Список литературы:

1. Анин Б.Ю. Защита компьютерной информации. – СПб.: - Санкт-Петербург, 2000. – 384 с.
2. Герасименко В.А., Размахнин М.К., Родионов В.В. Технические средства защиты информации // Зарубежная радиоэлектроника. 1989. № 12.
3. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
4. Домарев В.В. Защита информации и безопасность компьютерных систем. - К.: Издательство "Диа-Софт", 1999. - 480 с.
5. Защита информации в персональных ЭВМ. / Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. – М.: Радио и связь, МП «Веста», 1992. – 192 с.
6. Сяо Д., Керр Д., Мэдник С. Защита ЭВМ: Пер. с англ. – М.: Мир, 1082. – 264 с.

Поступила 10.01.2002

УДК 681.511:3

Маракова И.И, Мараков Д.А.

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ С ЦИФРОВЫМИ ВОДЯНЫМИ ЗНАКАМИ В РАМКАХ ЗАДАННЫХ ОГРАНИЧЕНИЙ

Традиционно принято считать, что криптография обеспечивает шифрование сообщений. С другой стороны, целью шифрования является обеспечение скрытия содержания секретных сообщений. Сокрытие информации (СИ) идет еще дальше, поскольку скрывает сам факт присутствия какого либо секрета. При этом секретные сообщения прячутся в не представляющих особый интерес данных, хранение и передача которых не вызывает никакого подозрения. Бурное развитие методов и средств СИ в настоящее время в частности объясняется весьма многообещающим практическим применением данного направления. СИ имеет несколько различных направлений: стеганография, водяные знаки, отпечатки пальцев, обеспечение анонимности. Предметом наших исследований являются только цифровые водяные знаки, основанные на компьютерных технологиях. В данном приложении основное сообщение должно быть соединено с другой информацией, а именно идентификатором собственника данных. Другими словами, водяные знаки - это такое направление СИ, где задача состоит не столько в сокрытии дополнительной информации, сколько в передаче с основной информации некоторой дополнительной (возможно и не секретной) информации, для которой нужно обеспечить невозможность удаления без значительного ухудшения качества основного сообщения. В работах по данной тематике, как правило, рассматривались различные способы погружения ВЗ без какой-либо теоретической оптимизации или исследования эффективности. Фундаментальные выкладки в данном направлении были сделаны в [2], где авторы описали способ сокрытия с верхними границами скоростей для надежной передачи ВЗ с точки зрения допустимого уровня искажений информации. К сожалению, это верно в асимптотике для покрывающих сообщений бесконечной длины, в то время, как на практике разработчики систем ВЗ имеют дело с основными покрывающими сообщениями конечной длины. Критерий оценки эффективности системы передачи ВЗ по вероятности пропуска ВЗ или вероятности ложного обнаружения были предложены в [3, 4]. Но в данных статьях не рассматривались все возможные случаи и прямая связь констант, характеризующих качество, с упомянутыми вероятностями.

В литературе можно найти описание различных систем с цифровыми водяными знаками, однако, их классификация и используемая терминология далеко не однозначная Будем придерживаться в этом вопросе принципы, изложенные в [1].

Система с цифровыми водяными знаками называется секретной, если при выделении дополнительной информации необходимо использование ключей. В частном случае это может быть основное покрывающее сообщение. Система с цифровыми водяными знака называется открытой или слепой, если для их выделения в декодере не нужно никаких секретных данных, т.е. все могут читать цифровые метки, но никто кроме тех, кто их создал, не могут их удалить, не испортив сообщения. Конечно, открытая система с цифровыми метками более удобна для исследований, поскольку спор об использовании чужой собственности может решиться и без участия собственника и предоставления его секретного ключа. Однако, подделка открытых систем значительно сложнее, чем секретных.

К системам с цифровыми водяными знака предъявляются следующие основные требования:

- невосприимчивость (погружение меток в основное покрывающее сообщение не должно изменять его качества выше уровня восприятия, в частности, при восприятии человеком изображения, видео, аудио он не должен чувствовать различия);
- робастность (сохранение меток при всех возможных преобразованиях стеганографического сообщения, которые не ухудшают, конечно, качества основного сообщения.
- исключение ложного обнаружения.

