УДК 004.056

А.А. Смирнов[1], Е.В. Мелешко[1], А.А. Кузнецов[2]

[1] *Кировоградский национальный технический университет, Кировоград*
[2] *Институт информационных технологий, Харьков*

АППАРАТНАЯ РЕАЛИЗАЦИЯ УСТРОЙСТВ СТЕГАНОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ АДАПТИВНО ФОРМИРУЕМЫХ ДИСКРЕТНЫХ СИГНАЛОВ

Предложена структурная схема аппаратной реализации усовершенствованного устройства встраивания и извлечения данных из пространственной области изображений с использованием адаптивно формируемых дискретных сигналов для стеганографической защиты информации.

Ключевые слова: *стеганография, расширение спектра, адаптивно формируемые дискретные сигналы*

1. Постановка проблемы в общем виде и анализ литературы

На сегодняшний день одним из перспективных направлений защиты информации является стеганография [1 – 10]. Среди широкого спектра стеганографических средств защиты информации, в последнее время динамично развиваются методы с использованием технологии прямого расширения спектра.

В результате проведенных исследований показано, что применение сложных дискретных сигналов для построения стеганографических систем защиты информации позволяет на основе использования технологии прямого расширения спектра скрытно встраивать информацию в используемые цифровые контейнеры, например, цифровые изображения [1 – 8]. При этом обеспечивается достижение высоких показателей безопасности стеганосистем, связанных с реализацией всех преимуществ широкополосных помехозащищенных систем цифровой скрытной связи. В тоже время, в ходе исследований установлено, что для повышения пропускной способности организуемых стеганоканалов необходимо использовать большие ансамбли дискретных последовательностей, а для обеспечения устойчивости стеганосистемы к аффинным атакам используемые дискретные последовательности должны обладать улучшенными (особыми) корреляционными свойствами [4-8]. Кроме того, при формировании дискретных последовательностей необходимо учитывать статистические свойства используемых контейнеров. В этом случае будет обеспечена высокая достоверность извлекаемых на приемной стороне сообщений при низкой величине вносимых искажений в цифровые контейнеры [4-8].

Малоизученным направлением стеганографии с использованием сложных дискретных сигналов и технологии прямого расширения спектра является реализация алгоритмов аппаратными средствами.

2. Описание известного устройства встраивания данных в пространственной области изображений с использованием адаптивно формируемых дискретных сигналов

Известно устройство для реализации стеганографического встраивания данных в пространственной области изображений, с использованием прямого расширения спектра, которое содержит: пять входов, выход, блок ввода информационных данных, блок ввода ключей шифрования, блок ввода ключей формирования псевдослучайных последовательностей, блок ввода ключей перемежения, блок ввода контейнеров, блок шифрования, блок помехоустойчивого кодирования, генератор псевдослучайных последовательностей, модулятор, блок перемежения, блок добавления, блок квантования, блок формирования и вывода стеганограммы [9, 10].

Первый вход устройства соединен с входом блока ввода информационных данных, выход которого соединен с первым входом блока шифрования. Второй вход устройства соединен с входом блока ввода ключей шифрования, выход которого соединен со вторым входом блока шифрования. Выход блока шифрования соединен с входом блока помехоустойчивого кодирования, выход которого соединен с первым входом модулятора. Третий вход устройства соединен с входом блока ввода ключей формирования псевдослучайных последовательностей, выход которого соединен с входом генератора псевдослучайных последовательностей. Выход генератора псевдослучайных последовательностей соединен со вторым входом модулятора, выход которого соединен с первым входом блока перемежения. Четвертый вход устройства соединен с входом блока ввода ключей перемежения, выход которого соединен со вторым входом блока перемежения. Выход блока перемежения соединен с первым вхо-

дом блока добавления. Пятый вход устройства соединен со входом блока ввода контейнеров, выход которого соединен с блоком добавления. Выход блока добавления соединен с входом блока квантования. Выход блока квантования соединен с входом блока формирования и вывода стеганограммы, выход которого соединен с выходом устройства.

