УДК 621.39

В.В. Баранник, доктор технических наук, профессор,
С.А. Сидченко, кандидат технических наук,
В.В. Ларин

МЕТОД ОЦЕНКИ ОПЕРАТИВНОСТИ ЗАЩИТЫ ВИДЕОИНФОРМАЦИИ НА ОСНОВЕ СТОЙКОГО К ДЕШИФРИРОВАНИЮ ПРЕДСТАВЛЕНИЯ

Получены математические выражения для оценки производительности технологии дешифрируемо-стойкого представления изображений и временных затрат при ее реализации в современных информационно-телекоммуникационных системах. Показано, что быстродействие выполнения дешифрируемо-стойкого представления изображений зависит от типа вычислительной системы, на которой выполняется преобразование.

***Ключевые слова**: дешифрируемо-стойкое представление, компактное представление изображений, полиадический код.*

Отримано математичні вирази для оцінки продуктивності технології дешифровано-стійкого представлення зображень і часових затрат при її реалізації у сучасних інформаційно-телекомунікаційних системах. Показано, що швидкодія виконання дешифровано-стійкого представлення зображень залежить від типу обчислювальної системи, на якій виконується перетворення.

***Ключові слова**: дешифровано-стійке представлення, компактне представлення зображень, поліадичний код.*

Mathematical expressions for an estimation of the productivity of the technology of images decoded-pro presentation and temporal expenses during its realization in modern informatively-telecommunication systems are got. The fact that the fast-acting of the implementation of decoded-proof presentation of images depends on the type of the computer system, is proved.

***Keywords**: decoded-proof presentation, compact presentation of images, poliadical code.*

Информация становится одним из ценнейших компонентов национального достояния и одним из важнейших политико-экономических и военных ресурсов. Развитие телекоммуникационных технологий в военной сфере происходит в направлении повышения производительности их функционирования с обеспечением требуемого уровня безопасности передаваемой информации. При этом наибольшие сложности возникают в процессе обработки и передачи оцифрованных видеоданных, занимающих основную часть суммарного информационного потока [1]. Поэтому *актуальной научно-прикладной задачей* является повышение объема видеоинформации, передаваемой за единицу времени с заданным уровнем конфиденциальности, с использованием информационно-

телекоммуникационных систем военного назначения. Для ее решения в работах [2–4] был предложен способ дешифрируемо-стойкого представления изображений (ДШСП) на основе интегрирования технологии компактного представления изображений на базе систем полиадического кодирования и специального криптографического преобразования на базе алгоритма ГОСТ 28147-89. *Целью исследований статьи* является оценка быстродействия предложенной технологии дешифрируемо-стойкого представления изображений при реализации ее в современных информационно-телекоммуникационных системах на основе программной реализации.

Технология дешифрируемо-стойкого представления изображений основывается на использовании систем: компрессии видеоданных на базе систем полиадического кодирования, что позволяет сократить длину сообщений, поступающих на шифрование, и снизить суммарное время на их обработку и передачу; специального криптографического преобразования на базе алгоритма ГОСТ 28147-89, что позволяет обеспечить стойкость относительно несанкционированной дешифровки видеоданных в открытых системах. Исходя из технологии ДШСП, временные затраты, необходимые на его выполнение, определяются выражением:

$$T_{ДШСП}=T_{сд}+T_{шсд}, \quad (1)$$

где $T_{сд}$ – время сжатия данных; $T_{шсд}$ – время на шифрование сжатых данных.

Суммарное время обработки и доставки видеоданных за счет выполнения ДШСП определяется выражением:

$$T_{обр}=T_{ДШСП}+T_{псш}=T_{сд}+T_{шсд}+T_{псш}, \quad (2)$$

где $T_{псш}$ – время на передачу данных после их сжатия и шифрования.

