ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ МЕТОДА ПСЕВДОГОЛОГРАФИЧЕСКОГО КОДИРОВАНИЯ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ К КОРРЕЛЯЦИОННОМУ АНАЛИЗУ

Урывская Д. А.

Учреждение Российской академии наук Институт систем обработки изображений РАН, Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет)

Аннотация

В статье исследован «регулярный» метод псевдоголографического кодирования цифровых изображений относительно его устойчивости к корреляционному анализу. Рассмотрен способ восстановления закодированного изображения в случае отсутствия информации о правиле нумерации. Приведена оценка эффективности применения корреляционного анализа для задачи несанкционированного доступа и восстановления исходного изображения. Определены границы применимости «регулярного» метода псевдоголографического кодирования при решении прикладных задач.

Ключевые слова: кодирование цифровых изображений, псевдоголограмма, корреляционный анализ, защита информации.

Введение

Существует целый ряд методов, объединённых под общим названием «псевдоголографическое кодирование цифровых изображений». Цель подобного кодирования заключается в преобразовании исходного изображения в псевдоголограмму (шумоподобное изображение), каждый участок которой, подобно физическому аналогу, содержит информацию обо всём изображении. Среди наиболее известных методов следует отметить: «регулярный» [1, 2, 3, 4], «псевдослучайный» [1, 3, 4], стохастический [5], квазиголографический [6, 7, 8], а также метод инверсной нумерации[9].

Данная статья посвящена исследованию именно «регулярного» метода псевдоголографического кодирования, поскольку исследования, проведённые в работах [10, 13], выявили ряд преимуществ данного преобразования относительно остальных методов рассматриваемой группы.

1. Регулярный метод псевдоголографического кодирования

Идея «регулярного» метода псевдоголографического представления данных [1, 4] заключается в том, что двумерный массив точек изображения разворачивается в одномерную последовательность по определённому правилу. При этом каждой точке на изображении ставится в соответствие не только пара координат (m, n) – адрес точки в двумерном массиве, но и некоторое число k, которое и определяет номер данной точки в кодируемой последовательности. При последовательном считывании полученной подобным образом одномерной последовательности в двумерный массив формируется закодированное изображение, имеющее шумоподобный вид, которое называется псевдоголограммой [10, 11, 12]. Следует отметить, что по любой части кодируемой последовательности можно реконструировать уменьшенную копию исходного изображения.

Переупорядочивание отсчётов осуществляется специальным образом по заранее выбранному пользователем правилу. Псевдоголографическое преобразование характеризуется параметрами p, N.

Пусть исходное изображение имеет размер $p^N \times p^N$, где p – простое число. (Рассмотрим основные положения на примере $p = 2$, $N = 8$.) Правило нумерации задаётся произвольно, пример приведён на рис. 1.

0	2
3	1

Рис. 1. Правило нумерации

Обозначим матрицу, изображённую на рис. 1, буквой A. Количество строк и столбцов этой матрицы должно быть одинаковым и равно p. Это соответствует элементарному (наименьшему размеру изображения) изображению $p \times p$.

Дополнительные функции, по которым и будет в дальнейшем определяться нумерация точек, определяются формулой:

$$\begin{cases} A_X(k) = n, \quad \exists \quad m : A(m,n) = k; \\ A_Y(k) = m, \quad \exists \quad n : A(m,n) = k. \end{cases} \tag{1}$$

Для заданного значения параметра $p = 2$ и правила нумерации дополнительные функции определяются, как показано на рис. 2. Здесь в первой строке перечислены значения k – аргумент функции, а во второй – значения n и m соответственно – значение функции.

Пусть (m, n) – пространственные координаты отсчёта на изображении, k – номер данного отсчёта в получаемой последовательности $\{h_k\}$, где $k = \overline{1, PN}$ ($PN = p^N \times p^N$).

A_X

0	1	2	3
0	1	1	0

A_Y

0	1	2	3
0	1	0	1

Рис. 2. Вид дополнительных функций

Начальный уровень нумерации ($N = 1$) определяется правилом нумерации, следующие уровни ($N = 2$ и $N = 3$) имеют вид, представленный на рис. 3*а*, *б*.

