

Ручай А., Явтушенко Е.

БЫСТРЫЙ ПОИСК ИЗОБРАЖЕНИЙ С ПОМОЩЬЮ ПЕРЦЕПТИВНЫХ ХЕШЕЙ НА ОСНОВЕ КАСКАДНОГО АЛГОРИТМА

В данной статье мы предлагаем перцептуальный метод хеширования, основанный на каскадном алгоритме, который может применяться для аутентификации, поиска и индексации изображений. Перцептуальные алгоритмы хеширования используются для поиска изображений, искажённых в результате сжатия, добавления шума, общей обработки сигнала, различных геометрических модификаций. Главный недостаток перцептуального хеширования – низкая скорость. В представленном каскадном алгоритме первоначально поиск осуществляется с помощью «короткого» хеша, благодаря чему большая часть ненужной информации отсеивается на первых этапах сравнения. Затем оставшиеся хеши изображений сравниваются по полному хешу для уточнения результата. Эксперименты показали, что каскадный алгоритм имеет высокую эффективность, а именно устойчивость хеша к различным модификациям изображений и небольшие временные затраты.

Ключевые слова: перцептивный хеш, поиск изображений, хеш изображений.

Ruchay A., Yavtushenko E.

FAST PERCEPTUAL IMAGE HASH BASED ON CASCADE ALGORITHM

In this paper, we propose a perceptual image hash algorithm based on cascade algorithm, which can be applied in image authentication, retrieval, and indexing. Image perceptual hash uses for image retrieval in sense of human perception against distortions caused by compression, noise, common signal processing and geometrical modifications. The main disadvantage of perceptual hash is high time expenses. In the proposed cascade algorithm of image retrieval initializes with short hashes, and then a full hash is applied to the processed results.

Computer simulation results show that the proposed hash algorithm yields a good performance in terms of robustness, discriminability, and time expenses.

Keywords: perceptual hash, fast hash, image hash.

1. Введение

С ускоряющимся темпом развития информационных технологий неизбежно увеличивается число данных, которые необходимо защищать. Таким образом, задачи охраны конфиденциальности, целостности, аутенти-

фикации и индексирования изображений становятся всё более актуальными¹⁻³. В частности, проблема аутентификации изображений привлекает большое внимание науки в последнее время, так как большинство приложений поддерживают работу с базами дан-

ных, по которым требуется осуществлять быстрый и эффективный поиск. В связи с этим хеширование изображений играет большую роль. Входному изображению сопоставляется короткий двоичный код, который должен отражать представление содержимого картинки. Стандартные криптографические хеш-функции не могут справиться с этой задачей, так как они чувствительны даже к небольшому изменению изображения. Перцептивные хеши представляют собой альтернативное решение. Они основаны на извлечении признаков изображения и вычислении последовательности бит хеша на основе этих признаков.

Хеш должен удовлетворять следующим условиям: робастность, устойчивость к коллизиям, безопасность¹⁴⁻¹⁶. Сложность аутентификации связана с наложением шума на изображения, их различными модификациями, такими как поворот, изменения масштаба¹⁷⁻¹⁸. Это необходимо учитывать при тестировании для достижения высокой точности алгоритмов. Тестирование нужно проводить на базе, состоящей из различных модификаций изображений.

Кроме того, существуют дополнительные требования к вычислению перцептивных хешей. Они особенно важны для анализа большого объема изображений (например, при поиске в интернете для проверки нарушения авторских прав).

В настоящее время существует большое количество различных видов схем хеширования, но не так много различных схем сравнения хешей²⁰⁻²¹. Схема *дискретного косинусного преобразования (ДКП) основана на вычислении коэффициентов для построения короткого хеша*. ДКП представляет входной сигнал как сумму синусоид с соответствующими частотами и амплитудами и извлекает низкие частотные компоненты изображения, которые несут больше всего информации. Недостаток данного метода в низких показателях робастности, но он обеспечивает высокую устойчивость к коллизиям²². Оператор Марра-Хилдрета основан на определении краёв изображения. При вычислении данного хеша к функции Гаусса применяется оператор Лапласа. Недостаток этого метода хеширования в чувствительности к повороту изображений. Перцептивная хеш-функция, основанная на преобразовании Радона представляет собой интегральное преобразование функции вдоль прямой, перпендикуляр-

ной вектору. В данном методе используется дисперсия вместо суммы значений пикселей. Результатом преобразования является вектор радиальной дисперсии. К нему применяется ДКП и формируется хеш, состоящий из первых 40 коэффициентов вектора. Остальные компоненты вектора исключаются^{20,23,24}.