Из анализа формул (1) и (2) видно, что на суммарное время обработки и доставки видеоданных $T_{обр}$ оказывают существенное влияние время сжатия видеоданных $T_{сд}$, время шифрования сжатых видеоданных $T_{шсд}$ и время на их доставку $T_{псш}$.

В общем случае время выполнения любого преобразования $T_{преоб}$ определяется отношением общего объема обрабатываемых данных $W_д$ к быстродействию этого преобразования $V_{преоб}$ по формуле:

$$T_{преоб}=\frac{W_д}{V_{преоб}}, \quad (3)$$

где $V_{преоб}$ – скорость выполнения преобразования, которая определяется по формуле:

$$V_{преоб}=\frac{V_{проц}}{Q}W_{блок}, \quad (4)$$

где $V_{проц}$ – производительность вычислительной системы (тактовая частота процессора); Q – количество элементарных операций (инструкций), необходимых для выполнения преобразования; $W_{блок}$ – размерность блока обрабатываемых преобразованием данных.

С учетом (4) выражение (3) примет вид:

$$T_{преоб} = \frac{W_д Q}{V_{проц} W_{блока}}. \quad (5)$$

Исходя из этого, временные затраты на выполнение компактного представления блока изображений размерностью 64 бита определяются соотношением:

$$T_{сд} = \frac{W_{ид} Q_{сд}}{64 V_{проц}}, \quad (6)$$

где $W_{ид}$ – объем исходного изображения; $Q_{сд}$ – количество элементарных операций (инструкций), необходимых для выполнения компактного представления одного блока исходного изображения.

Реализация ДШСП возможна в варианте криптографического шифрования служебной части, для которого достигается сокращение суммарного времени на обработку.

С учетом выражений (5) и (6) временные затраты на выполнение криптографического преобразования служебной составляющей блоками размерностью 64 бита определяются соотношением:

$$T_{шсд} = T_{шсс} = \frac{W_{сс} Q_{шд}}{64 V_{проц}}, \quad (7)$$

где $W_{сс}$ – объем служебной составляющей кодограммы сжатого представления; $Q_{шд}$ – количество элементарных операций (инструкций), необходимых для выполнения криптографического преобразования одного блока служебной составляющей кодограммы.

Кодирование и декодирование полиадических кодовых конструкций выполняется на основе целочисленных арифметических операций (инструкций) сложения, вычитания и умножения. При осуществлении полиадического кодирования дополнительно используются логические операции ИЛИ для нахождения оснований двумерного полиадического числа. Специальное криптографическое преобразование ГОСТ 28147-89 выполняется на основе целочисленных операций арифметического сложения, побитового сложения (логической операции исключающего ИЛИ) и логической операции циклического сдвига влево, а также операции преобразования кодов для реализации S-блоков.

Типы и количество операций (инструкций), необходимые для выполнения полиадического кода и алгоритма ГОСТ 28147-89, и число тактов (микроопераций) для выполнения этих операций на разных тинах процессоров, представлены в таблице 1. Суммарное количество тактов (микроопераций) для обработки блока данных длинной 64 бита этими преобразованиями на разных типах процессоров представлены в таблице 2. Из анализа данных таблиц 1 и 2 видно, что для выполнения полиадического кодирования блока данных размерностью 64 бита потребуется до 2-х раз меньше тактов процессора, чем для выполнения криптографического преобразования ГОСТ 28147-89 блока данных этого же размера. Приведенные значения тактов (микроопераций) для

выполнения одной операции (инструкции, команды) и рассчитанные на их основе суммарные затраты для обработки блока данных длинной 64 бита, приведенные в таблицах 1 и 2, являются минимальными. При этом пересылка данных и адресов, а так же другие дополнительные команды, необходимые для реализации преобразований (ДШСП, полиадического кода и алгоритма ГОСТ 28147-89) на разных языках программирования, могут увеличить реальное суммарное количество тактов до 2-х раз.

