© Barannik V., Sidchenko S., Barannik D., Barannik V. Estimation of the influence of undetermined characteristics on the efficiency of crypto-compression image coding in a differentiated base // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 3, pp. 168-180.

DOI: 10.18372/2225-5036.26.15155

ОЦЕНКА НЕДЕТЕРМИНИРОВАННЫХ ХАРАКТЕРИСТИК ПЛАВАЮЩЕЙ СХЕМЫ КОДИРОВАНИЯ МЕТОДА КРИПТОКОМПРЕССИОННОГО ПРЕДСТАВЛЕНИЯ ИЗОБРАЖЕНИЙ В ДИФФЕРЕНЦИРОВАННОМ БАЗИСЕ

Владимир Баранник[1], Сергей Сидченко[2], Дмитрий Баранник[3], Валерий Баранник[3]

[1]Харьковский национальный университет имени В.Н. Каразина, Украина
[2]Харьковский национальный университет Воздушных Сил имени Ивана Кожедуба, Украина
[3]Харьковский национальный университет радиоэлектроники, Украина

БАРАННИК Владимир Викторович, д.т.н., профессор.

Год и место рождения: 1971 год, г. Изюм, Харьковская область, Украина.
Образование: Харьковский военный университет, 1994 год.
Должность: профессор кафедры искусственного интеллекта и программного обеспечения Харьковского национального университета имени В.Н. Каразина.
Научные интересы: технологии кодирования, искусственный интелект, информационная безопасность.
Публикации: более 750 научных публикаций, среди которых монографии, учебники, учебные пособия, научные статьи и патенты на изобретения.
E-mail: vvbar.off@gmail.com.
Orcid ID: 0000-0002-2848-4524.

СИДЧЕНКО Сергей Александрович, к.т.н., старший научный сотрудник.

Год и место рождения: 1972 год, г. Веймар, Германия.
Образование: Харьковский военный университет, 1994 год.
Должность: докторант, Харьковский национальный университет Воздушных Сил им. И. Кожедуба, Украина, г. Харьков.
Публикации: более 250 научных публикаций, среди которых монографии, учебники, учебные пособия, научные статьи и патенты на изобретения.
E-mail: sidserg72@gmail.com.
Orcid ID: 0000-0002-1319-6263.

БАРАННИК Дмитрий Владимирович

Год и место рождения: 1997 год, г. Первомайск, Николаевская область, Украина.
Образование: Харьковский национальный университет радиоэлектроники, 2018 год.
Должность: аспирант, Харьковский национальный университет радиоэлектроники.
Научные интересы: технологии цифровой обработки изображений, информационная безопасность.
Публикации: более 50 научных публикаций, среди которых монография, научные статьи и патенты на изобретения.
E-mail: d.v.barannik@gmail.com.
Orcid ID: 0000-0003-4235-300X.

БАРАННИК Валерий Владимирович

Год и место рождения: 2000 год, г. Первомайск, Николаевская область, Украина.
Должность: студент, Харьковский национальный университет радиоэлектроники, Украина.
Научные интересы: технологии кодирования, искусственный интеллект, информационная безопасность.
Публикации: более 13 научных публикаций, среди которых научные статьи и патенты на изобретения.
E-mail: valera462000@gmail.com.
Orcid ID: 0000-0003-3516-5553.

Аннотация. *Для решения вопросов об обеспечении защищенности обьектов критической инфраструктуры необходимо провести оценку недетерминированных характеристик плавающей схемы кодирования для метода криптокомпрессионного представления изображений в дифференцированном базисе. А именно: оценка количества элементов изображения, формирующих кодовые конструкции; оценка длины сформированных кодовых конструкций. Доказано, что кодовые конструкции формируются на переменном (заранее неопределенном) количестве элементов исходного изображения. В формировании кода информационной составляющей криптокомпрессионного представления изображений в дифференцированном базисе при длине кодового слова в 64 бита может принимать участие от 8 до 64 и более элементов исходного изображения. Кодовые конструкций формируются переменной (заранее неопределенной) длины, которая находится в диапазоне от 57 до 64 бит при длине кодового слова в 64 бита. Без наличия открытой системы оснований невозможно априорно предсказать длину любого кода информационной составляющей криптокомпрессионного представления изображений. Тем более, нельзя разбить всю информационную составляющую на отдельные блоки, соответствующие отдельным кодовым конструкциям. Количество элементов, формирующих коды информационной составляющей криптокомпрессионного представления изображений, и длины самих информационных составляющих зависят только от исходных значений элементов изображения. Они являются разными, как для разных изображений, так и для разных цветовых плоскостей в пределах одного изображения.*

Ключевые слова: *криптокомпрессионное представление изображения, защита информации, шифрование, кодирование, компрессия изображения, конфиденциальность, плавающая схем, дифференцированный базис.*

Введение

Системы видеонаблюдения получили широкое распространения в повседневной жизни человека. Они применяются для решения большого количества задач, среди которых:

– соблюдение прав человека;

– обеспечение безопасности граждан, объектов и охраняемых территорий;

– получение видеоинформации оперативными, разведывательными органами и мониторинговыми миссиями;

– дистанционное управление объектами, в том числе средствами вооружения, военной и специальной техники;

– фиксация и документирование (получение фото и видео материалов) событий нарушения договоренностей (в том числе и между конфликтующими сторонами), правил дорожного движения, общественного порядка и правонарушений криминогенного характера, а так же документирования любых событий и т.д.

Системы видеонаблюдения в системах кризисного управления способствуют скрытности и оперативности получения информации и своевременному реагирования на нее, увеличению расстояния до места сбора данных, а так же дают возможность их съема в труднодоступных и опасных для жизни человека местах.

Очень часто в системах кризисного управления видеоданные, полученная с помощью средств видеонаблюдения, могут быть отнесены к конфиденциальной, служебной или секретной информации. А поэтому требуют обеспечения безопасности.

В процессе обеспечения безопасности видеоданных (статических и динамических) существует существенная проблема связанная с тем, что увеличение конфиденциальности информации приводит:

– либо к увеличению временных затрат на их обработку и доставку при сохранении заданного качества видеоданных;

– либо к снижению объема полезной информации для поддержания заданной оперативности.

Существуют различные подходы к обеспечению конфиденциальности изображений, которые организуются как для исходных (предварительно не сжатых) изображений, так и изображений, представленных в сжатом виде [1–44].

В работах [1, 2] представлены подходы по криптокомпрессионному кодированию изображений, обеспечивающие комплексирование технологий компрессии и шифрования, которые позволяют решить выявленную проблему.

Целью статьи является оценка недетерминированных характеристик плавающей схемы кодирования метода криптокомпрессионного представления изображений в дифференцированном базисе, а именно: оценка количества элементов изображения, формирующих кодовые конструкции; оценка длины сформированных кодовые конструкции.

Основная часть

Количество элементов изображения, формирующих информационную составляющую криптокомпрессионного представления (ККП) изображения, заранее не известно. А с учетом понижения динамического диапазона в ее формировании могут принимать участие элементы больше, чем одного столбца исходного сегмента изображения.

Проанализируем граничные состояния исходных элементов изображения, которые влияют на формирование информационной составляющей ККП, а именно:

– в одном обрабатываемом сегменте изображения во всех строках расположены элементы, принимающие, как минимальные нулевые значения $a_{\min}$=0, так и максимальные значения, равные $a_{\max}$=25. В данном варианте понижение динамического диапазона не организуется, а расстояние между элементами может быть максимальным, равным $a_{\max}$-$a_{\min}$ =25.

