УДК 004.052.2
doi:10.15217/issn1684-8853.2015.5.116

МАСКИРОВАНИЕ ЦИФРОВОЙ ВИЗУАЛЬНОЙ ИНФОРМАЦИИ: ТЕРМИН И ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

А. А. Востриков[а], *канд. техн. наук, доцент*
М. Б. Сергеев[а], *доктор техн. наук, профессор*
М. Ю. Литвинов[б], *канд. техн. наук, доцент*
[а]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*
[б]*Московский государственный технический университет им. Н. Э. Баумана, Москва, РФ*

Постановка проблемы: *в настоящее время для идентификации симметричных преобразований цифровой визуальной информации в целях ее сокрытия от несанкционированного ознакомления существует ряд терминов. Значительные расхождения в реализации преобразований, применение в них разных математических методов и связанных с этим требований к эффективности сокрытия приводят к необходимости уточнения соответствия терминов выполняемым процедурам. Ставится цель критически оценить термины «маскирование» и «демаскирование», рассмотреть альтернативные варианты терминологического обозначения преобразований, выполняемых для защиты цифровых изображений с малым временем актуальности, и закрепить наиболее подходящий вариант.* ***Результаты:*** *сопоставительный анализ терминологии, близкой по значению к описанию содержания процедур преобразования цифровой визуальной информации, показал, что в настоящее время отсутствуют сколь-нибудь более близкие термины, чем «маскирование» и «демаскирование», с определением, способным указать точное место рассматриваемых процедур среди способов защиты информации.* ***Практическая значимость:*** *показано, что термин «маскирование» и связанный с ним термин «демаскирование» наиболее близки к описанию сути преобразований цифровой визуальной видеоинформации с малым временем актуальности в целях ее сокрытия от несанкционированного ознакомления. Сформулированы основные определения применительно к матричным преобразованиям цифровой визуальной информации с использованием квазиортогональных базисов, приведены матричные соотношения для выполнения «маскирования» и «демаскирования».*

Ключевые слова *— защита визуальной информации, защита изображений, маскирование, демаскирование, квазиортогональные базисы, квазиортогональные матрицы, криптографические примитивы.*

Введение

Термины и терминология в целом составляют лингвистический инструментарий сообществ, работающих в определенной области знаний. В научной среде термины дополняют естественный язык и, таким образом, расширяют из года в год словарное множество в соответствующем направлении исследований. Появление новых терминов в большинстве случаев вызвано либо необходимостью замены неудобных трудновоспроизводимых или просто длинных языковых конструкций, либо открытием новых объектов, для которых ранее в языке определение не существовало.

Характерно то, что зачастую термины в их написании и произношении заимствуются из совершенно других областей человеческой деятельности, увеличивая омонимию или полисемию какого-либо слова. Это, как правило, естественный процесс, являющийся следствием стремления исследователей к удобству их восприятия и привычности звучания, хотя нередко причиной является просто отсутствие в языке более близких по значению понятий.

Предмет рассмотрения настоящей работы — термин «маскирование» — довольно обширен и уже длительное время используется в различных областях человеческой деятельности, таких как биология, военное дело, химия, психология, технология управления базами данных (БД), обработка фотографического изображения, область защиты аналоговых сигналов, цифровая обработка изображений.

И уже более восьми лет им пользуются в активно развивающейся научно-технической области — защита от несанкционированного доступа к цифровым изображениям с малым периодом актуальности.

Впервые такая терминология в отношении цифровых изображений была введена в работе [1], а затем более обстоятельно — в работе [2]. Предложенный вариант термина позволял авторам дистанцироваться от традиционных для защиты информации криптографических преобразований, которые, как было показано, в применении к цифровой визуальной информации и при реализации в распределенных встраиваемых системах имеют существенные недостатки [3].

В дальнейшем данный термин был подхвачен и используется до сих пор авторами работ, активно развивающими теоретическую и прикладную стороны применения нового множества недавно открытых вещественных квазиортогональных М-матриц [4].

Настоящая работа ставит своей целью критически оценить применение термина «маскирование» в прикладных задачах защиты цифровой визуальной информации от несанкционирован-

ного доступа, очертить границы применения и зафиксировать этот термин для терминологического описания процедур в указанных задачах.

Области применения термина «маскирование»

Маскирование в биологии. Основополагающие принципы маскирования (маскировки) заложены самой природой (мимикрия). Ряд видов, которые являются беззащитными перед некоторыми хищниками, имитируют другой вид, который избегается хищниками ввиду своей несъедобности или наличия специфических средств защиты. Соответственно, в биологии под маскированием понимается изменение внешнего вида животных, преимущественно окраски, в соответствии с условиями окружающей среды [5].