Работа известного устройства заключается в следующем. На первый вход устройства вводится последовательность информационных данных, которая с помощью блока ввода информационных данных подается на первый вход блока шифрования. На второй вход устройства подается ключ шифрования, который через блок блока ввода ключей шифрования подается на второй вход блока шифрования. В блоке шифрования по правилу, которое инициировано введенным ключом шифрования, выполняется шифрование для повышения конфиденциальности информационных данных. Зашифрованные информационные данные из выхода блока шифрования подаются на вход блока помехоустойчивого кодирования, в котором выполняется внесение специально формированной избыточности для повышения достоверности зашифрованных данных. Полученные данные из выхода блока помехоустойчивого кодирования подаются на первый вход модулятора. На третий вход устройства подается ключ формирования псевдослучайных последовательностей, который через блок ввода ключей формирования псевдослучайных последовательностей подается на вход генератора псевдослучайных последовательностей. Генератор псевдослучайных последовательностей по правилу, которое инициировано введенным ключом формирования псевдослучайных последовательностей, формирует дискретные сигналы, т.е. дискретные последовательности, элементы которых сформировано псевдослучайным образом. Сформированные псевдослучайные последовательности подаются на второй вход модулятора, в котором представленные, на первый вход, информационные данные модулируются по следующему правилу:

$$E_i = \sum_{j=0}^{k-1} m^*_{i_j} \Phi_j = \left(\sum_{j=0}^{k-1} m^*_{i_j} \phi_{j_0}, \sum_{j=0}^{k-1} m^*_{i_j} \phi_{j_1}, ..., \sum_{j=0}^{k-1} m^*_{i_j} \phi_{j_{n-1}} \right), \quad (1)$$

где $$m^*_{i_j} = \begin{cases} +1, m_{i_j} = 1; \\ -1, m_{i_j} = 0; \end{cases}$$

В данном правиле используются обозначения:

– E_i – блок модулированного информационного сигнала;

– $m_i = (m_{i_0}, m_{i_1}, ..., m_{i_{k-1}})$ – блоки информационных данных;

– $m_{i_j} \in [0,1]$ представляет собой отдельный бит информационных данных;

– $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ – сформированные псевдослучайные последовательности, которые, составляют ансамбль дискретных сигналов мощности $|\Phi| = M \geq k$ и используются в качестве секретных ключевых данных;

– k – число элементов в каждом блоке информационного сообщения не превышает мощности M ансамбля Ф используемых дискретных сигналов.

Сформированное таким образом модулированное сообщение подается на первый вход блока перемежения. На четвертый вход устройства подается ключ перемежения, который через блок ввода ключей перемежения подается на второй вход блока перемежения и инициирует соответствующее правило перемежения. В блоке перемежения выполняется перемежение представленного на его первый вход модулированного сообщения. Полученные данные подаются на блок добавления, в котором выполняется поэлементное сложение с данными контейнера, которые через блок ввода контейнеров из пятого входа устройства подаются на второй вход блока добавления. Полученные данные из выхода блока добавления подаются на вход блока квантования, который выполняет преобразование для хранения начального динамического диапазона изображения-контейнера, в результате чего формируются отдельные блоки стеганограммы, которые подаются на вход блока формирования и вывода стеганограммы. В блоке формирования и вывода стеганограммы завершаются стеганографическая обработка данных путем объединения отдельных блоков стеганограммы, формируется заполненный контейнер (стеганограмма) и подается на выход устройства.

Недостатком известного устройства-прототипа является то, что в процессе стеганографического встраивания данных информационного сообщения, не учитываются статистические свойства контейнера, т.е. цифровые данные отдельных фрагментов пространственной области изображения могут быть коррелированными с применяемыми дискретными сигналами, что может привести к возникновению ошибки при извлечении соответствующих блоков информационных данных на приёмной стороне.

3. Разработка усовершенствованного устройства встраивания данных в пространственной области изображений с использованием адаптивно формируемых дискретных сигналов

В основу исследований поставлена задача создать устройство стеганографического встраивания

данных в пространственной области изображений, с использованием прямого расширения спектра, которое, за счет учета статистических свойств контейнера, разрешит значительно повысить достоверность извлечения встроенных данных. Это достигается путем введения дополнительных ограничений на значение коэффициента корреляции используемых дискретных сигналов и отдельных фрагментов пространственной области изображения. Реализация устройства позволит значительно уменьшить количество возникающих ошибок, при извлечении соответствующих блоков информационных данных, на приёмной стороне.

Поставленная задача решается за счет того, что в известное устройство-прототип дополнительно вводится блок отбора псевдослучайных последовательностей, причем его первый вход соединен с выходом генератора псевдослучайных последовательностей, второй вход соединен с выходом блока ввода контейнеров, а выход соединен со вторым входом модулятора.