Данное граничное состояние позволит оценить минимальное количество элементов изображения, способных сформировать один код информационной составляющей ККП заданной длины:

– в одном обрабатываемом сегменте изображения во всех строках разница между минимальным и максимальным элементом равняется $a_{\max}$- $a_{\min}$ =1. Это даст возможность оценить максимальное количество элементов изображения (отличающихся между собой), формирующих код информационной составляющей ККП заданной длины;

– в одном обрабатываемом сегменте изображения расположены только одинаковые элементы $a=a_{\max}=a_{\min}$, что позволит оценить их влияние на изменение длины кодовой последовательности информационной составляющей ККП.

Оценку недетерминированных характеристик будем проводить при условии, когда длина кодового слова L_{cw} для кода информационной составляющей ККП не превышает 64 бита. Т.е. количество разрядов, выделяемых на хранение кода N не превышает 64 бита.

В общем виде процесс формирования информационной составляющей N ККП в дифференцированном базисе при условии векторного представления сегмента обрабатываемых данных можно описать выражением:

$$N=\sum_{\tau=1}^{V_{form}-1}\left((a_\tau-r_\tau)\cdot\prod_{\xi=\tau+1}^{V_{form}}(s_\xi-r_\xi)\right)+(a_{V_{form}}-r_{V_{form}}), \quad (1)$$

где V_{form} – количество элементов, формирующих код N информационной составляющей ККП; τ, ξ – линейные координаты, определяющие позиции элементов; a_τ – τ-й элемент, формирующих код; r_τ – понижающее значением динамического диапазона для τ-го элемента; s_τ – основание τ-го элемента; $a_{V_{form}}$ – последний элемент, формирующих код; $r_{V_{form}}$ – понижающее значением динамического диапазона для последнего элемента.

Рассмотрим первый вариант граничного состояния исходного сегмента изображения, когда во всех строках основание равно 256, т.е для всех элементов, формирующих код, $s_\tau=a_{\max}+1=256$, $\tau=\overline{1,V_{form}}$, а понижающее значением динамического диапазона равно $r_\tau=a_{\min}=0$. Следовательно, разница между основанием и понижающим значением динамического диапазона для каждой строки сегмента изображения равна 256.

Для удобства будем считать, что только максимальные элементы сегмента изображения принимают участие в формировании кода N, т.е $a_\tau=a_{\max}=255$.

С учетом данных особенностей выражение (1) для формирования кода информационной составляющей примет вид:

$$N=\sum_{\tau=1}^{V_{form}-1}\left((a_{\max}-a_{\min})\cdot\prod_{\xi=\tau+1}^{V_{form}}((a_{\max}+1)-a_{\min})\right)+(a_{\max}-a_{\min}). \quad (2)$$

А с учетом численных значений элементов значение кода будет равным:

$$N=\sum_{\tau=1}^{V_{form}-1}\left((255-0)\cdot\prod_{\xi=\tau+1}^{V_{form}}((255+1)-0)\right)+(255-0)=$$

$$=\sum_{\tau=1}^{V_{form}-1}\left(255\cdot\prod_{\xi=\tau+1}^{V_{form}}256\right)+255=255\cdot\left(\sum_{\tau=1}^{V_{form}-1}256^{V_{form}-\tau}+1\right). \quad (3)$$

Длина сформированного кода N информационной составляющей ККП не должна превышать длины выбранного кодового слова L_{cw}, т.е. должны выполняться условия:

$$N\le(2^{L_{cw}}-1)=(2^{64}-1), \quad (4)$$

$$[\log_2 N]+1\le L_{cw}=64. \quad (5)$$

Значение кода N, полученное с помощью выражения (3), будет удовлетворять условиям (4) и (5), когда количество элементов V_{form} будет равно 8. Это значение и есть минимальным количеством элементов, формирующих код N информационной составляющей ККП.

Изменение значения одного исходного элемента сегмента видеоданных может привести к изменению количества элементов, формирующих код информационной составляющей ККП, если этот элемент является минимальным или максимальным значением динамического диапазона в строке исходных данных.

Так на рис. 3 приведен пример формирования информационной составляющей ККП на основе плавающей схемы системы кодирования в дифференцированном базисе для сегмента изображения, в котором в отличии от примера на рис. 2 изменен элемент 6-ой строки 1-го столбца на 1 бит со значения равного 250 (в двоичной системе исчисления число 11111010) на значение 248 (11111000 в двоичной системе), что привило к уменьшению количества элементов, формирующих код на 1, с 20 элементов до 19. В данном примере изменение одного бита соответствует изменению значения элемента на 2 (10 в двоичной системе).

На рис. 3 измененный элемент обозначен жирным цветом в выделенной жирными линиями ячейки первой исходной матрицы (все дальнейшие, связанные с этим, изменения обозначены аналогично). Изменение привило к уменьшению понижающего значения динамического диапазона, что в свою очередь увеличило пониженные значения всех элементов строки, в которой расположен данный элемент, и пониженное значение основания для элементов данной строки.

В итоге значение кода было сформировано с учетом 19 исходных элементов.

Если сформировать код с учетом 20-го элемента, то его значение будет равно 3610168824544353336 5, что приводит к переполнению машинного слова (предельное значение равно 18446744073709551615).

Действительно, если воспользоваться выражениями (1), то при 19 элементах величина накопленного произведения оснований с учетом понижения их динамического диапазона N примет значение

равное 6 016 590 518 396 387 328, а при 20 элементах N =48 132 724 147 171 098 624, что превышает динамический диапазон.

Аналогично будет и в примере на рис. 4 при уменьшении значения исходного элемента видеоданных на 1 со значения равного 250 (двоичное число 11111010) на значение 249 (двоичное число 11111001 в двоичной системе), что привело к изменению двух бит данных. Эта так же привило к уменьшению количества элементов, формирующих код, до 19. При этом согласно выражения (1), при 19 элементах N =3 526 814 901 042 413 568, а при 20 элементах N =24 687 704 307 296 894 976, что так же превышает динамический диапазон.

Экспериментальные исследования относительно оценки количества элементов, формирующих код информационной составляющей ККП, подтвердили результаты математических оценок. В качестве примера, на рис. 5 приведены варианты исходных тестовых изображений "Lena" и "Зона аэропорта", имеющих размерность 512×512 элементов. Результаты экспериментальных исследований приведены в табл. 1.

Их анализа данных в табл. 1 можно сделать следующие выводы:

– коды информационной составляющей ККП формируются на переменном, заранее не известном количестве элементов и зависят только от значений обрабатываемых данных. Данный параметр индивидуален не только для изображения, но так же и для обрабатываемых плоскостей в пределах одного изображения;

– максимальное количество элементов, формирующих код, не ограничивается одним сегментов. Так, например, в изображении "Lena" максимальное количество элементов, формирующих код, равно 224. Это соответствует количеству данных из четырех сегментов, размерностью 8×8 элементов.