Часто система с ВЗ предполагает передачу одного бита причем под этим понимается специальный сигнал, определяют собственность его создателя. Однако, в общем случае (хотя под этим, обычно понимают «отпечатки пальцев») цифровые водяные могут содержать и цепочку бит, характеризующую собственника.

К основным характеристикам систем с цифровыми водяными знака относятся:

P_c - вероятность выделения цифровых водяных знаков легальным пользователем при всех преобразованиях стеганографического сообщения, осуществляемых атакующим которые для основного сообщения удовлетворяют постоянной искажений;

P_{fa} - вероятность ложного выделения цифровых меток в стеганографическом сообщении его не содержащем:

R – скорость передачи цифровых ВЗ, которая определяется как отношение числа бит ВЗ к числу бит основного сообщения, нужному для передачи ВЗ. В частном случае ВЗ может содержать лишь один бит сообщения, тогда скорость определяют числом бит сообщения, которые нужны для передачи этого бита.

Таким образом, эффективность систем с цифровыми водяными знаками описывается косвенно (прямо пропорционально P_{fa}, R, обратно пропорционально P_c).

Аналитически данные преобразования в системе с цифровыми ВЗ записываются следующим образом:

$$S = f(C, w, K)\ ,\quad S' = \Psi(S) = C'\ ,\quad w' = \varphi(S', w, C, K)\ , \tag{1.}$$

где w – код ВЗ, C – основное покрывающее сообщение, K – секретный ключ (может отсутствоваить), S – сформированное стеганографическое сообщение , S' – принятое стеганографическое сообщение. Причем, w, C, K, S, S' обычно дискретные последова- тельности, в общем случае многомерные. Конечно, более строго представить их непрерывными функциями времени, частоты или пространства, но удобнее рассматривать выборки этих функций.

Условие на невосприимчивость для кодера задается следующим уравнением

$$\rho(C, S) \le \varepsilon \tag{2}$$

где $\rho(C, S) \le \varepsilon$ - некоторая метрика скажений,

ε - шумовая реализация,

Условие на невосприимчивость декодера

$$\rho'(S,S') \le \varepsilon' \tag{3}$$

где $\rho'(S,S')$ некоторая, в частном случае совпадающая с $\rho(C,S)$ метрика искажений,

ε' - шумовая реализация на приемном конце.

Положим для простоты, что величины w, w' принимают только два значения:

- 1 в случае передачи и обнаружения ВЗ,
- 0 в случае отсутствия передачи и приема ВЗ.

Эффективность системы будем определять посредством оценки вероятности ошибок

$$P_m = 1 - P_c = P(w'=0/w=1) \tag{4}$$

Скорость передачи определяется длительностью сигнала C, необходимого для передач ВЗ. Фактически же, конечно, длина сообщения обычно бывает предварительно задана и важно, чтобы ее было достаточно для обеспечения требуемой эффективности системі с цифровыми ВЗ..

Фактически система ВЗ представляет собой своеобразную систему связи, где сообщением (битом 0 или 1) является w, помехами же, кроме помех канала распространения является C, причем, в отличие от обычной системы связи, эта помеха в точности известна на передающем конце, а также помеха в виде атак на канал, которая является случайной для кодера и декодера.

Рассмотрим простейший частный случай аддитивного кодера Линейное преобразование с дискретным временем в общем виде задается как

$$S_{K'} = \sum_{K} h_{K'K} S_K' \tag{5}$$

где $S'_{K'}$, $S_{K'}$ - последовательности на выходе и входе канала,

$h_{K'K}$- случайная функция для аргументов.

Еще более жестким атакующего канала является конкатенация линейного фильтра с постоянными параметрами и адекватного шума. Наконец, самым простым каналом атакующего является просто добавление аддитивного шума.

Задача разработчика системы ВЗ сигнала, обычно, состоит в том, чтобы разработать такой ВЗ кодер и декодер, которые при заданной вероятности P_{fa} минимизировали бы P_m при самой худшей атаке, удовлетворяющей условию (2).

С другой стороны, задача атакующего состоит в том, чтобы при известных кодере и декодере (с точностью до знания ключей) создать такой атакующий канал, чтобы ухудшить, насколько можно, характеристики системы ВЗ.

Рассмотрим следующую модель ВЗ и атакующего канала. Покрывающее сообщение

представляет собой прямоугольную картинку, состоящую из $n_1 n_2$ пикселей, каждый из которых имеет шкалу яркостей, принимающих вещественное значение на определенном интервале. Само изображение для кодера является детерминированным, а для канала атаки оно может характеризоваться некоторой статистикой, например, гауссовой и некоторыми пространственными корреляционными функциями.