Дополнительно введенный блок отбора псевдослучайных последовательностей реализуется таким образом, чтобы значение коэффициента корреляции псевдослучайных последовательностей и блоков данных контейнера не превышали значения заведомо установленного порога, т.е. в этом блоке реализуется правило отбора псевдослучайных последовательностей по следующему критерию:

$$\left|\rho\left(C_i, \Phi_j\right)\right| = \left|\frac{1}{n}\sum_{z=0}^{n-1} C_{i_z}\varphi_{j_z}\right| \le \rho_{max} . \qquad (2)$$

В данном критерии используются обозначения:

– C – исходный (пустой) контейнер;

– $\left|\rho\left(C_i, \Phi_j\right)\right|$ – значение коэффициента корреляции псевдослучайных последовательностей и блоков данных пустого контейнера;

– ρ_{max} – заведомо установленный порог коэффициента корреляции.

Структурная схема предложенного устройства стеганографического встраивания данных в пространственной области изображений с использованием прямого расширения спектр изображен на рис. 1.

Предложенное устройство содержит: пять входов, выход, блок ввода информационных данных, блок ввода ключей шифрования, блок ввода ключей формирования псевдослучайных последовательностей, блок ввода ключей перемежения, блок ввода контейнеров, блок шифрования, блок помехоустойчивого кодирования, генератор псевдослучайных последовательностей, модулятор, блок перемежения, блок добавления, блок квантования, блок формирования и вывода стеганограммы, и дополнительно введен блок отбора псевдослучайных последовательностей.

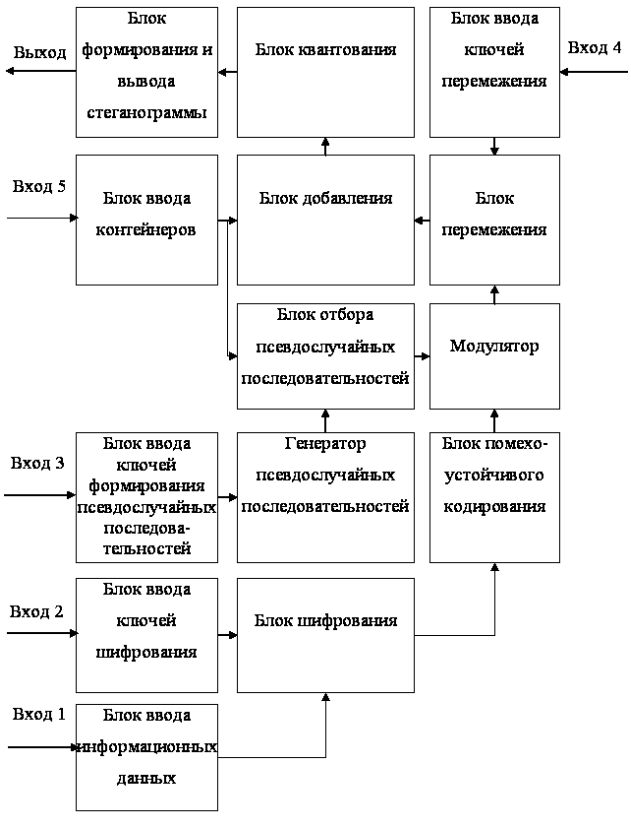

Рис. 1. Предложенное устройство встраивания данных в пространственной области изображений с использованием адаптивно формируемых дискретных сигналов

Элементы предложенного устройства соединены следующим образом. Первый вход устройства соединен с входом блока ввода информационных данных, выход которого соединен с первым входом блока шифрования. Второй вход устройства соединен с входом блока ввода ключей шифрования, выход которого соединен со вторым входом блока шифрования. Выход блока шифрования соединен с входом блока помехоустойчивого кодирования, выход которого соединен с первым входом модулятора. Третий вход устройства соединен с входом блока ввода ключей формирования псевдослучайных последовательностей, выход которого соединен с входом генератора псевдослучайных последовательностей. Выход генератора псевдослучайных последовательностей соединен с первым входом дополнительно введенного блока отбора псевдослучайных последовательностей, выход которого соединен со вторым входом модулятора. Выход модулятора соединен с первым входом блока перемежения. Четвертый вход устройства соединен с входом блока ввода ключей перемежения, выход которого соединен со вторым входом блока перемежения. Выход блока перемежения соединен с первым входом блока добавления. Пятый вход устройства соединен с входом блока ввода контейнеров, выход которого соединен с блоком добавления и вторым входом

дополнительно введенного блока отбора псевдослучайных последовательностей. Выход блока добавления соединен с входом блока квантования. Выход блока квантования соединен с входом блока формирования и вывода стеганограммы, выход которого соединен с выходом устройства.

