Алгоритм имитозащиты. В TLS данные, зашифрованные с помощью поточных или блочных алгоритмов, должны сопровождаться имитовставками. В BIGN_WITH_BELT в необходимых случаях применяется алгоритм вычисления имитовставки, определенный в СТБ 34.101.31 (belt-mac).

Алгоритм генерации псевдослучайных данных. В TLS алгоритм генерации псевдослучайных чисел (PRF-алгоритм в обозначениях [1]) используется для построения ключей и синхропосылок, а также для верификации сообщений протокола Handshake. Стандартный PRF-алгоритм последней редакции TLS строится на основе алгоритма HMAC, который, в свою очередь, строится на некотором алгоритме хэширования. Во всех криптонаборах BIGN_WITH_BELT используется стандартный PRF-алгоритм с алгоритмом хэширования СТБ 34.101.31 (belt-hash).

Алгоритмы формирования общего ключа. В протоколе TLS имеется определенная свобода выбора алгоритма (или, точнее, механизма) формирования общего ключа. Тем не менее, в [1] описаны четыре типа таких алгоритмов, которые применяются в большинстве существующих на сегодняшний день решений. Алгоритмы двух типов не обеспечивают защиту от атак типа «противник посередине» и «чтение назад». Поэтому в BTLS были включены алгоритмы только двух оставшихся типов:

– dht-bign – транспорт ключа на основе СТБ 34.101.45 (bign-keytransport);

– dhe-bign – протокол Диффи – Хэллмана с эфемерными ключами, которые подписываются с помощью алгоритмов СТБ 34.101.45 (bign-sign).

Дополнительно в BTLS определен алгоритм формирования общего ключа, соответствующий RFC 4279 [4]:

– dht-psk-bign – транспорт ключа типа DHT_BIGN с использованием предварительно распределенных общих секретов.

В перечисленных алгоритмах формирования общего ключа используется сертификат сервера с открытым ключом СТБ 34.101.45 (bign-pubkey).

Обязательный криптонабор. Любая реализация BTLS должна поддерживать криптонабор с алгоритмом шифрования belt-ctr, алгоритмом имитозащиты belt-mac и алгоритмом формирования общего ключа dht-bign. Поддержка остальных 8 криптонаборов является необязательной.

Методы аутентификации

Аутентификация в BTLS основана на проверке действительности сертификатов открытых ключей сторон и на проверке знания сторонами соответствующих личных ключей. Для криптонаборов с алгоритмом формирования общего ключа dht-psk-bign дополнительная аутентификация состоит в проверке знания общего секрета (предполагается, что этот секрет был надежно передан сторонам протокола, подлинность которых была предварительно проверена). При аутентификации используются сертификаты, в которых фиксируются открытые ключи алгоритмов СТБ 34.101.45 (bign-pubkey).

Аутентификация сервера. В протоколе Handshake сервер передает клиенту сертификат, который при использовании алгоритма dhe-bign содержит открытый ключ электронной цифровой подписи, а при использовании алгоритмов dht-bign и dht-psk-bign – открытый ключ транспорта. Последующее успешное завершение Handshake означает, что аутентификация сервера проведена успешно.

Аутентификация клиента. В протоколе Handshake сервер запрашивает у клиента его сертификат. В этом запросе указываются возможные типы сертификатов, который должен предоставить клиент, а также типы пар (алгоритм хэширования, алгоритм ЭЦП), которые разрешается использовать при проверке подписи сертификата. Разрешается использовать сертификаты открытых ключей типа bign-pubkey и пару алгоритмов (belt-hash, bign-sign). Сервер может запросить сертификат клиента только после предъявления своего сертификата. Успешное завершение Handshake означает, что аутентификация клиента проведена успешна.

Литература:

1. Dierks, T. The Transport Layer Security (TLS) Protocol. Version 1.2. RFC 5246 / T. Dierks, E. Rescorla. – August, 2008.

2. Проект руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа». – Минск, 1997.

3. Маслов, А.С. Криптонаборы протокола TLS, основанные на отечественных криптографических алгоритмах / А.С. Маслов, С.В. Агиевич, А.В. Федин, Д.В. Шпилевский // Информационные системы и технологии (IST'2010): Материалы VI Междунар. Конф. (Минск, 24-25 ноября 2010 г.). – Минск: А.Н. Вараксин, 2010. – С. 65–68.

