Электронная цифровая подпись на основе кодов, определяющих изображения с точностью до аффинных преобразований

В. Н. Козлов[1]

Первый и давний вариант защиты документа от подделки (используется и поныне) — это так называемая “живая” подпись (или факсимиле), и канцелярская печать. Однако в наши дни документооборот большей частью электронный, и, зачастую, с очень большим числом документов (электронные торги, банковские платежные системы, сделки в криптовалютах, и пр.). Здесь работает возникшая более сорока лет назад цифровая подпись. Как правило, сердцевиной цифровой подписи является функция, у которой ее значение при заданном значении аргумента вычисляется легко, а обратное, т.е. вычисление значения аргумента при известном значении функции, очень трудно.

В статье описывается аналог цифровой подписи на другой принципиальной основе, с использованием кодов изображений, определяющих их с точностью до аффинных преобразований.

Ключевые слова: электронная цифровая подпись, цифровая подпись, изображение, код изображения, аффинные преобразования, аутентификация изображения.

1. Введение

Здесь описан способ защиты электронного изображения от подделки и проверки подлинности полученной информации на основе аффинных преобразований. Способ предназначен для работы с любыми изображениями (потенциально, в том числе, и с трехмерными), или с информацией, приводимой к изображениям (например, со звуком). Этот способ может быть использован для защиты канала связи между отправителем информации в виде изображения и получателем от попыток третьих сторон отправить получателю информацию под видом информации от отправителя, а также аутентификации полученного изображения. Способ является аналогом известной электронной цифровой подписи, но на иной принципиальной базе. В основе принципа - теорема , доказанная более двадцати лет назад.

Описываемый способ запатентован [1, 2].

[1] *Козлов Вадим Никитович* — профессор каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: vnkozlov@mail.ru.

Kozlov Vadim Nikitovich — professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

2. Теоретические основы способа

Изображением [3, 4, 5] называем конечное (непустое) множество точек в евклидовых пространствах разной размерности. В частности, двумерное изображение — конечное множество точек на плоскости. Обосновываем это тем, что любую фигуру можно "аппроксимировать" конечным множеством точек, которые уже сами по себе делают фигуру вполне узнаваемой. При этом если точек много, то такая совокупность точек практически неотличима от исходной фигуры. Так же можно представлять и полутоновые, черно-бело-серые изображения, при этом разная плотность точек в разных частях изображения дает разные оттенки "серого цвета". Как известно, цветное изображение можно представлять как наложение трех монохроматических (аналогов черно-бело-серых) изображений. Это означает, что совокупностями точек можно представлять и цветные изображения. Трехмерные изображения — точки в трехмерном евклидовом пространстве. Наконец, трехмерный мир в динамике можно рассматривать как четырехмерное изображение (последовательность трехмерных сцен).

Далее рассматриваются двумерные изображения, но сказанное несложно обобщается и на случаи большей размерности.

Используется код изображения, который определяется следующим образом. Пусть задано изображение A произвольного вида (с числом точек больше трех). Перенумеровываем точки изображения A с единственным условием: разные точки — разные номера. Пусть M_A — множество номеров. Пусть S_{mnu} и S_{ksp} — площади треугольников с вершинами в точках с номерами соответственно m, n, u и k, s, p, и пусть $\rho_{mnu,ksp} = S_{mnu}/S_{ksp}$ (разумеется, S_{ksp} не равно нулю), и все числа ρ для всех пар троек m, n, u и k, s, p составляют множество T_A. При этом множество T_A — это только числа вида $\rho_{mnu,ksp}$, никакой информации об исходных треугольниках и их площадях уже нет. Код изображения A — пара $< M_A, T_A >$. Изображения A и B с кодами $< M_A, T_A >$ и $< M_B, T_B >$ назовем эквивалентными, если существует такая биекция $\psi : M_A \to M_B$, что для любых m, n, u и k, s, p из M_A выполнено $\rho_{mnu,ksp} = \rho_{\psi(m)\psi(n)\psi(u),\psi(k)\psi(s)\psi(p)}$. Ясно, что эквивалентность изображений содержательно означает одинаковость их кодов с точностью до перенумерации точек. Два изображения называем аффинно эквивалентными, если они переводимы друг в друга аффинными преобразованиями.