Второй вариант граничного состояния исходного сегмента изображения предполагает разницу между минимальным и максимальным элементом a_{max}- a_{min} =1. Следовательно, разница между основанием $s_\tau = a_{\max} + 1$ и понижающим значением динамического диапазона a_{min} для каждой строки сегмента изображения равна $s_\tau - a_{\min} = a_{\max} +$. $1 - a_{\min} = 2$. Здесь рассмотрим два варианта, когда в формировании кода принимают участие только: – максимальные элементы сегмента, т.е $a_\tau = a_{\max}$; – минимальные элементы сегмента, т.е $a_\tau = a_{\min}$. В первом случае, когда $a_\tau = a_{\max}$ значение кода вычисляется с помощью выражения (2), что с учетом численных значений элементов примет вид:

$$N = \sum_{\tau=1}^{V_{form}-1}\left(1\cdot\prod_{\xi=\tau+1}^{V_{form}}2\right)+1 = \sum_{\tau=1}^{V_{form}-1}2^{V_{form}-\tau}+1. \quad (6)$$

С учетом удовлетворения условий (4) и (5), значение кода N, полученное с помощью выражения (6), будет возможно при количестве элементов $V_{form} = 64$.

Данное значение и есть максимальным количеством элементов, отличающихся друг от друга и принимающих участие в формировании кода N информационной составляющей ККП.

Во втором случае, когда $a_\tau = a_{\min}$, значение кода с учетом выражения (1) принимает значение нуля:

$$N = \sum_{\tau=1}^{V_{form}-1}\left((a_{\min}-a_{\min})\cdot\prod_{\xi=\tau+1}^{V_{form}}((a_{\max}+1)-a_{\min})\right)+(a_{\min}-a_{\min}) =$$
$$= \sum_{\tau=1}^{V_{form}-1}\left(0\cdot\prod_{\xi=\tau+1}^{V_{form}}2\right)+0 = 0.$$

Это говорит о том, что значения, совпадающие со значением динамического диапазона, не несут нагрузки на код N (не изменяют его значение), а следовательно и не увеличивают его длину. Следовательно, количество таких элементов, которые принимают участие в формировании кода N информационной составляющей ККП, может быть без ограничения.

При третьем граничном состоянии, когда элементы обрабатываемого сегмента равны, т.е. $a = a_{\max} = a_{\min}$, выражение (1) примет следующий вид:

$$N = \sum_{\tau=1}^{V_{form}-1}\left((a-a)\cdot\prod_{\xi=\tau+1}^{V_{form}}((a+1)-a)\right)+(a-a) = \sum_{\tau=1}^{V_{form}-1}\left(0\cdot\prod_{\xi=\tau+1}^{V_{form}}1\right)+0 = 0.$$

Т.е. значение кода информационной составляющей ККП равно нулю, что свидетельствует, как и в предыдущем случае, что количество таких элементов в формировании кода номера может быть не ограниченным, т.е. $V_{form} \to \infty$.

Можно сделать следующие выводы:

– кодовые конструкции строятся на переменном, заранее неопределенном, количестве элементов исходного изображения и зависят только от источника данных (его значений);

– в формировании кода информационной составляющей ККП в дифференцированном базисе при длине кодового слова в 64 бита может принимать участие от 8 до 64 отличающихся друг от друга элементов исходного изображения. При условии, что длина кодового слова одного элемента изображения равна 8 бит, то в формировании кода с длиной кодового слова в 64 бита может принимать участие последовательность исходных элементов с общей длиной от 64 до 512 бит ;

– чем меньше расстояние между элементами, тем большее их количество участвует в формировании кода информационной составляющей ККП;

– элементы, принимающие значение равное значению динамического диапазона, не несут нагрузки на код и могут принимать участие в формировании кода информационной составляющей ККП без ограничения.

Это может значительно увеличить общее количество элементов, формирующих код (более 64), и,

следовательно, общую длину последовательности исходных элементов (более 512 бит).

Примеры формирования информационной составляющей ККП на основе плавающей схемы кодирования в дифференцированном базисе для сегмента изображения с контуром (большим перепадом в минимальном и максимальном значении элемента в строке исходного сегмента изображения) и без контура представлены на рис. 1 и 2. Из анализа примеров видно, что для формирования кода используется переменное количество элементов исходного сегмента изображения, при этом объем информационной составляющей кодограммы меньше объема выделяемого для исходных данных.

Так в примере на рис. 1 при формировании кода для сегмента изображения с контуром принимают участие 20 элементов исходных данных объемом 160 бит (по 8 бит каждый элемент) при выходном объеме информационной составляющей ККП в 64 бита, что больше в 2,5 раза. На рис. 2 объем исходных 38 элементов сегмента изображения без контура, принимающих участие в формировании кода, составляет 304 бита, что 4,75 раза больше выходного объеме информационной составляющей ККП.

Экспериментальные исследования относительно оценки количества элементов, формирующих код информационной составляющей ККП, подтвердили результаты математических оценок.

В качестве примера, на рис. 5 приведены варианты исходных тестовых изображений "Lena" и "Зона аэропорта", имеющих размерность 512×512 элементов. Результаты экспериментальных исследований приведены в табл. 1.

Их анализа данных в табл. 1 можно сделать следующие выводы:

– коды информационной составляющей ККП формируются на переменном, заранее не известном количестве элементов и зависят только от значений обрабатываемых данных. Данный параметр индивидуален не только для изображения, но так же и для обрабатываемых плоскостей в пределах одного изображения;

– максимальное количество элементов, формирующих код, не ограничивается одним сегментов. Так, например, в изображении "Lena" максимальное количество элементов, формирующих код, равно 224. Это соответствует количеству данных из четырех сегментов, размерностью 8×8 элементов;

– максимальное количество элементов, формирующих код, находится в диапазоне от 8 до 20 элементов. При этом, более 60 % всех кодовых значений информационных составляющих ККП сформированы на основе более 10 элементов.

Формирование кода информационной составляющей ККП по количеству разрядов, выделяемых на их хранение, бывают равномерными и неравномерными.

Для равномерного кода информационной составляющей ККП количество разрядов, выделяемых на его хранение, равно длине кодового слова $[\log_2(N)]+1=L_{cw}$. У данного подхода есть несколько существенных недостатков.

Во-первых, злоумышленник имеет априорную информацию относительно количества всех сформированных информационных составляющих ККП для данного изображения, т.к.:

$$L_{IC}=\frac{Q_{eIC}}{L_{cw}},$$

где L_{IC} – количество всех сформированных информационных составляющих ККП для данного изображения; $Q_{\text{e}IC}$ – объем (длина) всех информационных составляющих ККП, сформированных на основе равномерного выделения количества разрядов на их хранение, который вычисляется с помощью выражения:

$$Q_{eIC}=\sum_{i=1}^{L_{IC}}([\log_2(N_{eIC_i})]+1),$$

где i – линейный элемент, определяющий номер обрабатываемой информационной составляющей; N_{eIC_i} – i-я информационная составляющая, сформированная на основе равномерного выделения количества разрядов на ее хранение.

Кроме того, злоумышленник знает код каждой отдельной информационной составляющей N_{eIC_i}. Однако, эта информация не даст ему возможности дешифровать изображение, т.к. злоумышленнику не известны ключевые данные (служебная составляющая, которая передается и хранится в зашифрованном виде).

