УДК УДК 004.056.5+004.942+ 51-7

Модель реконфигурируемой стеганографической системы с применением технологии блокчейн

Е. В. Тимощенко, кандидат физ.-мат. наук, доцент, проректор по научной работе

E-mail: timoshchenko@msu.by

ORCID ID: 0000-0003-1373-5113

УО «Могилевский государственный университет имени А. А. Кулешова», ул. Космонавтов, д. 1, 212022, г. Могилёв, Республика Беларусь

А. Ф. Ражков, магистрант кафедры математики и информатики

E-mail: razhkov.a@mail.ru

ORCID ID: 0000-0001-5200-4167

УО «Могилевский государственный университет имени А. А. Кулешова», ул. Космонавтов, д. 1, 212022, г. Могилёв, Республика Беларусь

Аннотация. Рассмотрен эффективный способ решения проблемы безопасности передачи данных. Предложен новый подход к проектированию стеганографической системы, основывающейся на трёх основных методах – внедрение частей разделенного секрета в изображения с возможным, в дальнейшем, извлечением секретной информации, проверка подлинности частей секрета, самовосстановление данной системы безопасности. Такая система обеспечивает большую степень защищенности и безопасного хранения данных. Windows-приложение, которое реализует предложенную стеганографическую модель, не имеет аналогов и отвечает всем требованиям, поставленным к стеганографическому программному обеспечению.

Ключевые слова: защита данных; информационная безопасность; стеганография; дискретное косинусное преобразование; схема разделения секрета; (*k,n*)-пороговая схема, блокчейн, реконфигурируемая система, программное обеспечение, технология .NET

Для цитирования: Тимощенко, Е. В. Модель реконфигурируемой стеганографической системы с применением технологии блокчейн/ Е. В. Тимощенко, А. Ф. Ражков// Цифровая трансформация. – 2019. – № 3 (8). – С. 65–72.

Model of Reconfigurable Steganographic System Using Blockchain Technology

E. V. Timoschenko, Dr. Sc. (Phys.-Math.), Associate Professor, Vice-rector for scientific work

E-mail:timoshchenko@msu.by

ORCID ID: 0000-0003-1373-5113

"Mogilev State A. Kuleshov University", 1 Kosmonavtov Str. 212022 Mogilev, Republic of Belarus

A. F. Razhkov, Master's Degree student of Department of Mathematics and Computer Science

E-mail: razhkov.a@mail.ru

ORCID ID: 0000-0001-5200-4167

"Mogilev State A. Kuleshov University", 1 Kosmonavtov Str. 212022 Mogilev, Republic of Belarus

Abstract. An effective method for solving data security problems is proposed. A new approach to the design of steganographic system based on the three basic methods - the introduction of parts of a shared secret into images with the possibility of further extraction of secret information, authentication of parts of a secret, self-healing of this security system. Such a system provides a greater degree of protection and secure data storage. The Windows application implements the proposed steganographic model, has no analogues and meets all the requirements set for steganographic software.

Key words: data protection, information security, steganography, discrete cosine transform, secret sharing scheme, (k,n)-threshold scheme, blockchain, reconfigurable system, software, .NET technology
For citation: Timoschenko E. V., Razhkov A. F. Model of Reconfigurable Steganographic System Using Blockchain Technology. *Cifrovaja transformacija* [Digital transformation], 2019, 3 (8), pp. 65–72 (in Russian).

Введение. С появлением Интернета возросло число пользователей, обращающихся к нему за быстрым и легким доступом к информации и её передачи. В связи с этим актуализируется вопрос безопасности и достоверности транслируемых и принимаемых данных, особенно если это личные или конфиденциальные сообщения [5]. Стеганография, криптография и водяные знаки [13] – это решение для преодоления данных проблем, поэтому исследования в данной области обладают высокой актуальностью.

Стеганографический метод шифрования информации используется в случаях, когда помимо безопасного трансфера данных требуется дополнительно сохранить в тайне само существование секретного сообщения [4]. С его помощью они скрываются внутри других открытых данных, таким образом обеспечивается сокрытие и защита информации от несанкционированного доступа без раскрытия самого факта её наличия даже в зашифрованном виде.