Работа предложенного устройства заключается в следующем. На первый вход устройства вводится последовательность информационных данных, которая с помощью блока ввода информационных данных подается на первый вход блока шифрования. На второй вход устройства подается ключ K_1 шифрования, который через вход блока ввода ключей шифрования подается на второй вход блока шифрования. В блоке шифрования, по правилу, которое инициировано введенным ключом шифрования, выполняется шифрование для повышения конфиденциальности информационных данных. Зашифрованные информационные данные, из выхода блока шифрования, подаются на вход блока помехоустойчивого кодирования, в котором выполняется внесение специально формированной избыточности для повышения достоверности зашифрованных данных. Полученные данные $m_i = (m_{i_0}, m_{i_1}, ..., m_{i_{k-1}})$ из выхода блока помехоустойчивого кодирования подаются на первый вход модулятора. На третий вход устройства подается ключ K_2 формирования псевдослучайных последовательностей, который через блок ввода ключей формирования псевдослучайных последовательностей, подается на вход генератора псевдослучайных последовательностей. Генератор псевдослучайных последовательностей по правилу, которое инициировано введенным ключом K_2 формирования псевдослучайных последовательностей, формирует дискретные сигналы Φ_j, т.е. дискретные последовательности, элементы которых сформированы псевдослучайным образом. Сформированные псевдослучайные последовательности Φ_j подаются на первый вход дополнительно введенного блока отбора последовательностей, на второй вход которого, из пятого входа устройства, через блок ввода контейнеров, подаются фрагменты контейнера C_i. В блоке отбора последовательностей, по правилу (2), для всех фрагментов контейнера C_i, $i = 0,.., N-1$, рассчитывается значение коэффициента корреляции:

$$\rho(C_i, \Phi_j) = \frac{1}{n} \sum_{z=0}^{n-1} C_{i_z} \varphi_{j_z}, \qquad (3)$$

и сравнивается с заведомо определенным значением ρ_{max}.

В случае, когда хотя бы для одного $i \in \{0,.., N-1\}$, рассчитанное значение $\rho(C_i, \Phi_j)$ превысит значение порога ρ_{max}, сформированная псевдослучайная последовательность бракуется, т.е. дискретные сигналы Φ_j из $\rho(C_i, \Phi_j) > \rho_{max}$ хотя бы для одного $i \in \{0,.., N-1\}$ для стеганографического встраивания информационных данных не применяются.

Если, для сформированного дискретного сигнала Φ_j, и для всех $i = 0,.., N-1$, рассчитанные значения коэффициента корреляции $\rho(C_i, \Phi_j)$ меньше или равны установленному порогу ρ_{max}, т.е., если выполняется условие (2) для всех блоков данных контейнера, соответствующее значение Φ_j принимается к дальнейшему стеганографическому встраиванию информационных данных.

Сформированные, таким образом, псевдослучайные последовательности, составляют ансамбль дискретных сигналов $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$. Они учитывают статистические свойства контейнера и подаются в модулятор. На модулятор подается также блоки информационных данных $m_i = (m_{i_0}, m_{i_1}, ..., m_{i_{k-1}})$, $k \le M$, в котором они модулируются по правилу (1).

Сформированное таким образом модулированное сообщение E_i, подается на первый вход блока перемежения. На четвертый вход устройства подается ключ K_3 перемежения, который, через блок ввода ключей перемежения, подается на второй вход блока перемежения, и инициирует соответствующее правило перемежения. В блоке перемежения выполняется перемежение представленного на его первый вход модулированного сообщения E_i. Т.е., по правилу f, которое задает тайный ключ K_3, псевдослучайным образом переставляются местами элементы E_i.

Полученные данные $\overline{E_i} = f(E_i, K_1)$ подаются на блок добавления, в котором выполняется поэлементное добавление с фрагментами контейнера C_i (с данными цифрового изображения в пространственной области): $S_i = C_i + \overline{E_i} \cdot G$, где $G > 0$ – коэффициент усиления расширяющего сигнала, который задает «энергию» встроенных блоков информационного сообщения. Отдельные фрагменты контейнера C_i через блок ввода контейнеров из пятого входа устройства подаются на второй вход блока добавления.