Во-вторых, большинство кодов информационных составляющих ККП содержат в себе незначимые биты, т.к. $L_{cw}\geq[\log_2(N)]+1$, что приводит к увеличиваю общего объема (длины) всех сформированных информационных составляющих на объем, полученный с помощью выражения:

$$Q_{difIC}=Q_{eIC}-Q_{uneIC}=\sum_{i=1}^{L_{IC}}([\log_2(N_{eIC_i})]+1)-\sum_{i=1}^{L_{IC}}([\log_2(N_{uneIC_i})]+1)=$$
$$=\sum_{i=1}^{L_{IC}}([\log_2(N_{eIC_i})]-[\log_2(N_{uneIC_i})])=$$
$$\sum_{i=1}^{L_{IC}}(L_{cw}-[\log_2(N_{uneIC_i})]-1),$$

где Q_{difIC} – разница между объемами (длинами) всех сформированных информационных составляющих ККП, полученными на основе равномерного и неравномерного выделения количества разрядов на их хранение;

Q_{uneIC} – объем (длина) всех информационных составляющих ККП, сформированных на основе неравномерного выделения количества разрядов на их хранение, который вычисляется с помощью выражения:

$$Q_{uneIC}=\sum_{i=1}^{L_{IC}}([\log_2(N_{uneIC_i})]+1),$$

где N_{uneIC_i} – i-я информационная составляющая, сформированная на основе неравномерного выделения количества разрядов на ее хранение.

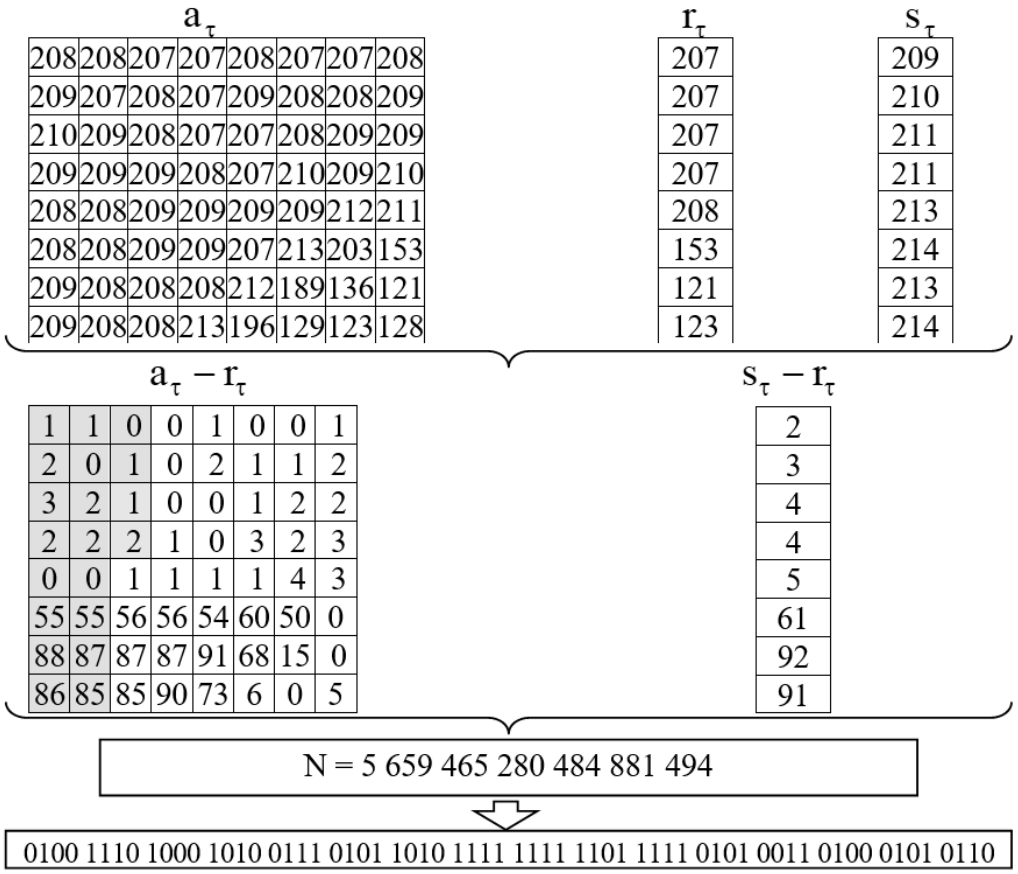


Рис. 1. Пример формирования кода на основе значений сегмента изображения с контуром

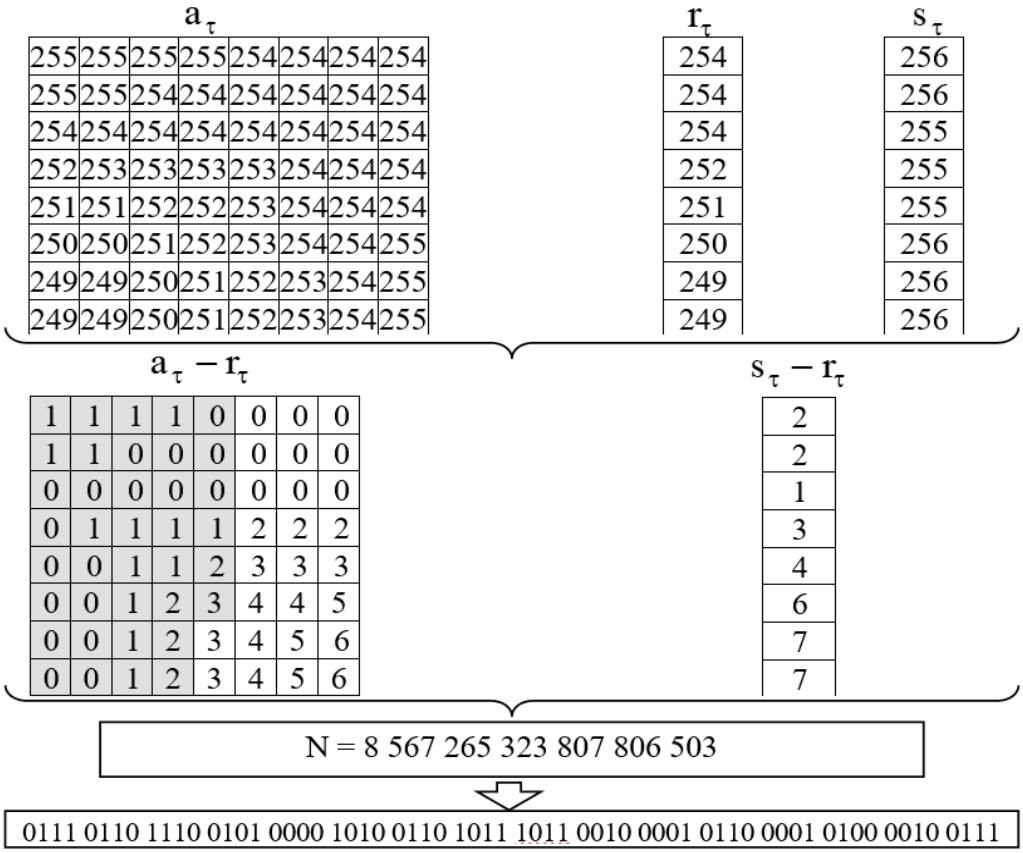


Рис. 2. Пример формирования кода на основе значений сегмента изображения без контура