Изображение назовем плоским, если все его точки не лежат на одной или двух параллельных прямых. Этим из рассмотрения исключаются два довольно узких и не существенных для практики класса изображений — все точки (именно все) лежат на одной или двух параллельных прямых.

Теорема 1 ([3, 4, 5, 6]). *Два плоских изображения эквивалентны тогда и только тогда, когда они аффинно эквивалентны.*

Отметим, что эта теорема доказана также в варианте для трехмерного пространства, и, в целом, для n-мерного ($n > 3$) [7].

Содержательно аффинные преобразования — это любая комбинация преобразований параллельного переноса, вращений, симметрии, изменений в размерах, сжатий и растяжений по любому направлению. Теорема означает, что любое изображение B, переводимое в A аффинными преобразованиями, имеет тот же (с точностью до перенумерации точек) код, что и A.

И обратное, если восстанавливать изображение по коду $< M_A, T_A >$, то получающееся изображение заведомо переводится в A аффинными преобразованиями.

Тем самым, код определяет изображение с точностью до аффинных преобразований.

Возможно использование и укороченного кода, когда в T_A присутствуют числа $\rho_{mnu,ksp}$ только для четырехточечников из A, но всех возможных четырехточечников. Это значит, что из исходного T_A отбираются только те числа $\rho_{mnu,ksp}$, у которых тройки m, n, u и k, s, p разнятся только одним номером. Такой код тоже представляет изображение с точностью до аффинных преобразований.

Возможное сокращение состоит еще в том, что, как следует из определения кода, если в нем есть элемент $\rho_{mnu,ksp}$ с двумя тройками индексов, то есть и обратный элемент — единица, деленная на $\rho_{mnu,ksp}$, поэтому можно оставить в коде только те элементы, которые меньше единицы, поскольку то, что больше единицы однозначно восстанавливается.

Помимо кода $< M_A, T_A >$ изображения A рассматриваем еще и стертый код: это множество Q_A чисел, получающихся из чисел множества T_A, но с удаленными индексами при них. Назовем Q_A стертым кодом для A. Восстановить по стертому коду Q_A код $< M_A, T_A >$, а значит и изображение A, практически невозможно [8].

Возможно и некое огрубление стертого кода. Для этого промежуток от нуля до единицы разбиваем на N интервалов, где каждый интервал длины 2Δ, и рассматривают центры интервалов. Все числа из кода попадают каждое в свой интервал. После чего оставляют только числа, являющиеся серединами интервалов (возможно, с учетом кратности, то есть количества попавших в данный интервал элементов исходного кода). Так получается возможный огрубленный стертый код.

3. Описание алгоритма

Исходим из наличия схемы с тремя взаимодействующими субъектами: отправителем информации A, получателем информации B, и третьей стороной, злоумышленником C. Между A и B имеется канал связи для передачи сообщений (от A к B). Злоумышленник C может подключаться к каналу связи и, имитируя отправителя A, посылать к получателю B свои (фальшивые) сообщения. Задача состоит в том, чтобы получатель имел возможность отсортировывать фальшивые сообщения от истинных. Для этой цели отправитель имеет закрытый ключ — некоторое изображение Z, получатель — открытый ключ, представляющий собой множество чисел, являющихся стертым кодом закрытого ключа Z. Злоумышленнику закрытый ключ не известен, открытый — известен. Посылаемое к B сообщение — изображение X с числом точек не меньше четырех (по смыслу задачи — существенно больше четырех). Злоумышленник предполагается предельно информированным: он имеет возможность читать посланные сообщения, в том числе, располагает архивом всех ранее посланных сообщений, знает о существовании закрытого ключа (сам ключ не знает), знает о процедуре формирования сообщений (в том числе о вводимых ниже проверочных изображениях), все о процедуре проверки полученного сообщения у получателя, знает, как уже упоминалось, открытый ключ, т.е. знает все, кроме закрытого ключа.

