**Инженерный вестник Дона**, №2 (2024)
ivdon.ru/ru/magazine/archive/n2y2024/9039

# О маскировании изображений, как основе построения схемы визуальной криптографии

*А. М. Сергеев, М. Б. Сергеев*
*Санкт-Петербургский государственный университет аэрокосмического приборостроения*

**Аннотация:** Рассматриваются особенности ($m$,$m$)-схемы реализации визуальной криптографии, отличающейся от существующих формированием теневых изображений (акций) изображения, содержащего секрет. Предлагаемый подход основан не на декомпозиции секретного изображения на акции, а на пошаговой их трансформации путем умножения на ортогональные матрицы Адамара. Получаемые при каждой трансформации акции изображения являются помехоустойчивыми в канале передачи данных.
**Ключевые слова:** изображение с секретом, декомпозиция изображения, трансформация изображения, ортогональные матрицы Адамара, двустороннее матричное умножение, помехоустойчивое кодирование изображений.

## Введение

В 1994 г. была открыта новая область криптографии, ставшая известной, как визуальная криптография [1]. В ней пароль или секретная информация, представляющие собой изображение, воспринимаются визуально человеком или сравниваются компьютером с эталонным цифровым изображением [2].

Интерес к применению визуальной криптографии постоянно возрастает, в частности, для защиты от несанкционированного использования передаваемых визуальных данных (паролей, конфиденциальных фотоматериалов и др.) или их копирования [3], для биометрической аутентификации пользователей информационных систем [4], и др.

Для безопасной передачи конфиденциальных изображений по открытым коммуникациям, они подвергаются разложению на «теневые» слои (акции) таким образом, что изображение (секрет) восстанавливается только при их сложении. Однако предложенные схемы разложения связаны либо с расширением представления пикселей изображения [2], либо с другими проблемами обеспечения безопасности.

Цель работы – предложение нового подхода к формированию акций изображения с текстовой информацией, обеспечивающего его восстановление не сложением акций, а последовательным их умножением как матриц в установленном порядке.

## Схемы визуальной криптографии

Существующие визуальные криптографические схемы можно представить следующим образом:

– (2,2) – схема, в которой секретное изображение разделяется на две акции и обе они необходимы для раскрытия секрета.

– (2,*m*) – схема, в которой секретное изображение делится на *m* акций, а для раскрытия секрета достаточно двух любых из них.

– (*m*,*m*) – схема, в которой секретное изображение делится на *m* акций, и для раскрытия секрета необходимы они все.

Таким образом, основа восстановления секрета в схемах (*k*,*m*)-визуальной криптографии – сложение акций (слайдов), представляющих декомпозицию по пикселям секретного изображения по правилам [5]. При этом, минимальное *k* называется порогом восстановления секрета.

Большинство отечественных и зарубежных работ по данной тематике рассматривают теоретические вопросы формирования акций, постулирующих обеспечение конфиденциальности визуально воспринимаемого секрета при его декомпозиции, и лишь в отдельных работах приводятся примеры разложений, подтверждающих базовую идею визуальной криптографии [5, 6].

Однако, визуальная информация значительно отличается от любой другой тем, что воспринимается зрительной системой человека (глазами и мозгом), которая имеет в своем составе ассоциативную составляющую. Таким образом, мало разделить секрет-изображение на акции. Необходимо быть уверенным в том, что любая из них не несет в себе ассоциаций, даже не полных, с самим

секретом. А это задача куда более трудоемкая, чем разложение на слои и их сборка для визуализации секрета

## Недостатки существующих методов визуальной криптографии

В качестве явных недостатков визуальной криптографии, можно выделить следующие:

– размер каждой акции больше размера исходного изображения, как минимум, в 4 раза;

– алгоритмы визуальной криптографии ориентированы на работу с бинарными изображениями (черно/белыми). Проблематично их применение для цветных и полутоновых изображений.

– в схеме ($k$,$m$) можно получить изображение секрета не по полному списку акций.

Однако для рассматриваемого в работе секрета – текстового сообщения, они не критичны: объем изображения с сообщением не велик, а само сообщение, как правило, одного цвета на фоне. Да и развитие визуальной криптографии сегодня обеспечивает возможность работы с цветными изображениями [7, 8].