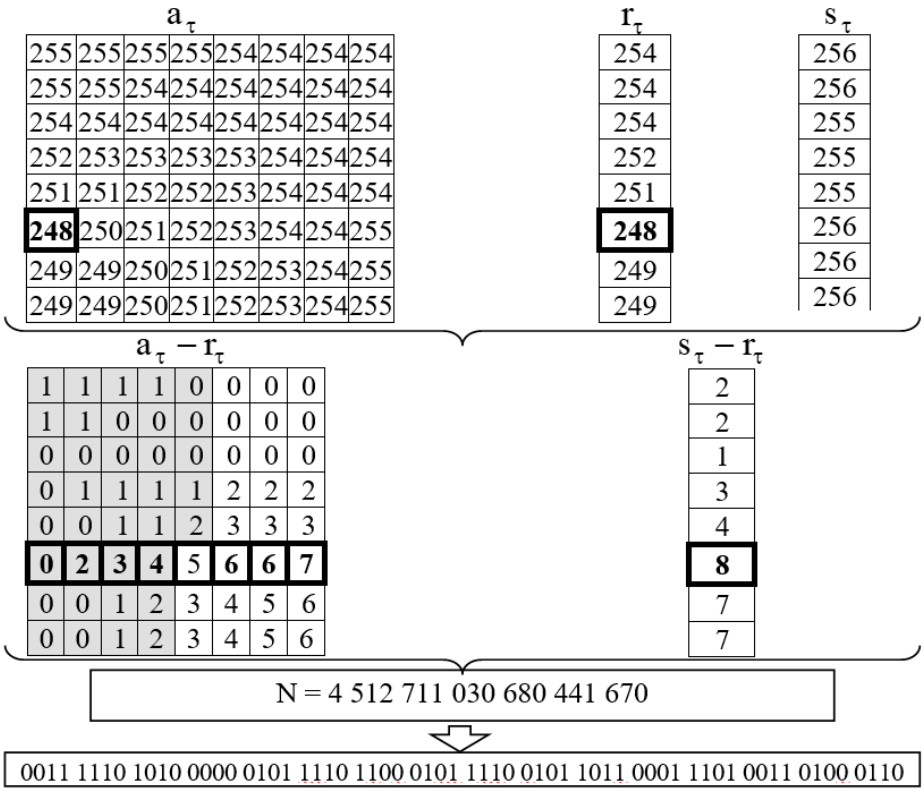


Рис. 3. Пример формирования кода при условии изменения значения одного из элементов исходного сегмента данных на 2

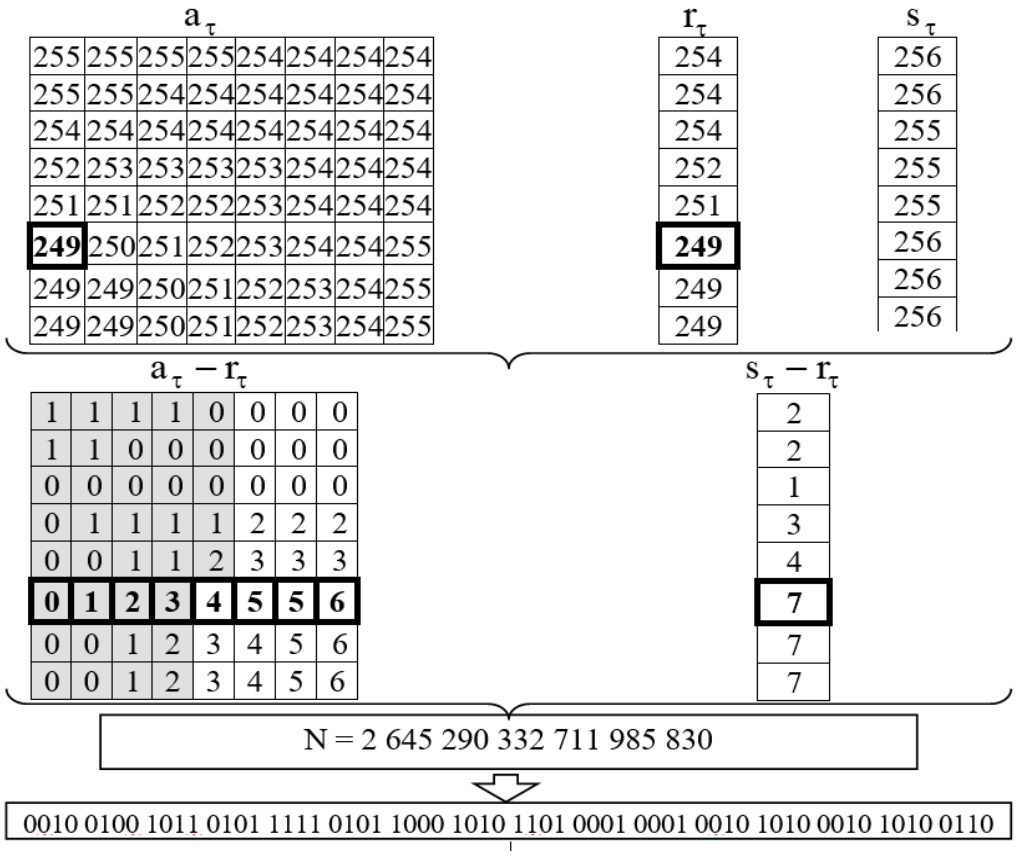
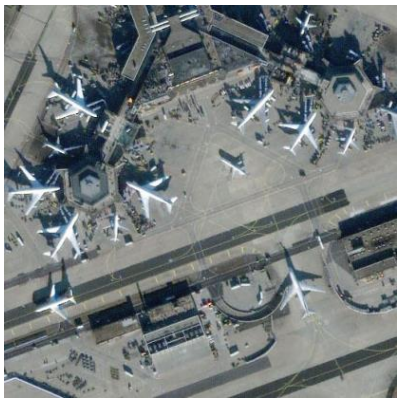


Рис. 4. Пример формирования кода при условии изменения значения одного из элементов исходного сегмента данных на 1

Lena



Зона аэропорта

Рис. 5. Примеры исходных изображений, размерностью 512×512

Таблица 1

Количество элементов исходного изображения, формирующих информационную составляющую ККП

Плоскость	Количество элементов											Max
	8-10	11-20	21-30	31-40	41-50	51-60	61-70	71-80	81-90	91-100	>100	
Lena												
R	3168	15379	341	19	6	4	1	2	0	0	0	76
G	5343	13855	430	27	8	1	0	1	1	0	0	81
B	3954	12080	1552	146	36	21	8	14	5	2	10	224
Суммарно	12465	41314	2323	192	50	26	9	17	6	2	10	–
Процентное соотношение	22,1	73,23	4,11	0,34	0,09	0,05	0,02	0,03	0,01	0	0,02	–
Зона аэропорта												
R	7405	12999	751	12	1	0	0	0	0	0	0	41
G	7697	12644	822	16	0	0	0	0	0	0	0	40
B	8121	12425	789	13	0	0	0	0	0	0	0	38
Суммарно	23223	38068	2362	41	1	0	0	0	0	0	0	–
Процентное соотношение	36,46	59,77	3,71	0,06	0	0	0	0	0	0	0	–

Для неравномерного кода информационной составляющей ККП количество разрядов, выделяемых на его хранение, заранее не известное и оно $[\log_2(N)]+1\le L_{cw}$.

Длина неравномерного кода информационной составляющей ККП зависит от значений служебной составляющей.

Ее максимальное значение ограничено длиной выбранного при кодировании кодового слова и равно L_{cw}.

