

Реконфигурируемая стеганографическая система с двухступенчатой скрытой аутентификацией

77-48211/422996

07, июль 2012

Багдасарян Т. А., Хачатуров А. Г.

УДК.00004

Армения, Государственный Инженерный Университет Армении (ГИУА)

tatbagg@gmail.com

Введение

На сегодняшний день в связи с широким распространением Интернета и ряда других технологий растет угроза потери, компрометации и целенаправленных атак на данные, которые должны оставаться закрытыми, находясь в сети и, в частности, в Интернете. Стеганография является одним из наиболее эффективных средств защиты цифровой информации. Стеганография – наука, связанная с созданием математических методов и средств защиты информации. Вопрос безопасности – важная часть концепции внедрения новых информационных технологий во все сферы жизни общества. Поэтому широкомасштабное использование вычислительной техники и телекоммуникационных систем приводит к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, т.е. к их высокой уязвимости. Таким образом, обеспечение целостности, достоверности и доступности информации – важные составные успеха деятельности любой организации. Формула успеха любой деятельности гласит [1]: кто владеет достоверной и полной информацией – тот владеет ситуацией, кто владеет ситуацией – тот способен управлять ею в своих интересах, кто способен управлять – тот способен побеждать. Эффективность механизмов защиты информации в значительной степени зависит от ряда принципов. Во-первых, механизмы защиты следует проектировать одновременно с разработкой информационной системы, что позволяет обеспечить их бесконфликтность, своевременную интеграцию в вычислительную среду и сокращение затрат. Во-вторых, вопросы защиты следует рассматривать комплексно в рамках единой системы защиты информации. [2]

Этимология слова «стеганография» берет свое начало в далеком прошлом. В переводе с греческого «стеганография» означает «тайнопись» (steganos – секрет, тайна; graphy – запись). История стеганографии уходит в глубокую древность, так, в частности, одной из первых книг, содержащих описание стеганографических систем, является «Steganographia», написанная Тритемием в 1499 году.

Основоположником современной компьютерной стеганографии можно считать американского математика Густава Симмонса, который первый стал использовать математические модели для проведения доказательства свойств стеганографических систем [3, 4].

Стеганография, так же как когда-то и криптография, превращается постепенно из технического искусства в отдельную область научных исследований и постепенно приобретает статус самостоятельной прикладной науки, изучающей способы и методы сокрытия секретных сообщений. Стеганография является одним из направлений достаточно широкой области исследований, в которой изучаются способы защиты информации. Строго говоря, стеганография изучает способы, с помощью которых производится *сокрытие самого факта передачи информации*.

Развиваясь параллельно с компьютерными технологиями, в настоящее время на базе математического аппарата компьютерная стеганография (КС) используется в различных программно-информационных комплексных системах, предназначенных для решения задач по обеспечению защиты данных. Наибольший интерес вызывают:

- антитеррористические аспекты применения КС;
- использование КС при проектировании депозитариев в промышленных информационных системах (так называемых стегодепозитариев);
- охрана служебной и коммерческой информации (в частности, банковских данных) посредством КС;
- защита документов и авторских прав с помощью специализированных КС-систем.

Современные стеганографические системы позволяют скрывать секретную информацию в изображениях или иных цифровых объектах, которые могут находиться на локальном компьютере, в локальной сети или Интернете. Интернет можно рассматривать как наиболее подходящую среду для скрытого хранения (и передачи) секретной информации.

Данные в Интернете могут скрываться на основе трех основных идей:

- обычной электронной почты
- публичной веб-страницы
- общей бесплатной онлайн электронной почты.

В первом случае отправитель может скрыть секретные данные в несущем файле (контейнере). Контейнером могут послужить фото, аудио или видео файлы различного типа (jpg, bmp, mp3, wav, mpeg, avi). Отправитель, используя стеганографическую систему, может спрятать данные в один из контейнеров и отправить письмо по электронной почте с прикрепленным стеганографическим файлом. Получатель, в свою очередь, используя ту же стеганографическую систему, может извлечь скрытые данные из контейнера. Во втором случае отправитель не посылает письмо с файлом, а просто используя возможности публичных веб-страниц, выставляет контейнер файл на одной из таких страниц. В данном случае имеет место свободный доступ к стеганографическому файлу, что может упростить действия противника. В последнем случае отправитель и получатель имеют общий почтовый ящик на одном из серверов бесплатной онлайн электронной почты. При этом отправитель может оставить в папке черновиков почтового ящика сообщение с приложенным стеганографическим файлом, который может забрать получатель и извлечь скрытые данные.