Вместе с тем остается ряд вопросов, связанных с применением визуальной криптографии в реальных системах (условиях), а именно:

– как ведут себя схемы ($m$,$m$) и ($k$,$m$) при потере или искажении в канале передачи части информации из акции, содержащейся, например, в пакете данных? Возможно ли восстановление секрета с такими потерями (искажениями)?

– какие изображения с текстовым сообщением подвержены восстановлению, а какие нет?

– можно ли восстановить секрет при потере или искажении пакета из акции в схеме ($k$,$m$) добавлением к $k$ еще одной акции?

**Предлагаемая новая схема визуальной криптографии**

В качестве основы для предложения принципиально новой схемы можно использовать богатый опыт маскирования визуальной информации [9] с использованием ортогональных и квазиортогональных матриц [10, 11]. При таком подходе получение акций и сборка их для прочтения секрета будет реализована следующим образом:

– акции изображения с секретом $\mathbf{X}_n$ размером $n \times n$ формируются последовательно: следующая на основе предыдущей путем умножения на ортогональную матрицу Адамара порядка $n$;

– изображение с секретом восстанавливается путем последовательного умножения на транспонированные матрицы Адамара порядка $n$ в обратной последовательности.

Получается, что таким образом реализуется схема $(m,m)$, когда восстановление возможно только при наличии всех акций. Если используются всего две ортогональные матрицы Адамара порядка $n$, обозначим их, как $\mathbf{A}_n$ и $\mathbf{B}_n$, то преобразование изображения секрета $\mathbf{X}_n$ осуществляется, как последовательное двустороннее умножение $\mathbf{Y}_n = \mathbf{A}_n\mathbf{X}_n\mathbf{B}_n$ – сначала слева, потом справа (или наоборот).

Восстановление изображения производится через обратное двустороннее умножение на транспонированные матрицы в виде $\mathbf{X}_n = \mathbf{A}_n^{\mathrm{T}}\mathbf{Y}_n\mathbf{B}_n^{\mathrm{T}}$.

Особенности такой реализации визуальной криптографии следующие:

– нарушение последовательности умножения не позволяет восстановить секрет, поскольку в основе лежит не декомпозиция на акциях, а пошаговая их трансформация;

– объем каждой акции в пикселях не превышает объема исходного изображения с секретом;

– предпочтительными для преобразования являются ч/б или полутоновые изображения. Однако принципиально возможна работа с цветными

изображениями, как декомпозицией изображения в моделях RGB или CMYK;

– акции изображения, полученные ортогональными преобразованиями, являются помехоустойчивыми в канале передачи данных [12, 13].

## Заключение

Визуальная криптография, ввиду ее актуальности, продолжает развиваться с появлением новых методов и подходов, например, QEVCS на основе QR-кода, с использованием квантовых вычислений, и др.

Для практического применения в распределенных системах требуют решения вопросы по устойчивости акций и секрета в целом к помехам (естественным и преднамеренным) в каналах передачи данных.

Понимание теории ортогональных преобразований является важным аспектом в области создания систем и средств защищенной передачи информации. Предлагаемое в работе решение сочетает в себе принципы визуальной криптографии и помехоустойчивого обмена данными (акциями).

## Благодарность

*Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2023-0003, "Фундаментальные основы построения помехозащищенных систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга".*

## Литература

1. Noar M., Shamir A. Visual cryptography. Advances in Cryptography (Eurocrypt’94) // Lecture Notes in Computer Science. 1994. Vol. 950. pp. 1 – 12.

2. Нысанбаева С.Е., Капалова Н.А., Бейсенова С.Б. Применение визуальной криптографии для защиты биометрических данных в системах

аутентификации // Вестник Алматинского университета энергетики и связи. 2023. Том 1, № 60. С. 141 – 149. DOI:10.51775/2790-0886_2023_60_1_141

3. Борискевич А. А. Алгоритм маркирования изображений на основе визуальной криптографии для защиты он несанкционированного распространения информации // Доклады БГУИР. 2012. № 5 (67). С. 73 – 79.

4. Косолапов Ю. В., Ласковец А. Д. Экспериментальное исследование схемы аутентификации на основе визуальной криптографии // Математические методы в технологиях и технике. 2021. № 7. С. 128 – 131. DOI: 10.52348/2712-8873_MMTT_2021_7_128

5. Ульянов С. В., Петров С. П. Квантовое распознавание лиц и квантовая визуальная криптография: модели и алгоритмы // Электронный журнал «Системный анализ в науке и образовании». 2012. №1. С. 160-176.