4. Eronen, P. Pre-Shared Key Ciphersuites for TLS. RFC 4279 / P. Eronen, H. Tschofenig. – December, 2005.

Abstract

The TLS protocol is under standardization in Republic of Belarus. The future standard will include additional TLS ciphersuites based on domestic cryptographic algorithms. In this paper we describe additional suites and related authentication methods.

Поступила в редакцию 18.05.2013 г.

СТЕГАНОГРАФИЯ: МОДЕЛИ И МЕТОДЫ ОЦЕНКИ НАДЕЖНОСТИ

УДК 519.2

Ю.С. Харин, Е.В. Вечерко,
НИИ ППМИ БГУ, г. Минск

Аннотация

В статье рассматриваются математические модели вкрапления, возникающие в задачах стеганографии. На основе марковских моделей контейнеров, среднеквадратических ошибок оценивания уровня вкрапления и вероятностей ошибок при проверке гипотез о факте вкрапления построены оценки надежности. Представлены результаты компьютерных экспериментов.

Введение

Стеганография имеет целью сокрытие сообщений в открытых цифровых данных, называемых контейнерами.

В последние годы стеганография интенсивно развивается и применяется для скрытой передачи сообщений в потоке «безобидных данных» и для скрытой маркировки цифровых данных с помощью цифровых водяных знаков в системах защиты авторских прав DRM (Digital Rights Management) [1–5].

В настоящее время в мировом научном сообществе наблюдается стремительно растущий интерес к проблемам стеганографии: создаются компьютерные стеганографические программы, ежегодно проводятся десятки международных научных конференций по стеганографии, издаются тысячи научных статей. В то же время современный уровень развития стеганографии в основном носит эмпирический характер: отсутствует единая математическая теория построения и анализа стеганографических алгоритмов и систем, подобная теории К. Шеннона в криптографии.

Настоящий доклад посвящен актуальной проблеме стеганографической защиты информации – развитию математической теории оценки надежности стеганографической защиты информации.

Развитие математической теории стеганографической защиты информации невозможно без построения и использования математических моделей контейнеров и стегоконтейнеров, т.е. контейнеров, в которых скрыто сообщение. Перечень используемых и перспективных математических моделей представлен на рисунок 1.

Рисунок 1 – Математические модели в стеганографии

1 Оценка надежности методами статистического анализа вкраплений

Проиллюстрируем применение марковской модели вкраплений для оценки надежности встраивания сообщений.

1.1 Марковская модель вкраплений

Введем обозначения: V = {0,1} – двоичный алфавит, V_t – пространство двоичных, t – мерных векторов, N – множество натуральных чисел, $I\{A\}$ – индикатор события A, $u_{t_1}^{t_2} = (u_{t_1},...,u_{t_2}) \in V_{t_2-t_1+1}$ ($t_1, t_2 \in N$, $t_1 \le t_2$) – двоичная строка из $t_2 - t_1 + 1$ символов, $w(\cdot)$ – вес Хемминга, $L\{\xi\}$ – закон распределения вероятностей случайной величины ξ, $B(\theta)$ – закон распределения вероятностей Бернулли с параметром $\theta \in [0,1]$.

Будем предполагать, что контейнер для встраивания сообщения есть двоичная последовательность $x_1^T \in V_T$, $x_t \in V$, $t = 1, ..., T$ длины T, являющаяся однородной двоичной цепью Маркова 1-го порядка с симметричной матрицей вероятностей одношаговых переходов $P = (p_{j_0,j_1}), j_0, j_1 \in V$:

$$P = \frac{1}{2}\begin{pmatrix} 1+\varepsilon & 1-\varepsilon \\ 1-\varepsilon & 1+\varepsilon \end{pmatrix},$$

$$p_{j_0,j_1} = \mathrm{P}\{x_{t+1} = j_1 \mid x_t = j_0\} = \frac{1}{2}(1+(-1)^{j_0+j_1}\varepsilon), \quad |\varepsilon| < 1. \qquad (1)$$

Здесь ε – параметр модели: случай ε = 0 соответствует схеме независимых испытаний и исследован в [3]; случай ε > 0 учитывает зависимость типа притяжения, ε < 0 – зависимость типа отталкивания. Отметим, что цепь Маркова (1) удовлетворяет условиям эргодичности [6] и имеет равномерное стационарное распределение вероятностей π = (1/2 1/2). Далее будем полагать, что цепь Маркова (1) является стационарной.