Стеганографический сигнал строятся аддитивным образом, т.е. как

$$S(w) = C + w = C(\bar{n}) + w(\bar{n}'), \tag{6}$$

где $\bar{n} = (n_1 n_2)$, $\bar{n} \in A_N$, $w(\bar{n}) \in I$

Атакующий канал заключает в себе пространственную фильтрацию S и добавление аддитивного шума, т.е.

$$S'(\bar{n}) = \sum_{AN} S(\bar{n}) h(\bar{n}' - \bar{n}) + \varepsilon(\bar{n}) \tag{7}$$

где $h(\bar{n}'-n)$ – некоторая детерминированная функция, определяющая временной

отклик фильтра,

$\varepsilon(\bar{n})$ - случайный аддитивный шум с некоторым вероятностным распределением.

Кодер последовательности $w(\bar{n})$ должен быть выбран таким образом, чтобы выполнялось условие на верность воспроизведения в квадратичной метрике

$$\|C - w\| = \sqrt{\sum_{n \in A_N} w^2(\bar{n})} \le \rho \qquad (.8)$$

Атакующий канал должен удовлетворять ограничениям по верности также в квадратичной метрике, т.е.

$$\|S - C\| = \sqrt{E\ (\sum_{n \in A_N} S'(\bar{n}) - C(\bar{n})^2} \le \rho' \qquad (.9)$$

Таким образом, задача разработчика системы ВЗ состоит в том, чтобы для модели и ограничений обеспечить при заданной P_{fa} минимальную величину P_m, имея в виду любые фильтры, преобразования и любые адаптивные шумы, но, конечно, удовлетворяло условию (9). Задача же атакующего – прямо противоположная. Обеспечить максимум P_m при заданной величине P_{fa}, за счет оптимизации фильтрации и аддитивного шума, предполагая, что декодер ВЗ будет оптимальным, и конечно выполнено ограничение (8), (9).

Требуется выполнить оптимизацию (с точки зрения разработчика) формы $w(\bar{n})$, оптимальные параметры $\varepsilon(\bar{n})$ и рассчитать вероятности ошибок P_m, P_{fa}.

Для получения количественных оценок необходимо получить аналитические выражения для P_m, P_{fa}. Для этого необходимо определить конкретные условия работы системы, в частности, с точки зрения использования или нет основного покрывающего сообщения кодером и декодером.

Рассмотрим случай, когда $C(\bar{n})$ не используется кодером, но известно декодеру.

В этом случае $w(\bar{n})$ разумно выбрать как $w(\bar{n}) = \pm\alpha$, где $\pm$ выбирается случайным образом и взаимно независимо для всех $\bar{n} \in A_N$. Такой выбор обеспечит невозможность для атакующего предсказать $w(\bar{n})$ и следовательно убрать его. С другой стороны, обеспечит выполнение условия

$$1/N \sum_{n \in A_N} E(w^2/\bar{n})) \le \rho, \qquad (10)$$

если параметр α удовлетворяет неравенству $\alpha^2 \le \rho$

В этом случае декодер (приемник) для выделения $w(\bar{n})$, очевидно, разумно (при неизвестно статистике шума атаки) построить по следующему правилу

$$\Lambda \subset ((S'(\bar{n}) - C(\bar{n}), w(\bar{n})) \ge \lambda \text{ , есть ВЗ,}$$

$$\Lambda \subset ((S'(\bar{n}) - C(\bar{n}), w(\bar{n})) < \lambda \text{ , нет ВЗ} \qquad (11)$$

Очевидно, что если в действительности ВЗ передан, тб скалярное произведение в левой части (10) будет иметь вид

$$\Lambda_1 = (w(\bar{n}) + \varepsilon(\bar{n}), w(\bar{n})) = N\alpha^2 + \sum_{\bar{n} \in A_N} \varepsilon(\bar{n}) w(\bar{n}) \qquad (12)$$

Если же ВЗ не передавался, то это скалярное произведение будет иметь вид

$$\Lambda_0 = f(\varepsilon(\bar{n}), w(\dot{n})) = \sum_{\bar{n} \in A_N} \varepsilon(\bar{n}) w(\bar{n}) \qquad (13)$$