Далее — более подробно об этой схеме, об алгоритме работы описываемой модели, и о его этапах (пункты I – VII).

I. У отправителя формируют закрытый ключ безопасности Z в виде электронного точечного изображения. Закрытый ключ имеется у отправителя и исходно представляет собой преимущественно физический носитель, такой как магнитная карта, листовой документ с магнитными метками, документ с печатными метками или символами (буквами, цифрами и пр.). Таким образом, закрытый ключ исходно — это любой объект, содержащий информацию, эквивалентом которой может быть электронное изображение. Каждая магнитная частица может быть представлена в виде точки и каждый пиксель отсканированного документа также может быть представлен в виде точки или совокупности точек, образовывая электронные изображения в виде конечного множество точек на декартовой плоскости. Для дальнейшей работы необходимо иметь указанное электронное изображение Z. Преобразование пикселя в точку и магнитной частицы в точку осуществляется очевидными простыми алгоритмами. В качестве примера, пусть дано электронное пиксельное чёрно-белое изображение, у пикселей есть градации темноты нуль (белый пиксель) и единица (черный пиксель). В этом

случае действуют следующим образом: пиксель — это маленький квадрат, и имея черно-белое изображение, белый пиксель оставляют пустым, а вместо черного пикселя ставят точку. И изображение из пикселей преобразуется в изображение из точек. Если изображение полутоновое чёрно-белое, тогда пиксели имеют градацию темноты от нуля до $K-1$. Преобразовывают это в изображение из точек следующим образом: снова ставят в квадрат точки, если с градацией единица (не белый квадрат) — ставят одну точку, если градация два (уже темнее) ставят 2 точки в этом квадрате и так далее вплоть до $K-1$ (до самого темного), и изображение из пикселей превращается в изображение из точек, где разная плотность точек в разных частях изображения обеспечивает светлый или темный тон. Градация определяется тем, что в пиксельных изображениях каждый квадрат уже изначально имеет одну из K — градаций, в этом состоит суть пиксельного изображения, т.е. градации определяются любыми доступными графическими программами.

Множествами точек можно представлять и цветные изображения, тогда необходимо применить преобразование пикселей в точки для каждого из цветных каналов RGB отдельно. Либо преобразовывают изображение в черно-белое, а только затем в точечное.

Предполагается, что магнитные частицы-точки изначально распределены хаотично, неважно откуда — с бумажного носителя или с магнитного. По аналогии с пиксельным преобразованием, если есть частица, в квадрате ставят точку, если нет — оставляют пустой, если есть скопления точек, обращаются к градациям.

Слова “изображение”, “электронное изображение”, “электронное точечное изображение” с очевидностью довольно близки по смыслу (исключая электронное пиксельное изображение), поэтому далее они рассматриваются как практически синонимы.

II. Далее формируют из подлинной исходной информации для отправления электронное пиксельное изображение. Фото, документы, иные материалы для отправления оцифровывают любыми известными аппаратными средствами, например, сканируют, так получают электронное пиксельное изображение для следующего этапа. Либо данные для передачи могут быть у отправителя в виде электронного пиксельного изображения изначально.

III. Из полученного электронного пиксельного изображения формируют сообщение X в виде электронного точечного изображения по аналогии с п. I.

IV. Кодируют закрытый ключ Z, формируя для получателя открытый ключ — конечное множество чисел Q_Z кода закрытого ключа Z.

V. Формируют как минимум одно проверочное аффинно-эквивалентное части закрытого ключа Z электронное точечное изображение Y у отправителя. В начале этапа у отправителя есть электронное точечное изображение X, которое он должен отправить получателю. У получателя есть открытый ключ. Ценность этапа состоит в том, что отправитель посылает получателю информацию, и предусмотрено средство, которое не позволит злоумышленнику, даже располагая подробной информацией о модели, получить данные о закрытом ключе и выдать себя за отправителя. Для этого отправляют сообщение X получателю, но для защиты снабжают его одним или несколькими дополнительными изображениями Y — проверочными. Поэтому в конце этапа у отправителя должны быть изображение X — сообщение, и некоторые изображения $Y_1 - Y_k$ — проверочные, сформированные у отправителя с помощью закрытого ключа, как будет описано ниже. Изображение Y — проверочное, тест и защита, его роль — участвовать в проверке подлинности сообщения X. Полагаем, изображение Y аффинно эквивалентно с некоторыми подизображениями (т.е. подмножествами точек) одновременно как в X, так и в Z, причем это максимальное по количеству точек такое изображение, т.е. при добавлении хотя бы одной точки аффинная эквивалентность нарушится.