Минимальное значение длины неравномерного кода информационной составляющей ККП можно определить с учетом процесса формировании кода N и контроля переполнения длины кодового слова L_{cw} при условии, что:

$$L_{cw}\ge[\log_2\prod_{\xi=1}^{V_{form}}(s_\xi-r_\xi)]+1=[\log_2\prod_{\xi=1}^{V_{form}-1}(s_\xi-r_\xi)+\log_2(s_{V_{form}}-r_{V_{form}})]+1.$$

При граничных значениях основания последнего элемента $s_{V_{form}}=256$ и понижающего значения динамического диапазона для него $r_{V_{form}}=0$, последний элемент V_{form} может максимально увеличивает длину кода N на $\log_2 256=8$ бит.

Исходя из этого, минимальное значение длины неравномерного кода информационной составляющей ККП, когда добавление нового элемента обеспечивает переполнение кодового слова, должно быть больше чем $(L_{cw}-8)$ бит.

Следовательно, длина неравномерного кода информационной составляющей ККП должна удовлетворять условию $L_{cw}-8<[\log_2 N]+1\le L_{cw}$. и находится в диапазоне $[L_{cw}-7, L_{cw}]$. Результаты экспериментальных исследования относительно оценки длины кодов информационной составляющей ККП для тестовых изображений, представленных на рис. 5, приведены в табл. 2.

Таблица 2

Длина кода информационной составляющей ККП

Плоскость	Длина кодовой последовательности, бит								
	63	62	61	60	59	58	57	56	Всего
Lena									
R	4179	4309	4028	3525	1922	761	188	8	18920
G	4270	4257	4047	3420	2103	1115	421	32	19665
B	4043	3950	4029	2855	1766	866	295	23	17827
Суммарно	12492	12516	12104	9800	5791	2742	904	63	56412
Процентное соотношение	22,14	22,19	21,46	17,37	10,27	4,86	1,6	0,11	100
Зона аэропорта									
R	4220	4340	4127	3505	2641	1630	615	89	21167
G	4329	4303	4006	3553	2552	1719	656	60	21178
B	4211	4221	4141	3550	2625	1799	703	97	21347
Суммарно	12760	12864	12274	10608	7818	5148	1974	246	63692
Процентное соотношение	20,03	20,2	19,27	16,66	12,27	8,08	3,1	0,39	100

Из анализа данных в табл. 2 можно сделать следующие выводы:

– коды информационной составляющей ККП формируются на основе переменной и заранее не известной длины. В эксперименте длина кодового слова была принята равной $L_{cw} = 63$, поэтому длина кодовых конструкций находится в диапазоне от 56 до 63 бит, что соответствует диапазону $[L_{cw} - 7, L_{cw}]$;

– длины кодов информационной составляющей ККП зависят только от исходных данных и являются разными для разных изображений. В пределах одного изображения для разных цветовых плоскостей формируется также разное количество кодов, имеющих разные длины;

– большинство кодов информационной составляющей ККП (более 60 %) имеет длину от 61 до 63 бит.

Еще одним неопределенным параметром в результате криптокомпрессионного представления изображения может быть размер исходного изображения. Это связано с тем, что в процессе ККП изображение подвергается компрессии с разным коэффициентом сжатия, который зависит от значений обрабатываемых данных. И для каждого изображения он разный.

Следовательно, зная общую длину криптокомпрессионного представления изображения злоумышленнику не возможно определить размер исходного изображения.

Однако, если злоумышленник знает характеристики аппаратуры, сформировавшей данные изображение, то ему априорно известен и размер формируемых изображений.

Кроме того, размер исходного изображения может быть вычислен на основе объема служебных данных. Хотя данный недостаток и может быть устранен за счет организации считывания информационной и служебной составляющей из файла данных в противоположном направлении (когда одни данные считываются с начала файла, а другие – с конца).

Сам факт знания общего объема исходного изображения и расположения служебных и информационных составляющих в файле криптокомпрессионного представления изображения не дает злоумышленнику никакой возможности относительно несанкционированного дешифрования данных.

Построение кодовых конструкций криптокомпрессионного представления изображений может быть равномерным или неравномерным. Равномерность кодовых конструкций может рассматриваться с позиции:

– количества элементов, принимающих участие в их формировании (равномерности служебной составляющей криптокомпрессионного представления);

– длины кодовой последовательности информационной составляющей (равномерности информационной составляющей криптокомпрессионного представления).

При этом для криптокомпрессионного представления в дифференцированном базисе равномерность информационной составляющей с позиции длины не соответствует равномерности с позиции количества элементов, принимающих участие в их формировании. То есть, при равномерных кодовых последовательностях информационных оставляющих наблюдаются неравномерные кодовые последовательности соответствующих им служебных составляющих (они содержат разное количество элементов).

И наоборот, равномерные состояния служебных составляющих (одинаковое количество элементов, выделяемое для формирования одной кодовой последовательности информационной составляющей) вызывают неравномерность в длине кодовых последовательностей информационных составляющих криптокомпрессионного представления изображений.

Равномерность информационных и служебных составляющих для криптокомпрессионного представления в дифференцированном базисе мо-

жет наблюдаться локально в случае однотипности трансформированных данных.

А так, как реалистическим изображениям характерны неоднородности в данных, то появление вышеописанных случаев маловероятно.

Равномерность самих информационных составляющих с позиции длины может наблюдаться только в случае принудительного выделения одинакового количества разрядов для каждой кодовой последовательности информационных составляющих.

Реально длины кодовых последовательностей информационной составляющей ККП находятся в диапазоне $[L_{cw}-7, L_{cw}]$. И в итоге они неравномерны.

Исходя из выше изложенного на практике могут наблюдаться четыре состояния относительно равномерности (неравномерности) кодовых конструкций криптокомпрессионного представления изображений:

– неравномерные служебные составляющие (разное количество элементов и соответственно разная длина) формируют равномерные информационные составляющие с позиции длины. Это происходит в случае выделения одинакового количества разрядов для каждой кодовой последовательности информационных составляющих;

– равномерные служебные составляющие (одинаковое количество элементов и соответственно одинаковая длина) формируют равномерные информационные составляющие с позиции длины, если для их хранения выделено одинаковое количество разрядов. Данный вариант является самым наихудшим с позиции выходного объема формируемых кодовых конструкций;

– равномерные служебные составляющие (одинаковое количество элементов и соответственно одинаковая длина) формируют неравномерные информационные составляющие с позиции длины. Их длина зависит от значений элементов служебных составляющих;

– неравномерные служебные составляющие (разное количество элементов и соответственно разная длина) формируют неравномерные информационные составляющие с позиции длины, которая находятся в диапазоне $[L_{cw}-7, L_{cw}]$ и зависит от значений элементов служебных составляющих. Данный вариант является наиболее предпочтительным. В результате него общая длина всех информационных составляющих криптокомпрессионного представления изображения будет минимальной.

Выводы

Плавающая недетерминированная схема формирования криптокомпрессионного представления изображений в дифференцированном базисе основана:

– на построении кодовых конструкций на переменном, заранее неопределенном, количестве элементов исходного изображения и системы оснований. Их количество зависит только от исходных значений самих элементов и чем больше значения сходятся друг с другом, тем большее их количество принимает участие в формировании кодов информационной составляющей.

