УДК 621.327

МЕТОД ОЦІНЮВАННЯ ОПЕРАТИВНОСТІ МАСКУВАННЯ ВІДЕОІНФОРМАЦІЇ У ВІЙСЬКОВО-ТЕХНІЧНИХ КОМПЛЕКСАХ ТА СИСТЕМАХ ОЗБРОЄННЯ

Сідченко С. О., канд. техн. наук

Харківський університет Повітряних Сил імені Івана Кожедуба

sidserg@list.ru

Наведено математичні вирази для оцінювання продуктивності технології дешифровано-стійкого представлення зображень і часових витрат при її реалізації в 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 are got for the estimation of the productivity of technology of decoded-pro of presentation of images and temporal expenses during its realization in the modern informatively-telecommunication systems. It is rotined that the fast-acting of implementation of decoded-proof presentation of images depends on the type of the computer system which transformation is executed on.

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

Вступ

На основі досягнень науково-технічного прогресу в інформаційній сфері інформація стає одним з найцінніших компонентів національного надбання та одним з найважливіших політико-економічних і військових ресурсів.

Аналіз останніх збройних конфліктів і локальних війн підтверджує думку, що успіх ведення бойових дій багато в чому визначається своєчасністю, повнотою та вірогідністю одержуваних розвідувальних даних про протиборчу сторону. Більшість даних надходять за допомогою засобів видової розвідки у вигляді зображень, як правило, у цифровій формі, а обробка ведеться на комп'ютерах з використанням інформаційно-телекомунікаційних систем.

Розвиток телекомунікаційних технологій у військовій сфері відбувається в напрямку підвищення продуктивності їх функціонування із забезпеченням необхідного рівня безпеки переданої інформації. При цьому найбільші складності виникають у процесі обробки та передачі оцифрованих відеоданих, що займають основну частину сумарного інформаційного потоку [1]. Тому ***актуальним науково-прикладним завданням*** є підвищення обсягу відеоінформації, переданої в одиницю часу із заданим рівнем конфіденційності, з використанням інформаційно-телекомунікаційних систем військового призначення. Для його вирішення в працях [2 — 4] запропоновано спосіб дешифровано-стійкого представлення зображень (ДШСП) на основі інтегрування технології компактного представлення зображень на базі систем поліадичного кодування та спеціального криптографічного перетворення на базі алгоритму ГОСТ 28147-89.

Мета дослідження — оцінювання оперативності технології дешифровано-стійкого представлення зображень при реалізації її у військово-технічних комплексах та системах озброєння (у тому числі в сучасних інформаційно-телекомунікаційних системах військового призначення) на основі програмної реалізації.

Основна частина

Технологія дешифровано-стійкого представлення зображень ґрунтується на використанні систем:

— компресії відеоданих на базі систем поліадичного кодування, що дозволяє скоротити довжину повідомлень, які надходять на шифрування, і знизити сумарний час на їх обробку та передачу;

— спеціального криптографічного перетворення на базі алгоритму ГОСТ 28147-89, що дає змогу забезпечити стійкість щодо несанкціонованого дешифрування відеоданих.

Виходячи з технології ДШСП, часові витрати, необхідні на його виконання, визначаються так:

$$T_{\text{ДШСП}} = T_{\text{сд}} + T_{\text{ш сд}}, \qquad (1)$$

де $T_{\text{сд}}$ — час на компактне представлення (стиснення) даних; $T_{\text{ш сд}}$ — час на шифрування стислих даних.

З аналізу формули (1) видно, що на час виконання ДШСП відеоданих $T_{\text{ДШСП}}$ впливають час стиснення відеоданих $T_{\text{сд}}$ і час шифрування стиснутих відеоданих $T_{\text{ш сд}}$. Отже, час, необхідний для виконання стиснення $T_{\text{сд}}$ та шифрування $T_{\text{ш сд}}$ даних, прямо залежить від кількості елемен-

тарних операцій (інструкцій), необхідних для виконання цих перетворень, продуктивності обчислювальних систем (процесорів), на яких виконуються перетворення, і обсягів оброблюваних даних.

У загальному випадку час виконання будь-якого перетворення $T_{\text{ï åðåò}}$ визначається відношенням загального обсягу оброблюваних даних $W_{\text{ä}}$ до швидкодії цього перетворення $v_{\text{ï åðåò}}$ за формулою:

$$T_{\text{ï åðåò}} = \frac{W_{\text{ä}}}{v_{\text{ï åðåò}}}, \qquad (2)$$

де $v_{\text{ï åðåò}}$ — швидкість виконання перетворення, що визначається по формулі:

$$v_{\text{ï åðåò}} = \frac{\nu_{\text{ï ðî ö}}}{Q} W_{\text{áëî ê}}, \qquad (3)$$

де $\nu_{\text{ï ðî ö}}$ — продуктивність обчислювальної системи (тактова частота процесора); Q — кількість елементарних операцій (інструкцій), необхідних для виконання перетворення; $W_{\text{áëî ê}}$ — розмірність блока, оброблюваних перетворенням даних.