В данной работе мы предлагаем новый перцептивный хеш, основанный на каскадном алгоритме сравнения, который может быть применён для аутентификации, поиска и индексирования изображений. Сравнение хешей упорядоченно бит за битом может происходить достаточно медленно при больших объёмах данных. Каскадный алгоритм решает эту проблему.

2. Предлагаемый алгоритм

В работе мы используем блочный хеш, построенный на основе среднего значения. Существуют четыре различные схемы формирования данного вида хеша, объединённые общими этапами:

1. Конвертирование изображения в оттенки серого и изменение размера;
2. Разбиение матрицы пикселей на блоки;
5. Вычисление среднего значения пикселей в каждом блоке элементов матрицы;
6. Получение среднего значения всех блоков;
7. Формирование последовательности бит хеша в зависимости от среднего значения по следующей формуле:

$$h_i = \begin{cases} 1, v_i > avg \\ 0, v_i < avg \end{cases}$$

где v_i - среднее значение блока с номером i , avg - среднее значение всех блоков. Сравнение хешей осуществляется с помощью расстояния Хемминга, которое вычисляется за короткое время²¹.

В работе рассмотрены два алгоритма на блочном хеше, основанном на среднем значении. Первый из них формирует хеш изображения размером 1024 бита (в дальнейшем будем называть его алгоритм полного хеша). Второй (каскадный) – производит последовательность битовых сравнений.

2.1. Алгоритм полного хеша

Для построения полного хеша изображения необходимо выполнить следующие шаги:

- 1) Предобработка включает в себя размытие изображения фильтром Гаусса. Благодаря этому из изображения удаляются шумы и

уменьшаются высокочастотные компоненты изображения.

2) Затем изображение конвертируется в оттенки серого и уменьшается до размера 32x32 (со ступенчатой интерполяцией). Таким образом, получается всего 1024 пикселей. Вычисляется их среднее значение.

3) Затем определяется каждый бит хеша в зависимости от среднего значения блоков.

Для сравнения хешей определённым образом задаётся порог. Если расстояние меньше выбранного порога, то считаем, что исходные объекты были достаточно схожие, иначе объекты различаются. Таким образом, выбор порога очень важен, так как от него зависит результат работы алгоритма полного хеша 20. Обозначим через $I1$, $I2$ сравниваемые изображения, R – порог, $h(I1)$, $h(I2)$ – значения перцептивных хешей изображений, $d(h(I1), h(I2))$ – расстояние Хемминга между соответствующими хешами, тогда можно определить:

$$I1 \simeq I2 \text{ if } d(h(I1), h(I2)) \leq R.$$

Оптимальное значение порога определяется как пересечение двух величин: ошибки первого рода, FRR (False Rejection Rate) и ошибки второго рода, FAR (False Acceptance Rate).

FRR – «не пропустить своего». В контексте данной работы это вероятность того, что в результате действия алгоритма не найдено изображений, подобных данному, несмотря на то, что они там есть. Одинаковые изображения идентифицируются как разные. Данная ошибка может появляться при повышении порога чувствительности или при сильном различии между изображениями. Эта вероятность является наиболее значимой в данном исследовании.

FAR – это вероятность «пропустить чужого», то есть алгоритм находит изображения, которые не являются сходными с входным объектом, идентифицируя их как похожие²⁰. Средняя ошибка EER (Equal Error Rate) используется для предопределения пороговых значений для FAR и FRR.

2.2 Каскадный алгоритм

Мы предлагаем новый подход к сравнению хешей, основанный на каскадах. Он выполняется на базе алгоритма полного хеша с дополнительными действиями. После вычисления полный хеш должен быть отсортиро-

ван, определены наиболее значимые (информативные) биты. При этом выполняются следующие действия:

1) Вычислить среднюю информативность E_i бита под номером i полного хеша:

$$E_i = \left| \frac{\sum_{l=1}^N (h_l)_i}{N} \right| - 0.5, i = 1, \dots, 1024,$$

где $(h_l)_i$ – бит под номером i хеша изображения под номером l , N – число изображений в базе данных.