Обычно [5] на практике сообщение перед встраиванием в контейнер подвергается криптографическому преобразованию, устраняющему статистическую избыточность, поэтому далее полагаем, что сообщение $\xi_1^M \in V_M$, $M \le T$, является последовательностью M независимых случайных величин Бернулли: $L\{\xi_t\} = B\{\theta_1\}$, $P\{\xi_t = j\} = \theta_j$, $j \in V$, $\theta_1 = 1 - \theta_0$, $t = 1, ..., M$. Как правило [5], $\{\xi_t\}$ имеет симметричное распределение вероятностей: $\theta_1 = \theta_0 = 1/2$.

Стегоключ γ_1^T определяет моменты времени, в которые биты сообщения ξ_1^M вкрапляются в последовательность x_1^T. Введем специальную (q, r)-блочную модель стегоключа (q, $r \in N$, $r \le q$), предполагая, что длина последовательности x_1^T кратна q: $T = Kq$. Для этого вначале разобьем последовательность x_1^T на блоки длины q: $x_{(1)} = x_1^q, x_{(2)} = x_{q+1}^{2q}, ..., x_{(K)} = x_{T-q+1}^T$. Введем вспомогательные независимые случайные величины $\varsigma_k \in V$, $L\{\varsigma_k\} = B\{\delta\}$, $k = 1, ..., K$, которые отвечают за выбор блоков $\{x_{(k)}\}$ для вкрапления сообщения: если $\varsigma_k = 1$, то в r случайно выбранных бит блока $\{x_{(k)}\}$ вкрапляются r бит сообщения; если $\varsigma_k = 0$, то вкрапление не производится. Отметим, что для такой модели стегоключа максимальная пропускная способность стегосистемы уменьшается до $Tr/q = Kr$ бит, а мощность множества всевозможных стегоключей сжимается до $(1 + C_q^r)^K$.

Случайная стегопоследовательность порождается следующим образом:

$$Y_t = \gamma_t \xi_{\tau_t} + (1-\gamma_t)x_t = \begin{cases} x_t, & \gamma_t = 0, \\ \xi_{\tau_t}, & \gamma_t = 1. \end{cases} \qquad (2)$$

Случайные последовательности $\{x_t\}$, $\{\xi_t\}$, $\{\gamma_t\}$ предполагаются независимыми в совокупности.

Заметим, что с практической точки зрения наибольшего внимания в рамках рассматриваемой здесь марковской модели вкраплений (1)–(2) заслуживает наиболее трудный для обнаружения вкраплений случай, когда $\theta_1 = \theta_0 = 1/2$, так как в этом случае при вкраплении одномерное распределение вероятностей не искажается: $P\{Y_t = j\} = P\{x_t = j\} = 1/2$, $j \in V$.

1.2 Статистическое оценивание параметров модели вкраплений

Разобьем множество V_t двоичных t-мерных векторов на t+1 непересекающихся подмножеств: $V_t = \Gamma_0^{(t)} \cup \Gamma_1^{(t)} \cup ... \cup \Gamma_t^{(t)}$, где $\Gamma_0^{(t)} = \{u_1^t \in V_t : u_t = 1\}$, $\Gamma_1^{(t)} = \{u_1^t \in V_t : u_t = u_{t-1} = 0\}$, $\Gamma_j^{(t)} = \{u_1^t \in V_t : u_t = 0, u_{t-1} = ... = u_{t-j-1} = 1, u_{t-j} = 0\}$, $1 < j < t$, и $\Gamma_t^{(t)} = \{u_1^t \in V_t : u_t = 0, u_{t-1} = ... = u_1 = 1\}$. Такое разбиение порождает разбиение всевозможных траекторий фрагментов стегоключа $\gamma_1^t = u_1^t \in V_t$. Определим функции двоичных переменных $u_1^t \in V_t$, $y_1^t \in V_t$:

$$\varphi_t(u_1^t, y_1^t) = \begin{cases} \theta_{y_t}, & u_1^t \in \Gamma_0^{(t)}, \\ (1 + (-1)^{y_t + y_{t-j}} \varepsilon^j)/2, & u_1^t \in \Gamma_j^{(t)}, 1 \le j \le t-1, \\ 1/2, & u_1^t \in \Gamma_t^{(t)}. \end{cases} \quad (3)$$