З урахуванням формули (3), вираз (2) набуде вигляду:

$$T_{\text{ï åðåò}} = \frac{W_{\text{ä}} Q}{\nu_{\text{ï ðî ö}} W_{\text{áëî ê}}}. \qquad (4)$$

Отже, часові витрати на виконання компактного представлення блока зображення розмірністю 64 біта визначаються співвідношенням:

$$T_{\text{ñä}} = \frac{W_{\text{âä}} Q_{\text{ñä}}}{64\nu_{\text{ï ðî ö}}}, \qquad (5)$$

де $W_{\text{âä}}$ — обсяг вихідного зображення; $Q_{\text{ñä}}$ — кількість елементарних операцій (інструкцій), необхідних для виконання компактного представлення (стиснення) одного блока вихідного зображення.

Реалізація ДШСП можлива в таких варіантах: криптографічне шифрування службової частини; криптографічне шифрування інформаційної частини; криптографічне шифрування відразу обох частин.

З наведених варіантів найбільші часові витрати на обробку необхідні у випадку криптографічного перетворення інформаційної та службової складових, тобто:

$$\grave{O}_{\text{ø ñä}} = \grave{O}_{\text{ø ³ñ}} + \grave{O}_{\text{ø ññ}},$$

де $\grave{O}_{\text{ø ñä}}$ — часові витрати на криптографічне перетворення стиснутих даних; $\grave{O}_{\text{ø ³ñ}}$, $\grave{O}_{\text{ø ññ}}$ — часові витрати на криптографічне перетворення відповідно інформаційної та службової частин кодограми компактного представлення відеоданих.

І навпаки, скорочення сумарного часу на обробку досягається для першого варіанта, коли криптографічному перетворенню піддається тільки службова складова, тобто

$$\grave{O}_{\text{ø ñä}} = \grave{O}_{\text{ø ññ}}.$$

З урахуванням виразів (4) і (5) часові витрати на виконання криптографічного перетворення службової складової блоками розмірністю 64 біта визначаються співвідношенням:

$$T_{\text{ø ñä}} = T_{\text{ø ññ}} = \frac{W_{\text{ñ.ñ}} Q_{\text{ø ä}}}{64\nu_{\text{ï ðî ö}}}, \qquad (6)$$

де $W_{\text{ñ.ñ}}$ — обсяг службової складової кодограми компактного представлення; $Q_{\text{ø ä}}$ — кількість елементарних операцій (інструкцій), необхідних для виконання криптографічного перетворення одного блоку службової складової кодограми.

Одним з основних параметрів, що впливають на час виконання будь-якого перетворення за допомогою виразів (4)—(6), є кількість елементарних операцій (інструкцій), необхідних для виконання цих перетворень.

Кодування та декодування поліадичних кодових конструкцій виконується на основі дійсних арифметичних операцій (інструкцій) додавання, вирахування та множення.

При здійсненні поліадичного кодування додатково використовуються логічні операції АБО для знаходження основ двовимірного поліадичного числа.

Спеціальне криптографічне перетворення ГОСТ 28147-89 виконується на основі дійсних операцій арифметичного додавання, побітового додавання (логічної операції, що виключає АБО) і логічної операції циклічного зсуву вліво, а також операції перетворення кодів для реалізації *S*-блоків.

Аналіз швидкодії процесорів 8088, 80286, 80386, *Pentium Plain*, *Pentium MMX*, *Pentium Pro*, *Pentium II* і *Pentium III* [5—8 та ін.] показав, що залежно від типу команди та типу процесора виконання різних елементарних операцій може займати від часток такту до декількох тактів.

Загальна тенденція в розробці процесорів полягає в зменшенні кількості тактів, що витрачаються на виконання елементарних операцій.

Типи та кількість операцій (інструкцій), необхідні для виконання поліадичного коду та алгоритму ГОСТ 28147-89, і число тактів (мікрооперацій) для виконання цих операцій на різних типах процесорів наведено в табл. 1.

Сумарна кількість тактів (мікрооперацій) для обробки блоку даних розмірністю 64 біта цими перетвореннями на різних типах процесорів подано в табл. 2.

