УДК 621.327:681.5

С. О. Сідченко — канд. техн. наук, старш. наук. співроб.
Харківський національний університет Повітряних Сил імені І. Кожедуба
orcid.org/0000-0002-1319-6263

Д. В. Бараннік
orcid.org/0000-0002-2848-4524
e-mail: Barannik_V_V@mail.ru

МЕТОД КРИПТОСЕМАНТИЧНОГО ПРЕДСТАВЛЕННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ПЛАВАЮЧОЇ СХЕМИ СИСТЕМИ ПОЛІАДИЧНОГО КОДУВАННЯ В ДИФЕРЕНЦІАЛЬНОМУ БАЗИСІ

Вступ

Процес впровадження систем відеоспостереження в життєдіяльність людини набирає глобальних масштабів. Ці системи використовують для передачі візуалізованої інформації в процесі візуального контролю, що здійснюєть за допомогою відеокамер та знаходять своє застосування:

– на об'єктах сектора безпеки і оборони, об'єктах критичної інфраструктури держави і регіону, а також інших об'єктах різного призначення суб'єктів усіх прав власності;

– у засобах аерокосмічного моніторингу, у тому числі і в засобахотримання видової розвідувальної інформації;

– на автомобільних, морських (річкових) і залізничних вокзалах, аеропортах;

– на дорогах і в місцях найбільш частого здійснення дорожньо-транспортних подій;

– у найбільш критичних місцях з позиції здійснення правопорушень (у місцях найбільш частого здійснення правопорушень);

– у місцях масового скупчення громадян і проведення масових заходів;

– у засобах відеоконтролю та фотофіксації (включаючи відеокамери терміналів самообслуговування і банкоматів, відеореєстратори транспортних засобів);

– у засобах дистанційного керування пересуванням мобільних об'єктів (техніки);

– під час проведення огляду, обшуку, відтворенні обстановки та обставин події і при проведенні інших слідчих дій;

– у процесі оперативної відеозйомки.

Будь-яке відеоспостереження призводить до отримання персональних даних [1], як безпосередньо, так і опосередковано. А будь-які персональні дані можуть бути віднесені до конфіденційної інформації на підставі закону або людиною, про яку ці дані збираються. При цьому законодавством України не встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними. Сучасний стан правового регулювання відеоспостереження в Україні є неналежним [1], багато питань регулюються підзаконними нормативними актами (внутрішніми наказами), які повинні деталізувати окремі положення закону, а в законі, у свою чергу, вони не відбиті. Способи і методи захисту відео- і фотоматеріалів на законодавчому рівні не визначені, хоча необхідність забезпечення належного зберігання закріплена у ряді нормативно-правових актів, у яких зачіпаються питання застосування систем відеоспостереження. При цьому, резолюція Парламентської Асамблеї Ради Європи щодо здійснення відеоспостереження в суспільних місцях рекомендує на законодавчому рівні закріпити практику кодування (шифрування) даних відеоспостереження для захисту їх від несанкціонованого доступу і модифікації, що може допомогти гарантувати достовірність ін-формації для кримінальних розслідувань [2].

Тому актуальним є питання забезпечення конфіденційності і оперативності доставки відеоінформаційного ресурсу за умови збереження його цілісності.

Аналіз останніх досліджень і публікацій

На сьогодні найбільш популярним рішенням для захисту конфіденційності інформації є шифрування. Для передачі відеоданих застосовується послідовна схема перетворення. На першому етапі здійснюється компресія початкових відеоданих, а на другому — шифрування кодованої послідовності. Проте в разі потокової передачі відеоінформації можливості найбільш популярних алгоритмів шифрування можуть бути обмежені зважаючи на їх недостатню швидкодію, що призведе до втрати оперативності доставки відеоінформаційного ресурсу.

За останні роки було запропоновано безліч спеціалізованих алгоритмів шифрування для рішення проблеми захисту цифрових зображень і потоку відеоінформації. Один з перших, широко поширених підходів до шифрування цифрових відеоданих, полягав у перестановці рядків або

стовпців кадрів відеопотоку [3]. Проте більшість таких алгоритмів не забезпечували достатню крипостійкість і були піддані розтину. Разом з тим, у даний час активно ведуть розробки в області візуальної криптографії, які вперше запропонували М. Наор та А. Шамір [4]. Вони представляють технологію забезпечення конфіденційності візуальної інформації на основі схеми розподілення секрету, відповідно до якої зображення розбивається на n частин [5–7].