С учетом введенных обозначений функция правдоподобия для модели вкраплений (1)–(2) имеет вид:

$$L(\varepsilon, \delta) = \sum_{u_1^t \in V_T} I\{ \sum_{h \in \{0,r\}} b_h(u_1^t) = \\ = 0\} (1-\delta)^{b_0(u_1^T)} (\delta / C_q^r)^{b_r(u_1^T)} \prod_{t=1}^{T} \varphi_t(u_1^t, y_1^t), \quad (4)$$

где $y_1^T \in V_T$ – наблюдаемая стегопоследовательность, $b_h(u_1^T) = \sum_{k=1}^{T/q} I\{w(u_{q(k-1)+1}^{qk}) = h\}$, $h \in \{0, ..., q\}$. Согласно определению (4), вычисление одного значения функции правдоподобия $L(\varepsilon, \delta)$ при фиксированных параметрах ε, δ имеет вычислительную сложность порядка $O(T(1 + C_q^r)^{T/q})$, то есть экспоненциальную сложность относительно длины стегопоследовательности T.

Оценки максимального правдоподобия $\hat{\varepsilon}, \hat{\delta}$ параметров ε, δ определяются как решение экстремальной задачи: $L(\varepsilon, \delta) \to \max_{\varepsilon \in (-1,1), \delta \in [0,1]}$. Решение этой задачи возможно только численными методами (например, методом табулирования $L(\varepsilon, \delta)$ на сетке или методом градиентного спуска), требующими вычисления функции правдоподобия для заданной последовательности точек.

Заметим, что если $q > r$, то $P\{\gamma_1^t \in \bigcup_{j=2r+2}^{t} \Gamma_j^{(t)}\} = 0$, $t > 2r+1$, и стегопоследовательность $\{Y_t\}$, определяемая в (2), при фиксированной последовательности $\{\gamma_t\}$ является управляемой цепью Маркова условного порядка $s_t \in \{0, ..., 2r+1\}$, причем порядок s_t зависит от ключевой последовательности $\{\gamma_t\}$: $s_t = j$, если $u_1^t \in \Gamma_j^{(t)}$. Это свойство позволяет построить полиномиальный относительно T алгоритм вычисления значения функции правдоподобия $L(\varepsilon, \delta)$ для (q, r)-блочной модели вкраплений при $q > r$.

Приведем примеры частотных оценок параметров модели вкраплений (1)–(2) при фиксированных значениях параметров (q, r). Обозначим $f_{j_0,...,j_{s-1}} = \sum_{t=1}^{T-s+1} I\{y_t^{t+s-1} = j_0^{s-1}\}$ абсолютную частоту s-граммы, $j_0^{s-1} \in V_s$.

Статистические оценки $\hat{\varepsilon}, \hat{\delta}$ параметров (1,1)-блочной модели вкраплений, для которой множество всевозможных стегоключей длины T совпадает с V_T, имеют вид:

$$\hat{\delta} = \begin{cases} 0, & g > 1, \\ 1 - g^{1/2}, & g \in [0,1], \\ 1, & g < 0, \end{cases}$$

$$\hat{\varepsilon} = \frac{f_{00} + f_{11} - f_{01} - f_{10}}{(1-\delta)^2 (T-1)}, \quad (5)$$

где $g = \frac{(f_{00} + f_{11} - f_{01} - f_{10})^2 (T-2)}{(f_{000} + f_{111} + f_{010} + f_{101} - f_{001} - f_{110} - f_{011} - f_{100})(T-1)^2}$.

Для модели вкраплений (1)–(2) статистики (5) является состоятельными при $T \to \infty$ оценками параметров модели δ, ε соответственно.

Аналогично, построены статистические оценки для (2,1)-блочной модели вкраплений.

Для (1, 1)-блочной модели вкраплений методом Монте-Карло вычислены среднеквадратические ошибки $v\{\hat{\delta}\} = 1/N \sum_{n=1}^{N} (\hat{\delta}^{(n)} - \delta)^2$, $v\{\hat{\varepsilon}\} = 1/N \sum_{n=1}^{N} (\hat{\varepsilon}^{(n)} - \varepsilon)^2$ оценивания параметров модели на основе частотных статистик (5) при следующих значениях параметров: $\varepsilon = 0{,}3$, $\delta = 0{,}15$ число прогонов $N = 10^3$. На рисунке 2 изображены графики зависимостей $v\{\hat{\delta}\}$, $v\{\hat{\varepsilon}\}$ от длины стегопоследовательности T.