Маскирование в военном деле — комплекс мероприятий, направленный на введение противника в заблуждение относительно наличия и расположения войск, военных объектов, их состояния и планов командования [6].

Маскирование в аналитической химии — процесс, позволяющий ускорить и упростить анализ смеси при снижении влияния отдельных ее компонентов на разделение, обнаружение или определение веществ без отделения маскируемого (мешающего) соединения от исследуемой смеси [7].

Маскирование в психологии — общий термин в исследованиях восприятия, обозначающий любой процесс, посредством которого различаемый (распознаваемый) стимул становится трудно или совсем не различимым (нераспознаваемым) из-за влияния второго стимула (маскировщика) во временной или пространственной близости к первому [8].

Маскирование изображений в психологии — процесс предъявления тестового зрительного стимула на фоне маскирующего структурированного стимула (изображения), в результате чего ухудшается обнаружение и опознание тестового стимула [9].

Маскирование данных (datamasking) — процесс идентификации конфиденциальных данных и наложения на них «защитной маски», которая сохраняет их «неприкосновенность» в БД, не нарушая при этом функциональной целостности приложения, использующего эти данные [10].

При маскировании данных заменяется конфиденциальная информация в БД, например номера кредитных карт или номера социального страхования на реалистичные значения, что позволяет безопасно использовать эти данные для разработки и тестирования или обмениваться ими с внешними партнерами. Другими словами, маскирование данных — процесс обезличивания конфиденциальной информации, хранящейся в БД [11].

Маскирование видеосигнала — способ защиты видеоизображения, представленного в аналоговой форме, как правило, путем перестановки участков сигнала, содержащих информацию о различных фрагментах изображения (чаще всего — строк). В англоязычном варианте устройства, осуществляющие маскирование видеосигнала, — маскираторы — известны под названием скремблеры (от англ. scramble — перемешивать, перепутывать) [12].

Маскирование речи — способ изменения аналогового или цифрового звукового сигнала в целях искажения характеристик голоса или сокрытия информационной составляющей речевого сообщения [13].

Нерезкое маскирование в области обработки фотографического изображения — технологический прием, позволяющий добиться эффекта ощущения большей резкости за счет усиления контраста тональных переходов [14].

Маскирование слоев в цифровой обработке изображений — способ создания композиций, предназначенный для объединения фотографий в единое изображение, а также для проведения локальных корректировок цветности и тона [15].

Маскирование цифровой визуальной информации. Наконец, в уже упомянутых работах [1, 2] вводится понятие маскирования цифровой визуальной информации как процесса преобразования изображения в кадре к шумоподобному виду. Для маскирования в этом случае используются криптографические примитивы и матричные преобразования.

Таким образом, общее толкование термина «маскирование» для различных областей его применения распадается на две группы:

1) маскирование как действие по сокрытию (защите, деактивации, независимой обработке) определенных частей чего-то целого (аналитическая химия, психология, фотография, цифровая обработка изображений);

2) маскирование как действие с целью обеспечить невозможность обнаружения, идентификации объектов и их частей (биология, военное дело, системы управления БД, защита визуальной информации).

Этимология термина

Термин «маскирование», разумеется, происходит от существительного «маска», имеющего прототипическое значение: «то, что скрывает что-либо» [16]. Из школьного этимологического словаря известно, что русское слово «маска» заимствовано в начале XVIII в. из французского языка (слово «masque») и итальянского

аналога «maschera», восходящего к арабскому слову «maskhara», означающего «маска», образованному в свою очередь от слова «насмешка».

В соответствии со словарем современного русского языка Ефремовой [17] слово «маскирование» означает процесс действия по глаголам: маскировать, маскироваться. К слову же «маскировать» приводятся следующие значения:

— одевать в маскарадный или не свойственный кому-либо костюм или надевать маску;

— переносное: делать что-либо незаметным, невидимым, скрывать что-либо посредством чего-либо показного, притворного;

— скрывать от противника с помощью разных приемов.

Итак, в прототипическом значении «маска» — это то, что скрывает что-либо. При этом в ряде перечисленных выше областей термин «маскирование» применяется не в значении спрятать целевой объект целиком, а выборочно защитить или скрыть лишь определенные его части.

В применении же к защите цифровой визуальной информации маскирование понимается как полное сокрытие целевой информации от ознакомления при отсутствии «ключа» у пытающегося открыть защиту. «Ключ» же предоставляется только доверенному кругу и скрывается от кого-либо еще. Таким образом, это определение полностью совпадает с одним из прямых значений слова из словаря Ефремовой: «Скрывать от противника с помощью разных приемов».