а)

0	8	2	10
12	4	14	6
3	11	1	9
15	7	13	5

б)

0	32	8	40	2	34	10	42
48	16	56	24	30	18	58	26
2	44	4	36	14	46	6	38
60	28	52	20	62	30	54	22
3	35	11	43	1	3	9	41
51	19	59	27	49	17	57	25
15	47	7	39	13	45	5	37
63	31	55	23	61	29	53	21

Рис. 3. Уровни нумерации

Правило нахождения пространственных координат отсчёта (m,n) по его номеру k в кодируемой подпоследовательности определяется по формуле:

$$\begin{cases} n = \sum\limits_{i=0}^{N-1} p^{N-1-i} A_X\left(\left[\dfrac{k}{p^{2i}}\right](\mathrm{mod}\ p^2)\right), \\ m = \sum\limits_{i=0}^{N-1} p^{N-1-i} A_Y\left(\left[\dfrac{k}{p^{2i}}\right](\mathrm{mod}\ p^2)\right), \end{cases} \quad (2)$$

где $[d]$ означает целую часть числа d.

Правило нахождения номера отсчёта k в кодируемой последовательности по его пространственным координатам (m, n) определяется по формулам (3.1) и (3.2):

$$\begin{cases} k_i = k_{i+1} \cdot p^2 + q(i); \\ q(i) = Q(m_i, n_i, i, p, N); \\ k_{N-1} = A(m,n); \\ i = \overline{0, N-2}, \end{cases} \quad (3.1)$$

$$\begin{cases} m_i = m_{i-1} (\mathrm{mod}\ p^{N-i}), \\ n_i = n_{i-1} (\mathrm{mod}\ p^{N-i}), \\ m_0 = m, \\ n_0 = n, \\ i = \overline{1, N-1}, \end{cases} \quad (3.2)$$

где $q(i)$ – номер квадрата, имеющий размер $p^{N-1-i} \times p^{N-1-i}$, в который попал отсчёт с пространственными координатами (m, n) на i-ом уровне кодирования; k_0 – значение номера отсчёта k в кодируемой последовательности; k_i – промежуточное значение k. Функция $Q(m_i, n_i, i, p, N)$ определяет номер квадрата $q(i)$ по координатам (m_i, n_i), функциям A_X и A_Y и вычисленным по значениям p, i и N границам квадратов следующего (более высокого) уровня кодирования: в выбранном квадрате с номером $q(i-1)$ определяется положение искомого отсчёта. Для этого рассчитывается пара новых «приведённых» координат (m_i, n_i) в заданном квадрате, которые могут принимать значения от 0 до $p^{N-i} - 1$. Далее, сопоставляя таблицы значений функций A_X и A_Y, получаем $q(i)$ число, соответствующее точке с двумерными координатами (m_i, n_i). Значение k_{N-1} определяется из последнего локализованного квадрата размером $p \times p$.

Отметим основные преимущества метода.

Псевдоголографическое представление изображения позволяет даже при потере некоторого блока информации восстановить либо полное изображение (погрешность восстановления при этом будет зависеть от объёма потерянной информации, тогда как при обычном методе хранения и передачи изображения потеря блока будет безвозвратной, то есть приведёт к утере фрагмента), либо уменьшенную копию исходного изображения [10].

Псевдоголографическое представление изображения оказывается эффективным в ситуациях, когда положение информационного блока, пришедшего на вход, оказывается неизвестным, то есть возможно восстановление изображения по произвольной части кодирующей подпоследовательности даже при отсутствии информации о положении данной подпоследовательности [13].

Данный метод кодирования изображения предоставляет возможность последовательного уточнения восстановленного изображения в распределённых сетях. Можно сказать, что пользователь может сам выбирать то соотношение времени и качества, которое его устраивает.