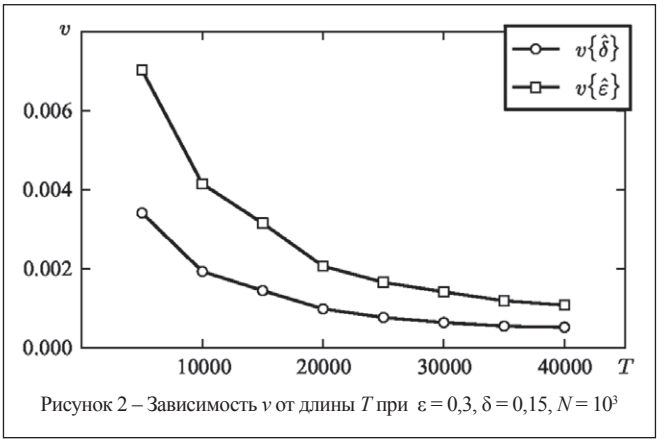

Рисунок 2 – Зависимость v от длины T при $\varepsilon = 0{,}3$, $\delta = 0{,}15$, $N = 10^3$

1.3 Оценка надежности вкрапления

Условимся говорить, что встраивание сообщения (вкрапление) является надежным (необнаруживаемым стегоаналитиком) при данном объеме материала (длине наблюдения) T, если среднеквадратическая ошибка оценивания уровня вкраплений δ достаточно велика: $E\{(\frac{\hat{\delta} - \delta}{\delta})^2\} \ge 1$, или, что эквивалентно, вариация оценки $\hat{\delta}$ удовлетворяет неравенству:

$$v\{\hat{\delta}\} = E\{(\hat{\delta} - \delta)^2\} \ge \delta^2. \quad (6)$$

Решая неравенство (6) относительно δ, находим критическую область допустимых уровней вкраплений: $\delta \in [0, \delta_+]$, где δ_+ – критический уровень вкраплений.

Для оценки $\hat{\delta}$, определяемой (5), при $T \to +\infty$ справедливо следующее выражение асимптотической дисперсии:

$$v\{\hat{\delta}\} = f(\varepsilon, \delta, T) = \frac{1}{T-1} \left(\frac{1}{2} - \frac{3}{4}(1-\delta)^2 + \frac{1}{4\varepsilon^2 (1-\delta)^2}\right). \quad (7)$$

Решая неравенство (6) с учетом (7), получаем зависимость критического уровня вкраплений δ_+ от длины наблюдения T и параметра контейнера ε: $\delta_+ = \delta_+(T, \varepsilon)$. На рисунке 3 построены графики этих зависимостей. Область под каждой кривой соответствует надежному встраиванию сообщений.