Стеганография является основой для создания перспективных систем защиты информации, технические характеристики которых определяются новыми информационными технологиями. Она позволяет не только успешно решать основную задачу – скрытно передавать данные, но и решать целый ряд других: создание помехоустойчивой аутентификации, защита от несанкционированного копирования, мониторинг информации в сетях связи, поиск информации в мультимедийных базах данных.

Данные могут быть дополнительно защищены с помощью различных аппаратных и программных технологий. Большой популярностью сейчас пользуется технология блокчейн, суть которой состоит в том, чтобы по определённым правилам сформировать непрерывную последовательную связную цепочку блоков информации. Копии таких цепочек блоков, чаще всего, хранятся независимо друг от друга на разных компьютерах. Впервые этот термин появился как название полностью реплицированной распределённой базы данных, реализованной в системе «Биткойн», поэтому блокчейн часто ассоциируют с транзакциями в различных криптовалютах. Отметим, что технология формирования цепочек блоков данных может быть распространена на любые взаимосвязанные информационные блоки [1], в связи с чем, в последнее время, технология блокчейна стала предметом все большего числа научных исследований [7, 8, 10, 11] и вызвала значительный интерес среди исследователей и разработчиков из-за высокого уровня доверия и безопасности.

В данной статье будет рассмотрен способ защиты данных, который включает в себя разделение информации по схеме разделения секрета Шамира, стеганографическое сокрытие информации в графических файлах, а также дополнительную защиту с помощью внедрения технологии блокчейн.

Основная часть. Разработка модели реконфигурируемой стеганографической системы проводилась в несколько этапов. На первом осуществлялось разделение секретной информации на части, которые Перейдем к рассмотрению первого этапа – разделению секретной информации на части, которые будут, в дальнейшем, внедрены в изображения.

Задача данного этапа заключается в том, чтобы разделить секретную информацию разделения секрета подразумевает под собой разделение секретной информации между участниками так, что только заранее заданные множества участников смогут ее восстановить., таким образом, вероятность компрометации предоставленных этой информации данных снижается.

Новые методы разделения информации расширяют области практического использования. ТакНапример, возможности разделения или управления компонентами секрета могут быть использованы в учреждениях государственного управления, военных формированиях или даже на промышленных предприятиях [12].

Наглядным примером методов разделения информации может послужить комната, в которой хранится нечто ценное для определенной группы лиц. Если закрыть комнату на несколько различных между собой замков, количество которых равно количеству участников, и раздать каждому члену этой группы по одному ключу, то открыть дверь смогут только все участники, собравшись вместе.

В 1979 году Ади Шамир в своей работе [6] предложил совершенную (*k,n*)-пороговую схему разделения секрета, в основе которой лежит интерполяция многочлена с коэффициентами из заданного поля Галуа с *p* элементами – *GF*(*p*). Пример схемы Шамира приведён на рисунке 1.

Схема, график которой приведен для иллюстрации идеи на рисунке 1, состоит из двух фаз. Во время первой фазы дилер генерирует многочлен *F* степени (*k*-1), генерируя случайным образом (*k*-1) элементов из *GF*(*p*). Эти элементы будут являться коэффициентами многочлена *f*, где $j \in (1,\ldots,k-1)$. Коэффициентом f становится значение секрета s_0.

Во время второй фазы каждому из *n* участников сопоставляется ненулевой номер, и дилер отправляет «тень», долю секрета, которая представляет из себя пару (*i,F*(*i*)), где *i* - порядковый номер участника, а *F*(*i*) - значение многочлена в этой точке.

Любой многочлен (*k*–1) степени можно однозначно восстановить по любым *k* различным точкам с помощью интерполяции. Для этого можно использовать, например, интерполяционную формулу Лагранжа. Таким образом, любые *k* и более участников смогут восстановить многочлен *F* и вычислить значение *F* в точке 0, что будет являться значением секрета.

