УДК 621.327:681.5

МЕТОДОЛОГІЧНІ ОСНОВИ КРИПТОСЕМАНТИЧНОГО ПРЕДСТАВЛЕННЯ ВІДЕОЗОБРАЖЕНЬ В ІНФОРМАЦІЙНИХ КОМУНІКАЦІЯХ

В. В. Бараннік, д-р техн. наук, проф.,
Науковий центр Харківського університету повітряних сил імені Івана Кожедуба

С. О. Сідченко, канд. техн. наук, старш. наук. співроб.
Науковий центр Харківського університету повітряних сил імені Івана Кожедуба

В. В. Ларін, канд. техн. наук, старш. інж.
Науковий центр Харківського університету повітряних сил імені Івана Кожедуба

Запропоновано основні компоненти розробки методологічних основ криптосемантичного представлення видових зображень. Наведено базові визначення криптосемантики, криптосемантичної стійкості. Охарактеризовано основні напрями науково-прикладних досліджень, що проводяться в даній галузі знань. Сформульовано базові складові побудови криптосемантичного представлення відеоданих.

Ключові слова: криптосемантичне представлення зображень.

The basic components of methodological bases development of cryptosemantic presentation of specific images are expounded. Base determinations over of cryptosemantics, cryptosemantic firmness are brought. Basic directions of the scientifically-applied researches conducted in this region of knowledges are given. The base constituents of cryptosemantic presentation construction of videoinformation are formed.

Keywords: cryptosemantic presentation of images.

Вступ

Розвиток технологій представлення відеоінформаційного забезпечення і його інтеграція в різні сфери діяльності суспільства виводить таку складову, як ресурс відеоінформації, на новий рівень значущості [1].

У зв'язку з цим стає актуальним питання про організацію безпеки відеоінформації. Водночас, як запропоновано в працях [2—4] існуючі інформаційні технології не справляються із збільшеними обсягами відеоданих щодо її своєчасної доставки, захисту в умовах забезпечення гарантованої цілісності інформації. Тому актуальними є напрями розвитку технологій захисту відеоінформації з використанням методів цифрової обробки зображень.

Основний матеріал

Для підвищення ефективності захисту відеоінформації, що доводиться у реальному часі, можливі два напрями, а саме:

1. Проводити модифікацію існуючих технологій компресії і криптографічних перетворень з позиції їх послідовного використання.

2. Розробити принципово новий підхід, що полягає у створенні технологій, що одночасно забезпечують підвищення оперативності доведення і захист відеоінформації на основі методів семантичної і синтаксичної обробки зображень.

Розглянемо **перший напрям**. Тут можливі два варіанти.

Перший варіант полягає в зниженні обчислювальної складності технологій обробки даних. Водночас використання криптографічних алгоритмів, що мають меншу обчислювальну складність, пов'язано зі зниженням ефективності захисту відеоінформації: вилучення етапу накладення гамми; скорочення довжини ключа; зменшення кількості раундів процесу шифрування (складання з ключовою послідовністю); використання менш складних алгоритмів шифрування.

Зниження обчислювальної складності для алгоритмів компресії досягається за рахунок: або збільшення ступеня спотворень, або різкого зниження коефіцієнта стиснення.

Спотворення на відновлених після стиснення з втратами зображень виявляються у вигляді: розмиття дрібних об'єктів аж до їх повного зникнення; ефекту блоковості; виникнення ефекту «снігу» — різка зміна кольору в окремих крапках; ефекту Гіббса, що виявляється у вигляді утворення своєрідного «німба» (ореолу) навколо контурів з різкими переходами кольорів (викликається втратами у високочастотних складових); муарів (розмиття чітких ліній; слабких смуг за напрямом розгортки.

При цьому за відсутності універсальної кількісної оцінки ступеня важливості інформації та універсальних методів визначення класу зображень, втрати якості можуть призвести до втрати важливої інформації.

Використовувані статистичні оцінки похибки відновлених зображень не є точними.

Існують типи похибок, які за критерієм середньоквадратичної похибки будуть визнані неістотними. Це значить, що такий шлях веде до втрати достовірності і підвищення часу доведення інформації.