За наявності лише (n – 1) частини зображення розшифрувати не можливо. Однак запропоновані підходи застосовують до вихідних відеоданих, але на практиці вихідний обсяг відеоінформаційних ресурсів може буди великим, що призведе до втрати оперативності при обробці даних у реальному режимі часу.

Тому виникла необхідність у розробці принципово нового підходу, що полягає в створенні технології, що одночасно забезпечує підвищення оперативності доведення та захист відеоінформації на основі методів семантичної і синтаксичної обробки зображень. У працях [8–10] була запропонована технологія криптосемантичного представлення (КСП) зображень, призначена для приховання семантичного змісту зображення з урахуванням як статистичних, так і структурних особливостей джерела інформації.

На основі розробленої технології у працях [11, 12] запропоновано метод КСП зображень на основі статичної схеми поліадичного кодування в двовимірному базисі. Одним з недоліків методу КСП зображень на основі статичної схеми є побудова інформаційної складової на основі однакової кількості вихідних елементів фрагмента відеоданих. На виході криптосемантичного представлення будуються кодограми різної довжини в бітовому представленні (менші за довжину, що виділяється для збереження кодового слова), що призводить до появи великої кількості незначущих нульових елементів у бітових послідовностях інформаційної складової КСП [13, 14]. Цей недолік впливає, з одного боку, на ступінь стиснення зображень (об'єм інформаційної складової КСП). З другого боку, він впливає на вихідні статистичні характеристики криптосемантичного представлення і на рівень конфіденційності загалом. Тому в працях [13, 14] було запропоновано метод КСП зображень на основі плаваючої схеми в базисі по верхніх межах. Службова складова КСП будується з максимальних значень початкових елементів фрагмента зображення по рядках, а в повнокольорових реалістичних зображеннях максимальні значення прагнуть до верхньої межі динамічного діапазону. Це призводить до того, що кількість елементів, що беруть участь у формуванні інформаційної складової КСП, значно не збільшується, а отже, об'єм КСП зображення так само значно не зменшився порівняно із статичною схемою побудови КСП. Тому для усунення даних недоліків пропонується знизити значення динамічного діапазону початкових елементів фрагмента зображення.

Мета статті (постановка завдання)

Розробка методу кодування зображень на основі плаваючої схеми поліадиченого кодування в диференціальному базисі, що забезпечує формування кодограм рівномірної довжини на основі змінної (заздалегідь невизначеної) кількості елементів початкового зображення, що представлені в пониженому динамічному діапазоні.

Виклад основного матеріалу

Кріптосемантичному перетворенню піддаються не все зображення цілком, а тільки його локальні фрагменти. При цьому початкове зображення розбивається на локальні фрагменти розмірністю $m \times n$, де m — кількість рядків фрагмента зображення, а n — кількість стовпців. На практиці дуже часто зображення розбивають на квадратні фрагменти, тобто кількість рядків у таких фрагментів зображення дорівнює кількості стовпців $m = n$.

Фрагмент зображення в початковому вигляді є двовимірною матрицею $A = \{a_{i,j}\}$, $i = \overline{1,m}$, $j = \overline{1,n}$, яка розглядається як двовимірне полиадичне число.

У процесі криптосемантичного представлення зображення формуються кодові комбінації, що складаються з інформаційної та службової складових.

На першому етапі КСП формується службова складова для перетворюваного фрагмента відеоданих, яка є ключовим елементом при формуванні інформаційної складової.

На другому етапі з урахуванням службової складової формуються значення коду інформаційної складової.

На третьому етапі, після формування всіх службових складових, для забезпечення конфіденційності передачі ключових елементів, службові складові КСП піддаються криптографічному перетворенню на майстер-ключі при їх зберіганні або на сеансовому ключі при їх передачі по каналах зв'язку.

Службова складова (система службових даних) КСП зображення на основі системи поліадичного кодування формується для кожного локального фрагменту зображення залежно від вибраної системи базисів криптосемантичного перетворення і складається з:

— системи підстав $G=\{g_i\}$ (де $i=\overline{1,m}$ або $\mathrm{i}=\overline{1,\mathrm{n}}$), елементи якої є максимальними значеннями елементів фрагмента зображення, що оброблюються по рядках і/або стовпцях, збільшені на 1 і використовуються для визначення динамічного діапазону локального фрагмента зображення;

— системи нормуючих значень $Z=\{z_i\}$ (де $i=\overline{1,m}$ або $i=\overline{1,n}$), елементи якої є мінімальними значеннями елементів фрагмента зображення, що оброблюються по рядках і/або стовпцях, і використовуються, як знижуючи значення динамічного діапазону локального фрагмента зображення і системи підстав.