   Обозначают через $Y + 1$ изображение "с добавленной точкой", т.е. это изображение в сравнении с Y имеет добавленную точку, и оно аффинно-эквивалентно с некоторым подмножеством точек в X. По построению, $Y+1$ уже не аффинно-эквивалентное ни с каким подизображением в Z (это и означает максимальность исходного изображения Y). Множество всех таких $Y+1$ обозначим через $\{Y+1\}$. Для каждого $Y+1$ из $\{Y+1\}$ проверяем условие: стертый код для $Y + 1$ не является подмножеством стертого кода Q_Z. Если условие не выполняется, то $Y + 1$ называем особым. Отправителю нет нужды направлять получателю информацию о множестве $\{Y + 1\}$ — оно легко строится по X и Y, исключая особые изображения, о них получателю сообщается. Здесь описана ситуация с одним проверочным изображением, но их может быть и несколько.

   Отметим для корректности, что полагаем исключенными очевидно вырожденные и легко проверяемые случаи, когда X совпадает с Z, или Z является частью X, или X является частью Z.

VI. Посылают получателю сообщение X и как минимум одно полученное проверочное электронное точечное изображение Y.

VII. Осуществляют аутентификацию полученного сообщения X по проверочному изображению Y и по стертому коду Q_Z.

Проверку по аффинной эквивалентности электронного точечного изображения Y подмножеству точек сообщения X и по Q_Z проводят следующим образом:

1) проверяется, является ли изображение Y аффинно-эквивалентным с некоторыми подизображениями (подмножествами точек) сообщения X,
2) является ли стертый код Q_Y проверочного изображения Y подмножеством стертого кода Q_Z закрытого ключа Z (т.е. подмножеством открытого ключа),
3) а) является ли стертый код каждого из изображений из $\{Y+1\}$, исключая особые, подмножеством открытого ключа,
   б) является ли стертый код каждого из особых изображений в $\{Y+1\}$ подмножеством открытого ключа.

Ответы “да” на вопросы 1 и 2, “нет” на 3а и “да” на 3б означают, что сообщение X подлинное и получено именно от авторизованного отправителя.

4. Возможные дополнения (опции)

Далее описаны (пункты 1 – 5) некоторые возможные дополнения для использования в алгоритме, представленном этапами I – VII.

1. Посылаемое изображение X может оказаться чрезмерно большим по количеству составляющих его точек, поэтому электронные точечные изображения подлинной исходной информации сообщения X могут быть сжаты в меньшие по объему с сохранением защиты данных. Для этого после формирования сообщения X в виде электронного точечного изображения на него накладывают виртуальную сетку из квадратных ячеек, задают каждому квадрату градацию по количеству точек в каждой ячейке и образовывают электронное точечное изображение с меньшим числом точек (аналогично пункту 1 в описании этапов алгоритма, т.е. через своеобразное прореживание сообщения X). Возможен при этом вариант, когда новые точки в каждой ячейке (числом меньшим, чем их было прежде) выбираем из множества прежних точек. Это означает

в этом случае, что стертый код нового изображения будет подмножеством стертого кода прежнего Получившееся новое сообщение X_1 используем далее по способу вместо сообщения X, а получателю посылаем сообщение X с наложенной виртуальной сеткой и изображение X_1.

2. Стертый код Q упрощают и сокращают следующими возможными способами:

   а) убирают в нем повторение чисел, т.е. от каждого множества одинаковых чисел (если они есть) оставляют в нем только одно число,

   б) оставляют в нем только числа меньшие или равные единице,

   в) разбивают сегмент от 0 до 1 на N частей длины $1/N = 2\Delta$.