В формировании кода информационной составляющей ККП в дифференцированном базисе при длине кодового слова в 64 бита может принимать участие от 8 до 64 и более элементов исходного изображения. При условии, что длина кодового слова одного элемента исходного изображения равна 8 бит, то в формировании кода с длиной кодового слова в 64 бита может принимать участие последовательность исходных элементов с общей длиной от 64 до 512 бит и более;

– на построении кодовых конструкций переменной, заранее неопределенной, длины, которая находится в диапазоне $[L_{cw}-7, L_{cw}]$, где L_{cw} – длина кодового слова, бит. Причем, длина последней кодовой конструкции информационной составляющей каждой цветовой плоскости может быть гораздо меньшей длины потому, что формируется на остаточном количестве элементов. Без наличия открытой системы оснований невозможно априорно предсказать длину любой кодовой конструкции информационной составляющей ККП и, тем более, разбить всю информационную составляющую на отдельные блоки, соответствующие отдельным кодовым конструкциям.

Причем, при кодировании разных цветовых плоскостей формируется разное количество кодовых конструкций информационной составляющей. Процентное соотношение длин кодовых комбинаций информационной составляющей ККП для разных изображений разное.

Литература

[1] Баранник В.В. *Основы теории структурно-комбинаторного стеганографического кодирования: монография* / В.В. Баранник, Д.В. Баранник. – Х.: Издательство «Лидер», 2017. – 256 с.

[2] Announcing the ADVANCED ENCRYPTION STANDARD (AES) // *Federal Information Processing Standards Publication* [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/FIPS/ NIST. FIPS.197.pdf.

[3] Auer. S., Bliem A., Engel. D., Uhl. A., Unterweger. A. Bitstream-based JPEG Encryption in Real-time //*International Journal of Digital Crime and Forensics*, 2013. – 17 p.

[4] Barannik V., Barannik N., Ryabukha Yu., Barannik D. Indirect Steganographic Embedding Method Based On Modifications of The Basis of the Polyadic System // *15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020)*, 2020. - pp. 699-702.

[5] Barannik V., Barannik, V.: Binomial-Polyadic Binary Data Encoding by Quantity of Series of Ones // *15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020)*, 2020. - pp. 775-780.

[6] Barannik V., Belikova T., Gurzhii P. The model of threats to information and psychological security, taking into account the hidden information destructive impact on the subconscious of adolescents // *2019 IEEE*

International Conference on Advanced Trends in Information Theory (ATIT), 2019. - pp. 656 – 661.

[7] Barannik V., Krasnoruckiy A., Hahanova A.: The positional structural-weight coding of the binary view of transformants // *East-West Design & Test Symposium (EWDTS)*. - Rostov-on-Don, 2013. - pp. 1-4.

[8] Barannik V.V., Ryabukha Yu.N., Kulitsa O.S. The method for improving security of the remote video information resource on the basis of intellectual processing of video frames in the telecommunication systems. Telecommunications and Radio Engineering, Vol. 76, No 9, 2017. - pp. 785-797.

[9] Barannik V., Shulgin S. The method of increasing accessibility of the dynamic video information resource // *2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, 2016, pp. 621-623.

[10] Barannik, V., Tarasenko, D. Method coding efficiency segments for information technology processing video // *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, 2017. - pp. 551-555.

[11] Chen Ch.-Ch., Wu W.-J. A secure Boolean-based multi-secret image sharing scheme // *Journal of Systems and Software*, Vol. 92, 2014. - pp. 107-114.

[12] Chen T.-H., Wu Ch.-S. Efficient multi-secret image sharing based on Boolean operation. *Signal Processing*, Vol. 91, Iss. 1, 2011.- pp. 90-97.

[13] Deshmukh M., Nain N., Ahmed, M. An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic // *IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016. - pp. 690-697.

[14] DSTU 7624:2014: *Information Technology. Cryptographic protection of information. Symmetric block transformation algorithm.* Order of the Ministry of Economic Development of Ukraine № 1484, 2014.

[15] DSTU GOST 28147:2009: *Information processing system. Cryptographic protection. Cryptographic transformation algorithm* GOST 28147-89, 2008.

[16] Dufaux, F., Ebrahimi, T.: Toward a Secure JPEG. *Applications of Digital Image Processing* XXIX, Vol. 6312, 2006.

[17] Farajallah M. *Chaos-based crypto and joint crypto-compression systems for images and videos* [Електронний ресурс]. Режим доступу: https://hal.archives-ouvertes.fr/ tel-01179610.

[18] Faraoun, K.M. A parallel block-based encryption schema for digital images using reversible cellular automata. *Engineering Science and Technology*, Vol. 17, 2014. - pp. 85–94.

[19] Honda T., Murakami Y., Yanagihara Y., Kumaki T., Fujino T. Hierarchical image-scrambling method with scramble-level controllability for privacy protection // *IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2013. - pp. 1371-1374.

[20] *Information technology – JPEG 2000 image coding system: Secure JPEG 2000*. International Standard ISO/IEC 15444-8; ITU-T Recommendation T.807, 2007. - 108 p.

[21] Ji Sh., Tong X. , Zhang, M.: *Image encryption schemes for JPEG and GIF formats based on 3D baker with compound chaotic sequence generator* [Електронний ресурс]. Режим доступу: arXiv preprint. arXiv: 1208.0999.

[22] Executive Summary *JPEG Privacy & Security Abstract and Executive Summary* [Електронний ресурс]. Режим доступу: https://jpeg.org/items/ 20150910_ privacy_ security _su mmary.html.

[23] Kobayashi H., Kiya H. Bitstream-Based JPEG Image Encryption with File-Size Preserving. // *IEEE 7th Global Conference on Consumer Electronics (GCCE)*, 2018. - pp. 1-4.

[24] Korshunov P., Ebrahimi T. Using warping for privacy protection in video surveillance // *18th International Conference on Digital Signal Processing (DSP)*, 2013. - pp. 1-6.

[25] V. Barannik, V. Barannik, D. Havrylov, A. Sorokun.: Development Second and Third Phase of the Selective Frame Processing Method // *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019. - pp. 54-57.

[26] Minemura, K. and Moayed, Z. and Wong, K. and Qi, X. and Tanaka, K.: JPEG image scrambling without expansion in bitstream size // *19th IEEE International Conference on Image Processing*, 2012. - pp. 261-264.

[27] Naor M., Shamir A. Visual Cryptography. In: Proceedings of the Advances in Cryptology – *EUROCRYPT'94. Lecture Notes in Computer Science*, Vol. 950, 1995. - pp. 1-12.

[28] Phatak A. A Non-format Compliant Scalable RSA-based JPEG Encryption Algorithm. *International Journal of Image, Graphics and Signal Processing*, Vol. 8, No. 6, 2016. - pp. 64-71.

[29] Ramakrishnan S. *Cryptographic and Information Security Approaches for Images and Videos. CRC Press*, 2018. -962 p.

[30] Rivest R.L., Shamir A., Adleman L.M. A method for obtaining digital signatures and public-key cryptosystems // *Communications of the ACM*, (2) 21, 1978. - pp. 120–126.

[31] V. Barannik, M. Karpinski, V.Tverdokhleb, D.Barannik, V. Himenk, M. Aleksander The technology of the video stream intensity controlling based on the bit-planes recombination // *2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, 20-21 Sept. 2018, Lviv, Ukraine.