Очевидно, что эта схема совершенна, так как любые *k* и более участников однозначно восстанавливают секрет, а любые группы из менее *k* участников не получают никакой дополнительной информации о секрете.

На втором этапе разработки модели осуществляется стеганографическое сокрытие частей

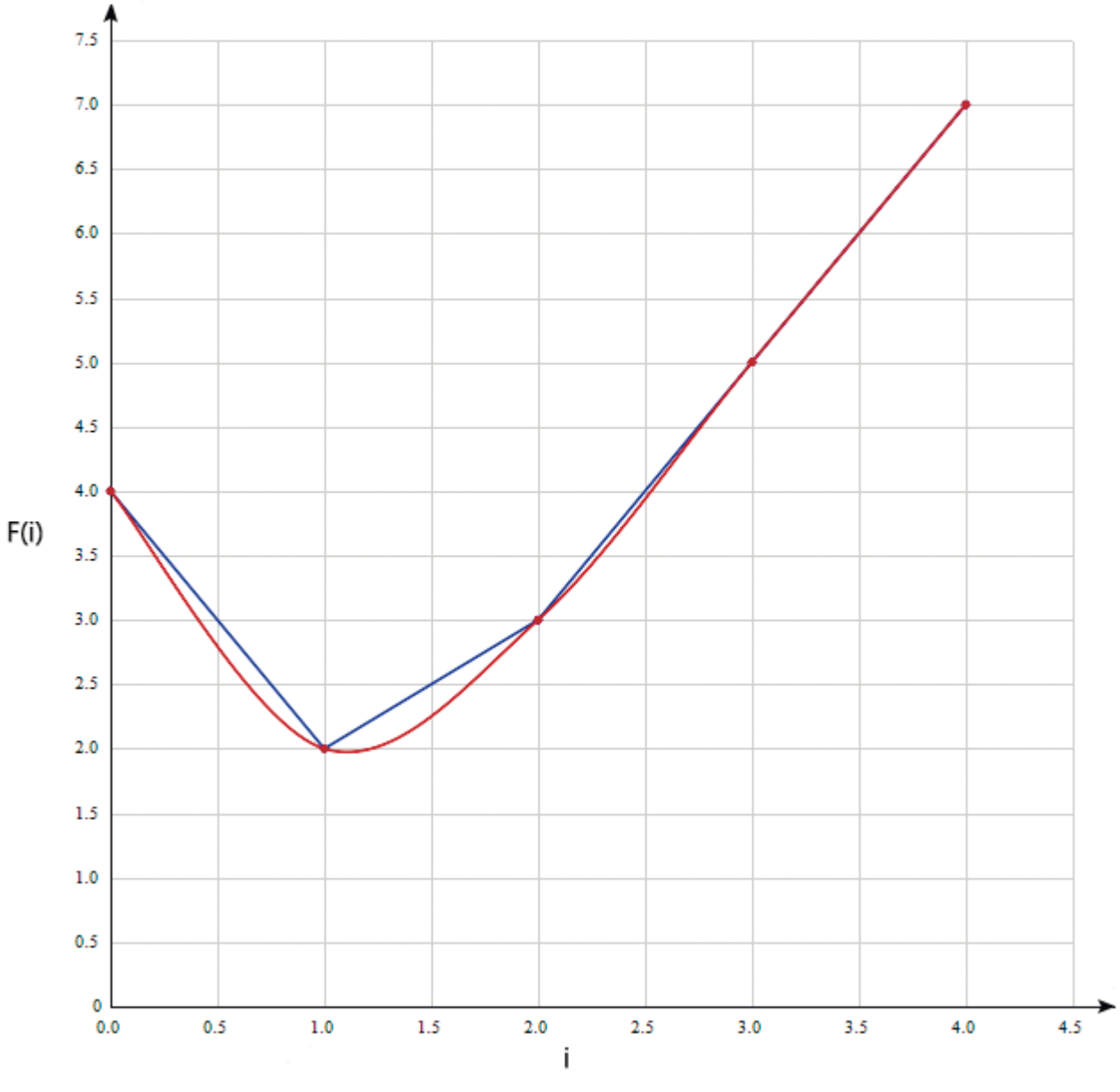

Рис. 1. Пример схемы Шамира
Fig. 1. An example of a Shamir's scheme

секретного сообщения в графические файлы форматов BMP, PNG с помощью метода относительной замены величин коэффициентов дискретно-косинусного преобразования.