Специфика определения и применения термина в области защиты цифровой визуальной информации

Одновременно с очевидной схожестью определения термина в целевой области с уже существующими определениями бросается в глаза и некоторое отличие. Оно заключается в том, что во всех иных значениях при маскировании не происходит изменение целевого объекта или его частей. А в применении к рассматриваемой области целевой объект (исходное изображение) подвергается преобразованию, т. е. изменяется сам. Данное отличие является, очевидно, наиболее существенным от устоявшихся уже вариантов применения термина, хотя цель сокрытия при этом сохраняется и выполняется.

Кроме этого, следует отдельное внимание уделить ударению в рассматриваемом слове. Дело в том, что в интересующем нас контексте «де-факто» закрепилось произношение: «маскИровать» и «маскИрование». Хотя, строго говоря, существующие словари не поддерживают, например, в слове «маскИровать» ударение на второй слог. Более того, часто такое ударение специально указывается как неправильное и утверждается, что верен лишь вариант «маскировАть» во всех его известных значениях.

В русском языке есть слова, в которых смысл напрямую зависит от их ударения. Типичный пример — слово «броня»: если ударение падает на первый слог, слово означает «закрепление», если же на последний — «защитную оболочку». То же относится к соответствующим глаголам: «брОня» — «бронИровать» (официально закреплять что-либо за кем-либо) и «бронЯ» — «бронировАть» (покрывать бронёй). Однако в этом случае фактически речь идет о двух словах с разным значением и происхождением. А варьирование ударения в слове «маскирование» смысл не меняет.

Тем не менее известно, что есть тенденции общего плана, которые затрагивают акцентные системы разных классов слов в русском языке. Такой общей тенденцией в ударении, по признанию многих лингвистов, считается так называемая тенденция к ритмическому равновесию, которая заключается в смещении ударения к центру слова. Процесс смещения ударения в многосложных словах к центру слова оправдан с практической точки зрения, так как в этом случае соблюдается более равномерная смена ударных и неударных слогов, что более удобно для произнесения [18]. Учитывая вместе с этим упомянутые выше специфические отличия маскирования как защиты визуальной информации от прочих вариантов толкования, можно констатировать, что в данном случае изменение ударной гласной позволяет термину подчеркнуть особенный вариант его применения.

Альтернативные варианты терминов

С учетом относительной новизны применения рассматриваемого термина целесообразно также рассмотреть возможные варианты обозначения соответствующего действия и образованных от них существительных. При этом близость смыслового определения следует соизмерять с благозвучностью терминов, в противном случае не будет гарантии, что термин приживется. В таблице приведены наиболее близкие по смыслу к рассматриваемому действию глаголы и существительные.

Как видно из таблицы, при достаточном многообразии близких по значению слов не удается найти термин, который можно было бы считать более подходящим для применения.

Выбор слова «маскирование» выглядит удачной находкой, поскольку позволяет указать место, занимаемое соответствующими преобразованиями в ряду методов защиты цифровой визуальной информации от несанкционированного доступа. Маскирование визуальной информации

■ Альтернативные варианты термина

Глагол	Существительное	Оценка
Скрывать	Сокрытие	Просторечное, «бытовое» звучание
Укрывать	Укрытие	
Прятать	Прятки	
Защищать	Защита	Общее понятие, требующее конкретизации с помощью длинной конструкции
Ограничивать	Ограничение	
Преобразовывать	Преобразование	
Камуфлировать	Камуфлирование/Камуфляж	Не соответствуют в точности целевому определению
Подменять	Подмена	
Шифровать	Шифрование/Шифрация	Предполагает полноценные криптографические преобразования, применение которых для целевого определения существенно ограничено [3]

не предназначено для разграничения доступа в процессе длительного хранения, как криптография, и, следовательно, ориентировано на данные с малым временем актуальности. Кроме этого, предмет защиты — изображение — по своей сути всегда является массивом со значительной степенью избыточности, что при шифровании не гарантирует полное устранение информативности для третьей стороны. В эталонном случае воспроизводимая визуальная информация распадается до белого шума. Но данный критерий труднодостижим, поэтому процедура маскирования предназначена для преобразования изображения в шум с неясным распределением, где не прослеживаются контуры скрываемого объекта или субъекта, даже в случае его перемещения в последовательности кадров видеоизображения.

Основные определения

На основании приведенных в настоящей работе сведений о процедуре маскирования цифровой визуальной информации, а также информации из опубликованных работ в целевом направлении исследований [1, 2, 3, 19–21] сформулируем основные определения терминов.