Представление изображения с использованием исследуемого метода таково, что разложение изображения обладает декоррелирующим свойством, что позволяет использовать его в задачах фильтрации коррелируемого импульсного шума при передаче данных по зашумлённому каналу [13].

2. Восстановление закодированного изображения при несанкционированном доступе к передаваемым данным

В работе [13] подробно рассматривалась задача восстановления получаемого изображения по части псевдоголограммы при условии, что порядок нумерации известен, а информация о позиции начального отсчёта переданного участка закодированных данных отсутствует. Был предложен алгоритм восстановления с последующим уточнением, основанный на корреляционных связях изображения.

Целью дальнейшего исследования была задача восстановления закодированного изображения при отсутствии информации о правиле нумерации.

Предположим, что известен сам способ кодирования («регулярный» метод ПГК) [10], псевдоголограмма и параметр p размера изображения ($p^N \times p^N$).

В данном случае восстановление сводится к нахождению правила нумерации, по которому была получена псевдоголограмма. Исходное правило нумерации устанавливается путём последовательного перебора всех $(p^2)!$ возможных нумераций и последующего анализа раскодированных (восстановленных) изображений.

Поскольку восстанавливаемое изображения неизвестно, так как псевдоголограмма имеет «шумоподобный» вид, решение о правильности выбранной нумерации принимается на операторном уровне, то есть в результате визуального анализа.

Если нумерация была определена (угадана) правильно, то в результате восстановления будет получено исходное изображение. Стоит отметить, что если угаданная матрица A, соответствующая искомой нумерации, транспонирована (1 или несколько раз) и(или) отображена, то в результате восстановления будет получено исходное изображение, повёрнутое и(или) отображённое соответственно (рис. 4*а*).

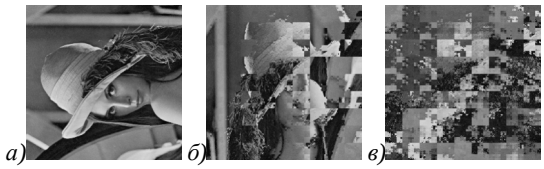

Рис. 4. Восстановленные изображения по различным нумерациям: правильная нумерация с точностью до транспонирования, отображения (а); нумерация с одной «ошибкой» (б); нумерация с большим количеством «ошибок» (в)

В случае восстановления по ошибочной нумерации результирующее изображение будет также искажено. Эти искажения имеют фрактальный характер, а их степень связана с количеством пар неверно размещённых отсчётов нумерации. То есть чем больше элементов матрицы A стоят не на своих местах (с точностью до транспонирования и отображения), тем сильнее «перемешано» результирующее изображение (рис. 4*б*).

Очевидно, что нумерация с большим количеством неверно угаданных пар порождает сильно искажённое изображение, которое с точки зрения визуального анализа неинформативно (рис. 4*в*). Принимая во внимание высокую корреляцию соседних отсчётов реальных изображений ($\rho \in (0{,}75,\ 0{,}95)$), можно, вычисляя соответствующий коэффициент, сразу отбрасывать «плохие» нумерации, не прибегая к визуальному анализу.

Нумерации, соответствующие искажённым восстановленным изображениям, содержащие информативные области (участки), подвергаются дальнейшей обработке до полного определения исходного порядка.

Для того чтобы определить долю информативных с точки зрения визуального анализа изображений, были проведены численные эксперименты над тестовыми изображениями (рис. 5*а-в*).

Каждое из тестовых изображений было закодировано в соответствии с «регулярным» методом ПГК ($p = 3$, $N = 5$). Затем полученная таким образом псевдоголограмма подвергалась обратному преобразованию каждой из всех возможных нумераций ($3^2! = 362880$). Для каждого восстановленного таким образом изображения вычислялся соответствующий коэффициент корреляции ρ. Распределение количества восстановленных тестовых изображений относительно коэффициентов корреляции представлено на рис. 6.

