Инженерный вестник Дона, №3 (2026)
ivdon.ru/ru/magazine/archive/n3y2026/10826

Анализ стойкости (*m*, *m*) схемы визуальной криптографии с использованием квазиортогональных матриц в условиях частичного компрометирования ключа

Е.К. Григорьев

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Аннотация: В работе рассматривается вариант модификации (*m*, *m*) схемы визуальной криптографии с использованием квазиортогональных матриц. Предложено использование матриц Мерсенна с двумя значениями уровней {*a*, -*b*}. Исследуется сценарий частичного компрометирования ключа, при котором потенциальному нарушителю известна структура матрицы-ключа, но отсутствует информация о конкретных значениях её уровней {*a*, -*b*}. Проведено численное моделирование процесса восстановления изображений с секретом в оттенках серого при использовании матриц Мерсенна фиксированного порядка и структуры с различными наборами параметров уровней. Показано, что даже при крайне малых отклонениях значений уровней от истинных восстановление визуально различимого изображения становится невозможным. Полученные результаты подтверждают, что использование матриц Мерсенна расширяет пространство ключей по сравнению более ранней схемой (*m*, *m*) с использованием матриц Адамара и обеспечивает дополнительный уровень защиты в задачах визуальной криптографии.
Ключевые слова: изображение с секретом, матрицы Адамара, матрицы Мерсенна, матричное умножение.

Введение

В современных условиях стремительного развития цифровых технологий обеспечение конфиденциальности и целостности информации приобрело фундаментальное значение для широкого круга приложений — от электронного документооборота и удаленных сервисов до распределенных вычислений и Интернета вещей. Традиционные криптографические методы, основанные на вычислительной сложности математических задач, обеспечивают высокий уровень защищенности, однако требуют существенных вычислительных ресурсов и сложных процедур управления ключами. Эти ограничения стимулируют поиск альтернативных криптографических схем, способных эффективно сочетать безопасность, простоту реализации и устойчивость к различным типам атак.

Одним из перспективных направлений исследований в области информационной безопасности является визуальная криптография (Visual Cryptography, VC), впервые предложенная Naor и Shamir в 1994 году [1]. Метод визуальной криптографии основан на разложении исходного изображения на несколько теневых (шаровых) структур таким образом, что восстановление скрытой информации возможно непосредственно визуальным восприятием без использования сложных вычислительных алгоритмов. Оригинальная схема «(2, M) визуальной криптографии» продемонстрировала принципиальную возможность разделения изображения на M теней, из которых любая пара восстанавливает исходное изображение, а отдельные тени не содержат полезной информации. Данный подход открыл новые перспективы для практической реализации защищенных систем, где минимизируется зависимость от цифровой обработки и вычислительных ресурсов.

С течением времени теоретические и прикладные исследования в области визуальной криптографии были значительно расширены. Существенное внимание уделено развитию обобщенных схем визуальной криптографии с произвольными пороговыми параметрами (k, m), позволяющими восстановление секретного изображения при наличии k теней из m [2, 3]. Требования современных приложений, таких как защищенные мобильные платформы и распределенные системы хранения, предъявляют новые критерии к адаптивности, масштабируемости и вычислительной эффективности схем визуальной криптографии [4, 5].

В работе [6] была предложена оригинальная схема (m, m) визуальной криптографии с использованием квазиортогональных матриц Адамара. Прямое и обратное преобразования при данном подходе осуществляются 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» [6].

Данный подход является перспективным. Использование матриц Адамара в качестве ключа безусловно уменьшает пространство всех возможных ключей, в сравнении, например, со случайными матрицами, поскольку требуется соблюдать попарную квазиортогональность строк матриц. Однако подбор матриц ключей высоких порядков переборными методами, все также остается весьма трудоемкой задачей на данном этапе развития вычислительной техники, даже с использованием квантовых компьютеров [7]. Между найденными компьютером матрицами Адамара 92 и 428 порядков прошло 43 года [8].

Тем не менее данный подход с применением квазиортогональных матриц можно улучшить. У матриц Адамара уровни матриц зафиксированы – {1;-1}, таким образом при формировании ключей в рамках одного порядка мы можем менять только конструкцию матрицы, например использовать Сильвестрову конструкцию или «ядро» с окаймлением [9]. Использование другого семейства квазиортогональных матриц – критских матриц Мерсенна у которых уровни не фиксированы, может предоставить дополнительный защитный механизм. Уровни матриц Мерсенна $\{a, -b\}$ можно менять. Поскольку уровень b зависит как от значения уровня a, так и от весовой функции $\omega(n)$ квазиортогональной матрицы [8, 9]. Таким образом для подбора ключа будет недостаточно подобрать порядок и структуру матрицы ключа, а потребуется еще и подбор пары значений a и b.