Маскирование — процесс преобразования цифровой визуальной информации с малым периодом актуальности к шумоподобному виду в целях ее защиты от несанкционированного ознакомления.

После выполнения маскирования полученный массив информации называется *маскированной цифровой визуальной информацией* или *маскированным изображением*.

Демаскирование — процесс обратного преобразования маскированной цифровой визуальной информации путем применения операций, являющихся обратными к маскирующим операциям, в целях восстановления исходного изображения.

Матричное маскирование и демаскирование — выполнение соответствующей процедуры прямого или обратного преобразования с применением базиса квазиортогональных матриц.

Для матричного маскирования матрицы должны выбираться так, чтобы они удовлетворяли следующим условиям [22]: квадратная матрица $\mathbf{A}$ порядка n с элементами $|aij| \le 1$, определенная над полем вещественных чисел и удовлетворяющая квадратичному уравнению связи $\mathbf{A}^T\mathbf{A} = \omega(n)\mathbf{I}$, где $\omega(n)$ — некоторая весовая функция, определяющая тип матрицы, а $\mathbf{I}$ — единичная матрица.

Криптографическое маскирование и демаскирование — выполнение соответствующей процедуры прямого и обратного преобразований с применением элементов криптографических методов.

Примечание: Под цифровой визуальной информацией понимаются как сохраненные или передаваемые статические изображения (данные, представляемые в виде двумерного массива значений яркости или цвета минимальной неделимой части такого изображения), так и видеоизображения, понимаемые как изображения, последовательно сменяющие друг друга во времени.

Криптографическое маскирование и демаскирование

При данном виде маскирования цифровой визуальной информации применяются криптографические методы или их элементы в совокупности с какими-либо еще преобразованиями.

Авторы методов криптографического маскирования сталкиваются с необходимостью вырабатывать специализированные подходы, позволяющие разрушить в маскированном изображении низкочастотные пространственные составляющие. Это связано с естественным свойством изображения как вида информации — избыточ-

ностью. Очевидно, что особенно остро такая проблема стоит при работе с высококонтрастными изображениями, содержащими общие планы или крупные объекты.

Кроме того, приходится сокращать вычислительную емкость собственно криптографических методов, нацеленных на длительную (в идеале — навсегда) защиту от несанкционированного доступа, обойти которую можно лишь путем подбора ключевой информации. Сокращение вычислительной емкости при маскировании изображений с малым временем актуальности по определению не требуется, а объем информации в то же время чрезвычайно велик.

Например, авторы работ [2, 3] предлагают применять модификацию блокового преобразования (например, в виде простейших операций замены и перестановки, аналогичных ГОСТ 28147-89) с некоторым изменяющимся параметром K, что позволяет обеспечить эффективное искажение структуры изображения и тем самым предотвратить наиболее распространенные методы атак. Само преобразование выполняется с использованием схемы сетей Фейстейла с не менее чем восьмью раундами, устойчивой ко всем известным в настоящее время атакам. Параметр K меняется для каждого нового блока изображения. Для обеспечения быстрой синхронизации, например при потере пакетов в коммуникационных системах, начальное значение параметра K_{i0} для пакета с номером i может быть установлено следующим образом: $K_{i0} = F(K_0, i)$.

В качестве функции $F(*,*)$ может быть выбрано простое арифметическое сложение 256-битных чисел с игнорированием разряда переполнения.

Преимуществом криптографического маскирования является более высокая устойчивость к атакам по сравнению с другим видом маскирования, недостатком — настолько же более высокая вычислительная ресурсоемкость.

Матричное маскирование и демаскирование

При матричном маскировании цифровой визуальной информации используется матричная арифметика и не используются криптографические подходы. Прикладной предпосылкой для защиты интенсивных потоков с помощью матричной арифметики сегодня является широкое применение интегральных схем цифровых сигнальных процессоров и программируемой логики в качестве вычислительной основы распределенных, встраиваемых и портативных устройств. Интегральные схемы данных классов обладают аппаратными модулями, ускоряющими операцию свертки и, соответственно, скалярного произведения векторов. Как результат, матричное умножение выполняется на аппаратном уровне, что определяет наилучшую производительность реализации вычислителя при одной и той же полупроводниковой технологии производства интегральных схем.

Использование матричных операций для маскирования цифровой визуальной информации первыми предложили И. Л. Ерош и М. Б. Сергеев [1]. Недостатком предложенного метода являлось то, что сама предложенная матрица — оператор преобразования — очень ресурсоемка для вычисления, а количество таких матриц крайне ограничено. Данного недостатка лишены новые уникальные ортогональные базисы, включающие матрицы Мерсенна, Эйлера, Ферма, Мерсенна — Уолша и др. [23–26].