Побудова КСП зображення здійснюється за інтегральним принципом у три етапи.

Етап 1. У результаті згортки значень елементів початкового фрагмента $\grave{A}$ і системи службових даних S на основі правила $f(\bullet)$ забезпечується формування значення інформаційної складової КСП N, що містить інформацію відразу про декілька елементів початкового фрагмента $\grave{A}$:

$$N=f(A;S). \qquad (1)$$

Етап 2. Система службових даних S піддається криптографічному перетворенню $E(\bullet)$ на ключі перетворення K:

$$S_c=E_K(S), \qquad (2)$$

де S_c — система службових даних в зашифрованому вигляді.

Етап 3. Для значень N і S_c забезпечується побудова кодограми криптосемантичного представлення зображення $\tilde{N}$:

$$\tilde{N}=\varphi_{\tilde{n}}(N;S_c), \qquad (3)$$

де $\varphi_c(\bullet)$ — оператор, що забезпечує виділення кількості розрядів для величини N з використанням інформації про службові дані S'.

У процесі відновлення криптосемантичного представлення зображення використовується зворотне криптографічне перетворення $D(\bullet)$ на ключі перетворення K:

$$S^{\bullet}=D_K(S_c). \qquad (4)$$

Якщо для виконання прямого та зворотного криптографічних перетворень використовувався автентичний ключ перетворення (один і той самий сеансовий ключ для симетричних систем або секретний і відповідний йому відкритий ключ перетворення для асиметричних систем шифрування), а так само зашифровані дані S_c не піддавалися навмисній або помилковій модифікації, то розшифровані дані $S^{\bullet}$ будуть ідентичні початковим службовим складовим КСП S біт в біт, тобто $S^{\bullet}=S$, а вираз (2) прийме вигляд:

$$S=D_K(S_c), \text{ тобто } S=D_K(E_K(S)). \qquad (5)$$

Розглянемо процес побудови криптосемантичного представлення зображень на основі плаваючої схеми системи поліадичного кодування в диференціальному базисі.

Для цього фрагмент зображення з двовимірної матриці $A=\{a_{i,j}\}$ перетворюється в одновимірний вектор

$$A=\{a_{i,j}\}=\{a_\tau\}_{\tau=\overline{1,mn}}=\{a_{m(j-1)+i}\},$$
$$i=\overline{1,m},\ j=\overline{1,n}. \qquad (6)$$

Службова складова КСП зображення на основі системи поліадичного кодування в диференціальному базисі складається з підстав (максимальних значень динамічного діапазону) і знижуючих (мінімальних) значень динамічного діапазону.

На попередньому етапі визначається система підстав $G^{(m)}=\{g_i\}$, $i=\overline{1,m}$, початкового фрагмента зображення по рядках. Підстава елементів *i*-го рядка g_i визначається, як максимальний елемент рядка початкового масиву збільшений на 1:

$$g_i=\max_{1\le j\le n}(a_{i,j})+1=\max_{1\le j\le n}(a_{m(j-1)+i})+1. \qquad (7)$$

Для зниження динамічного діапазону елементів $a_{i,j}$ початкового фрагмента зображення в рядках масиву відеоданих визначають мінімальні значення z_i за формулою

$$z_i=\min_{1\le j\le n}(a_{i,j})=\min_{1\le j\le n}(a_{m(j-1)+i}). \qquad (8)$$

Для зручності проведення розрахунків і для визначення відповідності елементів фрагмента зображення з підставами пропонується розширити систему підстав до потужності початкового фрагмента зображення в одномірному векторному вигляді. Для цього використовують формули

$$S^{(m\times n)}=\{s_\tau\}=\{g_{\tau-m\left[\frac{\tau-1}{m}\right]}\},\ \tau=\overline{1,mn}, \qquad (9)$$

$$R^{(m\times n)}=\{r_\tau\}=\{z_{\tau-m\left[\frac{\tau-1}{m}\right]}\},\ \tau=\overline{1,mn}. \qquad (10)$$

де $S^{(m\times n)}$ — система підстав початкового фрагмента зображення в одновимірному векторному вигляді розмірністю $m\times n$; $R^{(m\times n)}$ — система знижувальних значень елементів початкового фрагмента зображення в одновимірному векторному вигляді розмірністю $m\times n$.