Стеганографические алгоритмы разделены по категориям, которые представленыпредставленных на рисунке 2, в соответствии с форматами файлов изображений и областям, в которых производится сокрытие.

При разработке модели реконфигурируемой стеганографической системы для сокрытия информации в изображениях форматов BMP, PNG был использован метод относительной замены величин коэффициентов дискретно-косинусного преобразования (ДКП) (метод Коха-Жао). Этот метод, в сравнении с другими, обладает существенными достоинствами. Он проявляет устойчивость к большинству известных стеганографических атак, в том числе к атаке сжатием, к аффинным преобразованиям и геометрическим атакам [4], поэтому является одним из наиболее распространённых на сегодня методов сокрытия конфиденциальной информации в частотной области изображения.

Для реализации третьего этапа разработки модели реконфигурируемой стеганографической системы сокрытия информации в изображениях разработано специальное программное обеспечение.

С главной формы приложения, представленной на рисунке 3, возможно переключение на формы разделения секрета, последующего внедрения в изображения, восстановления секрета, и форму настроек.

При нажатии на следующие элементы управления кнопки «Secret Sharing», «Secret Recovery», «Secret Refreshing», «Settings» происходит переход на формы, предназначенные для выполнения функций разделения и внедрения его частей в имеющиеся изображения, восстановления секрета, «обновления» изображений с внедренными частями секрета, и настройки блокчейн-составляющей программного обеспечения.

Форма по разделению секрета и внедрению его частей в имеющиеся изображения представлена на рисунке 4. В текстовое поле вводится «секрет». Общее количество изображений получается путём подсчёта изображений в папке, предназначенной для исходных изображений. Также на данной форме приложения пользователь вводит необходимое для восстановления секрета количество изображений.

На рисунке 5 показана форма приложения по восстановлению секрета. В текстовое поле выводится «секрет», восстановленный из имеющихся изображений в соответствующей папке.

Форма настроек приложения представлена на рисунке 6. На вкладке «Data» выводятся публичный и приватный ключи. А также происходит ввод пароля для шифрования файла блокчейна и пароля для шифрования приватного ключа для дальнейшего использования. На вкладке «Blockchain» имеются функции создания блокчейна, добавления информации о хэшах изображений, которые использо-

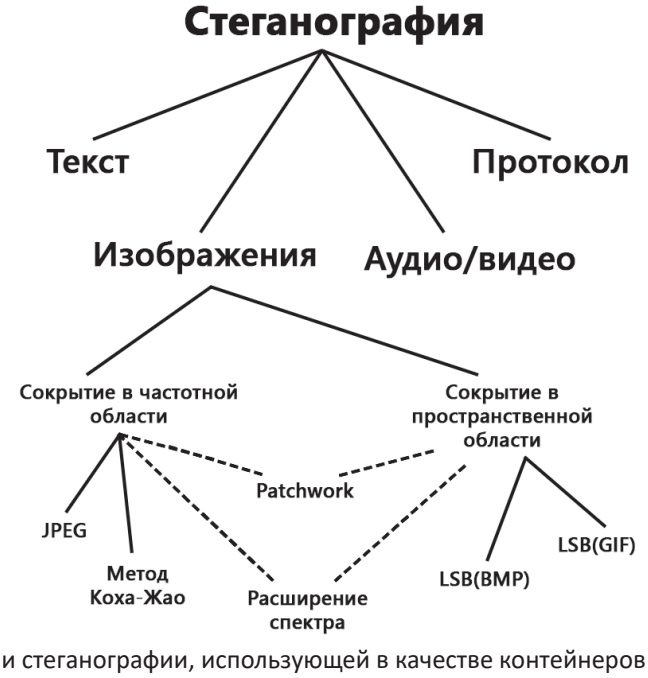

Рис. 2. Категории стеганографии, использующей в качестве контейнеров изображения
Fig. 2. Categories of steganography using containers as images