Такие матрицы хотя и включают в себя иррациональные значения, но обладают одним замечательным свойством: количество различных значений элементов (уровней) в общем случае исчисляется единицами [27]. Это свойство существенным образом способствует выбору в их пользу для прикладного применения, поскольку при вычислении произведения матриц малое количество возможных вариантов множителя позволяет исключить операцию умножения — она заменяется табличной выборкой, что увеличивает производительность вычислителя, сокращает необходимые аппаратные ресурсы.

В общем случае действия по матричному маскированию и демаскированию выполняются следующим образом. Подлежащее преобразованию изображение представляется в виде двумерной матрицы, элементы которой являются численными значениями яркости его пикселей. Суть метода матричного маскирования заключается в умножении сегмента исходного изображения (двумерного набора пикселей) на маскирующую матрицу в виде $\mathbf{S} = \mathbf{P} \cdot \mathbf{M}$, где $\mathbf{S}$ — маскированное изображение; $\mathbf{P}$ — сегмент исходного изображения; $\mathbf{M}$ — матрица преобразующего оператора (маскирующая матрица).

В варианте, дающем лучшие результаты, маскирование осуществляется как $\mathbf{S} = \mathbf{M} \cdot \mathbf{P} \cdot \mathbf{M}^{\mathrm{T}}$, где $\mathbf{M}^{\mathrm{T}}$ — транспонированная маскирующая матрица.

Восстановление маскированного изображения осуществляется обратным преобразованием, т. е. умножением матрицы $\mathbf{S}$ на матрицы, обратные $\mathbf{M}$ и $\mathbf{M}^{\mathrm{T}}$, в виде $\mathbf{S} = \mathbf{M}^{\mathrm{T}} \cdot \mathbf{P} \cdot \mathbf{M}$.

К настоящему времени опубликовано значительное количество работ, описывающих результаты исследований относительно поиска [28, 29] и применения найденных вещественных квазиортогональных матриц для защиты визуальной информации [19–22, 30, 31]. Кроме того, осуществляется исследовательская работа для проверки идеи о возможности одновременного решения за-

дачи защиты от несанкционированного ознакомления и задачи сжатия визуальной информации.

Действительно, применение таких матриц как базиса ортогональных преобразований позволяет получать пространственные спектры изображений, затем выполнять традиционные для методов сжатия изображений усекающие действия в отношении наименее информативной части спектра и, наконец, устранять избыточность в оставшемся объеме информации. А широкое множество открытых квазиортогональных матриц, возможность «заказа» размерности таких матриц для выполнения преобразований в совокупности с возможностью применять процедуру перестановок строк и столбцов дают возможность использовать такой базис в системах защиты с закрытым ключом.

Заключение

Термин как слово, обозначающее определенное понятие, должен характеризоваться однозначностью. На практике одно и то же слово или словосочетание получает спектр значений, находя применение в разных областях знаний. Например, рассмотренный термин «маскирование» имеет не менее восьми специализированных значений, помимо словарного. Расширение понятия отдельных слов — процесс неизбежный, поскольку увеличивается количество направлений исследований, требующих новых определений, а толковые словари пополняются намного медленнее.

В отношении применения термина «маскирование» в области защиты цифровой визуальной информации были определены факторы, способствующие его закреплению в данном исследовательском и прикладном направлении «де-юре». Приведен также ряд отличий и ограничений, которые формально способны препятствовать признанию термина, хотя они и не носят категорического характера.

По мнению авторов настоящей работы, в пользу действительной годности термина «маскирование» в данном случае выступают следующие факторы:

— в языке отсутствует сколь-нибудь более близкая терминология с определением, способным указать точное место рассматриваемых процедур среди способов защиты информации;

— по крайней мере, одно из всех словарных определений термина напрямую обозначает цель процедур маскирования в применении к цифровой визуальной информации;

— термин успешно прошел многочисленную апробацию в результате применения в более чем 20 опубликованных работах в рецензируемых изданиях и представленных докладах на международных конференциях.