Таблиця 1

Типи та кількість операцій (інструкцій), необхідні для виконання перетворень, і число тактів (мікроопераций) для виконання цих операцій на різних типах процесорів

Тип операції (інструкції)		Кількість операцій для блоку 64 біта	Мінімальне число тактів (мікроопераций) для процесора				
			8088	80286	80386	Plain, MMX	P Pro, II, III
Поліадичний код							
Додавання	ADD	8	3	2	2	1	1
Розрахування	SUB	16	3	2	2	1	1
Множення	MUL	8	70	13	12	11	1
Логічне АБО	OR	16	3	2	2	1	1
Алгоритм ГОСТ 28147-89							
Додавання	ADD	32	3	2	2	1	1
Перетворення кодів (*S*-бокс)	XLAT	32	11	5	5	4	1
Побітове додавання	XOR	32	3	2	2	1	1
Циклічний зсув ліворуч	ROL	32	15	3	3	1	1

Таблиця 2

Кількість тактів (мікроопераций) для обробки блоку даних розмірністю 64 біта різними перетвореннями для різних типів процесора

Тип процесора	Тип перетворення	
	Поліадичний код	Алгоритм ГОСТ 28147-89
Кількість операцій (інструкцій)	48	128
8088	680	1024
80286	184	384
80386	176	384
Pentium Plain і MMX	128	224
Pentium Pro, II і III (1 операція за такт)	48	128
Суперскалярні процесори	12 — 40	32 — 64

З аналізу даних табл. 1 і 2 видно, що для виконання поліадичного кодування блоку даних розмірністю 64 біт буде потрібно у два рази менше тактів процесора, ніж для виконання криптографічного перетворення ГОСТ 28147-89 блоку даних цього ж розміру.

Наведені значення тактів (мікроопераций) для виконання однієї операції (інструкції, команди) і розраховані на їх основі сумарні витрати для обробки блоку даних розмірністю 64 біт, що наведені в табл. 1 і 2, є мінімальними. Промахи кешу, нерівність, ненормальні операнди та виключення можуть значно збільшити кількість тактів, які необхідні для виконання однієї операції (інструкції). При цьому пересилання даних і адресів, а так само інші додаткові команди, необхідні для реалізації перетворень (ДШСП, поліадичного коду та алгоритму ГОСТ 28147-89) на різних мовах програмування, можуть збільшити реальну сумарну кількість тактів до двох разів.

При розрахунку сумарної кількості тактів для виконання перетворень також враховувалося, що сучасні процесори в кожному своєму ядрі містять кілька виконавчих блоків кожного типу (у тому числі й для операцій із плаваючою крапкою), які працюють паралельно і здатні виконувати більше однієї операції (інструкції) за такт.

Така особливість архітектури процесора називається суперскалярністю. Найбільш яскраво ця властивість виявилася в сучасних процесорах. Так, ядро двуядерного процесора Intel Core 2 Duo містить 2 пристрої обчислень над 64-бітними числами із плаваючою комою, які можуть виконувати по 2 зв'язані операції (множення та наступне додавання) у кожному такті, що теоретично дозволяють досягти пікової продуктивності до 4-х операцій за 1 такт у кожному ядрі.

Іншим основним параметром, що впливає на час виконання будь-якого перетворення за допомогою виразів (4)—(6), є продуктивність (швидкодія) обчислювальної системи $\nu_{\text{ïðîö}}$, яку пропонується визначати через тактову частоту за формулою:

$$\nu_{\text{ïðîö}} = 0{,}8 \cdot F_{\text{ïðîö}} 10^6 \text{ [тактів/с]}, \qquad (7)$$

де $F_{\text{ïðîö}}$ — частота процесора, МГц.

Третім параметром, який впливає на час виконання будь-якого перетворення за допомогою виразів (4)—(6), є обсяг оброблюваних даних, що у виразі (5) представлений обсягом вихідного зображення $W_{\text{âä}}$, а у виразі (6) — обсягом служ-

бової складової кодограми компактного представлення $W_{\text{ñ.ñ}}$.

Обсяг вихідного зображення, що складається з трьох площин, визначається за формулою:

$$W_{\text{âä}} = 3(L_{\text{ðÿä}} \cdot L_{\text{ñòî âï}}) \text{ [байт]} = \\ = 24(L_{\text{ðÿä}} \cdot L_{\text{ñòî âï}}) \text{ [біт]}, \quad (8)$$

де 3 — кількість площин вихідного зображення; $L_{\text{ðÿä}}$ — кількості рядків у зображенні (його ширина); $L_{\text{ñòî âï}}$ — кількість стовпців зображення (його висота).