Таблица 1

Типы и количество операций (инструкций), необходимых для выполнения преобразований, и число тактов (микроопераций) для выполнения этих операций на разных типах процессоров

Тип операции (инструкции)		Количество операций для блока 64 бита	Минимальное число тактов (микроопераций) для процессора				
			8088	80286	80386	Plain, MMX	P Pro, II, III
Полиадический код							
Сложение	ADD	8	3	2	2	1	1
Вычитание	SUB	16	3	2	2	1	1
Умножение	MUL	8	70	13	12	11	1
Логическое ИЛИ	OR	16	3	2	2	1	1
Алгоритм ГОСТ 28147-89							
Сложение	ADD	32	3	2	2	1	1
Преобразование кодов (S-бокс)	XLAT	32	11	5	5	4	1
Побитовое сложение	XOR	32	3	2	2	1	1
Циклический сдвиг влево	ROL	32	15	3	3	1	1

Таблица 2.

Количество тактов (микроопераций) для обработки блока данных длиной 64 бита разными преобразованиями для разных типов процессора

Тип процессора	Тип преобразования	
	Полиадический код	Алгоритм ГОСТ 28147-89
Количество операций (инструкций)	48	128
8088	680	1024
80286	184	384
80386	176	384
Pentium Plain и MMX	128	224
Pentium Pro, II и III (1 операция за такт)	48	128
Суперскалярные процессоры	12–40	32–64

При расчете суммарного количества тактов для выполнения преобразований также учитывалось, что современные процессоры в каждом своем ядре содержат несколько исполнительных блоков каждого типа (в том числе, и для операций с плавающей точкой), работающих параллельно и способных выполнять более одной операции (инструкции) за такт. Данная особенность архитектуры впервые появилась ещё в самом первом процессоре Pentium в 1993 году и называется

суперскалярность. Наиболее ярко это свойство проявилось в современных процессорах.

Другим основным параметром, влияющим на время выполнения любого преобразования с помощью выражений (5) – (7), является производительность вычислительной системы (тактовая частота процессора) $V_{проц}$. Одним из подходов для расчета производительности современных вычислительных систем является пиковая производительность компьютеров, которая рассчитывается по формуле:

$$V_{проц} = R_p = F_p n_p n_{такт} 10^{-6}, \quad (8)$$

где R_p – пиковая производительность; F_p – частота процессора (ядра процессора), МГц; n_p – количество процессоров или ядер в процессоре; $n_{такт}$ – количество инструкций (команд) процессора, выполняющихся за один такт.

Производительность вычислительной системы в исследовательских целях предлагается определять через тактовую частоту по формуле:

$$V_{проц} = 0{,}8 \cdot F_p 10^6 \text{ [тактов/сек.]}. \quad (9)$$

Третьим параметром, влияющим на время выполнения любого преобразования с помощью выражений (5) – (7), является объем обрабатываемых данных, который в выражении (6) представлен объемом исходного изображения $\tilde{W}_{ид}$, а в выражении (7) – объемом служебной составляющей кодограммы сжатого представления $W_{сс}$.

Объем исходного изображения, состоящий из трех плоскостей, определяется по формуле

$$W_{ид} = 3(L_{стр} \times L_{стлб}) \text{ [байт]} = 24(L_{стр} \times L_{стлб}) \text{ [бит]}, \quad (10)$$

где 3 – количество плоскостей исходного изображения; $L_{стр}$ – количество строк в изображении (его ширина); $L_{стлб}$ – количество столбцов изображения.

Общий объем данных ДШСП состоит из объемов информационной и служебной составляющих кодограммы сжатого представления и определяется по формуле:

$$W_{сд} = W_{ис} + W_{сс}, \quad (11)$$

где $W_{сд}$ – объем сжатого изображения; $W_{ис}$ – объем информационной составляющей кодограммы сжатого представления.

При этом, как правило, выполняется условие $W_{сс} < \tilde{W}_{ис} < W_{сд} < W_{ид}$.