Полученные данные S_i, из выхода блока добавления подаются на вход блока квантования, который выполняет преобразование для хранения начального динамического диапазона изображения-контейнера, в результате чего формируются отдельные блоки сте-

ганограммы $\overline{S_i}$, которая подается на вход блока формирования и вывода стеганограммы. В блоке формирования и вывода стеганограммы завершается стеганографическая обработка данных, путем объединения отдельных блоков стеганограммы и заполненный контейнер $\overline{S} = \overline{S_0} \cup \overline{S_1} \cup ... \cup \overline{S_{N-1}}$, формируется заполненный контейнер (стеганограмма) $\overline{S}$ и подается на выход устройства.

Таким образом, в результате работы предложенного устройства, за счет дополнительного введения блока отбора псевдослучайных последовательностей, который реализует правило отбора последовательностей по критерию (2), с учетом статистических свойств контейнера, удается значительно повысить достоверность извлечения встроенных данных.

4. Разработка усовершенствованного устройства извлечения данных из пространственной области изображений с использованием адаптивно формируемых дискретных сигналов

Известное устройство, избранное как прототип, которое реализует стеганографическое извлечение данных из пространственной области изображений с использованием прямого расширения спектра, содержит: четыре входа, выход, блок ввода и форматирования стеганограмм, блок ввода ключей деперемежения, блок ввода ключей формирования псевдослучайных последовательностей, блок ввода ключей дешифрования, блок фильтрации, блок деперемежения, генератор псевдослучайных последовательностей, демодулятор, блок помехоустойчивого декодирования, блок дешифрования, блок формирования и вывода информационных данных [1].

Первый вход устройства соединен с входом блока ввода и форматирования стеганограммы, выход которого, соединен с первым входом блока фильтрации. Выход блока фильтрации соединен с первым входом блока деперемежения. Второй вход устройства соединен с входом блока ввода ключей деперемежения, выход которого, соединен со вторым входом блока деперемежения. Выход блока деперемежения соединен с первым входом демодулятора. Третий вход устройства соединен с входом блока ввода ключей формирования псевдослучайных последовательностей, выход которого соединен с входом генератора псевдослучайных последовательностей. Выход генератора псевдослучайных последовательностей соединен со вторым входом демодулятора, выход которого соединен с входом блока помехоустойчивого декодирования. Выход блока помехоустойчивого декодирования соединен с первым входом блока дешифрования. Четвертый вход устройства соединен с входом блока ввода ключей дешифрования, выход которого соединен со вторым входом блока дешифрования. Выход блока дешифрования соединен с входом блока формирования и вывода информационных данных.

Работа известного устройства заключается в следующем. На первый вход устройства вводится стеганограмма, которая подается на вход блока ввода и форматирования стеганограммы, в котором формируются отдельные фрагменты (блоки) пространственной области стеганоизображения, которые подаются на вход устройства фильтрации. После фильтрации, полученные данные, подаются на первый вход блока деперемежения, на котором выполняется действие, инверсное перемежению на передающей стороне. Блок деперемежения инициирован ключом деперемежения, который подается на второй вход устройства, и через блок ввода ключей деперемежения, подается на второй вход блока деперемежения. Полученные, после деперемежения, данные, подаются на первый вход демодулятора, который выполняет функцию корреляционного приемника дискретных сигналов, по рассмотренному выше правилу.

На третий вход устройства подается ключ формирования псевдослучайных последовательностей, который через блок ввода ключей формирования псевдослучайных последовательностей подается на вход генератора псевдослучайных чисел. Генератор псевдослучайных чисел, который инициирован введенным ключом формирования псевдослучайных последовательностей, формирует ансамбль дискретных сигналов (псевдослучайных последовательностей), которые подаются на второй вход демодулятора. Последовательности, которые поступают в демодулятор из выхода генератора псевдослучайных последовательностей, являются тождественными тем, которые применяются на передающей стороне, при встраивании информационных сообщений.