Рис. 3. Главное окно программы
Fig. 3. The main window of the program

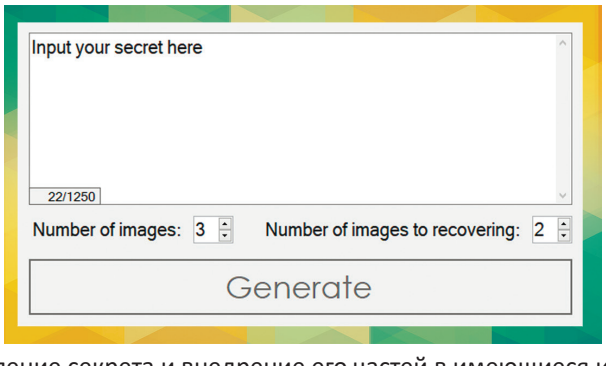

Рис. 4. Разделение секрета и внедрение его частей в имеющиеся изображения
Fig. 4. Sharing a secret and embedding parts of it in existing images

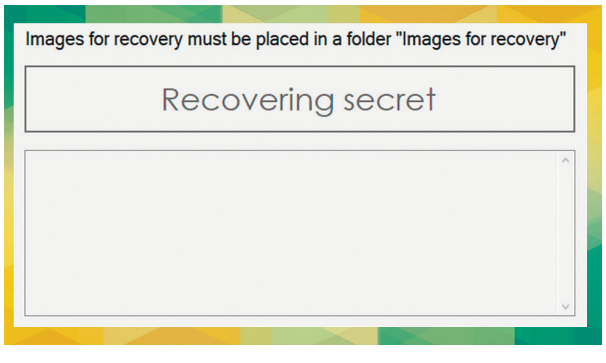

Рис. 5. Восстановление секрета
Fig. 5. Secret Recovery

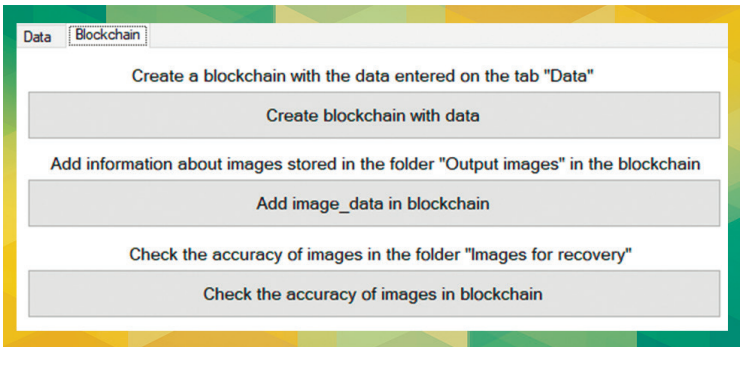

Рис. 6. Настройки приложения, касающиеся блокчейн-составляющей
Fig. 6. Blockchain-related application settings

вались для внедрения секрета в них, проверки актуальности изображений, которые пользователь решил использовать для восстановления секрета.

Разработанное приложение не имеет аналогов, отвечает всем требованиям, поставленным к стеганографическому программному обеспечению, и может использоваться для сокрытия данных в графических файлах форматов BMP, PNG, осуществляя при этом более безопасную передачу «секрета», благодаря использованию блокчейн-технологии.

На третьем этапе разработки модели для более защищенной передачи данных используется технология блокчейн.

Блокчейн – хронологическая база данных, где время добавления новой записи неразрывно связано с самими данными. Это делает её некоммутативной [2].

Кроме того, дополнительную защиту информации даёт хэш-код блока данных. Поскольку в формировании хэша текущего блока, помимо других входных данных, участвует и хэш предыдущего блока, любое изменение любых входных данных предыдущего блока приведет к изменению как предыдущего хэша, так и хэша блока, следующего за ним, который из-за этого перестанет соответствовать заданному условию, а следом за ним некорректной станет и вся последующая цепь. Более того, чем старее блок в цепи, тем сложнее его изменить.