6. Косолапов Ю. В. О построении ($k$,$n$)-схемы визуальной криптографии с применением класса линейных хэш-функций над бинарным полем // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2018. Т. 18, № 2. С. 227–239. DOI: 10.18500/1816-9791-2018-18-2-227-239

7. Hou Y.C. Visual cryptography for color images // Pattern Recognition. 2003. Vol. 173. P. 1-11.

8. Jin D., Yan W.Q., Kankanhalli M. Progressive color visual cryptography // Journal of Electronic Imaging. 2005. Vol. 14. № 3. pp. 1-13. DOI: 10.1117/1.1993625

9. Востриков А. А., Сергеев М. Б., Литвинов М. Ю. Маскирование цифровой визуальной информации: термин и основные определения // Информационно-управляющие системы. 2015. № 5. С. 116 – 123. DOI:10.15217/issn1684-8853.2015.5.116

10. Балонин Н. А., Сергеев М. Б. Специальные матрицы: псевдообратные, ортогональные, адамаровы и критские. – СПб: Политехника, 2019. 196 с.

11. Balonin N., Vostrikov A., Sergeev M. Mersenne-Walsh matrices for image processing // Smart Innovation, Systems and Technologies. 2015. Vol. 40. P. 141-147. DOI: 10.1007/978-3-319-19830-9_13

12. Vostrikov A., Sergeev M., Balonin N., Sergeev A. Use of symmetric Hadamard and Mersenne matrices in digital image processing // Procedia Computer Science. 2018. Vol.126. P. 1054-1061.

13. Хвощ С. Т. Матрицы Адамара в космической связи // Инженерный вестник Дона. 2014. №1. URL: ivdon.ru/ru/magazine/archive/n1y2024/8973 (дата доступа: 05.02.2024)

## References

1. Noar M., Shamir A. Lecture Notes in Computer Science. 1994. Vol. 950. pp. 1 – 12.

2. Nysanbaeva S.E., Kapalova N.A., Bejsenova S.B. Vestnik Almatinskogo universiteta energetiki i svyazi. 2023. Vol. 1 № 60. pp. 141 – 149. DOI: 10.51775/2790-0886_2023_60_1_141

3. Boriskevich A. A. Doklady BGUIR. 2012. № 5 (67). pp. 73 – 79.

4. Kosolapov YU. V., Laskovec A. D. Matematicheskie metody v tekhnologiyah i tekhnike. 2021. № 7. P. 128 – 131. DOI: 10.52348/2712-8873_MMTT_2021_7_128.

5. Ul'yanov S. V., Petrov S. P. Elektronnyj zhurnal «Sistemnyj analiz v nauke i obrazovanii». 2012. №1. pp.160-176.

6. Kosolapov YU. V. Izvestiya Saratovskogo universiteta. Seriya Matematika. Mekhanika. Informatika. 2018. Vol. 18, № 2. pp. 227–239. DOI: 10.18500/1816-9791-2018-18-2-227-239

7. Hou Y.C. Pattern Recognition. 2003. Vol. 173. pp. 1-11.

8. Jin D., Yan W.Q., Kankanhalli M. Journal of Electronic Imaging. 2005. Vol. 14. № 3. pp. 1-13. DOI: 10.1117/1.1993625

9. Vostrikov A.A., Sergeev M.B., Litvinov M.Yu. Informacionno-upravlyayushchie sistemy. 2015. № 5. pp. 116 – 123.

10. Balonin N.A., Sergeev M.B. Special'nye matricy: psevdoobratnye, ortogonal'nye, adamarovy i kritskie [Special matrices: pseudo-inverse, orthogonal, Hadamard and Cretan]. St. Peterburg: Polytechnica, 2019. 196 p.

11. Balonin N., Vostrikov A., Sergeev M. Smart Innovation, Systems and Technologies. 2015. Vol. 40. pp. 141-147. DOI: 10.1007/978-3-319-19830-9_13

12. Vostrikov A., Sergeev M., Balonin N., Sergeev A. Procedia Computer Science. 2018. Vol.126. pp. 1054-1061.

13. Hvoshch S.T. Inzhenernyj vestnik Dona. 2024. №1. URL: ivdon.ru/ru/magazine/archive/n1y2024/8973 (accessed: 05.02.2024).

**Дата поступления: 16.01.2024**

**Дата публикации: 21.02.2024**