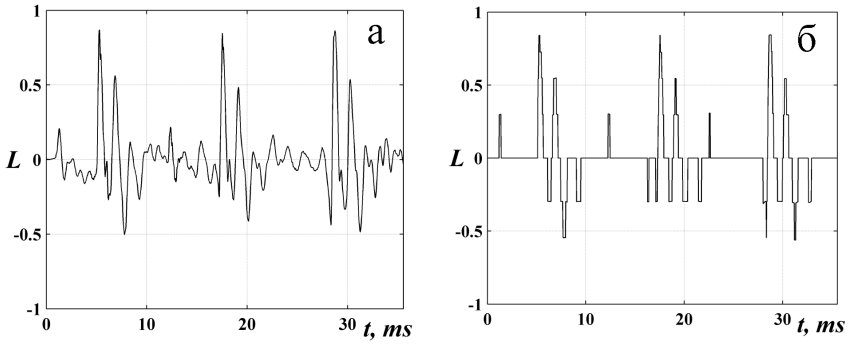

Рис. 5. Временные представления исходного сигнала ЦВЗ (а) и сигнала ЦВЗ, извлеченного из сигнала контента при $\alpha = 0.0001$ (б)

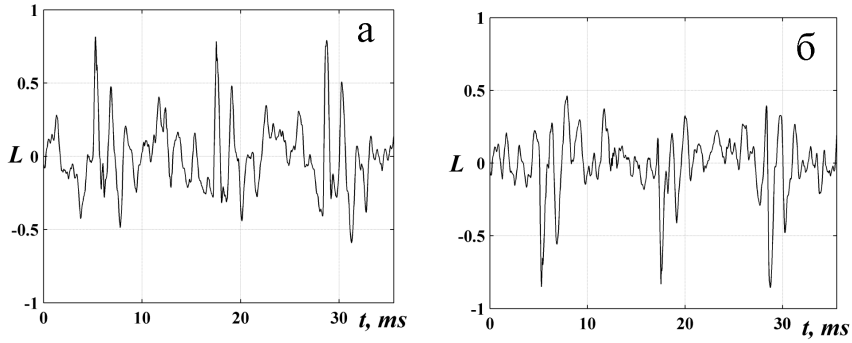

Рис. 6. Временное представление суммарного (а) и разностного (б) сигналов при $\alpha = 0.9$

5. Оценка вычислительной сложности метода

Произведем анализ количества операций, необходимого для внедрения ЦВЗ в контент и выделения ЦВЗ из контента при цифровой реализации метода.

Внедрение ЦВЗ в контент и последующее его извлечение может быть реализовано как цифровыми, так и аналоговыми устройствами, но при любой реализации вычислительная сложность указанных алгоритмов зависит линейным образом от временной длительности сигнала. Оценим, какое число операций требуется при цифровой реализации алгоритма.

Предположим, для упрощения анализа, что N – это количество отсчетов как контента, так и ЦВЗ. Формулы (1-19) показывают, что для ослабления ЦВЗ требуется произвести $7N$ операций, для внедрения ЦВЗ – $8N$, извлечения ЦВЗ – $4N$, усиления ЦВЗ – $7N$, извлечения контента $4N$, ослабления контента – $7N$. Итого на передающей стороне необходимо произвести $15N$ операций, а на приемной – $22N$. Все операции производятся в вещественной арифметике с неустранимыми ошибками округления.

Рассмотренные в данной работе алгоритмы были использованы в работе (*Zharkikh, Plastunov*, 2008) не для внедрения ЦВЗ, а для сокрытия полезного сообщения в контенте, т.е. для задач скрытой передачи сообщения. Так как в случае задачи из работы (*Zharkikh, Plastunov*, 2008) содержание самого контента не несет информационной нагрузки для получателя, то количество операций на приемной стороне оказывается меньшим, чем в случае задачи внедрения ЦВЗ. В методе для скрытой передачи сообщения (*Zharkikh, Plastunov*, 2008) для ослабления сообщения требуется произвести 7*N* операций, для внедрения сообщения в контейнер 8*N* операций. На приемной стороне для извлечения сообщения требуется 4*N* операций, для усиления извлеченного сообщения 7*N*. Таким образом, на передающей стороне в методе работы (*Zharkikh, Plastunov*, 2008) и методе данной работы число операций одинаково, а на приемной стороне число требуемых операций в данном методе возрастает в два раза.