Объем служебных данных полиадического представления одной плоскости изображения определяются с учетом таблиц минимальных и максимальных элементов по формуле:

$$W_{сс\,пл} = 2\frac{\tilde{L}_{стр} \times L_{стлб}}{n} \text{[байт]} = 16\frac{\tilde{L}_{стр} \times L_{стлб}}{n} \text{ [бит]}, \quad (12)$$

где n – размерность матрицы полиадического кодирования.

На практике часто принимает значение, равное 8. Исходя из этого, выражение (12) примет вид: $W_{cc.пл} = \frac{L_{стр} \times L_{стлб}}{4}$ [байт] $= 2(L_{стр} \times L_{стлб})$ [бит]

Объем служебных данных ДШСП изображений определяется как сумма объемов служебных данных плоскостей исходного изображения, подвергнутых полиадическому представлению, по формуле:

$$W_{сс} = 3W_{сс\,пл} = 6\frac{L_{стр} \times L_{стлб}}{n} \text{ [байт]} = 48\frac{L_{стр} \times L_{стлб}}{n} \text{ [бит]} = 6(L_{стр} \times L_{стлб}) \text{[бит]} \quad (13)$$

С учетом формул (6), (7), (9), (10) и (13) выражение (1) примет вид:

$$T_{ДШСП} = T_{сд} + T_{псш} = \frac{W_{ид} Q_{сд}}{64V_{проц}} + \frac{W_{сс} Q_{шд}}{64V_{проц}} \approx \frac{(L_{стр} \times L_{стлб})(4Q_{сд} + Q_{шд})}{8{,}53 \cdot F_p 10^6}, \quad (14)$$

где параметры $Q_{сд}$ и $Q_{шд}$ определяются по таблице 2 в тактах исходя из типа процессора.

Время передачи данных $T_{псш}$ зависит от пропускной способности каналов связи и объемов передаваемых данных и определяется соотношением:

$$T_{псш} = \frac{W_{сд}}{V_{канал}}, \quad (15)$$

где $V_{канал}$ – скорость канала передачи данных.

Объем передаваемых данных в силу применения систем компрессии зависят от коэффициента сжатия изображений. Коэффициент сжатия изображений определяется как соотношение исходного объема изображения $W_{ид}$ к объему его сжатого представления $W_{сд}$ соотношением:

$$k_{сж} = \frac{W_{ид}}{W_{сд}} \quad (16)$$

С учетом формул (10), (11), (13) соотношение (16) при единицах измерения объемов в байтах примет вид:

$$k_{сж} = \frac{W_{ид}}{W_{сд}} = \frac{W_{ид}}{W_{ис} + W_{сс}} = \frac{3(L_{стр} \times L_{стлб})}{W_{ис} + 6\frac{L_{стр} \times L_{стлб}}{n}}. \quad (17)$$

На практике иногда бывает необходимо знать коэффициент сжатия информационной составляющей ДШСП изображения, который определяется соотношением:

$$k^{и}_{сж} = \frac{W_{ид}}{W_{ис}}. \quad (18)$$

Коэффициенты сжатия $k_{сж}$ реалистичных изображений разной степени насыщенности (рис. 1) методом полиадического кодирования представлены в

таблице 3. Кроме того, в таблице представлены объемы исходного изображения $W_{ид}$, ДШСП изображения $W_{сд}$ и его составляющие $W_{ис}$, $W_{сс}$. В таблице 4 представлены средние значения коэффициента сжатия $k_{сж}$ для разных методов внутрикадровой обработки. Из анализа данных таблицы видно, что степень сжатия реалистических изображений методом полиадического кодирования уступает только методу сжатия JPEG.

а б в г

Рис. 1. Примеры изображений разной степени насыщенности:
а) слабая; б) средняя; в) средняя; г) сильная.