[32] Sharma, R. and Bollavarapu, S.: Data Security using Compression and Cryptography Techniques. *International Journal of Computer Applications*, Vol. 117, No. 14, 2015/ - pp. 15-18.

[33] V. Barannik, D. Barannik, V. Fustii, M. Parkhomenko Evaluation of Effectiveness of Masking Methods of Aerial Photographs // *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2-6 July 2019, Lviv, Ukraine.

[34] Barannik V.V., Ryabukha Yu. N., Tverdokhleb V.V., Barannik D.V.: Methodological basis for constructing a method for compressing of transformants bit

representation, based on non-equilibrium positional encoding // *Advanced Information and Communication Technologies (AICT), 2017 2nd International Conference*, 2017. - pp.188-192.

[35] Tsai Ch.-L., Chen Ch.-J., Hsu, W.-L. Multimorphological image data hiding based on the application of Rubik's cubic algorithm // *IEEE International Carnahan Conference on Security Technology (ICCST0)*, 2012. - pp. 135-139.

[36] Vasiliev, V.B., Okov, I.N., Strezhik, Yu.N., Ustinov, A.A., Shvetsov, N.V.Video data compression and protection in UAV information exchange radio channels //*Scientific and practical conference on Prospects for the development and use of complexes with unmanned aerial vehicles*, 2016. - pp. 202–204.

[37] Wong K.-W. Image encryption using chaotic maps. *Intelligent Computing Based on Chaos*, Vol. 184, 2009. -pp. 333–354.

[38] Wong K., Tanaka K. DCT based scalable scrambling method with reversible data hiding functionality // *4th International Symposium on Communications, Control and Signal Processing (ISCCSP)*, 2010. - pp. 1-4.

[39] Wu Yu., Agaian. S., Noonan J. Sudoku Associated Two Dimensional Bijections for Image Scrambling // *IEEE Transactions on multimedia* [Електронний ресурс]. Режим доступу: arXivpreprint.arXiv: 1207.5856v1.

[40] Yang, Ch.-N., Chen, Ch.-H., Cai, S.-R. Enhanced Boolean-based multi secret image sharing scheme. *Journal of Systems and Software*, Vol. 116, 2016. - pp. 22-34.

[41] Yang. Y., Zhu B.B., Li S., Yu1, N. Efficient and Syntax-Compliant JPEG 2000 Encryption Preserving Original Fine Granularity of Scalability. *EURASIP Journal on Information Security*, Vol. 2007, Article ID 56365, 2008. - 13 p.

[42] Yuan L., Korshunov. P., Ebrahimi T.Secure JPEG Scrambling enabling Privacy in Photo Sharing. // *11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, 2015. - pp. 1-6.

[43] Zhou Y., Panetta K., Agaian S., ChenC.L.P. Image encryption using P-Fibonacci transform and decomposition. *Optics Communications*, Vol. 285, Iss. 5, 2012. - pp. 594-608.

УДК 621.327:681.5

Бараннік В.В, Сідченко С.О., Бараннік Д.В., Бараннік В.В. Оцінка недетермінованих характеристик плаваючої схеми кодування методу криптокомпресійного представлення зображень в диференційованому базисі

Анотація. *Проведено оцінку недетермінованих характеристик плаваючої схеми кодування для методу криптокомпресійного представлення зображень в диференційованому базисі. А саме: оцінка кількості елементів зображення, які формують кодові конструкції; оцінка довжини сформованих кодових конструкцій. Доведено, що кодові конструкції формуються на змінної (заздалегідь невизначеної) кількості елементів вихідного зображення. У формуванні коду інформаційної складової криптокомпресійного представлення зображень в диференційованому базисі при довжині кодового слова в 64 біта може брати участь від 8 до 64 і більше елементів вихідного зображення. Кодові конструкції формуються змінної (заздалегідь невизначеної) довжини, яка знаходиться в діапазоні від 57 до 64 біт при довжині кодового слова в 64 біта. Без наявності відкритої системи підстав неможливо апріорно передбачити довжину будь-якого коду інформаційної складової криптокомпресійного представлення зображень. Тим більше, не можна розбити всю інформаційну складову на окремі блоки, що відповідають окремим кодовим конструкціям. Кількість елементів, що формують коди інформаційної складової криптокомпресійного представлення зображень, і довжини самих інформаційних складових залежать тільки від вихідних значень елементів зображення. Вони є різними, як для різних зображень, так і для різних колірних площин в межах одного зображення.*

Ключові слова: *криптокомпресійне представлення зображення, захист інформації, шифрування, кодування, компресія зображення, конфіденційність, плаваюча схема, диференційований базис.*

Barannik V., Sidchenko S., Barannik D., Barannik V. Estimation of the influence of undetermined characteristics on the efficiency of crypto-compression image coding in a differentiated base

Annotation. *The non-deterministic characteristics of the floating coding scheme for the method of cryptocompression representation of images in a differentiated basis are estimated. Namely: eestimation of the number of image elements that form code constructions; estimation of the length of the formed code structures. It is proved that code constructions are formed on a variable (predetermined) number of elements of the original image. In the formation of the code of the information component of the cryptocompression representation of images in a differentiated basis with a codeword length of 64 bitsmay involve from 8 to 64 or more elements of the original image. Code constructs are formed of variable (predetermined) length, which ranges from 57 to 64 bits with a codeword length of 64 bits Without an open system of grounds, it is impossible to priori predict the length of any code of the informational component of the cryptocompression image representation. Moreover, it is impossible to break all information component into separate blocks corresponding to separate code constructions. The number of elements that form the codes of the information component of the cryptocompression representation of images, and the lengths of the information components themselves depend only on the initial values of the image elements. They are different for different images and for different color planes within the same image.*

Key words: *cryptocompression image representation, information protection, encryption, coding, image compression, confidentiality, floating scheme, differentiated basis.*

Бараннік Володимир Вікторович, д.техн.,наук, професор, професор кафедри штучного інтелекту і програмування, Харківського національного університету імені В.Н. Каразіна.
Баранник Владимир Викторович, д.техн.наук, профессор, профессор кафедры искусственного интеллекта и программирования, Харьковского национального университета имени В.Н. Каразина.
Barannik Volodymyr, Doctor of Technical Sciences, Professor, Professor Department, V.N. Karazin Kharkiv National University.

Сідченко Сергій Олександрович, к. техн. наук, старший науковий співробітник, докторант Харківського національного університету Повітряних Сил імені І. Кожедуба.
Сидченко Сергей Александрович, к. техн. наук, старший научный сотрудник, докторант Харьковского национального университета Воздушных Сил шимени И. Кожедуба.
Sidchenko Serhii, associate professor, Doctoral Student in Ivan Kozhedub Kharkiv National Air Force University.

Бараннік Дмитро Володимирович, аспірант, Харківського національного університету радіоелектроніки.
Баранник Дмитрий Владимирович, аспирант, Харьковского национального университета радиоэлектроники.
Barannik Dmitriy, PhD student, Kharkov National University of Radio Electronics
Бараннік Валерій Володимирович, студент Харківського національного університету радіоелектроніки.

Бараннік Валерій Володимирович, студент Харківського національного університету радіоелектроніки.
Баранник Валерий Владимирович, студент Харьковского национального университета радиоэлектроники.
Barannik Valery, student, Kharkov National University of Radio Electronics, Kharkiv.

Отримано *26 жовтня 2020 року*, затверджено редколегією *15 грудня 2020 року*