Поскольку все $w(\bar{n})$ выбираются равновероятно, т.е. случайно и независимо, то можно положить, что обе суммы будут распределены по гауссовому закону, независимо от того, какой закон распределения выбран для $\varepsilon(\bar{n})$, причем

$$E(\Lambda_1) = N, \quad \alpha^2 \le m \ , \ E(\Lambda_0) = 0 \tag{14}$$

Дисперсии (вариации) Λ_1, Λ_2 будут в обоих случаях равными

$$\text{var}\,\Lambda_1 = \text{var}\,\Lambda_0 = E((\sum_{\bar{n}\in A_N} \varepsilon(\bar{n})w(\bar{n}))^2) = \sum_{\bar{n}\in A_N} E(\varepsilon^2(\bar{n}))E(w^2(\bar{n})) \ge \alpha^2 \sum_{\bar{n}\in A_N} E(\varepsilon^2(\bar{n})) \tag{15}$$

где учитывается взаимную независимость $w(\bar{n})$ и $\varepsilon(\bar{n}')$.

Отметим, что даже если здесь помеха $\varepsilon(\bar{n})$ является зависимой, то все равно, из-за независимости $w(\bar{n})$ вариация остается похожей и, таким образом, в этом случае нет смысла при атаке создавать неравномерную помеху.

Разумно предположить, что при атаке все помеховые компоненты $\varepsilon(\bar{n})$ будут выражены с одинаковой дисперсией, и тогда

$$\text{var}\,\Lambda_1 = \text{var}\,\Lambda_0 = \alpha^2 N \delta^2 \tag{16}$$

где δ^2 - дисперсия каждой из компонент помехи.

С другой стороны, ограничение (14) для независимых ВЗ и помехи атаки, примет вид

$$\alpha^2 + \delta^2 \le \rho' \ (17)$$

В лучшем случае для атакующего мы получаем равенство (16) и тогда, подставляя δ^2 из (16) в (15) и учитывая, что в лучшем для разработчика системы ВЗ случай $\alpha = \rho$, мы окончательно получим

$$\text{var}\ \ \Lambda_1 = \text{var}\ \ \Lambda_0 = \rho N(\rho' - \rho) \le \quad \delta^2 \tag{18}$$

Имея в виду гауссово распределение Λ_0 и Λ_1, а также условие (13), где $\alpha^2 = \rho$, и подставим δ мы получим следующее выражение для вероятностей пропуска цифровіх ВЗ и ложного обнаружения ВЗ.

$$P_m = 1 \ - Q(\frac{\lambda - N\rho}{\sqrt{\rho N(\rho' - \rho)}}) \ = 1 \ - Q \ ((\lambda_0 - \rho)\sqrt{\frac{N}{\rho(\rho' - \rho)}}) \tag{19}$$

$$P_{fa} = \frac{1}{\sqrt{2\pi\delta^2}} \int_{\lambda}^{\infty} e^{-\frac{x^2}{2\delta^2}} dx = \frac{1}{\sqrt{2\pi}} \int_{\frac{\lambda}{\delta}}^{\infty} e^{-\frac{t^2}{2}} dt = 1 \ - Q(\frac{\lambda}{\delta}) \ = Q(\ \lambda_0 \sqrt{\frac{N}{\rho(\rho' - \rho)}}) \tag{20}$$

где принято $Q(x) \ = \frac{1}{\sqrt{2\pi}} \int_{x}^{\infty} e^{-\frac{t^2}{2}} dt \ge 0$

x – дискрет реализации,

λ - порог, $\lambda \ = \lambda_0 N$,

m – среднее реализации $\lambda \ = \lambda_0 N$,

Здесь проявляется еще одно интересное обстоятельство. Из выражений (19), (20) видно, что чем больше ρ', тем хуже ситуация для разработчика системы ВЗ. При $\rho' \to \infty$ мы получаем P_m=P_{fa}=0.5, т.е. полную невозможность обнаружения. Это

вполне естественно, поскольку тогда помеху атаки не накладывается никаких ограничений и, следовательно, оно полностью подавляет обнаружение ВЗ.