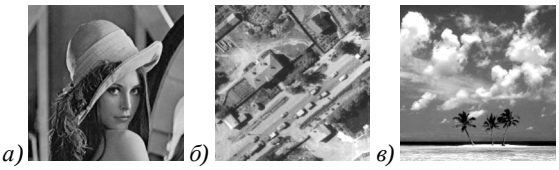

Рис. 5. Тестовые изображения: а) «Lena», б) «Way», в) «Sea»

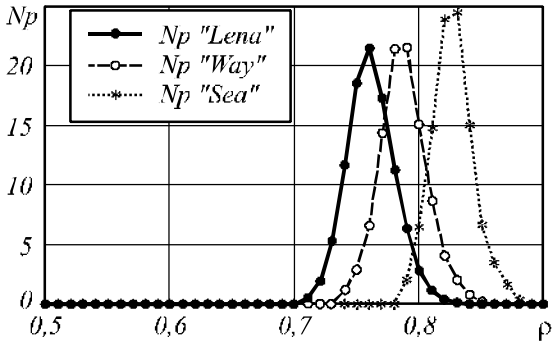

Рис.6. Распределение количества восстановленных изображений по всем возможным нумерациям относительно коэффициентов корреляции для тестовых изображений «Lena», «Way», «Sea»

С помощью визуального анализа для каждого набора соответствующего тестового изображения было выбрано (определено) пороговое значение коэффициента корреляции ρ_0, при котором изображения с $\rho > \rho_0$ являются информативными, и их целесообразно подвергнуть дальнейшей обработке операторным методом.

Исследования показали, что доля информативных изображений (для которых $\rho > \rho_0$), восстановленных по полностью либо частично угаданным нумерациям, весьма мала и составляет не более 0,5% от общего числа восстановленных по всем возможным нумерациям изображений.

В табл. 1 приведены численные результаты экспериментов для каждой группы тестовых изображений: пороговое значение коэффициента корреляции ρ_0 и доля информативных изображений:

$$\tilde{N}_{\rho_0} = \frac{N_{\rho_0}}{(p^2)!}, \qquad (4)$$

где N_{ρ_0} – количество нумераций, для которых коэффициенты корреляции восстановленных изобра-

жений превышают порог ($\rho > \rho_0$), а $(p^2)!$ – число всех возможных нумераций.

Таблица 1. Параметры восстановления для тестовых изображений

	«Lena»	«Way»	«Sea»
ρ_0	0,84	0,82	0,88
$\tilde{N}_{\rho_0}$	0,0045(0,45%)	0,0030(0,30%)	0,0029(0,29%)

Эксперименты показали, что вероятность угадать правильное либо «близкое» правило нумерации весьма мала, а полный перебор всех вариантов является малореалистичным. И если для небольших значений параметра p, таких как 2 или 3, полный перебор осуществим, то для $p = 4$ ($(p^2)! \approx 10^{13}$) такой способ будет уже нецелесообразен.

Отметим, что восстанавливать изображения для сокращения времени вычислений возможно в уменьшенном масштабе [10]. В любом случае для восстановления одного изображения размера $p^N \times p^N$ «регулярным» методом псевдоголографического кодирования необходимо произвести:

- сложений: $A(N) = 2\times(N-1)p^{2N}$;
- вычитаний: $S(N) = 2\times N\times p^{2N}$;
- умножений: $M(N) = 2\times(N^2 - N + 2)\times p^{2N}$;
- делений: $D(N) = 2\times N\times p^{2N}$.

Следует отметить, что высокий коэффициент корреляции сам по себе не является гарантией информативности изображения. Иными словами, сильнее искажённые восстановленные изображения могут иметь больший коэффициент, нежели менее искажённые. При восстановлении изображений меньшего масштаба, кратного размеру аттрактора p (с целью сокращения объёма вычислений), зависимость корреляции и информативности снижается. Такой вывод можно сделать, проанализировав графики, представленные на рис. 7*а-в*.

С уменьшением масштаба восстановленных изображений увеличивается количество изображений, имеющих «высокий» коэффициент корреляции, тогда как число информативных уменьшается в силу их меньшей детализации. Следовательно, в группу отбираемых для дальнейшей обработки попадает бóльшее количество неинформативных изображений.