В демодуляторе рассчитывается значение коэффициента корреляции между представленными на его первый вход данными (из выхода блока деперемежения), и последовательностями, которые представлены на его второй вход (из выхода генератора псевдослучайных последовательностей). Решение, относительно значения встроенных данных, принимается согласно значению рассчитанного коэффициента корреляции по следующему правилу:

$$m^*_{i_j} = \operatorname{sign}\left(\rho\left(S^*_i, \Phi_j\right)\right) = \begin{cases} -1, \rho\left(S_i, \Phi_j\right) < 0; \\ +1, \rho\left(S_i, \Phi_j\right) > 0. \end{cases} \quad (4)$$

Извлеченные данные подаются на вход блока помехоустойчивого декодирования, в котором, по определенному правилу, с использованием внесенной избыточности, исправляются некоторые ошибки, согласно корректирующей способности кода. Это приводит к некоторому повышению достоверности переданных данных. Полученные, после декодирования, данные, подаются на первый вход

блока дешифрования, инициированного ключом дешифрования. Ключ дешифрования подается на четвертый вход устройства и, через блок ввода ключей дешифрования, подается на второй вход блока дешифрования. Дешифрованные сообщения подаются на вход блока форматирования и вывода информационных данных, в котором завершается формирование информационных сообщений, которые подаются на выход устройства.

Недостатком известного устройства-прототипа является то, что в процессе стеганографического встраивания данных информационного сообщения не учитываются статистические свойства контейнера, т.е. цифровые данные отдельных фрагментов пространственной области изображения, могут быть коррелированными с применяемыми дискретными сигналами, что может привести к возникновению ошибки при извлечении соответствующих блоков информационных данных на приёмной стороне.

В основу исследований поставлена задача создания устройства для реализации стеганографического извлечения данных, из пространственной области изображений, с использованием прямого расширения спектра, который, за счет учета статистических свойств контейнера разрешит значительно повысить достоверность извлечения встроенных данных. Т.е., реализация устройства разрешит значительно уменьшить количество возникающих ошибок при извлечении соответствующих блоков информационных данных на приёмной стороне, путем введения дополнительных ограничений на значение коэффициента корреляции используемых дискретных сигналов и отдельных фрагментов пространственной области изображения.

Поставленная задача решается за счет того, что в известное устройство для реализации стеганографического извлечения данных, из пространственной области изображений, дополнительно вводится блок адаптации (запоминающее устройство), причем его вход соединен с выходом блока ввода ключей формирования псевдослучайных последовательностей, а выход соединен со вторым входом генератора псевдослучайных последовательностей.

Дополнительно введенный блок адаптации (запоминающее устройство) реализуется таким образом, чтобы значение коэффициента корреляции применяемых псевдослучайных последовательностей (дискретных сигналов) и блоков данных контейнера, не превышали значения заведомо установленного порога. Т.е. в этом блоке реализуется правило отбора псевдослучайных последовательностей по критерию (2). Блок адаптации может быть реализован в виде запоминающего устройства, в котором сохраняются псевдослучайные последовательности, тождественные тем, которые применяются на передающей стороне, при встраивании информационных сообщений.

Структурная схема предложенного устройства для реализации стеганографического извлечения данных из пространственной области изображений с использованием прямого расширения спектр изображена на рис. 2.

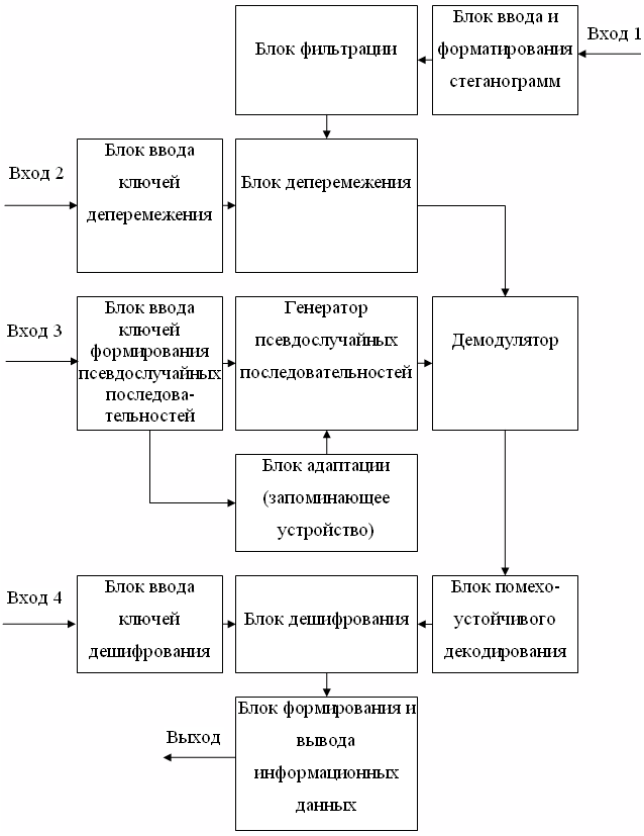

Рис. 2. Предложенное устройство извлечения данных из пространственной области изображений с использованием адаптивно формируемых дискретных сигналов

Предложенное устройство содержит: четыре входа, выход, блок ввода и форматирования стеганограмм, блок ввода ключей деперемежения, блок ввода ключей формирования псевдослучайных последовательностей, блок ввода ключей дешифрования, блок фильтрации, блок деперемежения, генератор псевдослучайных последовательностей, демодулятор, блок помехоустойчивого декодирования, блок дешифрования, блок формирования и вывода информационных данных, и дополнительно введен блок адаптации (запоминающее устройство).