Другий варіант, навпаки, пов'язаний з підвищенням складності технологічного процесу обробки даних. Проте в умовах обмеженої обчислювальної продуктивності це сприятиме зниженню оперативності обробки даних, підвищенню енергетичних витрат на організацію обчислювального процесу і до різкого подорожчання самих засобів дистанційного формування і збору видових зображень. Наприклад, наразі вартість одного безпілотника з бортовим устаткуванням може досягати $ 15 млн.

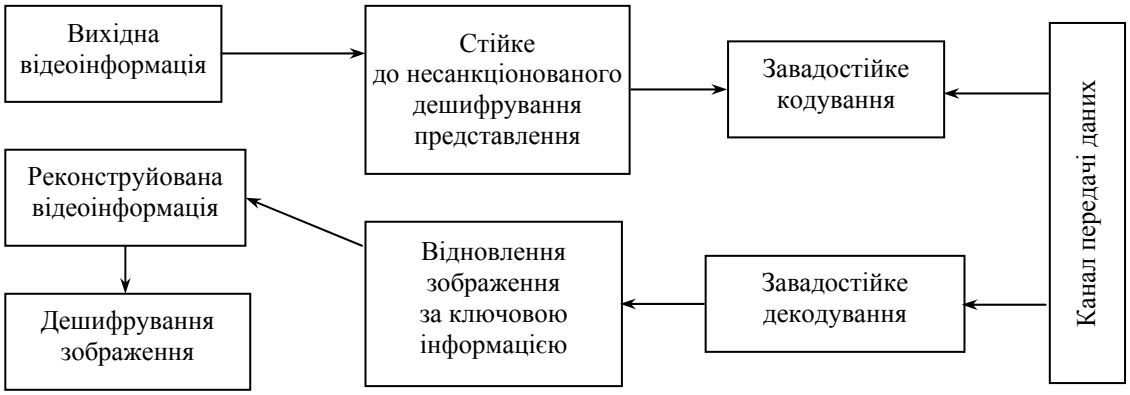
Загальним важливим недоліком для першого напряму є неузгодженість між фірмами-виробниками бортового устаткування або устаткування наземних точок доступу і фірмами-розробниками технологій захисту даних, що викликано, в першу чергу, патентними обмеженнями і конкурентними комерційними інтересами. Як правило, системи стиснення і захисту інформації розробляються і проводяться різними компаніями. Це призводить до невідповідності стандартів стиснення і криптографічного перетворення.

Для України характерним недоліком є і те, що використовуються здебільшого західні технології як для компресії зображень, так і для шифрування інформації в бездротових інформаційних комунікаційних технологіях.

Треба відзначити, що графічні формати містять у собі не тільки файл стислого зображення, але й службову частину.

Саме бітові поля службової складової графічних форматів використовують для стеганографічного вбудовування інформації. Тому інтегруючи в комплекс обробки відеоінформації технології компресії західного виробництва, немає упевненості, що там відсутні закладки, що дають змогу надати додаткову інформацію для криптоаналізу.

Другий напрям підвищення захисту оперативної відеоінформації полягає у створенні систем інформаційної скритності шляхом побудови методів стійких до несанкціонованого дешифрування (розпізнавання) зображень на базі систем їх цифрової обробки (див. рисунок).



Структурно-функціональна схема захисту зображень на основі СНД представлення

Під дешифруванням мається на увазі процес розпізнавання об'єктів, їх властивостей і взаємозв'язків за їх зображенням на знімку.

Під дешифруванням видових зображень розуміється процес ідентифікації, ототожнення і розпізнавання семантичного змісту зображень.

Іншими словами, дешифрування — це отримання інформації про об'єкти і сцени реального світу, яке було зафіксоване, зареєстроване і перенесене за допомогою сформованого зображення (візуальної моделі реальних образів і сцен).

Відповідно властивості (характеристики) об'єктів, що знайшли віддзеркалення на знімку і використовувані для розпізнавання, називаються *дешифрувальними ознаками* [1; 2].

Зображення можна розглядати як носій деякої важливої інформації (дешифрувальних ознак). Як джерело інформації зображення має свої кількісну і якісну сторони поняття невизначеності. Зображення I можна представити як об'єкт, що описується двома складовими

$$I = \{I_{\text{син}}; I_{\text{сем}}\},$$

де $I_{\text{син}}$, $I_{\text{сем}}$ — синтаксичні і семантичні складові зображення відповідно.

Синтаксична складова характеризується кількісною стороною поняття інформації.