Во всех случаях, если отправитель и получатель совпадают, можно говорить просто о скрытом хранении секретной информации в Интернете.

В качестве основного недостатка подобного хранения или передачи секретной информации нужно отметить риск повреждения или удаления стеганографических файлов вследствие целенаправленного воздействия противника или “естественных” причин, таких как закрытие или реорганизация соответствующих веб-страниц (почтовых ящиков) и др.

Одним из подходов к решению указанных проблем могут являться реконфигурируемые стеганографические системы. Основная идея реконфигурируемой стеганографической системы состоит в следующем. Скрываемая информация разделяется между N контейнерами с использованием в качестве параметра разделения псевдослучайного значения. Далее с определенной периодичностью восстанавливается скрытая информация на основе M неизменных контейнеров, причем $M \leq N$, и вновь осуществляется разделенное сокрытие. Иными словами производится периодическое обновление скрываемой информации. Важно отметить, что использование при разделении псевдослучайного значения приводят к тому, что новые составляющие секрета отличаются от предыдущих (до обновления). Таким образом, добытые противником составляющие после обновления перестают быть полезными для продолжения атаки на стеганографическую систему. Безопасность системы будет нарушена только в случае, если в промежутке между обновлениями противнику удастся захватить не менее M контейнеров и извлечь из них скрытые данные.

Такой подход может значительно повысить защищенность по отношению к большинству возможных атак на стеганографическую систему за счет того, что скрытые в отдельном контейнере данные представляют собой бессмысленный набор символов.

Работа реконфигурируемых стеганографических систем основывается на периодическом обновлении скрываемой информации или, иными словами, самовосстановлении системы безопасности. В случае стеганографии основная идея подобного самовосстановления заключается в периодическом пересокрытии секретных данных. Таким образом, не только обновляются скрываемые данные, но и “старые секреты” (т.е. секреты до обновления) делаются бесполезными для противника. В результате противник теряет контроль над ситуацией или становится вынужденным проявлять постоянную активность, рискуя быть выявленными соответствующими средствами обнаружения вторжений.

Для успешного функционирования стеганографической системы построенной на основе приведенных принципов реконфигурации необходимо иметь адекватные средства определения неизменных контейнеров. При этом очевидно, что система не должна ожидать пока определенное количество контейнеров будут изменены или удалены, а должна с заданной периодичностью производить самовосстановление независимо от активности противника.

Подобная реконфигурируемая стеганографическая система за счет обоснованного выбора периода самовосстановления может, по крайней мере теоретически, обеспечить сколь угодно долгое безопасное сокрытие секретной информации. Исходя из вышеизложенного, целью данной работы является исследование и разработка принципов проектирования реконфигурируемой стеганографической системы (РСС), призванной

обеспечить высокую степень защиты и долговременное хранение информации. Для достижения указанной цели в работе ставятся и решаются следующие основные задачи:

- исследовать и разработать принципы проектирования РСС, позволяющие существенно увеличить защищенность и время хранения данных;
- исследовать и разработать методы разделения информации, позволяющие распределенное хранение данных в локальных и глобальных сетях в частности в Интернете;
- исследовать и разработать механизм получения новых частей разделенного секрета, без восстановления самого секрета.

Структура системы хранения данных

На Рис.1 представлена структура системы хранения данных, с использованием распределенной стеганографии.

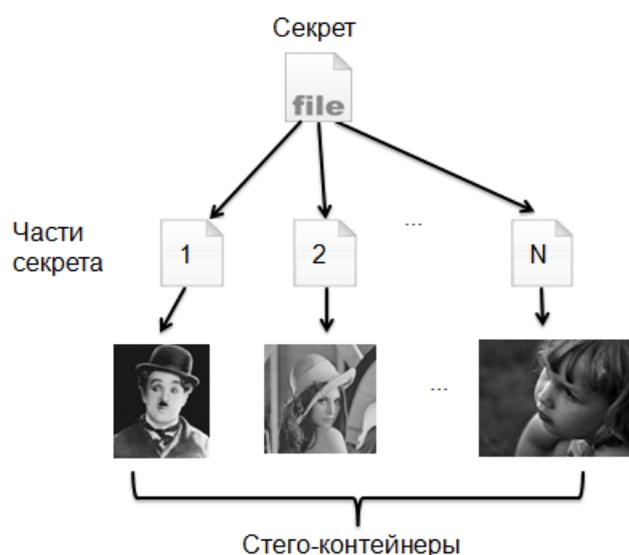


Рис. 1. Структура системы хранения данных

Алгоритм распределения секрета

Для разделения секрета необходимо использовать алгоритм, который позволяет однозначно восстанавливать информацию при наличии определенного количества носителей частей секрета. Этим требованиям соответствует пороговая схема Шамира [5] основанная на интерполяционном многочлене Лагранжа.