Каждый участник сети при первом запуске программного обеспечения генерирует случайный набор чисел (приватный ключ), с помощью которого формируется другой, более сложный набор символов (публичный ключ).

Хранение хэш-кодов контейнеров (изображений), полученных в результате работы разработанного программного обеспечения, осуществляется в приватном блокчейне на централизованном сервере [3]. Получение секретного сообщения возможно при наличии "актуальных" контейнеров (тех, у которых хэш-коды совпадают с хэш-кодами в последнем блоке блокчейна).

Такое решение значительно повышает степень защищенности по отношению к большинству возможных атак за счёт того, что скрытые в отдельном контейнере данные представляют собой бессмысленный набор символов.

Работа реконфигурируемых систем основывается на периодическом обновлении скрываемой информации или, иными словами, самовосстановлении системы безопасности. В случае стеганографии основная идея самовосстановления заключается в периодическом извлечении и повторном сокрытии секретных данных. Таким образом, не только обновляются скрываемые данные, но в то же время «старые секреты» (т. е. секреты до обновления) становятся бесполезными для противника. В результате он теряет контроль над ситуацией или становится вынужденным проявлять постоянную активность, рискуя быть выявленным соответствующими средствами обнаружения вторжений.

На рисунке 7 и рисунке 8 проиллюстрирована схема данной модели.

Заключение. Предложенный подход к проектированию реконфигурируемой стеганографической системы позволяет реализовать защиту передаваемой информации путём разделения

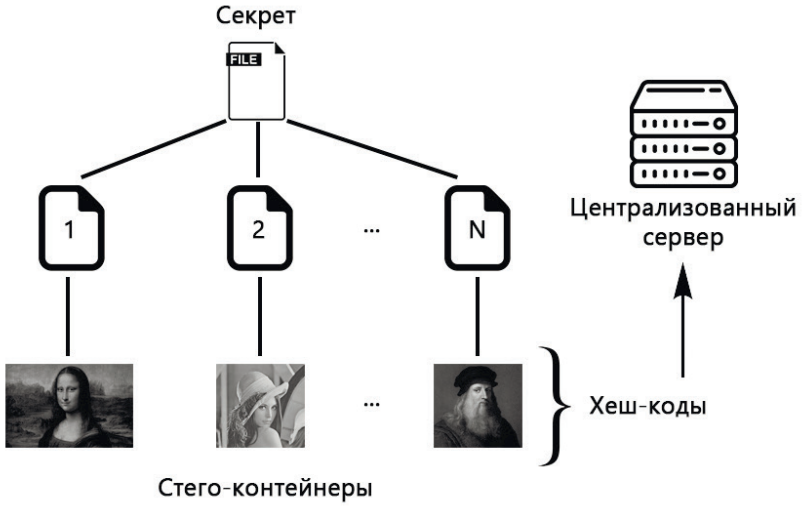

Рис. 7. Схема разделения, внедрения секрета
Fig. 7. The scheme of separation, the introduction of secret