Зниження динамічних діапазонів елементів a_τ зображення задається виразом

$$u_\tau=a_\tau-r_\tau,\ \tau=\overline{1,mn}, \qquad (11)$$

де u_τ — τ-й елемент масиву відеоданих, представлений в одновимірному векторному вигляді із зниженим динамічним діапазоном.

У цьому випадку нерівномірність зменшення діапазону забезпечується за рахунок нерівномірності розподілу значень елементів зображення в масиві. Представлення даних у поліадичній системі при нерівномірному зниженні динамічного діапазону даних організовується на основі таких етапів:

1. Формується обмеження на динамічний діапазон системи підстав з урахуванням його зменшення для всіх елементів

$$p_\tau = s_\tau - r_\tau,\ \tau = \overline{1,mn}, \qquad (12)$$

де p_τ — величина динамічного діапазону елементів одновимірного вектора відеоданих після вирахування мінімального значення.

2. Обчислення вагового коефіцієнту H_τ для τ-го елементу одновимірного вектора відеоданих, яке задається виразом:

$$H_\tau = \prod_{\xi=\tau+1}^{mn} p_\xi = \prod_{\xi=\tau+1}^{mn} (s_\xi - r_\xi),\ \tau = \overline{1,mn}. \qquad (13)$$

3. Формування значення інформаційної складової N описується виразом:

$$N = \sum_{\tau=1}^{mn} u_\tau H_\tau. \qquad (14)$$

З урахуванням співвідношень (11), (12) і (13) вираз (14) прийме вигляд

$$N = \sum_{\tau=1}^{mn} \left\langle (a_\tau - r_\tau) \prod_{\xi=\tau+1}^{mn} (s_\xi - r_\xi) \right\rangle =$$

$$\sum_{\tau=1}^{mn} \left\langle (a_\tau - z_{\tau - m\left[\frac{\tau-1}{m}\right]}) \prod_{\xi=\tau+1}^{mn} (g_{\xi - m\left[\frac{\xi-1}{m}\right]} - z_{\xi - m\left[\frac{\xi-1}{m}\right]}) \right\rangle. \qquad (15)$$

Для контролю переповнювання кодового слова при формуванні інформаційної частини КСП N введемо додаткову величину, рівну накопиченому добутку підстав з урахуванням пониження їх динамічного діапазону для Q елементів, що беруть участь у формуванні коду, яка визначається за формулою

$$L_Q = \prod_{\xi=1}^{Q} p_\xi = \prod_{\xi=1}^{Q} (s_\xi - r_\xi) = \prod_{\xi=1}^{Q} \left(\mathbf{g}_{\xi - m\left[\frac{\xi-1}{m}\right]} - z_{\tau - m\left[\frac{\tau-1}{m}\right]} \right). \qquad (16)$$

Переповнювання кодового слова не станеться, якщо виконується нерівність

$$L_Q \le 2^M - 1, \qquad (17)$$

де $2^M - 1$ — найбільше число, яке може зберігатися в кодовому слові довжиною M елементів (біт).

Максимальна кількість елементів, що беруть участь у формуванні коду, визначається як значення аргументу, за якого величина L_Q сягає максимуму за умови виконання нерівності (17) і розраховується за формулою

$$Q_{\text{пр}} = \arg\max_Q (L_Q) = \arg\max_Q \left(\prod_{\xi=1}^{Q} p_\xi \right) = \arg\max_Q \left(\prod_{\xi=1}^{Q} (s_\xi - r_\xi) \right) = \arg\max_Q \left(\prod_{\xi=1}^{Q} (\mathbf{g}_{\xi - m\left[\frac{\xi-1}{m}\right]} - z_{\tau - m\left[\frac{\tau-1}{m}\right]}) \right). \qquad (18)$$

З урахуванням співвідношення (18) вирази (14) і (13) для визначення інформаційної складової КСП наберуть вигляду

$$N = \sum_{\tau=1}^{Q_{np}} u_\tau H_\tau = \sum_{\tau=1}^{Q_{np}} (a_\tau - r_\tau) H_\tau; \qquad (19)$$

$$H_\tau = \begin{cases} \prod_{\xi=\tau+1}^{Q_{np}} p_\xi = \prod_{\xi=\tau+1}^{Q_{np}} (s_\xi - r_\xi), & \tau < Q_{np} < mn; \\ 1, & \tau = Q_{np} \le mn. \end{cases} \qquad (20)$$