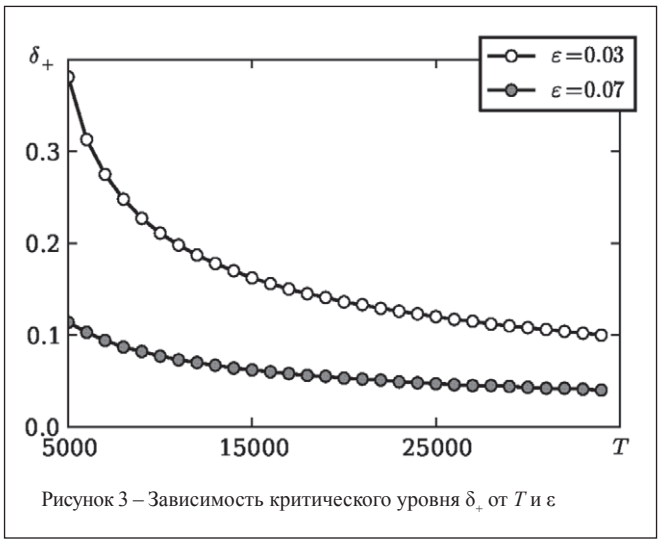

Рисунок 3 – Зависимость критического уровня δ_+ от T и ε

Укажем еще один подход к количественной оценке надежности стеганографического алгоритма, основанный на теории статистической проверки гипотез. Определим гипотезу $H_0 = \{\delta = 0\}$ о том, что контейнер не содержит вкраплений, и альтернативу $H_1 = \overline{H}_0 = \{\delta > 0\}$, означающую, что наблюдаемый поток данных $y_1^T \in V_T$ представляет собой стегоконтейнер. Предположим, что для проверки гипотез H_0, H_1 построен оптимальный тест $d = d_0(y_1^T) \in V$, который минимизирует вероятность ошибки II рода $\beta = P_{H_1}\{d = 0\} = \beta(\varepsilon, \delta, T; \alpha_0)$ среди всех тестов, вероятность ошибки I рода для которых не превосходит некоторый заданный уровень $\alpha_0 \in (0,1)$: $P_{H_0}\{d = 1\} \le \alpha_0$. Функция $\beta(\cdot) \in [0,1]$ характеризует вероятность того, что факт вкрапления в ситуации ε, δ, T не будет обнаружен «самым лучшим стегоаналитиком». Являясь характеристикой необнаруживаемости вкрапления, функция $\beta = \beta(\varepsilon, \delta, T; \alpha_0)$ может быть принята в качестве характеристики надежности стеганографического алгоритма. Емкость заполнения контейнера δ при заданных значениях его размера T, параметра ε и уровня ложных тревог α_0 следует выбирать из условия гарантированного уровня надежности $\beta_{min} \in (0,1)$:

$$\beta = \beta(\varepsilon, \delta, T; \alpha_0) \ge \beta_{min}. \quad \textbf{(8)}$$

Литература:

1. Pevny, T. Steganalysis by subtractive pixel adjacency matrix / T. Pevny, P. Bas, J. Fridrich // Proceedings of the 11-th ACM Multimedia and Security Workshop. – Princeton, 2009. – P. 75–84.

2. Bas, P. Break Our Steganographic System – the ins and outs of organizing BOSS / P. Bas, T. Filler, T. Pevny// Proceedings of Information Hiding Conference. – Prague, 2011.

3. Пономарев, К.И. Параметрическая модель вкрапления и ее статистический анализ. Дискретная математика. – Т. 21, вып. 4. – 2009. – С. 148–157.

4. Харин, Ю.С. О некоторых задачах статистической проверки гипотез в стеганографии / Ю.С. Харин, Е.В. Вечерко // Вести НАН Беларуси. Серия физ.-мат. наук. – Вып. 4. – 2010. – С. 5–12.

5. Харин, Ю.С. Математические и компьютерные основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Новое знание, 2003.

6. Кемени, Дж. Конечные цепи Маркова / Дж. Кемени, Дж. Снелл. – Наука, 1982.

Abstract

In this paper we describe some important mathematical models of embedding. Estimators of securely embedding based on markov models are constructed. The results of computer experiments are presented.

Поступила в редакцию 18.05.2013 г.

ОПРЕДЕЛЕНИЕ ОБЛАСТЕЙ ИЗОБРАЖЕНИЙ ДЛЯ ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

УДК 004.056.5

М.С. Абрамович, М.Н. Мицкевич,
НИИ ППМИ БГУ, г. Минск

Аннотация

В статье описывается алгоритм встраивания цифровых водяных знаков в графические изображения. На основании визуальной характеристики определяются области изображений с высокой детализацией для встраивания данных.

Введение

Цифровые водяные знаки (ЦВЗ) предназначены для маркировки мультимедийной информации с целью ее идентификации, аутентификации, а также мониторинга ее распространения и копирования. ЦВЗ представляет собой определенную информацию, которая добавляется к цифровому объекту и может быть обнаружена или извлечена для предъявления прав на этот объект. В системах с ЦВЗ, так же как и в стеганографии, применяются методы, с помощью которых одни данные скрываются в других.

Незаметность ЦВЗ является общим требованием для всех систем ЦВЗ. Это означает, что искажения, которые вносятся водяными знаками, должны оставаться ниже определенного порога «видимости».

В связи с этим важной практической задачей при встраивании ЦВЗ в графические изображения является задача определений областей графических изображений, встраивание ЦВЗ в которые не приведет к визуальным искажениям изображений [1].

Классификация областей изображения

При встраивании данных в изображение классифицируем точки изображения на три группы. Эта классификация построена на простейших свойствах системы человеческого зрения (СЧЗ):

– точки текстур, которые не существенны для СЧЗ. В сильно текстурированные области (области которые