Целью настоящей работы является анализ возможности восстановления исходного изображения при использовании квазиортогональных матриц Мерсенна в случае, когда третьей стороне

известна структура матрицы, но отсутствует информация о конкретных значениях уровней $\{a,-b\}$.

Описание эксперимента

Для начала следует вкратце описать используемый математический аппарат. Формулы преобразований описывались, в работе [6], однако для определенности приведем их ниже.

$$\mathbf{Y}_n = \mathbf{A}_n \mathbf{X}_n \mathbf{B}_n, \quad (1)$$

$$\mathbf{X}_n = \mathbf{A}^T{}_n \mathbf{Y}_n \mathbf{B}^T{}_n. \quad (2)$$

Здесь $\mathbf{A}_n$ и $\mathbf{B}_n$ – квазиортогональные матрицы, $\mathbf{Y}$ – защищенное изображение. Операция транспонирования в (2) справедлива для ортогональных и квазиортогональных матриц, у которых обратная равна транспонированной.

Перейдем непосредственно к описанию эксперимента. Был отобран набор изображений размером 511×511 пикс, в оттенках серого, сохранённые в формате png. Для визуального примера на рис.1 показаны изображения cameraman и peppers, как одни из наиболее часто используемых в соответствующей предметной области.

а) Cameraman

б) Peppers

Рис. 1. – Исходные изображения

Чтобы минимизировать влияние структуры матрицы на результаты умножения, и проанализировать влияние значений уровней {*a*, -*b*} матриц Мерсенна в рамках эксперимента примем $\mathbf{A}_n = \mathbf{B}_n$. В качестве основы матрицы-ключа была выбрана матрица Мерсенна на основе псевдослучайной последовательности с порождающим полиномом $x^9+ x^4+1$. Портретное представление данной матрицы представлено на рис. 2, где белому и черному квадрату соответствуют значения «*a*» и «-*b*» соответственно. Алгоритм построения подобных матриц, а также принцип вычисления пар значений {*a*, -*b*} подробно рассмотрен в работе [10]. В данных матрицах элемент *b* вычисляется на основе *a*, как $b = at \Big/ \left(t + \sqrt{t}\right)$, где *t* натуральное число и связано с порядком матрицы N=4t-1.

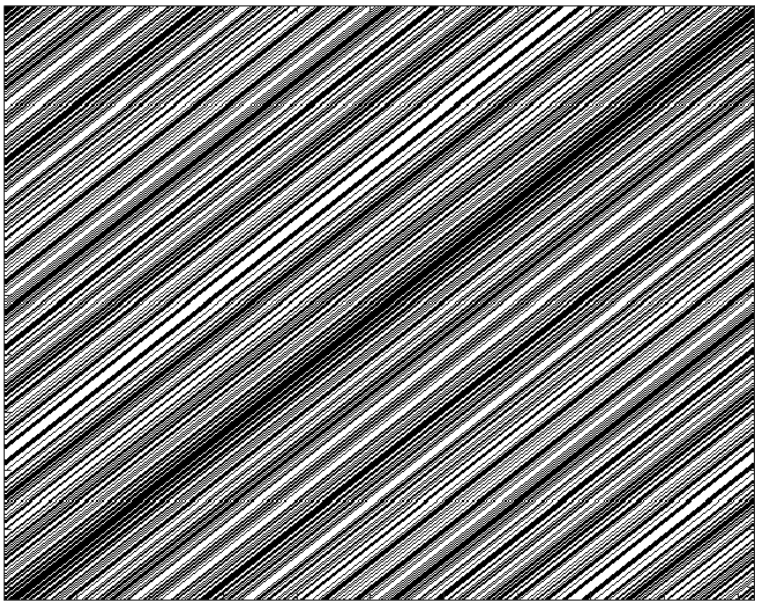


Рис. 2. – Портрет матрицы $\mathbf{A}_n$

Для преобразования по (1) были использованы следующие значения a=1 и b=0.91878

Далее осуществлялась попытка восстановления изображения с секретом по формуле (2), при помощи матрицы с аналогичной структурой но с отличающимися значениями {*a*, -*b*}. Конкретные пары значений представлены в таблице 1.