Кількісна сторона інформації оцінює ступінь невизначеності за кількісними ознаками.

Синтаксична складова формується з урахуванням особливостей представлення зображення в цифровому вигляді.

Найвідомішими базовими кількісними заходами для оцінки ступеня невизначеності цифрового опису зображення є міри Хартлі і Шеннона.

Кількість $|I_{\text{син}}|$ інформації в зображенні в загальному випадку визначається як

$$|I_{\text{син}}| = F(P_{\text{син}}),$$

де $F(P_{\text{син}})$ — функціонал, який залежить від набору $P_{\text{син}}$ кількісних ознак зображень, властивих генеруючому їх джерелу.

Ступінь невизначеності через функціонал $F(P_{\text{син}})$ оцінюється як кількість можливих зображень (станів зображення) для джерела з характеристиками, що задаються множиною $P_{\text{син}}$.

Набір $P_{\text{син}}$ кількісних ознак може задаватися шляхом переліку характеристик або на основі деякого операторного опису. Кількісні ознаки використовуються для опису статистичних, структурних, частотних, просторових, яскравості і психовізуальної закономірностей зображень.

У сучасній теорії інформації найчастіше кількість інформації вимірюється в бітах (двійкових розрядах). Для цього використовується логарифмічне перетворення за підставою два, тобто

$$V(I_{\text{син}}) = \log_2 F(P_{\text{син}}), \text{ біт.}$$

Якісна сторона відповідає за смисловий (семантичний) зміст зображення. Зрештою інтерес викликає саме смислова, (семантична) складова зображення. Зрозуміло, що інтерес викликає смислова інформація, що міститься в зображенні, яка використовується для вторинної і третинної обробки, зокрема з метою ухвалення рішень. Звідси виникає необхідність утаєння від несанкціонованого доступу саме семантичної сторони зображення.

Семантична складова зображення в загальному випадку характеризується такими компонентами: архітектура контурів, деталювання об'єктів, забарвлення і яскравість когерентних областей (фонових областей), зв'язність об'єктів між собою і їх прив'язка до областей сцени зображення.

Розробка універсальних заходів для оцінювання якісної сторони поняття інформації на сьогодні є відкритим питанням науково-прикладних досліджень. Це ускладнює розвиток методів семантичної обробки зображень і обмежує коло їх прикладного застосування.

Далі наведемо кількісну і якісну складову зображення стосовно його фрагментів $A_{\text{син}}$ та $A_{\text{сем}}$, що задається співвідношеннями

$$I_{\text{син}} = \sum_{\xi=1}^{\nu_{\text{фр}}} A_{\text{син},\xi} \text{ та } I_{\text{сем}} = \bigcup_{\xi=1}^{\nu_{\text{фр}}} A_{\text{сем},\xi},$$

де $\nu_{\text{фр}}$ — кількість непересічних фрагментів, на які розкладається зображення.

В окремому випадку, коли $\nu_{\text{фр}} = 1$ оброблення і аналіз синтаксичної і семантичної складових здійснюється для всього зображення.

Для забезпечення утаєння семантичної інформації, що міститься в зображеннях, пропонується створювати стійке до несанкціонованого дешифрування (СНД) представлення зображень [3; 4]. Таке утаєння може досягатися за рахунок руйнування семантичного змісту зображення, тобто криптографування смислового змісту зображення.

Математично це можна подати таким чином: фрагмент зображення на синтаксичному рівні опису $A_{\text{син}}$ повинен мати такий формат уявлення $N(A_{\text{син}})$

$$N(A_{\text{син}}) = f_{\text{ск}}(A_{\text{син}}),$$

для якого виконуватиметься умова:

$$A_{\text{сем}} \cap N(A_{\text{сем}}) \to \varnothing, \qquad (1)$$

де $A_{\text{сем}}$ — семантична складова відкритого (початкового) фрагмента зображення; $N(A_{\text{сем}})$ — семантичний опис початкового фрагмента A, одержане в результаті перетворення $f_{\text{ск}}(A_{\text{син}})$ відповідного фрагмента на синтаксичному рівні; $f_{\text{ск}}(A_{\text{син}})$ — функціонал перетворення початкового (відкритого) синтаксичного опису фрагмента зображення до формату $N(A_{\text{син}})$, для семантичної складової якого виконуватиметься умова (1).