Таким образом, необходимо вычислить сумму соответствующих значений бит хеша всех имеющихся в базе изображений, разделить на их количество и вычесть 0.5. Наиболее информативными являются те биты, среднее значение которых близко к 0.5, так как в исходных изображениях соответствующие биты равновероятно принимали значение 0 и 1 (то есть определяли индивидуальные особенности изображений, а не общие черты).

2) Расположить биты в возрастающем порядке. Наиболее важными являются близкие по значению к 0.5.

3) Отсортировать биты хеша в соответствии с полученным порядком информативности бит, начиная от самого важного (меньшего) значения.

4) После сортировки хеш разбивается на несколько блоков. Обозначим блоки N_i , $i = 1, 2, \dots, 5$, где размер соответствующего блока составляет 8, 8, 16, 32, 960. Таким образом, 8 бит одного хеша сравниваются с 8 битами другого хеша, в соответствии с предопределённым порогом часть хешей отбрасывается, а оставшаяся часть передаётся на другой каскад. Сравниваются следующие 8 бит и т.д. Фильтр на каждом этапе отсеивает часть хешей, не проходящих по порогу. Кроме того был рассмотрен другой набор блоков: S_i , $i = 1, \dots, 7$, где где размер соответствующего блока составляет 8, 8, 16, 32, 64, 128, 768 соответственно. При этом скорость поиска увеличивается.

3. Оценка и тестирование предложенных алгоритмов

В этом разделе представлены результаты компьютерного моделирования рассматриваемых алгоритмов. Произведён анализ с точки зрения эффективности, скорости и точности.

Для экспериментов была собрана база данных из 10000 изображений. Для анализа работы алгоритмов было исследовано 25 видов модификаций изображений²⁶:

- 1) Сжатие (JPG Q=40, JPG Q=75, JPG Q=90);
- 2) Фильтрация (фильтр Гаусса, увеличение резкости, медианный фильтр)
- 3) Геометрические искажения (масштабирование с коэффициентами 0.5, 2.0; удаление части изображения (2%, 5%, 10%, 20%); сдвиг

- ние (2) + удаление части изображения (5%), поворот (2 градуса) + масштабирование (0.5) + удаление части изображения (10%), поворот (-2 градуса) + масштабирование (1.5) + удаление части изображения (1%));
- 4) Наложение шума (Гауссов шум (0.01),

Таблица 1.

Значения средней ошибки алгоритма с соответствующим порогом для каждого типа модификации.

Тип модификации изображения	Средняя ошибка	Значение порога
JPG Q=40	0,0005	201
JPG Q=75	0,0003	191
JPG Q=90	0,0001	171
Фильтр Гаусса	0,0015	231
Увеличение резкости	0	111
Медианный фильтр	0	101
Масштабирование 0.5	0,0008	221
Масштабирование 2.0	0,0001	171
Удаление части изображения, 2%	0,0168	321
Удаление части изображения, 5%	0,0361	361
Удаление части изображения, 10%	0,0346	351
Удаление части изображения, 20%	0,0748	391
Сдвиг фрагмента изображения, 2%	0,0051	281
Сдвиг фрагмента изображения, 5%	0,0128	311
Поворот (2 градуса) + масштабирование (0.5) + удаление части изображения (2%)	0,0287	351
Поворот (5 градусов) + масштабирование (2) + удаление части изображения (5%)	0,094	401
Поворот (-2 градуса) + масштабирование (0.5) + удаление части изображения (5%)	0,0925	371
Поворот (-5 градусов) + масштабирование (2) + удаление части изображения (5%)	0,048	401
Поворот (2 градуса) + масштабирование (0.5) + удаление части изображения (10%)	0,0514	371
Поворот (-2 градуса) + масштабирование (1.5) + удаление части изображения (1%)	0,0247	341
Гауссов шум (0.01)	0,0074	311
Шум «соль и перец» (0.02)	0,0005	211
«Пятнистый» шум (0.01)	0,0047	281
Эквализация гистограмм	0,0067	281
Увеличение яркости	0,0088	291

фрагмента изображения (2%, 5%); смешанные преобразования (поворот (2 градуса) + масштабирование (0.5) + удаление части изображения (2%), поворот (5 градусов) + масштабирование (2) + удаление части изображения (5%), поворот (-2 градуса) + масштабирование (0.5) + удаление части изображения (5%), поворот (-5 градусов) + масштабиро-

«соль и перец» (0.02), «пятнистый» шум (0.01))

5) Световые искажения (эквализация гистограмм, увеличение яркости).

