УДК 519.81:621.372

А.А. Засядько, *sagitta@bigmir.net*
Черкаський університет банківської справи УБС НБУ, Черкаси, Україна

ЗНИЖЕННЯ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ЗА ДОПОМОГОЮ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМІЗАЦІЇ В ЗАДАЧІ НЕЛІНІЙНОГО ПРОГРАМУВАННЯ

При розв'язанні задачі нелінійного програмування (ЗНП) великої розмірності для планування об'єктів АСУ доводиться мати справу з проблемою багатоекстремальності цільової функції в області обмежень, або, іншими словами, "ефектом лабіринту" [1]. Щоб знайти глобальний екстремум цільової функції, необхідно за допомогою комбінаторного пошуку організувати повний перебір усіх екстремумів, що є обчислювально складною процедурою [1]. Багатокритеріальні методи оптимізації дозволяють ефективно вирішувати задачі досить широкого класу [2-4]. Особливе місце в цих методах займає нелінійна схема компромісів або згортка А.Н. Вороніна, уведена в [2, 3]. Відомо, що, на відміну від інших скалярних критеріїв, нелінійна схема компромісів дозволяє знайти оптимальний по Парето розв'язок, а у випадку опуклих частинних критеріїв – унімодальний (єдиний) розв'язок. Тому мета даної роботи – зменшити обчислювальну складність ЗНП за допомогою багатокритеріальної оптимізації на основі нелінійної схеми компромісів.

Представлення ЗНП більш складною багатокритеріальною задачею виправдане зниженням обчислювальної складності задач оптимального планування об'єктів АСУ високої розмірності, через регуляризацію некоректної задачі і зменшення її розмірності. Здійснюється редукція ЗНП великої розмірності в ЗНП меншої розмірності, яку можна розв'язувати звичайними оптимізаційними методами.

Список літератури

1. Черноруцкий И.Г. Оптимальный параметрический синтез. – Л.: Энергоатомиздат, 1987. – 126 с. 2. Векторная оптимизация динамических систем/А.Н.Воронин, Ю.К. Зиатдинов, О.И.Козлов, В.С. Чабанюк: Под ред. А.Н.Воронина. – К.: Техніка, 1999. – 284 с. 3. Воронин А. Н. Многокритериальный синтез динамических систем.—Киев: Наук.думка, 1992.—160 с. 4. Засядько А.А. Два этапа в методике гибкой адаптации в задачах многокритериальной оптимизации // Вісник ЧДТУ, 2002. - №. 2 – С.14 -17.

УДК 004:34

В.Г. Іванов,
М.Г. Любарський,
В.В. Карасюк,
Н.А. Кошева,
Ю.В. Ломоносов, *inform@nulau.edu.ua*
Національний університет «Юридична академія України ім. Ярослава Мудрого, Харків, Україна

СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ АВТОРСЬКИХ ПРАВ МУЛЬТИМЕДІЙНИХ ДАНИХ

Основним напрямом застосування комп'ютерної стеганографії для захисту від копіювання та несанкціонованого використання аудіо даних [1, 2] є використання надмірності аудіо і візуальної інформації. Цифровий звук – це ряд чисел, який представляє інтенсивність звукового сигналу в моменти часу, що послідовно йдуть. Всі ці числа не точні, оскільки не точні пристрої оцифрування аналогових сигналів, є шуми квантування. Молодші розряди цифрових відліків містять дуже мало корисної інформації про поточні параметри звуку і візуального образу. Їх заповнення відчутно не впливає на якість сприйняття, що і дає можливість для утаєння додаткової інформації

Вбудовування повідомлення в цифровий контейнер (зображення або аудіо-файл) може проводитися за допомогою ключа, одного або декількох. Ключ – псевдовипадкова послідовність (ПВП) біт, породжувана генератором, що задовольняє певним вимогам (криптографічний безпечний генератор). Як основа для роботи генератора може використовуватися, наприклад, лінійний рекурентний регістр. Тоді адресатам для забезпечення зв'язку може повідомлятися початкове заповнення цього регістра. Числа, що породжуються генератором ПВП, можуть визначати позиції відліків, що модифікуються, у разі фіксованого контейнера або інтервали між ними у разі потокового контейнера.

Популярність мультимедіа-технологій викликала безліч досліджень, пов'язаних з розробкою алгоритмів ЦВЗ для використання в стандартах MPEG, JPEG, захисту DVD-дисків від копіювання.

Всі алгоритми вбудовування прихованої інформації можна розділити на кілька підгруп:

• Ті, що працюють з самим цифровим сигналом. Наприклад, метод найменш значущих бітів (Least Significant Bit, LSB) [3].

• «Впаювання» прихованої інформації. В даному випадку відбувається накладення прихованого зображення (звуку, іноді тексту) поверх оригіналу. Часто використовується для вбудовування ЦВЗ [4].

• Використання особливостей форматів файлів. Сюди можна віднести запис інформації в метадані або в різні інші зарезервовані поля файлу, які не використовуються [5].

В даний час найбільш поширеним, але найменш стійким є метод заміни молодших значущих бітів (LSB). Молодший значущий біт зображення несе в собі найменше інформації, і людина зазвичай не здатна помітити зміну в цьому біті. Тому його можна використовувати для вбудовування інформації, і, наприклад,

для напівтонового зображення обсяг вбудованих даних може становити 1/8 обсягу контейнера. У зображення розміром 512 × 512 пікселів можна вбудувати 32 кілобайт інформації.