Однако, слишком близкую величину ρ' брать нельзя. Вполне естественно задать ρ' исходя из ограничений на отношение сигнал/шум, но относительно к созданным помехам. Пусть среднеквадратичное значение ОПС равно δ_S^2, которое может быть средним значением мощности сигнала. Если задано отношение сигнал/шум $\frac{\delta_S^2}{\rho'} = \eta$, где δ_S^2 - среднеквадратическое значение основного покрывающего сообщения, и данное отношение обеспечивает требуемое качество изображения, то найдем отсюда $\rho' = \rho_0' = \frac{\delta_S^2}{\eta}$ и (19), (20) можно представить в виде

$$P_m = 1 - Q\left((\lambda_0 - \rho)\sqrt{\frac{N}{\rho\left(\frac{\delta_S^2}{\eta} - \rho'\right)}}\right) = 1 - Q\left(\left(\frac{\lambda_0}{\rho} - 1\right)\sqrt{\frac{N\eta}{\eta' - \eta}}\right) \quad (21)$$

$$P_{fa} = Q(\lambda_0)\sqrt{\frac{N}{\rho\left(\frac{\delta_S^2}{\eta} - \rho\right)}} = Q\left(\frac{\lambda_0}{\rho}\right)\sqrt{\frac{N\eta}{\eta' - \eta}} \quad (22)$$

где введено дополнительное обозначение $\eta = \frac{\delta_S^2}{\rho}$ - отношение сигнал/шум для ВЗ:

$\lambda'_0 = \frac{\lambda_0}{\delta_S^2}$ - нормированный порог при $\lambda_0 = \frac{\lambda}{N}$

Обсудим полученные результаты .

Характеризующие эффективность системы с ВЗ для рассматриваемого случая вероятности P_m и P_{fa} зависят только от N, η', η при выбранном $\frac{\lambda_0}{\rho}$. где η', η - допустимые отношения сигнал/шум для ВЗ и канала атаки, причем всегда .. Если $\eta' \to \eta$, т.е. требование по искажениям в канале атаке приближаются к требованиям по искажениям при формировании ВЗ, то при правильном выборе порога, когда $\frac{\lambda_0}{\rho}$ - 1 <0 или η, вероятности P_m и P_{fa} стремятся к нулю, т.е. обеспечивается идеальное обнаружение ВЗ.

Представляется реальным выбрать $\eta' > \eta$, поскольку η выбирается с запасом (чтобы практически не искажать покрывающее сообщение). Практически, можно на основании заключений экспертов задать η (например 30...50 дБ), а затем по заданному N и оптимальному правилу и заданным P_m и P_{fa} рассчитать максимально допустимую величину η, при которой эта характеристика обеспечивается и если она недопустима мала, то это и будет означать, что разработанная система ВЗ эффективна.

С другой стороны, из соотношения (21), (22) следует, что любые заданные

вероятности P_m и P_{fa} могут быть обеспечены при любых η , $\eta' > \eta$, $\eta > 0$ (и, конечно, правильном выборе порога) если $N \to \infty$, т.е. снижении параметров ВЗ.

Поскольку приемник ВЗ не знает уровня шума, использованного при атаке, то он должен быть робастным, т.е. обеспечивать при некотором фиксированном пороге $\frac{\lambda_0}{\rho}$ требуемые вероятности P_m и P_{fa} при любых $\eta > \eta_0$ (конечно, до предела, при котором происходит недопустимые потери качества сообщений)

И наконец, если $\eta \to 0$, т.е. $\frac{\delta_S^2}{\rho'} \to 0$ (допустимы любые искажения атакой), то P_m и P_{fa} становятся равными 0.5, т.е. система ВЗ перестает существовать

Представляется интересным применить предложенную методику для случав с менее жесткими ограничениями, получить соответствующие аналитические выражения, выполнить количественную оценку для различных вариантов построения систем с цифровыми ВЗ..

Список литературы:

1. S.Katzenbeisser, F.Petiticolas "Information Hiding", Artech HouseInc., 2000
2. P.Moulin, J.O'Sullivan, "Information Theoretic Analysis of Information Hiding", Proc. IEEE Symp. on IT'1998
3. J.Linnartz, T.Klaker, G.Deprovere "Modeling the False Alarm and Missed Defection rate for Electronic Watermarks", Second Intern. Workshop, IH'98/LNCS, N1525, p.p.329-343
4. R.Sugihara, "Practical Capacity of Digital Watermarks", Forth Information Hiding Workshop, LNCS N, p.p.329-342

Поступила 20.01.2002