Умова (1) може бути виражена через вірогідність $P(A_{\text{сем}})_{\text{дш}}$ правильного дешифрування семантичної складової $A_{\text{сем}}$ відкритого фрагмента. В даному випадку повинна виконуватися умова

$$P(A_{\text{сем}}; N(A_{\text{сем}}))_{\text{дш}} \to 0, \qquad (2)$$

тобто вірогідність правильного дешифрування семантичного змісту відкритого фрагмента $A_{\text{сем}}$ за семантичною складовою $N(A_{\text{сем}})$, одержаної в результаті перетворення $f_{\text{ск}}(A_{\text{син}})$ повинно прагнути до нуля.

Зрозуміло, що $P(A_{\text{сем}}; A_{\text{сем}})_{\text{дш}} = 1$, і навпаки, $P(A_{\text{сем}}; \varnothing)_{\text{дш}} = 0$, де $\varnothing$ — порожня множина, тобто відповідає варіанту відсутності будь-якої інформації, наприклад, фрагмент зображення, забарвлений у чорний колір.

Таким чином, вираз (2) задає умову, за якої досягається утаєння смислового змісту відкритого зображення.

Причому умова (2) повинна виконуватися навіть, якщо кількість інформації синтаксичного опису початкового фрагмента $V(A_{\text{син}})$ буде дорівнювати кількості інформації $V(N(A_{\text{син}}))$ син-

таксичного опису формату $N(A_{\text{син}})$, одержаного після прямого перетворення, тобто

$$V(A_{\text{син}}) = V(N(A_{\text{син}})).$$

Окремий випадок, коли $N(A_{\text{сем}}) = \varnothing$, то $V(N(A_{\text{син}})) = 0$, тобто і на синтаксичному рівні кількість інформації може дорівнювати нулю, наприклад, коли наперед відомо, що в результаті перетворення $f_{\text{ск}}(A_{\text{син}})$ ми одержимо формат $N(A_{\text{син}})$ відповідний чорному квадрату. Проте в загальному випадку не завжди варіант $N(A_{\text{сем}}) = \varnothing$ приводить до $V(N(A_{\text{син}})) = 0$.

Наприклад, одержана у разі повного руйнування семантичного змісту картинка суцільного іскристого снігу не означає, що кількість інформації на синтаксичному рівні буде дорівнювати нульовому значенню.

Прихований опис зображення створює складнощі щодо встановлення того факту, що саме передається в зображенні.

Проте основна увага в процесі організації утаєння інформації повинна приділятися семантично важливим об'єктам. У цьому випадку не обов'язково забезпечити виконання умови $A_{\text{сем}} \bigcap N(A_{\text{сем}}) \to \varnothing$, тобто може бути $A_{\text{сем}} \bigcap N(A_{\text{сем}}) = \tilde{A}$, де $|\tilde{A}| > 0$. Але при цьому вірогідність дешифрування (розпізнавання) інформативних об'єктів $A_{\text{інф}}$ повинна дорівнювати нулю, $P(A_{\text{инф}}; N(A_{\text{сем}}))_{\text{дш}} = 0$.

Зображення, на відміну від інших видів інформації, є значно складнішою формою її передачі. Для створення систем з СНД зображень необхідно використовувати комплексні кодово-фільтрувальні перетворення, для яких досягається утаєння семантичного змісту переносника інформації.

Стійким до несанкціонованого дешифрування (СНД) зображень називається таке уявлення, яке забезпечує утаєння (маскування, руйнування) семантичного змісту зображень і формується на основі технологій їх цифрової обробки.

Стійке до несанкціонованого дешифрування представлення зображень (криптосемантичне уявлення) — це процес приховування смислового змісту зображення, і в першу чергу, значущих дешифрувальних ознак, з метою забезпечення конфіденційності відеоінформації, тобто запобігання вилученню семантичної інформації несанкціонованим користувачем.

На відміну від класичної криптографії для систем з СНД головним завданням є утаєння не синтаксичної структури зображення (кількісна сторона інформації), а його семантичного змісту (якісної сторони відеоінформації).

Звідси уявлення, стійке до несанкціонованого дешифрування, пропонується називати ***криптосеман-тичним*** (від грец. κρυπτός — прихований та σημαντική — сенс).

Криптосемантичним перетворенням зображень називається процес утаєння або семантичного маскування дешифрувальних ознак зображень для забезпечення гарантованої конфіденційності відеоінформації.