Интерполяция Лагранжа позволяет вычислить однозначно определенную кривую, которая проходит по заданной системе точек. Используя данное свойство интерполяции можно воссоздать разделенный секрет при участии определенного количества разделенных частей.

В качестве секрета в данной работе будут представлены обычные числа. Скрываемую информацию можно раздробить на части таким образом, что размер каждой новой части

будет такого размера, на которые можно применить алгоритм разделения секрета. Существует граница размера скрываемой информации (условно обозначим H) при большем размере скрываемой информации, чем H , потребуется большое количество вычислительных ресурсов.

Определение. Пусть $t;w$ – целые положительные числа, причем $t \leq w$. $(t;w)$ -пороговой схемой разделения секрета называется метод разделения секрета S между w участниками (обозначим их через P) так, что любые t участников могут вычислить значение S , но никакая группа из $t-1$ или менее участников сделать этого не может. Ниже на рисунке 2 представлена $(3;w)$ -пороговая схема с тремя или более участниками. В данном случае, $(3;4)$ -пороговая схема.

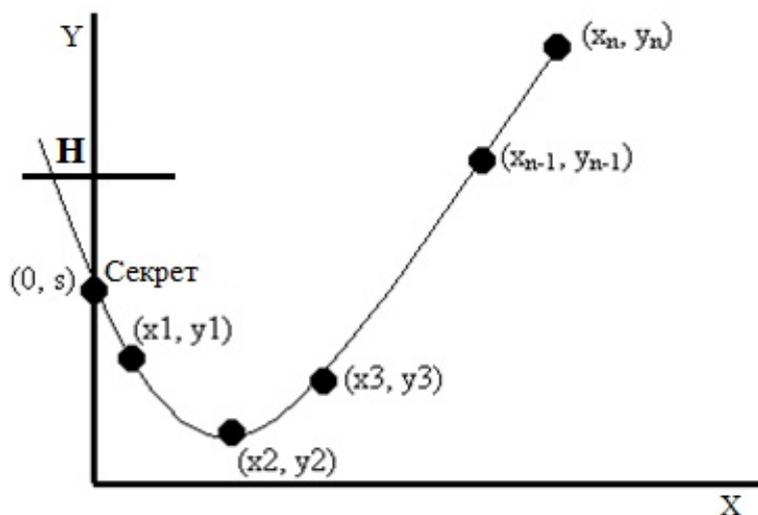


Рис.2.Пример функции

Функция $f(x) = ax^2 + bx + s$, заданная полиномом, представляет собой на графике параболу, легко восстанавливаемую по трем точкам. Поэтому нам необходимо минимум три точки для восстановления секрета S , представленного свободным членом s , являющимся на графике точкой пересечения параболы с осью Y , т.е. $f(0) = s$. Для создания w частей секрета необходимо произвольным образом выбрать w точек на параболе. Можно создать схемы с любым нужным нам значением t , используя функцию, заданную полиномом степени $(t-1)$. В данном случае каждому i -ому хранителю части секрета выдаются координаты x_i, y_i , а секретом является свободный член s .

Рассмотрим пример информационного поля из n участников, характеристика этого поля - F_p и $p > n$. Секрет S распределяется между n участниками. Для восстановления секрета S необходимо присутствие выбранного количество частей ($m+1$ частей).

Распределение секрета S между n участниками

Каждый из участников получает элемент из заданного поля $x \in F_p, i = [1, \dots, n]$. Диллер выбирает случайные элементы a_j из поля F_p , где $j = [0, \dots, m]$ и количество частей, которые необходимы для восстановления секрета, равно $m + 1$, где $1 \leq m < n$. Составим многочлен

$$f(x) = \sum_{j=0}^m a_j x^j$$

Предположим секрет $S = f(0) = a_0$. Для элементов x_i вычислим значение многочлена $f(x)$, $S_1 = f(x_1), \dots, S_n = f(x_n)$, каждый из участников получает пару чисел $(x_i, S_i), i = [1, \dots, n]$.