Актуальным также является вопрос о выборе порога фильтрации восстановленных изображений. Поскольку оригинал изображения неизвестен, а диапазон значений коэффициента корреляции реальных изображений достаточно велик, выбор фиксированного значения этого параметра приведёт к тому, что при восстановлении изображений с более высоким коэффициентом корреляции для дальнейшего анализа будет отобрано слишком много претендентов, а в случае изображений с более низким значением – наоборот, слишком мало. В любом случае это приведёт к увеличению объёма вычислений, в первом случае на этапе операторного анализа, а во втором – на предварительном этапе перебора перестановок.

Заметим, что транспозиции в нумерации не эквивалентны с точки зрения значения коэффициента корреляции восстановленных изображений.

В силу особенностей исходного изображения одно и то же количество перестановок пар отсчётов по разным направлениям (по вертикали, горизонтали, диагонали) может порождать разную степень искажённости изображений, восстановленных по этим нумерациям. Также имеет значение положение переставленных отсчётов: если содержательная часть изображения находится в центре, как, например, у тестовой картинки «Lena», то менее критичными будут перестановки боковых, крайних отсчётов. Однако в среднем более трёх пар перестановок делает изображение непригодным для дальнейшего анализа.

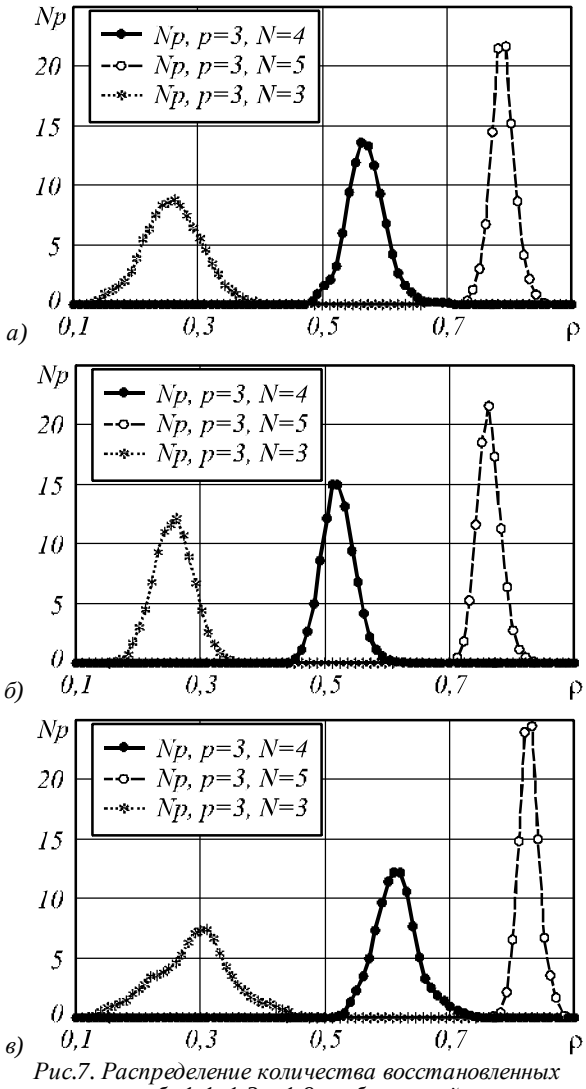

Рис.7. Распределение количества восстановленных в масштабе 1:1, 1:3 и 1:9 изображений по всем возможным нумерациям относительно коэффициентов корреляции для тестовых изображений: а) «Lena», б) «Way», в) «Sea»

Выводы

Исходя из всего вышеизложенного, можно заключить, что корреляционный анализ в данном случае является малоэффективным.

Результаты исследований показали, что метод псевдоголографического кодирования цифровых изображений, выполняя по сути шифрование-перенумерацию исходного изображения, может использоваться в качестве защиты от несанкционированного доступа к закодированным данным (отсутствие у злоумышленника информации о правиле нумерации), поскольку обладает достаточно высокой степенью устойчивости к взлому.