   Затем заменяют каждое число в стертом коде на середину части, в которую он попадает. Обозначают через Q'_Z множество получившихся чисел.

   Эти три пункта меняют вопрос 2 при проверке аутентификации в преимущественном описании способа выше следующим образом:

   1) имеется ли для каждого числа, меньшего или равного единице, из стертого кода Q_Y проверочного изображения Y, число из Q'_Z, отличающееся от него не более, чем на Δ. Вопросы в пункте 3 меняются на следующие:

   2) а) имеется ли для каждого числа, меньшего или равного единице, из стертого кода каждого из изображений в $\{Y+1\}$, исключая особые, число из Q'_Z, отличающееся от него не более, чем на Δ.

      б) имеется ли для каждого числа, меньшего или равного единице из кода особого изображения в $\{Y+1\}$, число из Q'_Z, отличающееся от него не более, чем на Δ.

      В целом это дополнение к основному описанию сокращает стертый код (открытый ключ), и упрощает алгоритм проверки сообщения X на достоверность.

3. Особые изображения среди изображений множества $\{Y+1\}$ из пункта V описания способа возникают по следующим причинам. Если некоторое изображение B аффинно эквивалентно части изображения A, то стертый код Q_B есть подмножество стертого кода

Q_A, но обратное неверно, т.е. стертый код Q_B может быть подмножеством стертого кода Q_A, но B при этом не аффинно эквивалентно части изображения A. Элементы стертых кодов — просто обезличенные числа, поэтому среди большого множества чисел Q_A могут "разрознено", "случайно" найтись все числа из небольшого Q_B, хотя вместе они в A не составляли код некоторого подизображения. Такое маловероятно, но возможно, поэтому такое изображение и называется особым.

4. Поиск на изображении Z (закрытом ключе) и X (сообщении) общего подизображения Y, а также проверка получателем совпадения (разумеется, с точностью до аффинных преобразований) проверочного изображения Y с каждым из некоторого множества частей сообщения X, имеют нечто общее, заключающееся в том, что нужно определить, является ли некоторое изображение B частью (с точностью до аффинных преобразований) некоторого изображения A. Конечно, это можно сделать тривиальным перебором по всем подизображениям, но это не рационально. Делают так: на изображении A выбирают три точки a_1, a_2, a_3 (произвольные, но не лежащие на одной прямой). Выбирают на B три точки b_1, b_2, b_3 (произвольные, но не лежащие на одной прямой). Совмещают аффинным преобразованием точки b_1, b_2, b_3 с точками соответственно a_1, a_2, a_3, такое преобразование существует и единственно. Если B аффинно эквивалентно с частью изображения A, причем с соответствием точек b_1, b_2, b_3 точкам a_1, a_2, a_3, то и остальные точки изображения B совместятся с соответствующими точками изображения A. Если нет, то проделывается описанное со всеми тройками точек на A и всеми вариантами соответствия между точками в тройках из A и B. Либо получается совмещение B с частью A, либо делается вывод, что B аффино не эквивалентно никакой части в A.

5. В пункте V описания алгоритма в рамках поиска на изображении Z (закрытом ключе) и X (сообщении) общего для них подизображения Y, а также проверке получателем совпадения (с точностью до аффинных преобразований) проверочного изображения Y с каждым из некоторого множества частей сообщения X, присутствовала общая для них подзадача, заключающаяся в том, что нужно определить, является ли некоторое изображение B частью (с точностью до аффинных преобразований) некоторого изображения A. Но может статься, что такого общего подизображения Y, с числом точек больше трех, нет. Тогда для Y, по-прежнему аффинно эквивалентного части X, полного аффинного совпадения с частью в Z можно не требовать, а требовать только "приблизительного совпа-

дения", с "зазором ε", и называть это ε-эквивалентностью. Выяснение, является ли некоторое изображение B частью (с точностью до ε-эквивалентности) некоторого изображения A, выглядит следующим образом.