Термін «маскування» в теорії цифрової обробки зображень використовується в таких випадках: підкреслення і виділення контурів (детектування меж об'єктів); накладення камуфляжу під основний фон.

Тому пропонується використовувати термін семантичного маскування. Під *семантичним маскуванням* розуміється процес утаєння як дешифрувальних ознак, так і всього відеозображення в цілому.

Криптосемантика зображень — наука про методи і засоби забезпечення семантичного маскування зображень з метою утаєння їх змісту для гарантованої конфіденційності і цілісності.

Якщо для *криптографії* передбачається створення такого опису (шифру), для якого досягається утаєння самого тексту, (при цьому не важливо, яка саме інформація передається в повідомленні), то для *криптосемантики* передбачається створення таких маскувальних перетворень, які направлені на утаєння семантичного змісту повідомлення, наприклад текст, відео-, аудіо- або мова.

Обробка синтаксичного рівня проводиться залежно від семантичного змісту повідомлень. У цьому випадку, в першу чергу, для утаєння зображень становлять інтерес їх семантичний аспект, включаючи дешифрувальні ознаки. У такому разі під *інформативністю зображень* розуміється їх семантична складність.

Основними характеристиками криптосемантики є стійкість, обчислювальна складність, пропускна спроможність криптосемантичних каналів. На основі показника стійкості криптосемантичної системи оцінюється безпека її використання для захисту відеоінформаційних ресурсів.

Криптосемантичною стійкістю називається здатність системи приховувати від несанкціонованого користувача смисловий зміст зображень або їх значущі дешифрувальні ознаки, і протистояти спробам спотворення, реконструкції або їх заміни, а також здатність підтвердити або спростувати достовірність відеоінформації. Для зловмисника в криптосемантичних системах завдання відновити не бітове представлення початкового зображення (синтаксичний рівень опису),

а його семантичний сенс або значущі дешифрувальні ознаки. Додатково зловмисник використовуватиме методику візуального аналізу. Це додатковий механізм, який є у криптоаналітика в разі дешифрування прихованих зображень порівняно з класичною криптографією.

Теорія криптосемантики зображень — відносно новий теоретичний напрям теорії інформаційної боротьби, що формується на стику положень таких теорій, як: теорії інформації і кодування, криптографічного захисту інформації, дешифрування зображень, цифрової обробки зображень, включаючи фільтрацію, сегментацію, локалізацію об'єктів і контурів, розпізнавання об'єктів, стиснення зображень.

Тут визначаються об'єкти й елементи захисту відеоінформації; основні чинники, які впливають на зміст і ефективність захисту відеоінформації, а також визначає і вивчає погрози відеоінформації і методологічні основи її захисту, систему показників оцінки ефективності захисту відеоінформації, загальну математичну модель захисту відеоінформації, організаційно-технічні і правові основи захисту відеоінформації.

Як базові криптосемантичні перетворення можуть виступати технології на основі методів фільтрації, локалізації (виділення інформативних областей) і скорочення різних видів надмірності, зокрема компресії на рівні джерела генерування зображень.

Висновки

Показана необхідність забезпечення безпеки відеоінформаційних ресурсів з використанням технологій цифрової обробки зображень.

Розроблено методологічні основи криптосемантичного представлення видових зображень. Наведено базові визначення криптосемантики, криптосемантичної стійкості. Запропоновано основні напрями науково-прикладних досліджень, що проводяться в даній області знань. Сформульовано базові складові побудови криптосемантичного представлення відеоданих.

Література

1. *Кашкин В. Б.* Цифровая обработка аэрокосмических изображений: конспект лекций / В. Б. Кашкин. — Красноярск : ИПК СФУ, 2008. — 121 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. — К., 2009. — Вип. 4(19). — С. 24—30.

3. *Баранник В. В*. Метод криптосемантического представления изображений на основе комбинированного подхода / В. В. Баранник, С.А. Сидченко, В. В. Ларин // Сучасна спеціальна техніка. — К., 2010. — №3(22). — С. 33—38.

4. *Баранник В. В*. Метод дешифрируемостойкого представления изображений / В. В. Баранник, С. А. Сидченко, В. В. Ларин // Сучасна спеціальна техніка. — К., 2011. — № 1(24). — С. 22—28.

Стаття надійшла до редакції 04.06.2012.