6. Заключение

Предлагаемый метод внедрения в аудиосигнал цифрового водяного знака в виде аудиосигнала принципиально отличается от методов стеганографии, рассмотренных в (*Грибунин и др.*, 2002). Данный метод является еще одним подтверждением возможности использования алгебры конформных преобразований единичного круга (*Лаврентьев, Шабат*, 1987) для защиты аналоговых сообщений и их цифровых отсчетов. В качестве вопросов, требующих дополнительного исследования, мы бы назвали исследование устойчивости метода к различным видам помех и преднамеренных искажений. Многочисленные результаты моделирования метода, результаты графической и звуковой интерпретаций метода показали его работоспособность и эффективность.

Литература

Cox I.J., Miller M., Bloom J., Fridrich J., Kalker T. Digital watermarking and steganography. *Morgan Kaufmann*, 593 p., 2007.

Cvejic N. Algorithms for audio watermarking and steganography. *Academic dissertation, Department of Electrical and Information Engineering, Information Processing Laboratory, University of Oulu*, 111 p., 2004.

Cvejic N., Seppänen T. Digital audio watermarking techniques and technologies: Applications and benchmark. *Idea Group Inc*, 328 p., 2007.

Zharkikh A., Plastunov V. New steganography technique, based on the Lorentz's transformation, of embedding audiosignal into audiosignal. *In proceedings: PRIA-9-2008 9th International conference on pattern recognition and image analysis: New information technologies. Nizhny Novgorod*, v.2, p.359-362, 2008.

Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. Аспекты защиты. *М., Солон-Пресс*, 261 с., 2002.

Жарких А.А. Аналоговый метод стеганографии звукового сигнала в звуковом сигнале. *Сборник докладов XI Междунар. научно-техн. конференции "Радиолокация, навигация, связь", Воронеж, ВГУ*, т.2, с.624-639, 2005a.

Жарких А.А. Идентификация линейных стационарных систем при гомоморфных отображениях сигналов. *Труды IV Междунар. конференции "Идентификация систем и задачи управления" SICPRO'05. Институт проблем управления им. В.А. Трапезникова РАН. М., Институт проблем управления им. В.А. Трапезникова РАН*, с.321-332, 2005b.

Жарких А.А. Конформная стеганография звукового сигнала в звуковом сигнале. *Сборник докладов XI Всеросс. конференции "Математические методы распознавания образов", М., ВЦ РАН*, с.305-307, 2003.

Жарких А.А. Конформное гаммирование звукового сигнала хаотическим сигналом. *Труды российского НТО РЭС им. А.С. Попова: LX сессия, посвященная Дню Радио. М., Радиотехника*, т.LX-1, с.146-147, 2005c.

Жарких А.А. Конформное преобразование формы сигнала для защиты аналоговых сообщений. *Сборник тезисов и докладов Междунар. научно-техн. конференции КГТУ. Калининград, КГТУ*, ч. 4, с.123, 1999a.

Жарких А.А. Проблемы криптоанализа как проблемы распознавания образов. *Сборник докладов X Всеросс. конференции "Математические методы распознавания образов", М., ВЦ РАН*, с.209-212, 2001.

Жарких А.А. Система шифрования с бегущим ключом. *Тезисы докладов V Междунар. конференции "Радиолокация, навигация, связь". Воронеж, ВГУ – ВНИИС*, т.3, с.1886-1894, 1999b.

Лаврентьев М.А., Шабат Б.В. Методы теории функций комплексного переменного. *М., Наука*, 688 с., 1987.