Таблица 3

Коэффициент сжатия изображений разной степени насыщенности методом полиадического кодирования

Номер рисунка	Тип насыщенности	Размер изображения $L_{стр} \times L_{стлб}$	Объем изображения, байт				$k_{сж}$	$k^{и}_{сж}$
			$W_{ид}$	$W_{сд}$	$W_{ис}$	$W_{сс}$		
1, а	слабая	369×551	609957	330606	180408	150198	1,84	3,38
1, б	средняя	630×412	778680	461934	270936	190998	1,69	2,87
1, в	средняя	369×551	609957	466006	315808	150198	1,31	1,93
1, г	сильная	430×357	460530	447846	335856	111990	1,03	1,37

Таблица 4

Значение коэффициента сжатия $k_{сж}$ для методов внутрикадровой обработки

Метод сжатия	Степень насыщенности и тип изображения		
	сильная $0,3 \le r \le 0,7$	средняя $0,9 < r$	слабая $p < 0,1$
	реалистическое		искусственное
КДС	0.9	1,7	10
Арифметическое кодирование	1,17	1,7	5,7
LZW	1.3	2.2	13
Полиадическое кодирование	1,32	1,8	2
JPEG, q=0	2	3	3.5

Зная объем и степень насыщенности исходного изображения, а также соответствующее ему среднее значение коэффициента сжатия $k_{сж}$ для полиадического кодирования (таблице 6) с помощью формул (10), (11), (13) и (16) можно рас-

считать оценочное значение объема информационной части ДСШП (полиадического кода) для этого изображения с помощью выражения:

$$W_{ис} = W_{сд} - W_{сс} = \frac{W_{ид}}{k_{сж}} - W_{сс} = 6(L_{стр} \times L_{стлб})\left(\frac{4}{k_{сж}} - 1\right)[\text{бит}] = \tag{19}$$

$$= 3(L_{стр} \times L_{стлб})\left(\frac{1}{k_{сж}} - \frac{1}{4}\right)[\text{байт}],$$

а для одной плоскости изображения с помощью выражения:

$$W_{ис.пл} = 2(L_{стр} \times L_{стлб})\left(\frac{4}{k_{сж}} - 1\right)[\text{бит}] = (L_{стр} \times L_{стлб})\left(\frac{1}{k_{сж}} - \frac{1}{4}\right)[\text{байт}]. \tag{20}$$

Оценочное значение объема информационной части ДСШП изображения, зная среднее значение коэффициента сжатия информационной части $k^{и}_{сж}$, на основании формул (10) и (17) можно рассчитать с помощью выражения:

$$W_{и.с} = \frac{W_{ид}}{k^{и}_{сж}} = \frac{24(L_{стр} \times L_{стлб})}{k^{и}_{сж}}[\text{бит}] = \frac{3(L_{стр} \times L_{стлб})}{k^{и}_{сж}}[\text{байт}]. \tag{21}$$

а для одной плоскости изображения с помощью выражения:

$$W_{и.с.пл} = \frac{8(L_{стр} \times L_{стлб})}{k^{и}_{сж}}[\text{бит}] = \frac{L_{стр} \times L_{стлб}}{k^{и}_{сж}}[\text{байт}]. \tag{22}$$

На основании формул (18) – (21) коэффициент сжатия информационной составляющей ДШСП изображения $k^{и}_{сж}$ можно рассчитать через коэффициент сжатия изображения $k_{сж}$ (усредненное значение которого для полиадического кода представлено в таблице 6) с помощью выражения:

$$k^{и}_{сж} = \frac{4k_{сж}}{4 - k_{сж}}. \tag{23}$$

С учетом формул (10) и (16) соотношение (15) примет вид:

$$T_{доп} = \frac{W_{сд}}{V_{канал}} = \frac{W_{ид}}{k_{сж} V_{канал}} = \frac{24(L_{стр} \times L_{стлб})}{k_{сж} V_{канал}} \tag{24}$$