Восстановление секрета

Для восстановления секрета S необходимо участие любых частей в количестве $m+1$. Используя интерполяционный многочлен Лагранжа, получится

$$L_n(x) = \sum_{i=0}^n y_i \prod_{i \neq k} \frac{x - x_k}{x_i - x_k}; \quad f(x) = \sum_{j=0}^m S_j \prod_{j \neq k} \frac{x - x_k}{x_j - x_k};$$

Восстановим секрет

$$S = f(x_0) = f(0) = \sum_{j=0}^m S_j c_j, \text{ где } c_j = (-1)^m \prod_{j \neq k} \frac{x_k}{x_j - x_k}.$$

Таким образом, применив этот метод для разделения секрета, однозначно можно сказать, что при участии определенного количества частей, возможно, однозначно восстановить секрет.

Выбор, в качестве алгоритма разделения секрета схемы Шамира, обусловлен следующими причинами:

- Совершенная безопасность (Perfect Security) [5] – информационная теоретическая безопасность. При наличии t частей секрета возможно единственным образом восстановить S . Зная $t-1$ или менее частей секрета и диапазон $0 \leq S < m - 1$, восстановление секрета остается сложной задачей.

- Идеальная (Ideal) [5] – размер (битовый размер) секрета совпадает с размером каждой из составляющих частей секрета

- Независимая(Independent) - в отличие от многих криптографических схем, безопасность схемы разделения информации напрямую не зависит от сложности информации.

- Свойство гомоморфизма (Homomorphic property) [5] – для схемы Шамира имеет место (+, +) гомоморфизм. Например, предположим, что есть два секрета S и R. Они зашифрованы по схеме разделения секретов Шамира: $(f(1), \dots, f(n))$, определенные из полинома $f(x)$ $(g(1), \dots, g(n))$ – из полинома $g(x)$ для S и R соответственно. Допустим, каждый i-ты участник протокола просуммирует: $h(i) = f(i) + g(i)$ ($i = [1, \dots, n]$). Каждая из полученных сумм в свою очередь является частью секрета S+R, определяемого из полинома $h(x) = f(x) + g(x)$ и $h(0) = S + R$.

В результате разработана система, которая позволяет распределять и хранить данные в локальных и глобальных сетях в частности в столь популярной сети Интернете. Так как, Интернет является открытой сетью, нельзя с уверенностью утверждать, что данные хранящиеся в сети защищены, даже в случае если используется стеганография.

Для повышения безопасности разработанной системы, в системе предусмотрены 3 необходимых модуля:

- модуль проверки истинности частей разделяемого секрета
- модуль восстановления потерянных частей разделенного секрета, без восстановления самого секрета
- модуль полного обновления частей секрета, без восстановления самого секрета.

Проверка истинности частей разделенного секрета

Как и в других криптографических системах, так и в системах разделения секрета участники не доверяют друг другу и каждый из них, как и сам дилер, может оказаться противником. Стойкость систем, основанных на распределении секрета, также основывается на безопасной передаче частей секрета. Для обеспечения стойкости разработанной системы используется алгоритм проверки подлинности частей секрета, с которым каждый участник может проверить подлинность выданной ему части секрета. Алгоритм основывается на следующих действиях

1. Как известно в схеме Шамира дилер выбирает любой многочлен степени t, где $S = a_0$, $Q(x) = a_0 + a_1x + a_2x^2 + \dots + a_tx^t$
2. Выбираются любые простые числа p и q, таким образом, что $p = 2q + 1$, эти числа не секретны и публикуются
3. Выбирается число g так, что $g^q \bmod p = 1$
4. Дилер вычисляет $r_i = g^a \pmod p, i = 0, \dots, t$ и публикует число r_0, r_1, \dots, r_t .
5. Дилер для любых чисел $j=1, \dots, n$ вычисляет значения частей секрета $S_j = Q(j)$ и

по закрытому каналу передает участникам части секрета.