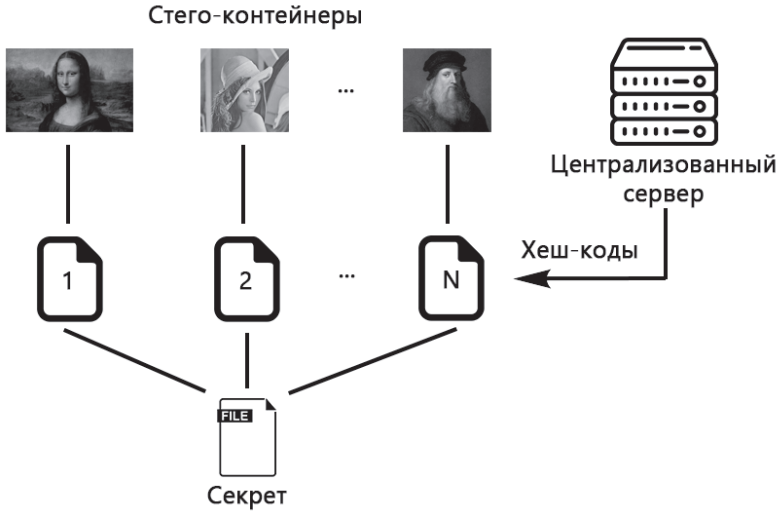

Рис. 8. Схема извлечения секрета
Fig. 8. Scheme of secret extraction

«секрета» на несколько частей, последующего внедрения частей «секрета» в изображения с возможным, в дальнейшем, их извлечением из изображений. Система основывается на трёх основных методах – внедрение частей разделенного секрета в изображения с возможным извлечением секретной информации, проверка подлинности частей секрета, самовосстановление данной системы безопасности. Таким образом, обеспечивается большая степень защищенности и безопасного хранения данных. Наличие двух условий: достоверность частей и периодическое перераспределение новых частей достаточны для того, чтобы гарантировать, что новые файлы-носители хранят достоверные части секрета и система остается работоспособной долгое время.

Совместно с применением схем разделения секрета и технологии блокчейн система защиты информации становится более надёжной и эффективной за счет того, что разделяемый секрет путем математических преобразований разделяется на части с последующим внедрением в изображения, которые выдаются участникам структуры. А благодаря технологии блокчейн система становится более безопасной и прозрачной для пользователей.

Список литературы

1. Генкин, А. Блокчейн. Как это работает и что ждет нас завтра / А. Генкин, А. Михеев – М.: Альпина Паблишер, 2017. – 592 с.
2. Пряников М. М. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы [Текст] / М. М. Пряников, А. В. Чугунов // International Journal of Open Information Technologies. – 2017. – Т. 5. – № 6. – С. 49–55.
3. Ражков, А. Ф. Модель реконфигурируемой стеганографической системы с применением технологии блокчейн / А. Ф. Ражков, Е. В. Тимощенко // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: материалы XXII Республиканской научной конференции студентов и аспирантов – Гомель, 2019. – С. 290–291.
4. Ражков, А. Ф. Использование стеганографического метода Коха и Жао для сокрытия информации в цифровых изображениях / А. Ф. Ражков, Е. В. Тимощенко // Первый шаг в науку – 2018: материалы Междунар. форума студ. и учащ. молодежи в рамках Междунар. науч.-практ. инновац. форума «INMAX'18». Ч.4. – Мн: Лаборатория интеллекта, 2018. – С. 66-68.
5. Тимощенко, Е. В. Обеспечение информационной безопасности методом стеганографии / Е. В. Тимощенко // Актуальные проблемы правовых, экономических и гуманитарных наук: материалы IX Международной научно-практической конференции профессорско-преподавательского состава, аспирантов, магистрантов и студентов. Минск, 9 апреля 2019 г.: в трех частях / ред. кол. С.Ф. Сокол [и др.]. – Минск: БИП, 2019. – Ч. 2. – С.95-96.
6. Shamir, A. How to share a secret/ A. Shamir. – Communications of the ACM – 1979. – 22(11). – pp. 612–613.
7. Miller, D. Blockchain and the internet of Things in the industrial sector IT Professional/ D. Miller. – 2018. – 20 (3). – pp. 15-18.

8. Fiaidhi, J., EDI with blockchain as an enabler for extreme automation IT Professional/ J. Fiaidhi, S. Mohammed, S. Mohammed – 20 (4). – 2018. – pp. 66-72.
9. Johnson, N. F., Jajodia, S., «Steganalysis of Images Created Using Current Steganography Software», Proceedings of the 2nd Information Hiding Workshop, April 1998. – p. 276.
10. Kan, L. A multiple blockchains architecture on inter-blockchain communication 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) / Y. Wei, A. Hafiz Muhammad, W. Siyuan, G. Linchao, H. Kai– 2018. – pp. 139-145.
11. M. Samaniego, R. Deters Blockchain as a service for IoT 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) – 2016.– pp. 433-436.
12. Ogiela, M.R., Ogiela, U. Linguistic cryptographic threshold schemes International Journal of Future Generation Communication and Networking.– 2009. – 1 (2).– pp. 33-40.
13. O. Cetin dan A. T. Ozocerite, "A new steganography algorithm based on color histograms for data embedding into raw video streams," Computers & Security, 2009. – vol. XXVIII. – no. 7. – pp. 670–682.