Для каждого типа модификации были получены значения FAR, FRR и EER. Значения ERR с соответствующим порогом для всех типов искажений представлены в Таблице 1.

Графики FAR и FRR для всех типов моди-

фикаций представлены на Рисунке 1, где ERR составляет 0.04. В ходе исследования было решено убрать из рассмотрения следующие типы модификаций: удаление части изображения 5%, удаление части изображения 10%, удаление части изображения 20%, поворот (2 градуса) + масштабирование (0.5) + удаление части изображения (2%), поворот (5 градуса) + масштабирование (2) + удаление части изображения (5%), поворот (-5 градуса) + масштабирование (2) + удаление части изображения (5%), поворот (2 градуса) + масштабирование (0.5) + удаление части изображения (10%), поворот (-2 градуса) + масштабирование (1.5) + удаление части изображения (1%). Данные типы модификаций показали самое высокое значение ошибки. Таким образом, в дальнейшем мы будем рассматривать 16 из 25 видов искажений изображения. FAR и FRR для сокращённого списка модификаций представлен на Рисунке 2, где ERR составляет 0.0054 при значении порога 300. Для данного исследования большую роль играет ошибка первого рода, поэтому мы можем установить значении порога равным 380 и получить значения FAR= 0.04922 и FRR= 0.00125. Среднее время выполнения алгоритма полного хеша для каждого изображения составляет 0.49 секунд для одного изображения.

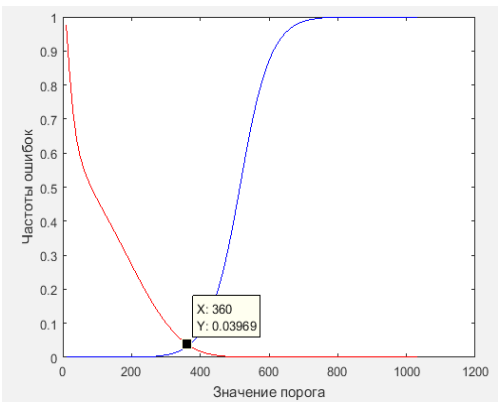


Рисунок 1. График вероятностей ошибок для всех типов модификаций

Работа каскадного алгоритма также была проанализирована. Были найдены значения порога для каждого каскада по отдельности для 16 типов модификаций. Значения FAR, FRR и значение порога для каждого из пяти каскадов представлены в Таблице 2. Средняя ошибка нашего алгоритма с пятью каскадами составляет 0.00385, время выполнения – 0.35 секунд для каждого изображения – меньше,

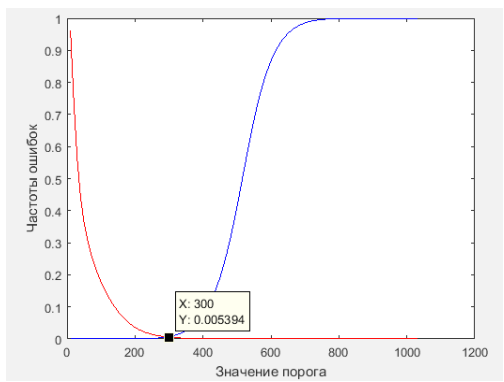


Рисунок 2. График вероятностей ошибок для 16 типов модификаций

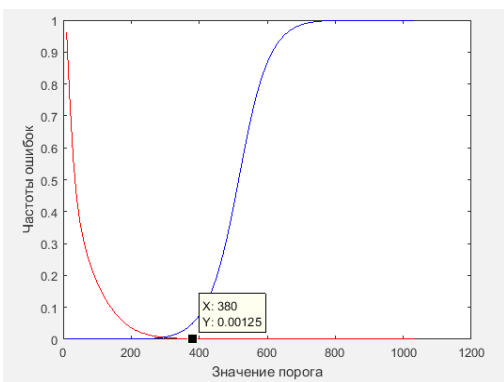


Рисунок 2. График вероятностей ошибок для изменённого значения порога.

чем для алгоритма по полному хешу. Значения FAR, FRR и значение порога для каждого из семи каскадов представлены в Таблице 3. Средняя ошибка в этом случае составляет 0.0032, время выполнения – 0.298 секунд для каждого изображения.