Литература

1. **Ерош И. Л., Сергеев М. Б.** Скоростное шифрование разнородных сообщений //Вопросы передачи и защиты информации: сб. ст. СПб.: СПбГУАП, 2006. С. 133–155.
2. **Литвинов М. Ю.** Алгоритмы маскирующих преобразований видеоинформации: автореф. дис. ... канд. техн. наук. — СПб.: ГУАП, 2009. — 23 с.
3. **Беззатеев С. В., Литвинов М. Ю., Трояновский Б. К., Филатов Г. П.** Выбор алгоритма преобразования, обеспечивающего изменение структуры изображений // Информационно-управляющие системы. 2006. № 6(25). С. 2–6.
4. **Балонин Н. А., Сергеев М. Б.** М-матрицы // Информационно-управляющие системы. 2011. № 1(50). С. 14–21.
5. **Научно-технический** энциклопедический словарь. http://ucheba.su/dictionary/word/1120538/ (дата обращения: 26.04.2014).
6. **Словарь** военных терминов / сост. А. М. Плехов, С. Г. Шапкин. — М.: Воениздат, 1988. — 336 с.
7. **Химическая** энциклопедия / под ред. И. Л. Кнунянца. — М.: Сов. энциклопедия, 1988. — 623 с.
8. **Оксфордский** толковый словарь по психологии: в 2 т. / под ред. А. Ребера; пер. с англ. Е. Ю. Чеботарева. — М.: Вече АСТ, 2003. Т. 1. — 592 с.
9. **Большой** психологический словарь/ под ред. Б. Г. Мещерякова, акад. В. П. Зинченко. — М.: Прайм-ЕВРОЗНАК, 2003. — 672 с.
10. **Сайт** компании Oracle. http://www.oracle.com/ (дата обращения: 04.05.2014).
11. **SecurityLab.ru,** IBM представила ПО для маскировки закрытых данных. http://www.securitylab.ru/news/301841.php (дата обращения: 03.05.2014).
12. **Железняк В. К., Барков А. В.** Экспериментальное исследование метода адаптивного маскирования видеосигнала от утечки по техническим каналам// Вестник Полоцкого государственного университета. Сер. С. Фундаментальные науки. 2014. № 4. С. 18–23.
13. **kunegin.narod.ru,** Маскиратор. http://kunegin.narod.ru/ref8/shifr/mas.htm (дата обращения: 03.08.2015).
14. **Нерезкое** маскирование. http://ru.wikipedia.org/wiki/%CD%E5%F0%E5%E7%EA%EE%E5_%EC%E0%F1%EA%E8%F0%EE%E2%E0%ED%E8%E5 (дата обращения: 11.05.2014).
15. **Справка** по Photoshop. Разд. «Маскирование слоев». http://helpx.adobe.com/ru/photoshop/using/masking-layers.html (дата обращения: 11.05.2014).
16. **Маска,** фр. masque — этимология. http://www.proza.ru/2013/05/07/483 (дата обращения: 03.08.2015).
17. **Ефремова Т. Ф.** Современный словарь русского языка три в одном: орфографический, словообра-

зовательный, морфемный. — М.: АСТ, 2010. — 699 с.
18. **Валгина Н. С.** Активные процессы в современном русском языке: учеб. пособие. — М.: Логос, 2001. — 304 с.
19. **Востриков А. А., Чернышев С. А.** Об оценке устойчивости к искажениям изображений, маскированных М-матрицами // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5. С. 99–103.
20. **Востриков А. А.** О матрицах Адамара — Мерсенна и маскировании изображений // Информационные технологии. 2013. № 11. С. 37–39.
21. **Балонин Ю. Н., Востриков А. А.** Матрицы Адамара — Мерсенна как базис ортогональных преобразований при маскировании видеоизображений // Приборостроение. 2014. № 1. С. 15–19.
22. **Востриков А. А., Мишура О. В., Сергеев А. М., Чернышев С. А.** О выборе матриц для процедур маскирования и демаскирования изображений // Фундаментальные исследования. 2015. № 2 (ч. 24). С. 5335–5339.
23. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара — Мерсенна // Информационно-управляющие системы. 2012. № 5(60). С. 92–94.
24. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара — Ферма // Информационно-управляющие системы. 2012. № 6(61). С. 90–93.
25. **Балонин Н. А., Сергеев М. Б.** О двух способах построения матриц Адамара — Эйлера // Информационно-управляющие системы. 2013. № 1(62). С. 7–10.
26. **Балонин Н. А., Балонин Ю. Н., Востриков А. А., Сергеев М. Б.** Вычисление матриц Мерсенна — Уолша // Вестник компьютерных и информационных технологий. 2014. № 11. С. 51–55.
27. **Сергеев А. М.** Обобщенные матрицы Мерсенна и гипотеза Балонина // Автоматика и вычислительная техника. 2014. № 4. С. 35–43.
28. **Балонин Н. А., Сергеев М. Б.** К вопросу существования матриц Мерсенна и Адамара // Информационно-управляющие системы. 2013. № 5(66). С. 2–8.
29. **Балонин Н. А., Сергеев М. Б.** Матрицы локального максимума детерминанта // Информационно-управляющие системы. 2014. № 1(68). С. 2–15.
30. **Балонин Ю. Н., Востриков А. А., Сергеев М. Б.** О прикладных аспектах применения М-матриц // Информационно-управляющие системы. 2012. № 1(56). С. 92–93.
31. **Vostrikov A., Chernyshev S.** Implementation of Novel Quasi-Orthogonal Matrices for Simultaneous Images Compression and Protection//Frontiers in Artificial Intelligence and Applications. 2014. Vol. 262, «Smart Digital Futures». P. 451–461. doi:10.3233/9781614994053451