References

1. Genkin A, Miheev A. Blokchejn. Kak eto rabotaet i chto zhdet nas zavtra [Blockchain. How it works and what awaits us tomorrow]. M.: Al'pina Pablisher, 2017, p. 592 (In Russian).
2. Pryanikov M. M., CHugunov A. V. Blokchejn kak kommunikacionnaya osnova formirovaniya cifrovoj ekonomiki: preimushchestva i problemy [Tekst] [Blockchain as a communication basis for the formation of a digital economy: advantages and problems [Text]] International Journal of Open Information Technologies, 2017, vol. 5, no. 6, pp. 49–55 (In Russian).
3. Razhkov A. F. Timoshchenko E. V. Model' rekonfiguriruemoj steganograficheskoj sistemy s primeneniem tekhnologii blokchejn [Model of reconfigurable steganographic system using blockchain technology]. Novye matematicheskie metody i komp'yuternye tekhnologii v proektirovanii, proizvodstve i nauchnyh issledovaniyah: materialy XXII Respublikanskoj nauchnoj konferencii studentov i aspirantov. Gomel', 2019, pp. 290–291 (In Russian).
4. Razhkov A. F. Timoshchenko E. V. Ispol'zovanie steganograficheskogo metoda Koha i ZHao dlya sokrytiya informacii v cifrovyh izobrazheniyah [Using the steganographic method of Koch and Zhao to hide information in digital images]. Pervyj shag v nauku, 2018, materialy Mezhdunar. foruma stud. i uchashch. molodezhi v ramkah Mezhdunar. nauch.-prakt. innovac. foruma «INMAX'18». CH.4. Mn: Laboratoriya intellekta, 2018, pp. 66-68. (In Russian).
5. Timoshchenko E.V. Obespechenie informacionnoj bezopasnosti metodom steganografii [Information security by steganography] Aktual'nye problemy pravovyh, ekonomicheskih i gumanitarnyh nauk: materialy IX Mezhdunarodnoj nauchno-prakticheskoj konferencii professorsko-prepodavatel'skogo sostava, aspirantov, magistrantov i studentov. Minsk, 9 aprelya 2019 g.: v trekh chastyah / red. kol. S.F. Sokol [i dr.]. Minsk: BIP, 2019, CH. 2., pp. 95–96. (In Russian).
6. Adi Shamir. How to share a secret. Communications of the ACM. 1979, 22(11), pp. 612–613.
7. Miller D./ Blockchain and the internet of Things in the industrial sector IT Professional, (2018), 20 (3), pp. 15-18.
8. Fiaidhi J., Mohammed S., Mohammed S. EDI with blockchain as an enabler for extreme automation IT Professional, 2018, 20 (4), pp. 66-72.
9. Johnson N. F., Jajodia S. «Steganalysis of Images Created Using Current Steganography Software», Proceedings of the 2nd Information Hiding Workshop, April 1998, p. 276.
10. L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, G. Linchao, H. Kai A multiple blockchains architecture on inter-blockchain communication 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2018, pp. 139–145.
11. M. Samaniego, R. Deters Blockchain as a service for IoT 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016, pp. 433-436.
12. Ogiela M. R., Ogiela U. Linguistic cryptographic threshold schemes International Journal of Future Generation Communication and Networking, 2009, 1 (2), pp. 33–40.
13. O. Cetin dan A. T. Ozocerite, "A new steganography algorithm based on color histograms for data embedding into raw video streams," Computers & Security. 2009, vol. XXVIII, no. 7, pp. 670–682.

Received: 27.09.2019 *Поступила: 27.09.2019*