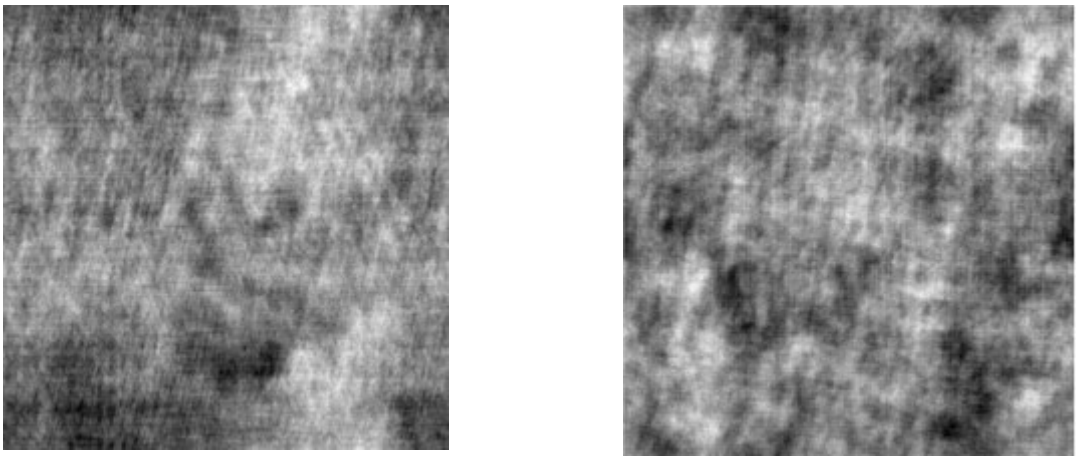
Таблица №1

Пары значений $\{a, -b\}$ используемые в эксперименте

№ попытки	Пары значений	
	a	b
1	3	2.75636
2	2	1.83757
3	0.9	0.82691
4	0.99	0.90960
5	1.1	1.01066
6	1.01	0.92797
7	1.001	0.91970
8	1.0001	0.91888
9	1.00001	0.91879

Результаты моделирования

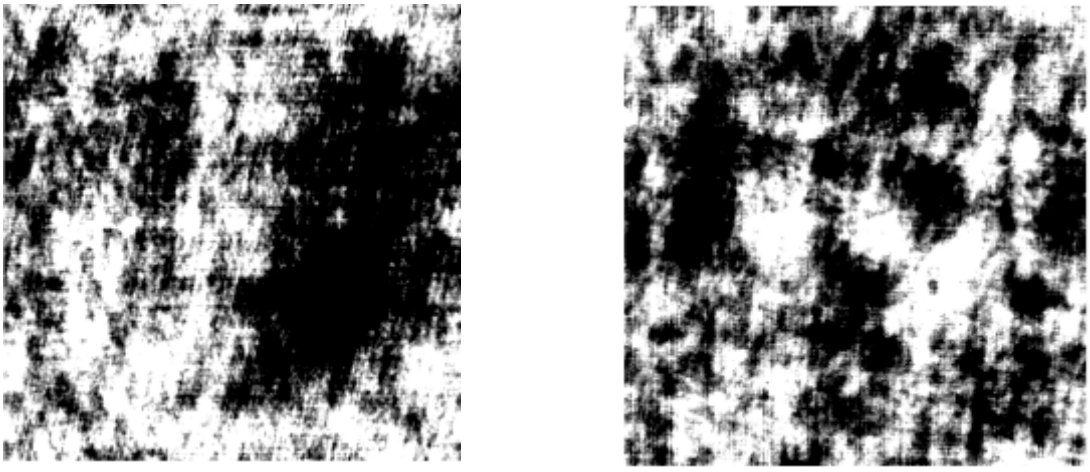
На рис. 3 представлены результаты преобразования по (1) исходных изображений. В обоих случаях контуры исходных изображений полностью разрушены. Визуально распознать любые детали изображения с секретом – невозможно.



а) Cameraman б) Peppers

Рис. 3. – Результат преобразования по (1)

Последовательные попытки восстановления изображения с секретом при помощи пар значений $\{a, -b\}$ из таблицы 1 не привели к удовлетворительному результату. Ни в одном случае нельзя визуально распознать контуры изображения с секретом. В качестве подтверждения на рис. 4 представлены результаты попытки №9 из таблицы 1.



а) Cameraman б) Peppers

Рис. 4. – Результат преобразования по (2) с использованием пары значений a=1.00001, b=0.91879

Разница между истинным значением элемента a и значением из попытки составила всего 0.001%. Как не трудно заметить, даже в этом случае изображение с секретом надежно защищено.

Заключение

В настоящей работе предложена дополнительная возможность защиты изображений с секретом в (m, m) схеме визуальной криптографии с использованием квазиортогональных матриц. Проведен анализ возможности восстановления изображения с секретом в условиях частичной априорной осведомлённости нарушителя о структуре матрицы-ключа. В рамках вычислительного эксперимента показано, что знание структуры матрицы без точного знания параметров уровней $\{a, -b\}$ не позволяет восстановить

исходное изображение даже при их минимальном расхождении с истинными значениями.