UDC 004.052.2
doi:10.15217/issn1684-8853.2015.5.116

Masking of Digital Visual Data: the Term and Basic Definitions

Vostrikov A. A.[a], PhD, Tech., Associate Professor, vostricov@mail.ru
Sergeev M. B.[a], Dr. Sc., Tech., Professor, mbse@mail.ru
Litvinov M. Yu.[b], PhD, Tech., Associate Professor
[a]Department of Computing Systems and Networks Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaya St., 190000, Saint-Petersburg, Russian Federation
[b]BaumanMoscowStateTechnicalUniversity, 5/1,ul. Baumanskaya 2-ya,105005, Moscow, Russian Federation

Purpose: At present, there are several terms to describe symmetric conversions of digital visual information in order to conceal it from unauthorized review. Significant differences in the implementation of conversions, different mathematical methods and respective demands on the efficiency make it necessary that the terms are in compliance with the procedures. Our goal is to take stock of the terms "masking" and "demasking", to consider alternative terminology for conversions performed when protecting digital images with a short relevance, and to fix the most appropriate option. **Results:** A comparative analysis of terminology close in meaning to the description of the contents of digital visual information converters showed that at the moment there are no more accurate terms than "masking" and "demasking", with a definition that can specify the exact place of the discussed procedures among the information protection methods. **Practical relevance:** It is shown that the term "masking" and the associated term "demasking" are closest to the conceptual description of digital video data protective conversion with a short relevance. Basic definitions are formulated for matrix conversions of digital visual information using quasi-orthogonal bases. Matrix equations are given for the implementation of "masking" and "unmasking".

Keywords — Visual Data Protection, Image Protection, Masking, Unmasking, Quasi-Orthogonal Bases, Quasi-Orthogonal Matrix, Cryptographic Primitives.

References

1. Erosh I. L., Sergeev M. B. High-Speed Encryption Disparate Messages. *Voprosy peredachi i zashchity informatsii* [Transmission and Protection of Information]. Saint-Petersburg, GUAP Publ., 2006, pp. 133–155 (In Russian).
2. Litvinov M. Y. *Algoritmy maskiruiushchikh preobrazovanii videoinformatsii*. Dis. kand. tehn. nauk [Algorithms of Video Masking Transforms. PhD tech. sci. diss.]. Saint-Petersburg, GUAP Publ., 2006. 23 p. (In Russian).