Сравнение теоретических и экспериментально полученных значений времени работы алгоритма представлено в Таблице 4. Теоретическое время выполнения алгоритма рассчитывалось как количество бит хеша для реализации поиска в базе данных из 10000 изображений. Экспериментальное время определялось как среднее количество секунд, которые были потрачены на поиск одного изображения в базе данных. Из полученных результатов можно сделать вывод, что показатели алгоритма могут быть улучшены при дальнейшей оптимизации. Предлагаемый каскадный алгоритм является эффективным для поиска изображений.

4. Выводы

В данной статье мы представили алгоритм перцептуального хеширования изображений

Таблица 2.

Значения FAR и FRR, величина порога для каждого из пяти каскадов по отдельности.

№ каскада	FRR	FAR	Значение порога
1	0,0011	0,6218	5
2	0,0070	0,2828	4
3	0,0016	0,1714	8
4	0,0006	0,0934	14
5	0,0052	0,0025	250

Таблица 3.

Значения FAR и FRR, величина порога для каждого из семи каскадов по отдельности.

№ каскада	Ошибка 1 рода	Ошибка 2 рода	Значение порога
1	0,0011	0,6218	5
2	0,007	0,2828	4
3	0,0016	0,1714	8
4	0,0006	0,0934	14
5	0,0015	0,0385	22
6	0,0008	0,0198	43
7	0,0046	0,0018	200

Таблица 4.

Сравнение теоретических и экспериментально полученных значений времени работы

Алгоритм	Теоретический расчёт времени	Экспериментальный расчёт времени	ERR
Алгоритм полного хеша	$0.1024 \cdot 10^7$	0,49	0.0054
Каскадный метод (8, 8, 16, 16, 16, 32 и 928 бит)	$0.01126 \cdot 10^7$	0,35	0.00385
Каскадный метод (8, 8, 16, 32, 64, 128, 768 бит)	$0.0049 \cdot 10^7$	0,2983	0.0032

на основе каскадного метода, который может применяться для аутентификации, поиска и индексирования изображений. Были реализованы два перцептуальных алгоритма на основе блочного метода построения хеша по среднему значению: алгоритм полного хеша и каскад-

ный алгоритм. Тестирование проводилось на базе из 10000 изображений. Результаты построения моделей алгоритмов показали, что предлагаемый каскадный алгоритм обеспечивает высокую эффективность и скорость выполнения по сравнению с методом полного хеша.

Примечания

1. Sochenkov I., Vokhmintsev A. Visual duplicates image search for a non-cooperative person recognition at a distance // *Procedia Engineering*. — 2015. — Vol. 129. — P. 440-445.
2. Effective indexing for face recognition / I. Sochenkov, A. Sochenkova, A. Vokhmintsev et al. // *Proc. SPIE*. — Vol. 9971. — 2016. — P. 997124—9.
3. Iwanowski M., Cacko A., Sarwas G. Comparing Images for Document Plagiarism Detection // *International Conference: Computer Vision and Graphics (ICCVG)* — Cham : Springer International Publishing, 2016. — P. 532-543.
4. Ovhal P. Detecting plagiarism in images // *2015 International Conference on Information Processing (ICIP)*. — 2015. — P. 85—89.
5. Korsunov N. I., Toropchin D. A. Recognition method of near-duplicate images based on the perceptual hash and image key points using // *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. — Vol. 1. — 2015. — P. 261-264.
6. Govindaraj P., Sandeep R. Ring partition and dwt based perceptual image hashing with application to indexing and retrieval of near-identical images // *2015 Fifth International Conference on Advances in Computing and Communications (ICACC)*. — 2015. — P. 421-425.
7. A method of face recognition using 3d facial surfaces / B.A. Echeagaray-Patron, V. Kober, V. Karnaukhov, V. Kuznrtsov // *Journal of Communications Technology and Electronics*. — 2017. — Vol. 62, no. 6. — P. 648652.
8. Echeagaray-Patron B. A., Kober V. Face recognition based on matching of local features on 3d dynamic range sequences // *Proc. SPIE*. — Vol. 9971. — 2016. — P. 997131-6.