Выбирают на B три точки b_1, b_2, b_3 (произвольные, но не лежащие на одной прямой), ставят им в соответствие три произвольные (но не на одной прямой) точки a_1, a_2, a_3 изображения A. Берут на B точку x_1, сопоставляют ей некоторую точку y_1 на A. Если теперь элементы кода изображения из точек b_1, b_2, b_3 и x_1 отличаются от соответствующих элементов кода изображения из точек a_1, a_2, a_3 и y_1 на A не более, чем на ε, то точку y_1 называют приемлемой при соответствии с точкой x_1. Если точка y_1 оказалась не приемлемой, то берут другую точку из A в качестве точки y_1 и повторяют рассуждение. Затем то же делают для точки x_2, и т.д. Пусть B состоит из точек b_1, b_2, b_3, $x_1, ..., x_k$, и для точек $x_1, ..., x_k$ найдены соответствующие приемлемые точки $y_1, ..., y_k$ на A. Тогда для изображения B из точек b_1, b_2, b_3, $x_1, ..., x_k$ и изображения A' из точек a_1, a_2, a_3, $y_1, ..., y_k$ (при указанном соответствии) проверяют в целом различие всех соответствующих элементов их кодов не более, чем на ε. При положительном результате проверки подизображение A' изображения A называют искомым.

Если первоначально выбранные тройки точек a_1, a_2, a_3 и b_1, b_2, b_3 не дали возможность для каждой из точек $x_1, ..., x_k$ подобрать приемлемые точки $y_1, ..., y_k$, то проделывается описанное со всеми тройками точек на A и B и всеми вариантами соответствия между точками в тройках. В результате либо находят искомое изображение, либо делают вывод, что такого изображения нет.

Разумеется, при сравнении чисел из Q_Y с числами из Q_Z для Y, подобранного в рамках описанной процедуры, нужно учитывать величину ε.

В частном случае при $\varepsilon = 0$ процедура с очевидностью превращается в поиск на A части, аффинно эквивалентной с B, но, в отличие от предыдущего пункта 4, только по коду, без использования геометрических преобразований.

5. Заключение. Атаки на подпись

В заключение представим три типа возможных "атак" на модель со стороны третьих лиц и ее "реакцию" на атаки. Атака может состоять в том, что третье лицо со стороны, не имеющее закрытого ключа, пытается отправить получателю сообщение под видом сообщения от отправителя.

Полагаем, он располагает максимально подробной информацией о модели, ее алгоритмах, включая примеры ранее посланных сообщений с проверочными изображениями.

Первый и простой случай состоит в том, что вместе с X в качестве проверочного отправляется изображение Y, взятое наугад из числа подизображений сообщения X. Поскольку Y не является подизображением для Z, то проверка на открытом ключе выявит это. Конечно, возможно случайное совпадение Y с подизображением на Z, однако это маловероятно. Действительно, по смыслу предполагаемых разными изображений X и Z у них сравнительно немного аффинно совпадающих подизображений. При этом если, например, X содержит 100 точек (не очень много), то оценка сверху для числа всех его подизображений — два в степени 100. Это число с тридцатью знаками. Маловероятно, чтобы наугад взятое из этого множества изображение совпало с одним из общих для X и Z.

Более сложный случай — взять одно из ранее посланных проверочных изображений Y, присоединить его как часть к фальшивому изображению, все вместе назвать сообщением X, и Y сделать при нем проверочным изображением. Тогда Y пройдет проверку и на то, чтобы быть подизображением сообщения X, и на то, что его стертый код есть подмножество открытого ключа. Но он не выдержит проверку на максимальность как подизображения в "составном" сообщении X, то есть проверку на стертые коды изображений из множества $\{Y + 1\}$ на открытом ключе.

Если, наконец, полагать, что это третье лицо, собрав статистику всех ранее посланных проверочных изображений, попытается по ней восстановить закрытый ключ, то оно столкнется с комбинаторной проблемой, некоторым аналогом которой, например, можно считать гипотезу Улама из теории графов [9]. Эта проблема сложна, стоит с 1945 года и до сих пор не решена.

Список литературы

[1] Козлов В. Н., Способ аутентификации электронного изображения. Патент на изобретение №2779379. Дата государственной регистрации в Государственном реестре изобретений Российской Федерации 06 сентября 2022 года.