6. Каждый из участников проверяет следующее уравнение

$$g^{S_j} = r_0 \cdot (r_1)^j \cdot \dots \cdot (r_t)^{j^t} \pmod p,$$

для того чтобы убедиться, что его часть действительно является частью секрета. И действительно имеет место следующее равенство

$$r_0 \cdot (r_1)^j \cdot \dots \cdot (r_t)^{j^t} = g^{a_0} \cdot g^{a_1 j} \cdot \dots \cdot g^{a_0 + a_1 j + \dots + a_t j^t} = g^{Q(j)} \pmod{p}$$

Модуль получения новых частей секрета без восстановления самого секрета

Цель данного модуля состоит в том, что пользователям предоставляется возможность обновить части секрета без участия диллера и восстановления самого секрета. Без восстановления секрета, участники согласовываясь получают новые части секрета, не изменяя секрета, т.е. оставив свободный член многочлена неизменным. Одно из условий схемы восстановления частей является необходимость сохранения у каждого участника имеющиеся на данный момент части разделенного секрета.

Секрет S разделяется между n участниками. Любые t части способны воссоздать секрет S . Необходимо получить многочлен $f(x)$ степени $t-1$. Данная схема основывается на следующих действиях:

1. Каждый i -тый ($i \in [1..n]$) участник произвольно, из конечного поля F_p выбирает коэффициенты в количестве $t-1$ и произвольно получает многочлен $P_i(x)$, чей свободный член равен 0.
2. На основе полученного многочлена $P_i(x)$ каждый участник для всех участников, в том числе и для себя самого, вычисляет новые координаты
3. Каждый i -тый участник ($i \in [1..n]$) получает следующие координаты $P_1(i), \dots, P_n(i)$
4. Каждый i -тый участник, получив от других участников координаты, суммирует их к своей старой части и получает новую часть секрета. Как уже было сказано, схема Шамира обладает гомоморфизмом

$$E(x * y) = E(x) \oplus E(y), E(x * y) = E(x) \otimes E(y),$$

5. Каждый i -тый участник удаляет старую часть секрета.

Схема восстановления потерянных частей.

Возможно такая ситуация, что со стороны активного противника файл носитель был изменен или удален с целью нарушения работоспособности системы. Или представим такую ситуацию, что один из хранителей частей секрета (предположим, участник под номер r), как это ни банально, потерял свою часть. На первый взгляд простым решением данной проблемы является следующая схема: восстановить секрет с имеющимися частями, а затем заново разделить. Это не является целесообразным решением. Для таких случаев в системе также предусмотрен модуль, который помогает восстановить потерянную часть секрета без восстановления самого секрета. Работа данной схемы заключается в следующем:

1. Каждый i -тый участник (кроме r) из конечного поля произвольно выбирает $t-1$ коэффициентов и получает многочлен $P_i(x)$, чей свободный член не равен 0
 $P_i(r) = 0 \wedge P_i(0) \neq 0, i \in [1..r-1], [r+1, \dots, n]$

2. На основе полученного многочлена $P_i(x)$, каждый участник вычисляет новые части для остальных участников за исключением участника g
3. Каждый i -тый участник, получив части от остальных (за исключением участника g) прибавляет свою старую часть и получает новую часть для g -ого участника

$$h(i) = f(i) + \sum_{c=1}^{r-1} P_c(i) + \sum_{k=r+1}^n P_k(i)$$

g -й участник получив части для восстановления нового многочлена восстанавливает его.

Скрытая аутентификация пользователя в реконфигурируемой стеганографической системе

Ключевой особенностью стеганографических систем является скрытый канал передачи данных, и естественно, что использование стеганографии не должно афишироваться. Следовательно, стеганографическая система нуждается в прикрытии. В качестве прикрытия предлагается использовать графический редактор со стандартным набором операций. Для обеспечения скрытности стегосистемы предлагается как минимум два шага аутентификации. На первом шаге используется относительно простая поведенческая аутентификация. Второй шаг: предлагается более сложная аутентификация на основе графических паролей.

Скрытая поведенческая аутентификация пользователя – это последовательность стандартных операций, порожденная пользователем традиционной системы прикрытия стеганографической системы (в нашем случае – графический редактор). В роли ключа выступает представленная структура.

$$D = \langle d_{j_1}, d_{j_2}, \dots, d_{j_k} \rangle, \text{ где } d_{j_r} \in \{d_i(a_{i_1}, a_{i_2}, \dots, a_{i_n}), d^*, d^m\}$$

$d_i(a_{i_1}, a_{i_2}, \dots, a_{i_n})$ - элементарная операция в графическом редакторе.

d^* - начальная операция стеганографического ключа.

d^m - конечная операция стеганографического ключа.