9. Echeagaray-Patron B. A., Kober V. 3d face recognition based on matching of facial surfaces // Proc. SPIE. — Vol. 9598. — 2015. — P. 95980V-8.
10. Mendoza-Morales A. I., Miramontes-Jaramillo D., Kober V. Illumination-invariant hand gesture recognition // Proc. SPIE. — Vol. 9598. — 2015. — P. 95980W-8.
11. Miramontes-Jaramillo D., Kober V. A fast matching algorithm based on local gradient histograms // Proc. SPIE. — Vol. 8499. — 2012. — P. 849927-8.
12. Shin J., Ruland C. Perceptual Image Hashing Technique for Image Authentication in WMSNs // Robust Image Authentication in the Presence of Noise — Cham : Springer International Publishing, 2015. — P. 75—103.
13. A robust and discriminative image perceptual hash algorithm / W. Zhen-kun, Z. Wei-zong, Ouyang-Jie et al. // 2010 Fourth International Conference on Genetic and Evolutionary Computing. — 2010. — P. 709—712.
14. Liu F., Cheng L.-M. Wave Atom-Based Perceptual Image Hashing Against Content-Preserving and Content-Altering Attacks // Transactions on Data Hiding and Multimedia Security X / Ed. by Yun Q. Shi. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2015. — P. 21—37.
15. A robust and secure perceptual hashing system based on a quantization step analysis / Azhar Hadmi, William Puech, Brahim Ait Es Said, Abdellah Ait Ouahman // Signal Processing: Image Communication. — 2013. — Vol. 28, no. 8. — P. 929—948.
16. A visual model-based perceptual image hash for content authentication / X. Wang, K. Pang, X. Zhou et al. // IEEE Transactions on Information Forensics and Security. — 2015. — Vol. 10, no. 7. — P. 1336—1349.
17. Ruchay A., Kober V. Clustered impulse noise removal from color images with spatially connected rank filtering // Proc. SPIE. — Vol. 9971. — 2016. — P. 99712Y-10.
18. Ruchay A., Kober V. A correlation-based algorithm for recognition and tracking of partially occluded objects // Proc. SPIE. — Vol. 9971. — 2016. — P. 99712R-9.
19. Chen X., Qin C., Ji P. Perceptual image hashing using block truncation coding and local binary pattern // 2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA). — 2015. — P. 856—859.
20. Zauner C., Steinebach M., Hermann E. Rihamark: perceptual image hash benchmarking // Proc. SPIE. — Vol. 7880. — 2011. — P. 78800X-15.
21. Winter C., Steinebach M., Yannikos Y. Fast indexing strategies for robust image hashes // Digital Investigation. — 2014. — Vol. 11. — P. S27—S35.
22. Chang L., Yan W.-G., Wang W.-D. Research on Robust Image Perceptual Hashing Technology Based on Discrete Cosine Transform // Business, Economics, Financial Sciences, and Management. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2012. — P. 799—809.
23. Weng L., Preneel B. A Secure Perceptual Hash Algorithm for Image Content Authentication // Communications and Multimedia Security: 12th IFIP TC6/TC International Conference (CMS 2011). — Berlin, Heidelberg : Springer Berlin Heidelberg, 2011. — P. 108—121.
24. Robust Image Content Authentication Using Perceptual Hashing and Watermarking / Li Weng, Rony Darazi, Bart Preneel et al. // Advances in Multimedia Information Processing (PCM 2012) — Berlin, Heidelberg : Springer Berlin Heidelberg, 2012. — P. 315—326.
25. Niu X., Gu F., Yang B. Block mean value based image perceptual hashing // Intelligent Information Hiding and Multimedia Signal Processing, International Conference on. — 2006. — P. 167—172.
26. Yang B., Gu F., Niu X. Block mean value based image perceptual hashing // Second International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IHH-MSP 2006). — 2006. — P. 167—172.

РУЧАЙ Алексей Николаевич, кандидат физ.-мат. наук, доцент кафедры компьютерной безопасности и прикладной алгебры Челябинского государственного университета; ran@csu.ru; тел.: +7(351)7997292.

ЯВТУШЕНКО Евгения Дмитриевна, студентка физического факультета Челябинского государственного университета; evgeniya_40@mail.ru.

RUCHAY Alexey, PhD., associate professor of Computer security and applied algebra department of Chelyabinsk state university; ran@csu.ru; tel.: +7(351)7997292.

YAVTUSHENKO Evgeniya, graduating student of physic department, Chelyabinsk State University, information security specialist, evgeniya_40@mail.ru.