Благодарности

Работа выполнена при финансовой поддержке гранта РФФИ №09-01-00511-а.

Литература

1. **Bruckstein, A.M.** Holographic representation of images / A.M. Bruckstein, R.J. Holt, A.N. Netravali // IEEE Transactions on Image Processing. – 1998. – N 7. – P. 1583-1587.
2. **Bruckstein, A.M.** On Holographic Transform Compression of Images / A.M. Bruckstein, R.J. Holt, A.N. Netravali. – John Wiley & Sons Inc, – 2001. – P. 244-252.
3. **Bruckstein, A.M.** Holographic image representations: the subsampling method / A.M. Bruckstein, R.J. Holt, A.N. Netravali // IEEE Int. Conference on Image Processing – Santa Barbara, California, USA, October. – 1997. – Vol. 1. – P. 177-180.
4. **Bruckstein, A.M.** US 6,091,394: "Technique for Holographic Representation of Images" / A.M. Bruckstein, R.J. Holt, A.N. Netravali – July 18, 2000. – 6 p.
5. **Колесов, В.В.** Псевдоголографическое кодирование цифровой информации / В.В. Колесов, Н.Н. Залогин, Г.М. Воронцов // Радиотехника и электроника. – 2002. – Т. 2, № 5. – С. 583-588.
6. **Кузнецов, О.П.** Квазиголографический подход к поиску в массиве цифровых изображений / О.П. Кузнецов, А.В. Марковский // Искусственный интеллект. – 2004. – № 2. – С. 320-324.
7. **Марковский, А.В.** О квазиголографическом кодировании цифровых изображений / А.В. Марковский // Автоматика и телемеханика. – 2001. – № 9. – С. 163-173.
8. **Кузнецов, О.П.** Квазиголографический подход к кодированию графической информации / О.П. Кузнецов, А.В. Марковский // Искусственный интеллект. – 2002. – № 2. – С. 474-482.
9. **Dovgard, R.** Holographic image representation with reduced aliasing and noise effects / R. Dovgard // Image Processing, IEEE Transactions. – 2004. – No. 13(7). – P. 867-872.
10. **Баринова, Д.А.** Разработка и исследование алгоритмов обработки цифровых изображений, представленных в псевдоголографических кодах / Д.А. Баринова // Компьютерная оптика. – 2005. – № 27. – С. 149-154.
11. **Баринова, Д.А.** Анализ псевдоголографического метода с точки зрения *P*-адических метрик / Д.А. Баринова // Компьютерная оптика. – 2005. – № 28. – С. 128-131.
12. **Баринова, Д.А.** Анализ псевдоголографического метода с точки зрения *P*-адических метрик / Д.А. Баринова // Сборник трудов Всероссийского семинара по моделированию, дифракционной оптике и обработке изображений, июль, 2006. – С. 34-37.
13. **Воронин, В.В.** Голографическое представление в задачах обработки изображений / В.В. Воронин // Тезисы конференции РОАИ – 5. – 2000. – С. 237-241.