3. Bezzateev S. V., Litvinov M. Y., Troyanovskii B. K., Filatov G. P. The Choice of the Transformation Algorithm that Ensures a Structural Change of Videoinformation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2006, no. 6(25), pp. 2–6 (In Russian).
4. Balonin N. A., Sergeev M. B. M-Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2011, no. 1(50), pp. 14–21 (In Russian).
5. *Nauchno-tekhnicheskii entsiklopedicheskii slovar'* [Scientific and Technical Encyclopedic Dictionary]. Available at: http://ucheba.su/dictionary/word/1120538/ (accessed 26 April 2014).
6. Plehov A. M., Shapkin S. G. *Slovar' voennykh terminov* [Dictionary of Military Terms]. Moscow, Voenizdat Publ., 1988. 336 p. (In Russian).
7. Knunjanc I. L. *Khimicheskaia entsiklopediia* [Chemical Encyclopedia]. Moscow, Sovetskaia entsiklopediia Publ., 1988. 336 p. (In Russian).
8. Reber A. *Oksfordskii tolkovyi slovar' po psikhologii* [The Oxford Dictionary of Psychology]. Moscow, Veche AST Publ., 2003. Vol. 2. 592 p. (In Russian).
9. Meshherjakova B. G., Zinchenko V. P. *Bol'shoi psikhologicheskii slovar'* [The Big Psychological Dictionary]. Moscow, Praim-EVROZNAK Publ., 2003. 672 p. (In Russian).
10. *Sait kompanii Oracle* [Saite of Company Oracle]. Available at: http://www.oracle.com/ (accessed 04 May 2014).
11. *IBM predstavila PO dlia maskirovki zakrytykh dannykh* [IBM Introduced the Software to Mask Sensitive Data]. Available at: http://www.securitylab.ru/news/301841.php (accessed 03 May 2014).
12. Zheleznjak V. K., Barkov A. V. Experimental Study of Adaptive Video Masking Method for Protection Against Leakage Through Technical Channels. *Vestnik Polotskogo gosudarstvennogo universiteta. Ser. C. Fundamental'nye nauki*, 2014, no. 4, pp. 18–23 (In Russian).
13. *Maskirator* [Scrambler]. Available at: http://kunegin.narod.ru/ref8/shifr/mas.htm (accessed 03 August 2015).
14. *Nerezkoe maskirovanie* [Unsharp Masking]. Available at: http://ru.wikipedia.org/wiki/%CD%E5%F0%E5%E7%EA%EE%E5_ %EC%E0%F1%EA%E8%F0%EE%E2%E0%ED%E8%E5 (accessed 11 May 2015).
15. *Spravka po Photoshop. Razdel "Maskirovanie sloev"* [Help Photoshop. Section "Masking Layers"]. Available at: http://helpx.adobe.com/ru/photoshop/using/masking-layers.html (accessed 11 May 2015).
16. *Maska, fr. masque — etimologiia* [Mask fr. masque — Etymology]. Available at: http://www.proza.ru/2013/05/07/483 (accessed 03 August 2015).
17. Efremova T. F. *Sovremennyi slovar' russkogo iazyka tri v odnom: orfograficheskii, slovoobrazovatel'nyi, morfemnyi* [Modern Dictionary of the Russian Language in One of Three: Spelling, Word-Formation, Morphemic]. Moscow, AST Publ., 2010. 699 p. (In Russian).
18. Valgina N. S. *Aktivnye protsessy v sovremennom russkom iazyke* [Active Processes in Modern Russian]. Moscow, Logos Publ., 2001. 304 p. (In Russian).
19. Vostrikov A. A., Chernyshev S. A. On Distortion Assessment of Images Masking with M-Matrices. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2013, no. 5, pp. 99–103 (In Russian).
20. Vostrikov A. A. On Hadamard–Mersenne Matrices and Image Masking. *Informatsionnye tekhnologii*, 2013, no. 11, pp. 37–39 (In Russian).
21. Balonin Y. N., Vostrikov A. A. Hadamard–Mersenne Matrices as a Basis of Orthogonal Transformation for Video Masking Encoding. *Priborostroenie*, 2014, pp. 15–19 (In Russian).
22. Vostrikov A. A., Mishura O. V., Sergeev A. M., Chernyshev S. A. The Choice of Matrices for Images Masking and Demasking Procedures. *Fundamental'nye issledovaniia*, 2015, no. 2 (part 24), pp. 5335–5339 (In Russian).
23. Balonin N. A., Sergeev M. B., Mironovsky L. A. Calculation of Hadamard–Mersenne Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2012, no. 5(60), pp. 92–94 (In Russian).
24. Balonin N. A., Sergeev M. B. Mironovsky L. A. Calculation of Hadamard–Fermat Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2012, no. 6(61), pp. 90–93 (In Russian).
25. Balonin N. A., Sergeev M. B. Two Ways to Construct Hadamard–Euler Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 1(62), pp. 7–10 (In Russian).
26. Balonin N. A., Balonin Yu. N., Vostrikov A. A., Sergeev M. B. Computation of Mersenne–Walsh Matrices. *Vestnik komp'iuternykh i informatsionnykh tekhnologii*, 2014, no. 11, pp. 51–55 (In Russian).
27. Sergeev A. M. The Generalized Matrices of Mersenne and Balonin's Conjecture. *Avtomatika i vychislitel'naia tekhnika*, 2014, no. 4, pp. 35–43 (In Russian).
28. Balonin N. A., Sergeev M. B. On the Issue of Existence of Hadamard and Mersenne Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 5(66), pp. 2–8 (In Russian).
29. Balonin N. A., Sergeev M. B. Local Maximum Determinant Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 1(68), pp. 2–15 (In Russian).
30. Balonin Yu. N., Vostrikov A. A., Sergeev M. B. Applied Aspects of M-Matrix Use. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2012, no. 1(56), pp. 92–93 (In Russian).
31. Vostrikov A., Chernyshev S. Implementation of Novel Quasi-Orthogonal Matrices for Simultaneous Images Compression and Protection. *Frontiers in Artificial Intelligence and Applications*, 2014, vol. 262, "Smart Digital Futures", pp. 451–461. doi:10.3233/9781614994053451