Незважаючи на переваги цього методу, які полягають в його простоті і порівняно великому обсязі вбудованих даних, він має серйозні недоліки. По-перше, зловмисникові точно відомо, де знаходиться місце розташування всього повідомлення, і, отже, не забезпечена секретність вбудовування інформації. По-друге, приховане повідомлення легко зруйнувати, оскільки система людського зору не помітить зміни в цих бітах.

Для подолання зазначених недоліків пропонується вбудовувати таємні повідомлення не в усі пікселі зображення, а лише до деяких з них, що визначаються за псевдовипадковим законом відповідно до ключа, відомого законному користувачеві. Однак при цьому зменшується пропускна здатність стегосистеми, що потребує подальшого дослідження.

Список літератури

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 261 с. 2. Хорошко В.А., Шелест М.Е. Введение в компьютерную стеганографию. – К.: НАУ, 202. – 140 с. 3. Алиев А.Т., Аграновский А.В. Вопросы построения криптостеганографических систем. Модель стеганографического канала передачи данных // Информационное противодействие угрозам терроризма. – 2006. – № 8. – С. 79-91. 4. Кошкина Н.В. Обзор спектральных методов внедрения цифровых водяных знаков в аудиосигналы // Проблемы управления и информатики. – 2010. – № 5. – С. 132-144. 5. Кустов В.Н., Федчук А.А. Методы встраивания скрытых сообщений // Защита информации. Конфидент. – 2002. – № 3. – С. 34-37.

УДК 681.3.05

В.Г. Красиленко, *krasilenko@mail.ru*
С.К. Грабовляк, *svetlana.grabowliak@yandex.ru*
Вінницький соціально-економічний інститут у-ту «Україна»

МОДИФІКАЦІЇ СИСТЕМИ RSA ДЛЯ СТВОРЕННЯ НА ЇЇ ОСНОВІ МАТРИЧНИХ МОДЕЛЕЙ ТА АЛГОРИТМІВ ДЛЯ ЗАШИФРУВАННЯ ТА РОЗШИФРУВАННЯ ЗОБРАЖЕНЬ

За декілька останніх років суттєво зросла кількість задач, в яких необхідно виконувати криптографічні перетворення над багатовимірними сигналами, серед яких важливе місце займають різноманітні напівтонові, кольорові зображення та двовимірні масиви.

У роботі [1] на основі матричних афінних шифрів запропонований алгоритм та процедура створення цифрового сліпого підпису на текстографічні документи. Відомі також результати моделювання алгоритмів створення 2D ключа [2], суть яких полягає в узагальненні відомих протоколів створення та генерування ключів на матричний випадок. У роботах [3] було запропоновано модифіковані так звані матричні афінно-перестановочні алгоритми. Але недоліком таких матричних афінних чи афінно-перестановочних алгоритмів є необхідність у використанні декількох великорозмірних матричних ключів.

Тому метою роботи є пошук, розробка та моделювання матричних алгоритмів криптоперетворень зображень зі зменшеною кількістю матричних ключів при достатній їх стійкості.

Теоретичні основи та результати. На відміну від скалярної криптосистеми RSA, суть якої полягає у виборі двох простих чисел k і l; обчислення їх добутка $n = (k \cdot l)$; та виборі довільного числа e ($e < n$), такого, що $НСД(e, \psi(n)) = 1$, де $\psi(n) = (k-1)(l-1)$; знаходженні до числа e оберненого до нього за модулем $\psi(n)$ числа d та публікації двох чисел (e, n) – як відкритого ключа ми пропонуємо узагальнити це на матричний випадок. При зашифруванні відправник розбивав своє повідомлення на рівні блоки по $k \equiv \lfloor \log_2(n) \rfloor$ біт і для кожного і-го числа-блока m_i обчислював $c_i \equiv ((m_i)^e)_{\bmod n}$. При розшифруванні з кожного отриманого *і*-го числа-блока криптограми c_i обчислювався $d_i \equiv ((c_i)^d)_{\bmod n}$.

Ми пропонуємо до кожного *і*-го компонента застосовувати свою і-пару взаємопов'язаних ключів (e_i, d_i), що вибираються з допустимої множини $(E, D) = \{e_1, \ldots e_{N \times M}, d_1, \ldots d_{N \times M}\}$ пар для даних вибраних чисел k і l у відповідності до відомих правил. У відповідності до цього сукупності ключів e_i та d_i назвемо матричними ключами KEYP та OKEY. Тоді процеси зашифрування та розшифрування можна представити у вигляді таких матричних моделей: $C \equiv M^{[\wedge]KEYP} \bmod n \cdot 1$; $D \equiv C^{[\wedge]OKEY} \bmod n \cdot 1$, де $[\wedge]$ – операція поелементного піднесення у степінь за модулем n; а 1 - одинична матриця.

Розглянемо процес зашифрування та розшифрування зображень на основі таких матричних моделей модифікації системи RSA у програмному середовищі MathCad. 1) Формування ключів: вибираються два простих числа k, l, знаходиться їх добуток і за допомогою функції Ейлера знаходиться кількість взаємно простих з kl чисел; методом генерування випадкових чисел формується випадкове зображення G2 для створення ключа; коригується зображення G2 шляхом додавання до кожного значення його пікселя 1 та формується ключ KEYP(Рис.1*b*); знаходиться ключ розшифрування OKEY, в якому елементи є оберненими до елементів ключа KEYP. 2) Зашифрування зображення: обране вхідне зображення S1 коригується і в резуль-