Загальний обсяг даних ДШСП складається з обсягів інформаційної та службової складових кодограми компактного представлення та визначається за формулою:

$$W_{\text{ñä}} = W_{\text{з.ñ}} + W_{\text{ñ.ñ}}, \quad (9)$$

де $W_{\text{ñä}}$ — обсяг стиснутого зображення; $W_{\text{з.ñ}}$ — обсяг інформаційної складової кодограми компактного представлення.

При цьому, як правило, виконується умова

$$W_{\text{ñ.ñ}} < W_{\text{з.ñ}} < W_{\text{ñä}} < W_{\text{âä}}.$$

Обсяг службових даних поліадичного представлення однієї площини зображення визначається з урахуванням таблиць мінімальних і максимальних елементів за формулою:

$$W_{\text{ñ.ñ.ï ë}} = 2\frac{L_{\text{ðÿä}} \cdot L_{\text{ñòî âï}}}{n} \text{ [байт]} = \\ = 16\frac{L_{\text{ðÿä}} \cdot L_{\text{ñòî âï}}}{n} \text{ [біт]}, \quad (10)$$

де n — розмірність матриці поліадичного кодування.

На практиці n часто набуває значення, що дорівнює 8. Виходячи з цього, вираз (10) набуває вигляду:

$$W_{\text{ñ.ñ.ï ë}} = \frac{L_{\text{ðÿä}} \cdot L_{\text{ñòî âï}}}{4} \text{ [байт]} = 2(L_{\text{ðÿä}} \cdot L_{\text{ñòî âï}}) \text{ [біт]}.$$

Обсяг службових даних усіх площин зображення однаковий. Обсяг службових даних ДШСП зображень визначається як сума обсягів службових даних площин вихідного зображення, підданих поліадичному представленню, за формулою:

$$W_{\text{ñ.ñ}} = 3W_{\text{ñ.ñ.ï ë}} = 6\frac{L_{\text{ðÿä}} \cdot L_{\text{ñòî âï}}}{n} \text{ [байт]} = \\ = 48\frac{L_{\text{ðÿä}} \cdot L_{\text{ñòî âï}}}{n} \text{ [біт]} = 6(L_{\text{ðÿä}} \cdot L_{\text{ñòî âï}}) \text{ [біт]}. \quad (11)$$

З урахуванням формул (5)—(8) і (11) вираз (1) набуде вигляду:

$$T_{\text{ÄØ ÑÏ}} = T_{\text{ñä}} + T_{\text{ø ñä}} = \frac{W_{\text{âä}} Q_{\text{ñä}}}{64\nu_{\text{ï ðî ö}}} + \frac{W_{\text{ñ.ñ}} Q_{\text{ø ä}}}{64\nu_{\text{ï ðî ö}}} \approx \\ \approx \frac{(L_{\text{ðÿä}} \cdot L_{\text{ñòî âï}})(4Q_{\text{ñä}} + Q_{\text{ø ä}})}{8{,}53\, F_{\text{ï ðî ö}} 10^6},$$

де параметри $Q_{\text{ñä}}$ та $Q_{\text{ø ä}}$ визначаються за табл. 2 у тактах, виходячи з типу процесора.

Висновок

Створення дешифровано-стійкого представлення зображень дозволяє, з одного боку, скоротити довжину повідомлень, що надходять на шифрування, і знизити час на виконання перетворення, а з іншого боку, забезпечити стійкість щодо несанкціонованого дешифрування відеоданих у відкритих системах.

У статті отримано математичні вирази для оцінювання продуктивності технології дешифровано-стійкого представлення відеоданих і часових витрат при її реалізації у військово-технічних комплексах та системах озброєння (у тому числі в сучасних інформаційно-телекомунікаційних системах). Показано, що швидкодія виконання дешифровано-стійкого представлення зображень залежить від типу обчислювальної системи, на якій виконується перетворення.

ЛІТЕРАТУРА

1. *Баранник В. В.* Структурно-комбинаторное представление данных в АСУ / В. В. Баранник, Ю. В. Стасев, Н. А. Королева // Монография. — 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 // Міжнародна науково-практична конференція «Інформаційні технології та комп'ютерна інженерія» / Вінницький національний технічний університет. — Вінниця: 2010. — С. 40—41.

5. *Джордейн Р.* Справочник программиста персональных компьютеров типа IBM PC, XT и AT / Р. 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 [Электронный ресурс] / Агнер Фог. — Режим доступу: 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.

Стаття надійшла до редакції 15.05.11.