Элементы предложенного устройства соединены следующим образом. Первый вход устройства соединен с входом блока ввода и форматирования стеганограммы, выход которого соединен с первым входом блока фильтрации. Выход блока фильтрации соединен с первым входом блока деперемежения. Второй вход устройства соединен с входом блока ввода ключей деперемежения, выход которого соединен со вторым входом блока деперемежения. Выход блока деперемежения соединен с первым входом демодулятора. Тре-

тий вход устройства соединен с входом блока ввода ключей формирования псевдослучайных последовательностей, выход которого соединен с первым входом генератора псевдослучайных последовательностей и входом дополнительно введенного блока адаптации (запоминающего устройства). Выход блока адаптации соединен со вторым входом генератора псевдослучайных последовательностей.

Выход генератора псевдослучайных последовательностей соединен со вторым входом демодулятора, выход которого соединен с входом блока помехоустойчивого декодирования. Выход блока помехоустойчивого декодирования соединен с первым входом блока дешифрования. Четвертый вход устройства соединен с входом блока ввода ключей дешифрования, выход которого соединен со вторым входом блока дешифрования. Выход блока дешифрования соединен с входом блока формирования и вывода информационных данных.

Работа предложенного устройства заключается в следующем. На первый вход устройства вводится стеганограмма $\overline{S}$, которая подается на вход блока ввода и форматирования стеганограммы, в котором формируются отдельные фрагменты (блоки) $\overline{S_i}$ пространственной области стеганоизображения, которые подаются на вход устройства фильтрации. После фильтрации, полученные данные $\overline{\overline{S_i}}$, подаются на первый вход блока деперемежения, на котором выполняется действие, инверсное перемежению на передающей стороне.

Блок деперемежения инициирован ключом деперемежения K_1, который подается на второй вход устройства, и, через блок ввода ключей деперемежения, подается на второй вход блока деперемежения. Полученные после деперемежения данные S^*_i, подаются на первый вход демодулятора, который выполняет функцию корреляционного приемника дискретных сигналов, по рассмотренному выше правилу.

На третий вход устройства подается ключ формирования псевдослучайных последовательностей K_2, который, через блок ввода ключей формирования псевдослучайных последовательностей, подается на вход генератора псевдослучайных чисел и на вход дополнительно введенного блока адаптации (запоминающего устройства). Блок адаптации выполняет корректирование работы генератора псевдослучайных последовательностей таким образом, чтобы коэффициент корреляции формированных дискретных сигналов и блоков данных контейнера, не превышал значения заведомо установленного порога. Т.е. в этом блоке реализуется правило отбора псевдослучайных последовательностей по критерию (2). В простейшем случае, блок адаптации может быть реализован в виде запоминающего устройства, в котором сохраняются псевдослучайные последовательности, тождественные тем, которые применяются на передающей стороне, при встраивании информационных сообщений.

Исходное действие, дополнительно введенного блока адаптации, подается на второй вход генератору псевдослучайных чисел, который инициирован введенным ключом формирования псевдослучайных последовательностей. Генератор формирует ансамбль дискретных сигналов $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ (псевдослучайных последовательностей). Сформированные дискретные сигналы Φ_j подаются на второй вход демодулятора. Последовательности, которые поступают в демодулятор из выхода генератора псевдослучайных последовательностей, являются тождественными тем, которые применяются на передающей стороне, при встраивании информационных сообщений.

В демодуляторе рассчитывается значение коэффициента корреляции между представленными на его первый вход данными S^*_i (из выхода блока деперемежения) и последовательностями Φ_j, которые представлены на его второй вход (из выхода генератора псевдослучайных последовательностей). Решение, относительно значения встроенных данных, принимается согласно значению рассчитанного коэффициента корреляции по правилу (4).