Соотношение (15) с учетом формул (10), (11), (13) и (17) примет вид:

$$T_{доп} = \frac{W_{сд}}{V_{канал}} = 6(L_{стр} \times L_{стлб})\frac{4/k^{и}_{сж} + 1}{V_{канал}}. \tag{25}$$

В итоге суммарное расчетное время обработки и доставки видеоданных за счет выполнения ДШСП, определяемое выражением (2), примет вид:

– с учетом формул (14) и (22):

$$T_{обр} = T_{ДШСП} + T_{псш} = (L_{стр} \times L_{стлб}) \left(\frac{4Q_{сд} + Q_{шд}}{8{,}53 \cdot F_p 10^{9}} + \frac{24}{k_{сж} V_{канал}} \right); \quad (26)$$

– с учетом формул (14) и (23):

$$T_{обр} = T_{ДШСП} + T_{псш} = (L_{стр} \times L_{стлб}) \left(\frac{4Q_{сд} + Q_{шд}}{8{,}53 \cdot F_p 10^{6}} + 6\frac{4/k^{и}_{сж} + 1}{V_{канал}} \right). \quad (27)$$

При этом выигрыш в суммарном времени обработки и доставки дешифрируемых видеоданных с обеспечением безопасности информации относительно несанкционированного доступа за счет использования дешифрированно-стойкого представления изображений будет достигаться, если верно условие

$$T_{шд} + T_{пд} \geq T_{сд} + T_{шсд} + T_{псш}, \quad (27)$$

где $T_{шд}$ – время шифрования исходных данных; $T_{пд}$ – время передачи шифрованных исходных данных.

Создание дешифрируемо-стойкого представления изображений позволяет, с одной стороны, сократить длину сообщений, поступающих на шифрование, и снизить время обработки, а, с другой стороны, обеспечить стойкость относительно несанкционированной дешифровки видеоданных в открытых системах.

В статье получены математические выражения для оценки производительности технологии дешифрируемо-стойкого представления изображений и временных затрат при ее реализации в современных информационно-телекоммуникационных системах. Показано, что быстродействие выполнения дешифрируемо-стойкого представления изображений зависит от типа вычислительной системы, на которой выполняется преобразование.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Баранник В.В.* Структурно-комбинаторное представление данных в АСУ : Монография / В.В. Баранник, Ю.В. Стасев, Н.А. Королева. – Х. : ХУПС, 2009. – 252 с.
2. *Баранник В.В.* Методология создания криптографических преобразований на базе методов исключающих избыточность / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. – 2009. – № 4 (19). – С. 5–12.
3. *Баранник В.В.* Метод криптосемантического представления изображений на основе комбинированного подхода / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. – 2010. – № 3 (22). – С. 33–38.
4. *Баранник В.В.* Формирование дешифрируемо-стойкого представления изображений в системах компрессии / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Міжнар. наук.-практ. конф., Вінниця, 19–21 травня 2010 р. / Вінницький національний технічний університет, "Інформаційні технології та комп'ютерна інженерія". – Вінниця, 2010. – С. 40–41.
5. *Джордейн Р.* Справочник программиста персональных компьютеров типа IBM PC, XT и AT / Роберт Джордейн; пер. с англ. Н.В. Гайского. – М. : Финансы и статистика, 1992. – 544 с.
6. *Шагурин И.И.* 80386: описание и система команд / И.И. Шагурин, В.Б. Бродин, Г.П. Мозговой. – М. : МП "Малип", 1992. – 160 с.
7. *Фог А.* Оптимизация для процессоров семейства Pentium / Агнер Фог – [Электронный ресурс]. – Режим доступа : http://www.wasm.ru/series.php?sid=11.
8. *Корнеев В.В.* Современные микропроцессоры / В.В. Корнеев, А.В. Киселев. – М. : Нолидж, 2000. – 320 с.

Отримано 15.09.2011