Інформаційна складова КСП зображень на основі плаваючої схеми системи поліадичного кодування в диференціальному базисі формується в три етапи, так, що:

1. На першому етапі (попередньому для виконання КСП зображення, що полягає в підготовці початкових даних і визначенні службових складових):

— початкове зображення розбивається на фрагменти розмірністю $m \times n$, де m — кількість рядків фрагмента зображення, а n — кількість стовпців;

— визначається службова складова КСП, що складається з системи підстав $G^{(m)} = \{g_i\}$ початкового фрагмента зображення на основі виразу (7) і системи знижувальних (мінімальних) значень динамічного діапазону $Z^{(m)} = \{z_i\}$ на основі виразу (8);

— перетворюється початковий фрагмент зображення на основі виразу (6) з двовимірної матриці $A = \{a_{i,j}\}$, $i = \overline{1,m}$, $j = \overline{1,n}$ в одновимірний вектор $A = \{a_\tau\}$ — полиадичне число;

— розширюється система підстав $G^{(m)} = \{g_i\}$ до потужності початкового фрагмента зображення в одновимірному векторному вигляді $S^{(m \times n)} = \{s_\tau\}$ на основі виразу (9);

— розширюється система знижувальних значень динамічного діапазону $Z^{(m)} = \{z_i\}$ до потужності початкового фрагмента зображення в

одновимірному векторному вигляді $R^{(m\times n)} = \{r_\tau\}$ на основі виразу (10);

— знижується динамічний діапазон поліадичного числа і елементів розширеної системи підстав на основі виразів (11) і (12) відповідно.

2. На другому етапі розраховується максимальна кількість елементів Q_{np} поліадичного числа, що беруть участь у формуванні інформаційної складової схеми кодування в диференціальному базисі, із співвідношення

$$Q_{np} = \arg\max_{Q}\left(\prod_{\xi=1}^{Q} p_\xi\right) = \arg\max_{Q}\left(\prod_{\xi=1}^{Q}(s_\xi - r_\xi)\right), \quad (21)$$

якщо

$$\prod_{\xi=1}^{Q} p_\xi = \prod_{\xi=1}^{Q}(s_\xi - r_\xi) \le 2^M - 1. \quad (22)$$

3. На третьому етапі безпосередньо формується інформаційна складова КСП на основі виразів (19) і (20). Значення коду є інтегрованим, і формується з урахуванням службових даних по оператору $f(A; G)$, де:

$$f(A;G) = N = \sum_{\tau=1}^{Q_{np}} u_\tau H_\tau = \sum_{\tau=1}^{Q_{np}} u_\tau \prod_{\xi=\tau+1}^{Q_{np}} p_\xi = \\ = \sum_{\tau=1}^{Q_{np}} (a_\tau - r_\tau) \prod_{\xi=\tau+1}^{Q_{np}} (s_\xi - r_\xi). \quad (23)$$

Висновки

Розроблений метод криптосемантичного представлення зображень на основі плаваючої схеми поліадичного кодування в диференційованому базисі забезпечує:

— одночасне виконання процесів компресії і кодування (шифрування) відеоданих;

— виключення надмірності одночасно без внесення погрішності;

— значне зменшення кількості незначущих елементів (незначущих нульових біт) на початку кожної бітової послідовності кодів КСП;

— формування кодограм рівномірної довжини на основі змінної (заздалегідь невизначеної) кількості елементів початкового зображення;

— додаткове зниження вихідного об'єму зображень в кодованому вигляді.

При цьому формування інформаційної складової КСП зображень організовується:

— не на системі підстав, а на їх представленні в зниженому динамічному діапазоні;

— не на початкових значеннях елементів зображення, а на їх представленні з урахуванням обмежень на динамічний діапазон.

Перспективи подальших досліджень

У свою чергу, потребує подальшій розвиток запропонованої технології в напрямку побудови рекурентної схеми формування інформаційної складової на основі плаваючої схеми поліадичного кодування в диференціальному базисі та методів декодування криптосемантічного представлення.