То есть, совершая конкретно изначально заданные действия в графическом редакторе, пользователь скрытым образом проходит первую ступень аутентификации. На рисунке 3 показана внешняя оболочка реконфигурируемой стеганосистемы – графический редактор.



Рис. 3 Графический редактор

После успешного прохождения первого шага пользователю предлагается пройти аутентификацию на основе графических паролей. Главная идея графических паролей основывается на том, что в большинстве своем люди лучше запоминают образы или изображения, нежели искусственные слова (сложные алфавитно-цифровые пароли). Визуальный или образный объект предлагает значительно более широкий спектр применимых паролей. В качестве пароля пользователь выбирает последовательность точек на рисунке. Это приводит к огромному количеству возможностей, если рисунок сложный, и если у него высокое разрешение. Для того чтобы пройти аутентификацию, пользователь должен щелкнуть по выбранным точкам, в соответствующей последовательности. Так как практически невозможно щелкать несколько раз повторно на одной и той же точке, в схеме предусмотрен коэффициент допустимости ошибки r в местах щелчков мышью (например диск с радиусом r). Это делается посредством дискретизации местоположений щелчков [8], используя три разные квадратные решетки. У каждой решетки ширина между решеточными линиями (горизонтальными или вертикальными) составляет br . Каждая из трех решеток находится в шахматном расположении по отношению к предыдущей решетке, с расстоянием $2r$ вертикально и $2r$ горизонтально. На рисунке 4 показана часть такой решетки [8].

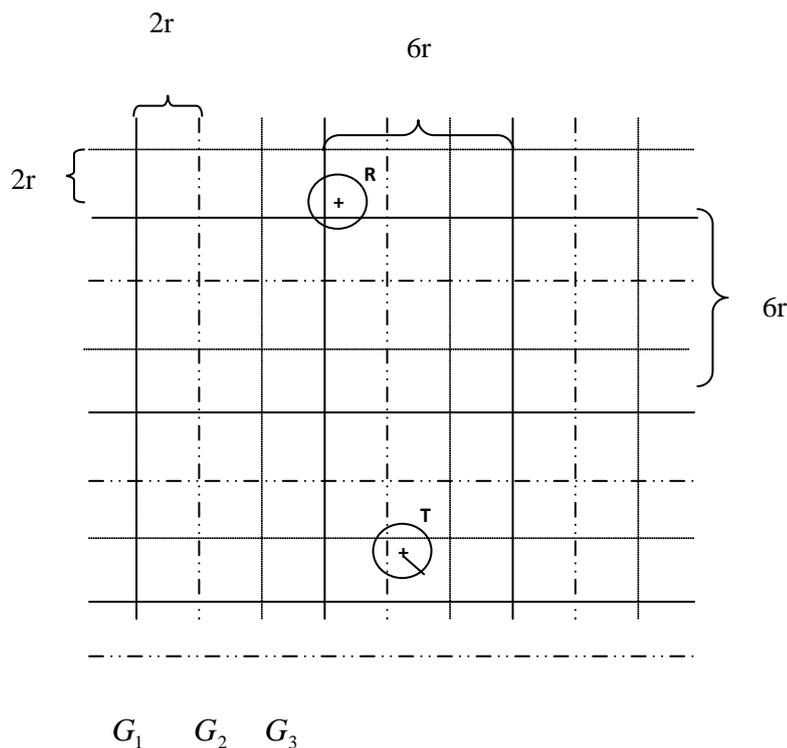


Рис. 4. Три решетки G_1 , G_2 , и G_3 . Точка T находится в G_1 ; R находится в G_2 и в G_3

Последовательность выбранных точек представляется последовательностью решеток и решеточных квадратов, т.е. для каждого щелчка вычисляется значение G_1, G_2 и G_3 . При выборе пяти точек на изображении в качестве пароля вычисляется следующая строка (пример):

$G_1(2,3) G_2(-5,-2) G_3(1,2) G_1(-2,-2) G_2(1,1) G_3(3,2) G_1(5,2) G_2(1,1) G_3(-6,-1) G_1(4,2) G_2(10,6)$
 $G_3(-2,-52) G_1(8,2) G_2(11,3) G_3(7,8)$ и на основе этой строки вычисляется ее хеш значение

(a37c779d77b10a41b471d3156181b093), которое записывается в базу данных для дальнейшей проверки. При наличии изображения с большим расширением, количество возможных паролей достаточно велико, и атаки типа полный перебор требуют определенных ресурсов.