Результаты моделирования демонстрируют высокую чувствительность процедуры восстановления к значениям уровней матрицы Мерсенна: визуальная информация полностью разрушается уже при отклонениях параметров менее одной тысячной процента. Это позволяет рассматривать параметры уровней матриц Мерсенна как дополнительную составляющую ключа, существенно усложняющую задачу несанкционированного подбора.

Таким образом, применение квазиортогональных матриц Мерсенна в схемах (m, m) схемах с использованием матриц представляется перспективным направлением развития визуальной криптографии, обеспечивающим расширение пространства ключей без увеличения порядка матриц и усложнения вычислительных процедур. Полученные результаты могут быть использованы при построении защищённых систем визуального хранения и передачи информации, а также служат основой для дальнейших исследований, направленных на формализацию криптостойкости подобных схем и анализ их устойчивости к различным типам атак.

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. V. 950. Pp. 1-12.

2. Li P., Yin L., Ma J. Visual Cryptography Scheme with Essential Participants. Mathematics. 2020. V. 8. №5. Pp. 838.

3. Yan X., Liu F., Yan W.Q., Lu Y. Applying Visual Cryptography to Enhance Text Captchas. Mathematics. 2020. V. 8. №3. Pp. 332.

4. Wafy M. Gradual Improvements in the Visual Quality of the Thin Lines Within the Random Grid Visual Cryptography Scheme. Electronics. 2025. V. 14. №16. Pp. 3212.

5. Ibrahim D., Sihwail R., Arrifin K.A.Z., Abuthawabeh A., Mizher M. A Novel Color Visual Cryptography Approach Based on Harris Hawks Optimization Algorithm. Symmetry. 2023. V. 15. №7. Pp. 1305.

6. Сергеев А.М., Сергеев М.Б. О маскировании изображений, как основе построения схемы визуальной криптографии // Инженерный вестник Дона. 2024. №2. URL: ivdon.ru/ru/magazine/archive/n2y2024/9039

7. Хвощ С.Т. Матрицы Адамара как источник тестов квантовых компьютеров // Инженерный вестник Дона. 2023. №3. URL: ivdon.ru/ru/magazine/archive/n3y2023/8265

8. Dokovic D. Z. Some new symmetric Hadamard matrices. Information and Control Systems. 2022. № 2. P. 2-10.

9. Григорьев Е.К., Сергеев А.М. Метод вычисления двухуровневых циклических квазиортогональных матриц на порядках, равных произведению простых чисел-близнецов // Информационно-управляющие системы. 2025. №1(134). С. 2-8.

10. Григорьев Е.К. Методы формирования квазиортогональных матриц на основе псевдослучайных последовательностей максимальной длины // Инженерный вестник Дона. 2025. №1. URL: ivdon.ru/ru/magazine/archive/n1y2025/9796

11. История открытия матрицы Адамара H_{92}. URL: mathscinet.ru/catalogue/hadamard92/ (дата доступа 12.01.2026)

References

1. Noar M., Shamir A. Lecture Notes in Computer Science. 1994. V. 950. Pp. 1-12.

2. Li P., Yin L., Ma J. Mathematics. 2020. V. 8. №5. Pp. 838.

3. Yan X., Liu F., Yan W.Q., Lu Y. Mathematics. 2020. V. 8. №3. Pp. 332.

4. Wafy M. Electronics. 2025. V. 14. №16. Pp. 3212.

5. Ibrahim D., Sihwail R., Arrifin K.A.Z., Abuthawabeh A., Mizher M. Symmetry. 2023. V. 15. №7. Pp. 1305.

6. Sergeev A.M., Sergeev M.B. Inzhenernyj vestnik Dona. 2024. №2. URL: ivdon.ru/ru/magazine/archive/n2y2024/9039

7. Khvoshch S.T. Inzhenernyj vestnik Dona. 2023. №3. URL: ivdon.ru/ru/magazine/archive/n3y2023/8265.

8. Dokovic D. Z. Information and Control Systems. 2022. № 2. Pp. 2-10.

9. Grigoriev E.K., Sergeev A.M. Informatsionno-upravlyayushchie sistemy. 2025. №1 (134). Pp. 2-8.

10. Grigoriev E.K. Inzhenernyj vestnik Dona. 2025. №1. №1. URL: ivdon.ru/ru/magazine/archive/n1y2025/9796

11. Istoriya otkrytiya matritsy Adamara H_{92} [History of the discovery of the Hadamard matrix H_{92}].URL: mathscinet.ru/catalogue/hadamard92/ (accessed 12.01.2026)

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 9.01.2026

Дата публикации: 28.02.2026