ЛІТЕРАТУРА

1. **Соколан Т. С.** Адміністративно-правове регулювання застосування відеоспостереження правоохоронними органами України / Тетяна Сергіївна Соколан // Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07. — Київ : Київський національний університет імені Тараса Шевченка. — 2016. — 210 с.

2. **Resolution** of PACE 1604 (2008) "Video surveillance of public areas" [Електронний ресурс]. — Режим доступу: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17633&lang=en.

3. **Володин А. А.** Обработка видео в системах телевизионного наблюдения / А. А. Володин, В. Г. Митько, Е. Н. Спинко // Вопросы защиты информации. — 2002. — № 4 (59). — С. 34–47.

4. **Visual** cryptography / M. Naor and A. Shamir // In EUROCRYPT'94. — Springer-Verlag Berlin, 1995 [Електронний ресурс]. — Режим доступу: http://www.fe.infn.it/u/filimanto/scienza/webkrypto/visualdecryption.pdf.

5. **Shamir A.** How to share a secret / A. Shamir // Communications of the ACM. — N.Y.: ACM Press, 1979. —Vol. 22. — P. 612–613.

6. **Gobby C.** Quantum key distribution over 122 km of standard telecom fiber / C. Gobby, Z. L. Yuan, A. J. Shields // Applied Physics Letters. — N.Y.: American Institute of Physics, 2004. — V. 84, № 19. — P. 3762-3764.

7. **International** Standards Organization 1984. «OSI-Basic Reference Model», ISO 7498, International Standards Organization, Geneva.

8. **Barannik V.** Methodology compression of videoinformation in the cryptographic systems / V. Barannik, S. Sidchenko, V. Larin // Science-based technologies. — 2011. — Vol. 11. No. 3–4, doi.org/10.18372/2310-5461.11.5260 (eng).

9. **Баранник В. В.** Синтез комбинированных криптокомпрессионных систем для обеспечения безопасности видеоинформации в инфокоммуникациях / В. В. Баранник, С. А. Сидченко, И. М. Тупица // Автоматизированные системы управления и приборы автоматики. — Х.: ХНУРЭ. — 2014. — Вып. 169. — С. 39–44.

10. **Баранник В. В.** Методология позиционирования полиадических кодовых конструкций на основе классифицирующих признаков в системе криптокомпрессионного представления / В. В. Баранник, С. А. Сидченко, И. М. Тупица, Н. А. Королева// Інформаційно-керуючі системи на залізнично-

му транспорті. — 2015. — № 4. — С. 56–60, doi.org/10.18664/ikszt.v0i4.53977 (rus).

11. **Баранник В. В.** Метод дешифрируемостойкого представления изображений / В. В. Баранник, С. А. Сидченко, В. В. Ларин // Сучасна спеціальна техніка. — 2011. — №1 (24). — С. 24–29.

12. **Barannik V. V.** The Decoded-proof Presentation of Images on the Basis of the Polyadycal Encoding Systems / V. V. Barannik, S. A. Sidchenko, V. V. Larin // XIth International Conference CADSM 2011, The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv-Polyana, Ukraine, Lviv Polytechnic National University, February 23 — 25, 2011. — P. 182.

13. **Сидченко С. А.** Способ представления изображений стойких к дешифрированию на основе плавающей схемы кодирования / С. А. Сидченко // Системи озброєння і військова техніка. — 2011. — Вип. 3 (27). — С. 68–70.

14. **Баранник В. В.** Метод криптосемантического представления изображений на основе плавающей схемы в базисе по верхним границам / В. В. Баранник, С. А. Сидченко, И. М. Тупица // Радиоэлектроника и информатика. — 2015. — № 4. — С. 9–12.

Сідченко С. О., Бараннік Д. В.

МЕТОД КРИПТОСЕМАНТИЧНОГО ПРЕДСТАВЛЕННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ПЛАВАЮЧОЇ СХЕМИ СИСТЕМИ ПОЛІАДИЧНОГО КОДУВАННЯ В ДИФЕРЕНЦІАЛЬНОМУ БАЗИСІ