[2] Козлов В. Н., Способ защиты электронного изображения на основе аффинных преобразований. Патент на изобретение №2791834. Дата государственной регистрации в Государственном реестре изобретений Российской Федерации 13 марта 2023 года.

[3] Козлов В. Н., *Введение в математическую теорию зрительного восприятия*, М.: Издательство Центра прикладных исследований при механико-математическом факультете МГУ, 2007, 136 с.

[4] Kozlov V. N., "Conclusiveness and Heuristics in Visual Recognition", *Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications*, **24**:4 (2014), 1–7

[5] Kozlov V. N., "Image Coding and Recognition and Some Problems of Stereovision", *Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications*, **7**:4 (1997), 448–466

[6] Кудрявцев В. Б., Гасанов Э. Э., Подколзин А. С., *Введение в теорию интеллектуальных систем*, МАКС Пресс, 2006, 208 с.

[7] Агниашвили П. Г., "О восстановлении изображений по кодам в некоторых вырожденных случаях", *Интеллектуальные системы. Теория и приложения*, **17**:1-4 (2013), 11-15

[8] Алексеев Д. В., "Необходимые и достаточные условия существования изображения с заданным кодом", *Интеллектуальные системы. Теория и приложения*, **24**:2 (2020), 55–66

[9] Емеличев В. А., О.И.Мельников О. И.В., Сарванов В. И., Тышкевич Р. И.,, *Лекции по теории графов*, Наука, 1990, 384 с.

Electronic digital signature based on codes, defining images up to affine transformations

Kozlov V.N.

The first and long-standing variant of protecting a document from forgery (it is still used today) is the so-called "living" signature (or facsimile), and a clerical seal. However, nowadays the document flow is mostly electronic, and often with a very large number of documents (electronic trading, bank payment systems, transactions in cryptocurrencies, etc.). The digital signature that emerged more then forty years ago works here. As a rule, the core of a digital signature is a function whose value is easily calculated for a given argument value, and the reverse, i.e. calculating the value of an argument given the value of a function is very difficult.

The article describes an analogue of a digital signature on a different fundamental basis, using image codes that define them up to affine transformations.

Keywords: digital signature, image, image code, affine transformations, image authentication.

References

[1] Kozlov V. N., A method for authenticating an electronic image. Patent for invention No. 2779379. Date of state registration in the State Register of Inventions of the Russian Federation September 06, 2022.

[2] Kozlov V. N., A method for protecting an electronic image based on affine transformations. Patent for invention No. 2791834. Date of state registration in the State Register of Inventions of the Russian Federation March 13, 2023.

[3] Kozlov V. N., *Vvedenie v matematicheskuyu teoriyu zritel'nogo vospriyatiya [Introduction to the mathematical theory of visual perception]*, Publishing House of the Center for Applied Research at the Faculty of Mechanics and Mathematics of Moscow State University, Moscow, 2007 (in Russian), 136 c.

[4] Kozlov V. N., "Conclusiveness and Heuristics in Visual Recognition", *Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications*, **24**:4 (2014), 1–7

[5] Kozlov V. N., "Image Coding and Recognition and Some Problems of Stereovision", *Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications*, **7**:4 (1997), 448–466

[6] Kudryavtsev V. B., Gasanov E. E., Podkolzin A. S., *Vvedenie v teoriyu intellektual'nykh sistem [Introduction to the theory of intelligent systems]*, MAKS Press, 2006 (in Russian), 208 c.

[7] Agniashvili P. G., "On image restoration from codes in some degenerate cases", *jour Intelligent systems. Theory and applications*, **17**:1-4 (2013), 11-15 (in Russian)

[8] Alekseev D. V., "Necessary and sufficient conditions for the existence of an image with a given code", *Intelligent Systems. Theory and Applications*, **24**:2 (2020), 55–66 (in Russian)

[9] Emelichev V. A., Melnikov O. I., Sarvanov V. I., Tyshkevich R. I.,, *Lectures on graph theory*, Science, 1990 (in Russian), 384 c.