References

1. **Bruckstein, A.M.** Holographic representation of images / A.M. Bruckstein, R.J. Holt, A.N. Netravali // IEEE Transactions on Image Processing. – 1998. – N 7. – P. 1583-1587.
2. **Bruckstein, A.M.** On Holographic Transform Compression of Images / A.M. Bruckstein, R.J. Holt, A.N. Netravali. – John Wiley & Sons Inc., 2001. – P. 244-252.
3. **Bruckstein, A.M.** Holographic image representations: the subsampling method / A.M. Bruckstein, R.J. Holt, A.N. Netravali // IEEE Int. Conference on Image Processing. – Santa Barbara, California, USA, October, 1997. – Vol. 1. – P. 177-180.
4. **Bruckstein, A.M.** US 6,091,394: "Technique for Holographic Representation of Images" / A.M. Bruckstein, R.J. Holt, A.N. Netravali – July 18, 2000. – 6 p.
5. **Kolesov, V.V.** The pseudo holographic coding of the digital information / V.V. Kolesov, N.N. Zalogin, G.M. Vorontsov // Radioengineering and electronics. – 2002. – V. 2, N 5. – P. 583-588. – (in Russian).
6. **Kyznetchov, O.P.** The quasiholographic approach to search in a set of digital images / O.P. Kyznetchov, A.V. Markovskiy // Artificial intelligence. – 2004. – N 2. – P. 320-324. – (in Russian).
7. **Markovskiy, A.V.** About quasiholographic coding of digital images / A.V. Markovskiy // Automatics and telemechanics. – 2001. – N 9. – P. 163-173. – (in Russian).
8. **Kyznetchov, O.P.** The quasiholographic approach to coding of the graphic information / O.P. Kyznetchov, A.V. Markovskiy // Artificial intelligence. – 2002. – N 2. – P. 474-482. – (in Russian).
9. **Dovgard, R.** Holographic image representation with reduced aliasing and noise effects / R. Dovgard // Image Processing, IEEE Transactions. – 2004. – N 13(7). – P. 867-872.
10. **Barinova, D.A.** Algorithms of image processing presented in pseudo-holographic codes: development and research / D.A. Barinova // Computer Optics. – 2005. – N 27. – P. 149-154. – (in Russian).
11. **Barinova, D.A.** The analysis of a pseudo-holographic method from the point of view p-adicheskih metrics / D.A. Barinova // Computer Optics. – 2005. – N 28. – P. 128-131. – (in Russian).
12. **Barinova, D.A.** The analysis of a pseudo-holographic method from the point of view p-adicheskih metric / D.A. Barinova // Proc. All-Russia seminar on modeling, diffraction optics and image processing, July, 2006. – P. 34-37. – (in Russian).
13. **Voronin, V.V.** Holographic representation in problems of image processing / V.V. Voronin // Proc. Conf. PRIA – 5. – 2000. – P. 237-241. – (in Russian).

ROBUSTNESS EVALUATION OF THE PSEUDO-HOLOGRAPHIC CODING METHOD OF DIGITAL IMAGES TO THE CORRELATION ANALYSIS

D.A. Uryvskaya
S.P. Korolyov Samara State Aerospace University,
Image Processing Systems Institute of the RAS

Abstract

In this paper, the "regular" method of pseudo-holographic coding of digital images concerning its stability to the correlation analysis is investigated. The method of recovery of the coded image in a case, when the information on a numbering rule is missed is offered. The estimation of expediency of application of correlation analysis for the task of illegal access and source image recovery is resulted. Borders of applicability of a "regular" method of pseudo-holographic coding are defined at the decision of concrete applied problems.

Key words: coding of digital images, ccorrelation analysis, iinformation protection, the pseudo-hologram.

Сведения об авторе

Урывская Дарья Александровна, 1982 года рождения. В 2005 году окончила Самарский государственный аэрокосмический университет имени академика С.П. Королёва (СГАУ) по специальности «Прикладная математика». В настоящее время является аспирантом кафедры геоинформатики и информационной безопасности СГАУ и по совместительству стажёром-исследователем в Учреждении Российской академии наук Институт систем обработки изображений РАН. Круг научных интересов включает цифровую обработку сигналов и изображений, защиту информации. Имеет 5 публикаций, из них 2 статьи.

E-mail: *dbrnv@smr.ru*

Daria Alexandrovna Uryvskaya (1982 b.) graduated from the S. P. Korolyov Samara State Aerospace University (SSAU)), majoring in Applied Mathematics at 2005. At present she is a post-graduate student at SSAU's Geoinformatics and Information Security sub-department, holding a part-time position of a trainee-researcher at the Image Processing Systems Institute of the Russian Academy of Sciences. The area of interests includes digital signals and image processing, information security. She is author of 5 scientific papers, including 2 articles.

Поступила в редакцию 12 ноября 2010 г.