У статті наголошено про необхідність кодування (шифрування) даних відеоспостереження, у тому числі і в суспільних місцях, тому що ці данні можуть бути віднесені до персональних (конфіденційних) та можуть використовуватися у кримінальних розслідуваннях. Розглянуті основні особливості побудови кріптосемантичного представлення (КСП) зображення. Розроблено метод КСП зображень на основі плаваючої схеми поліадичного кодування в диференційованому базисі, який забезпечує конфіденційність і оперативність доставки відеоінформаційного ресурсу за умови збереження його цілісності. Основними характеристиками розробленого методу є: одночасне виконання процесів компресії і кодування (шифрування) відеоданих; виключення надмірності одночасно без внесення погрішності; значне зменшення кількості незначущих елементів (незначущих нульових біт) на початку кожної бітової послідовності кодів КСП; формування кодограм рівномірної довжини на основі змінної (заздалегідь невизначеної) кількості елементів початкового зображення; додаткове зниження вихідного об'єму зображень в кодованому вигляді. При цьому формування інформаційної складової КСП зображень організовується: не на системі підстав, а на їх представленні в зниженому динамічному діапазоні; не на значеннях елементів зображення, а на їх представленні з урахуванням обмежень на динамічний діапазон.

Ключові слова: криптосемантичне представлення зображень; захист інформації; шифрування; кодування; компресія зображення; поліадичний код; плаваюча схема; диференційований базис.

Sidchenko S. A., Barannik D.V.

THE METHOD OF CRYPTOSEMANTIC PRESENTATION OF IMAGES BASED ON THE FLOATING SCHEME OF THE POLYADICAL CODING SYSTEM IN THE DIFFERENTIAL BASIS

In the article noted the need for encoding (encryption) of video surveillance data, including in public places, because these data can be classified as personal (confidential) and can be used in criminal investigations. The main features of the construction of the cryptosemantic presentation of image are considered. A method for cryptosemantic presentation of images based on the floating scheme of polyadical coding in a differentiated basis is developed, which ensures the confidentiality and speed of delivery of the video information resource provided its integrity is preserved. The main characteristics of the developed method is: simultaneous execution of compression and encoding (encryption) of video data; elimination of redundancy at the same time without introducing an error; significant reduction in the number of insignificant elements (insignificant zero bits) at the beginning of each bit sequence of codes of the cryptosemantic presentation; the formation of uniform-length codograms based on the variable (previously undefined) number of elements of the original image; an additional reduction in the initial amount of images in coded form. At the same time, the formation of the information component of the cryptosemantic presentation of images is organized: not on the basis system, but on their presentation in a reduced dynamic range; not on the original values of the image elements, but on their presentation, taking into account the limitations on the dynamic range.

Keywords: cryptosemantic presentation of images; data protection; encryption; coding; image compression; polyadical code; floating scheme; differentiated basis.

Сидченко С. А., Баранник Д. В.

МЕТОД КРИПТОСЕМАНТИЧЕСКОГО ПРЕДСТАВЛЕНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ПЛАВАЮЩЕЙ СХЕМЫ СИСТЕМЫ ПОЛИАДИЧЕСКОГО КОДИРОВАНИЯ В ДИФФЕРЕНЦИАЛЬНОМ БАЗИСЕ

В статье отмечено про необходимость кодирования (шифрования) данных видеонаблюдения, в том числе и в общественных местах, потому что эти данные могут быть отнесены к персональным (конфиденциальным) и могут использоваться в уголовных расследованиях. Разработан метод КСП изображений на основе плавающей схемы полиадического кодирования в дифференцированном базисе, обеспечивающий конфиденциальность и оперативность доставки видеоинформационного ресурса при условии сохранения его целостности. Основными характеристиками разработанного метода является: одновременное выполнение процессов компрессии и кодирования (шифрования) видеоданных; исключение избыточности одновременно без внесения погрешности; значительное уменьшение количества незначащих элементов (незначимых нулевых бит) в начале каждой битовой последовательности кодов КСП; формирование кодограмм равномерной длины на основе переменного (предварительно неопределенного) количества элементов исходного изображения; дополнительное снижение исходного объема изображений в кодированном виде. При этом формирование информационной составляющей КСП изображений организуется: не на системе оснований, а на их представлении в пониженном динамическом диапазоне; не на исходных значениях элементов изображения, а на их представлении с учетом ограничений на динамический диапазон.

Ключевые слова: криптосемантическое представление изображений; защита информации; шифрование; кодирование; компрессия изображения; полиадический код; плавающая схема; дифференцированный базис.

Стаття надійшла до редакції 15.02.2017 р.
Прийнято до друку 18.02.2017 р.
Рецензент — д-р техн. наук, проф. О. К. Юдін