Извлеченные данные m_i подаются на вход блока помехоустойчивого декодирования, в котором, по определенному правилу, с использованием внесенной избыточности, исправляются некоторые ошибки, согласно корректирующей способности кода. Это приводит к некоторому повышению достоверности переданных данных. Полученные, после декодирования, данные, подаются на первый вход блока дешифрования, инициированного ключом дешифрования K_3. Ключ дешифрования K_3 подается на четвертый вход устройства и, через блок ввода ключей дешифрования, подается на второй вход блока дешифрования. Дешифрованные сообщения подаются на вход блока форматирования и вывода информационных данных, в котором завершается формирование информационных сообщений, которые подаются на выход устройства.

Выводы

Предложено устройство для аппаратной реализации методов стеганографии, усовершенствованное за счет дополнительного введения блока адаптации (запоминающего устройства), который реализует правило отбора последовательностей по критерию (2) с учетом статистических свойств контейнера, что позволяет значительно повысить достоверность извлечения встроенных данных.

Список литературы

1. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ [Текст]: учеб. пособие для вузов / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин. – М.: Вузовская книга, 2009. – 220 с.

2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – СПб.: Солон-Пресс, 2002. – 272 с.

3. Конахович Г.В. Компьютерная стеганография. Теория и практика / Г.В. Конахович, А.Ю. Пузыренко. –К.: МК-Пресс, 2006. – 288 с.

4. Кузнецов А.А. Встраивание данных в контейнеры-изображения с использованием сложных дискретных сигналов / А.А. Кузнецов, А.А. Смирнов // Радиотехника: Всеукраинский межведомственный научно-технический сборник. Темат. выпуск «Информационная безопасность». – Вып. 166. – Х.: ХНУРЭ, 2011. – С. 134-141.

5. Kuznetsov A.A. Use of Complex Discrete Signals for Steganographic Information Security / A.A. Kuznetsov, A.A. Smirnov // International Journal of Engineering Practical Education. – Vol. 1, Issue 1. – USA, Indiana, Riley: Science and Engineering Publishing Company. – 2012. – P. 21-25.

6. Смирнов А.А. Методы и средства компьютерной стеганографии с применением сложных дискретных сигналов для защиты информации в компьютерных системах и сетях: монография / А.А. Смирнов. – К.: Изд. «КОД», 2012. – 350 с.

7. Смирнов А.А. Стеганографическое встраивание данных в неподвижные изображения методом прямого расширения спектра / А.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Вип. 2(6). – Х.: ХУПС, 2011. – С. 126-129.

8. Смирнов А.А. Метод стеганографического встраивания информации в неподвижные изображения с использованием сложных дискретных сигналов и прямого расширения спектра / А.А. Смирнов // Науково-технічний журнал «Захист інформації». – Вип.. 4 (53). – К.: НАУ. – 2011. – С. 64-70.

9. Marvel L. Image Steganography for hidden communication. PhD Thesis. // Univ.of Delaware, 1999. – 115p.

10. Patent No.: US 6,557,103 B1, Int.Cl. G06F 11/30. Charles G. Boncelet Jr., Lisa M. Marvel, Charles T. Retter. Spread Spectrum Image Steganography. – № 09/257,136; Filed Feb. 11, 1999; Date of Patent Apr. 29, 2003.

Поступила в редколлегию 4.02.2014

Рецензент: д-р техн. наук проф. И.В. Рубан, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

АПАРАТНА РЕАЛІЗАЦІЯ ПРИСТРОЇВ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ АДАПТИВНО ФОРМОВАНИХ ДИСКРЕТНИХ СИГНАЛІВ

О.А. Смірнов, Є.В. Мелешко, О.О. Кузнецов

Запропоновано структурну схему апаратної реалізації вдосконаленого пристрою вбудовування і отримання даних з просторової області зображень з використанням адаптивно формованих дискретних сигналів для стеганографічного захисту інформації.

Ключові слова: *стеганографія, розширення спектру, адаптивно формовані дискретні сигнали.*

HARDWARE IMPLEMENTATION OF STEGANOGRAPHIC INFORMATION SECURITY USING ADAPTIVE FORMED DISCRETE SIGNALS

A.A. Smirnov, E.V. Meleshko, A.A. Kuznetsov

A structural diagram of a hardware implementation improved device integration and retrieval of spatial domain images using adaptive discrete signals generated for steganographic data protection.

Keywords*: steganography, spread spectrum, adaptively formed discrete signals.*