Одним из главных атрибутов предлагаемого метода является тот факт, что лежащие в основе пароля изображения не ограничены определенными рисунками. В качестве изображения могут быть использованы комплексные изображения из реального мира, а также сами пользователи могут вводить изображения на свой выбор.

На рисунке 5 показана полная модель системы.

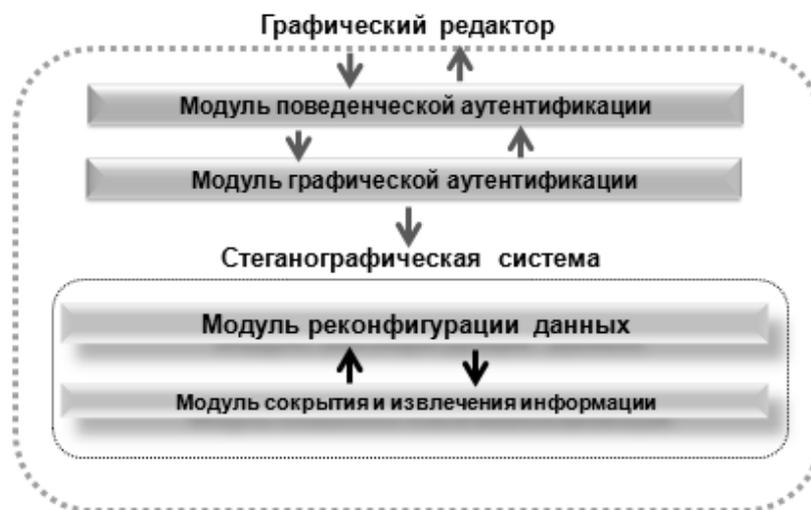


Рис. 5 Полная модель системы

Заключение

Таким образом, предлагаемый новый подход к проектированию стеганографической системы, позволяет создавать скрытое пространство в Интернете для безопасного и длительного хранения данных. Система основывается на трех основных методах – реконфигурируемая стеганография, средство восстановления потерянных частей секрета, перераспределение частей разделенного секрета, проверка подлинности частей секрета. Такая система призвана для обеспечения большой степени защищенности и длительного хранения данных. Наличие двух условий: достоверность частей и периодическое перераспределение новых частей достаточны, чтобы гарантировать, что новые файлы носители хранят достоверные части секрета и система остается работоспособной долгое время. Для обеспечения скрытого использования реконфигурируемой стеганографической системы предусмотрена двухступенчатая система аутентификации, скрытая под графическим редактором.

В дальнейшем предусматривается, что система будет функционировать в качестве web-сервиса и, как результат, может быть доступна в любом месте, где имеется выход в Сеть. И, естественно, предполагается обеспечить доступность для мобильных устройств (смартфоны, КПК и т.д.).

Литература

1. Столингс, Вильям. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ.-М.: Издательский дом «Вильямс», 2001.-672 с.: ил.
2. Р.Р. Хамидулин, И.А. Бригаднов, А.В. Морозов. Методы и средства защиты компьютерной информации. Учеб. Пособие. – СПб: СЗТУ, 2005.- 178 с.
3. Simmons G.J. An introduction to shared secret and/or shared control schemes and their application, Contemporary Cryptology // In: The Science of Information Integrity (Gustavus J. Simmons, Ed.). — IEEE Press, 1991. P. 441-497.
4. Simmons G.J. The prisoners' problem and the subliminal channel, Advances in Cryptology // In: Proceedings of Crypto 83 (David Chaum, Ed.). Plenum Press, 1984. P. 51-67.

5. A. Shamir, How to Share a Secret, Communications of the ACM, Volume 22, Issue 11, November 1979, 612-613
6. P. Gemmell, An introduction to threshold cryptography, Crypto-Bytes, Technical Newsletter of RSA Laboratories, Volume 2 , Issue 3, Winter 1997, 7-12
7. G. Margarov, V. Markarov, A. Khachaturov, “Steganographic system with dynamically reconfigurable structure”, Proceedings of the 2009 International Conference on Security & Management, SAM'09, Volume 1, Las Vegas, 43-45, CSREA Press, 2009.
8. Маркаров В. Г., Хачатуров А. Г. “Аутентификация пользователей в реконфигурируемой стеганографической системе ” // Доклады международной научно-практической конференции по вопросам безопасности информационных систем, Ереван Армения, Май 26-27, 2011 стр. 97-101.