25, No. 6. — P. 402–407. 17. Rogers G. L. Neugebauer revisited: random dots in halftone screening / G. L. Rogers // J. Color. Res. Appl. —1998. — Vol. 23. — P. 104–113. 18. Yule J.A.C. The penetration of light into paper and its effect on halftone reproductions / J.A.C. Yule, W. J. Nielsen // Proc. TAGA. — 1951. — Vol. 3. — P. 65–76.

АНАЛИТИЧЕСКОЕ РЕШЕНИЕ СИСТЕМ АВТОТИПНЫХ УРАВНЕНИЙ

Предложено общее векторное уравнение автотипного синтеза цветов на печатном оттиске с учётом базовых векторов цветов триадных красок. Обосновано принципиальную возможность воспроизведения произвольного цвета на цветном оттиске двумя цветными и чёрной красками, условия которых определяются положением цвета на CaS-диаграмме. Получено аналитические решения трёх систем автотипных уравнений. На основании полученных аналитических выражений приводятся результаты численных расчётов триадных красок цветов по данным RGB-координат.

ANALYTICAL SOLVE OF THE SYSTEMS OF AUTOTYPE EQUALIZATIONS

The general vector equation of autotype synthesis of colors on a printed impression was offered with taking into account the base vectors of color set. The principle possibility of the arbitrary color reproduction is based on a chromotype two coloured and black inks, the terms of which are determined by position of color on the CaS-diagram. There were got the analytical solves of three systems of autotype equations. There were resulted the numeral calculations of color set from data RGB-coordinates based on the got analytical expressions.

Стаття надійшла 11.03.10

УДК 004.056

Б. В. Дурняк, І. М. Лях
Українська академія друкарства

СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ЗАСОБАХ МАСОВОЇ ІНФОРМАЦІЇ

Окреслено найпоширеніші методи захисту даних у засобах масової інформації.

Інформація, захист, засоби масової інформації, аутентифікація, конфіденційність, інтегральність, доступність

Залежно від можливостей систем масової інформації та алгоритму послуг, отримуваних за допомогою систем масової інформації, можна створити значний перелік різних небезпек, з якими стикаються як окремі користувачі, так і власники систем масової інформації. Для більш систематичного визначення їх насамперед встановимо базові типи небезпек впливу на роботу системи масової інформації щодо захисту даних, передаваних її каналами. Основні небезпеки визначено в рамках систем, що використовують криптографію як

один з важливих способів захисту інформації та являють собою стандартизовані поняття, якими є:

аутентифікація;

конфіденційність передаваної інформації;

інтегральність передаваної інформації;

доступність до засобів інформації [1].

Аутентифікація джерела інформації реалізується різними механізмами ідентифікації, найпоширенішими серед яких є паролі, коди, таємні ключі. Крім того, у галузі інформаційних технологій використовуються механізми, суть яких полягає в ідентифікації мітками часу та ідентифікації, що ґрунтується на застосуванні алгоритмів шифрування, та інші.

Ідентифікація мітками часу реалізується кількома методами. Так, приміром, використовується фіксований інтервал часу, протягом якого отримана інформація повинна бути розпізнана як така, що дійсно походить від легального абонента. Цей час призначається на дешифрацію, якщо повідомлення було зашифроване, або на реалізацію інших алгоритмів, які використовуються для контролю даних, що передаються. Другий спосіб використання часу полягає в приписуванні переданим даним мітки часу, котра відповідає часу надання інформації відповідним джерелом. Для цих способів ідентифікації характерне дотримання режиму реального часу при роботі відповідних апаратних і програмних засобів.

Спосіб аутентифікації, що базується на використанні шифрування із симетричним ключем, хоч і має недоліки, але доволі широко застосовується при передачі даних. Досить часто для таких цілей використовують асиметричні шифри, які мають таємний і явний ключі; найвідомішим асиметричним алгоритмом шифрування є алгоритм RSA [2]. Процес аутентифікації можна реалізувати, застосовуючи код MAC разом з ключами шифрування. У даному випадку до повідомлення додається код MAC, що формується на основі використання цього повідомлення і разом з повідомленням передається адресату. Адресат на підставі отриманого повідомлення за відомим йому алгоритмом вираховує код MAC і порівнює його з кодом MAC, переданим адресату разом з повідомленням. Якщо порівнювані коди збігаються, то повідомлення приймається як таке, що відповідає оригіналу.

Одним з основних методів забезпечення конфіденційності даних, що передаються каналами систем масової інформації, є шифрування. У кожній з областей захисту інформації використовуються різні класи шифрів — від перестановочних до складних, що ґрунтуються на застосовуванні модульної арифметики, теорії груп та інших математичних дисциплін, які дозволяють розв'язувати основні задачі шифрування. До таких задач належать:

перетворення кодів, що шифруються, таким способом, який не дозволяє без знання таємних ключів здійснити дешифрацію за важливий період часу;

вибір чисел, які можна було б використовувати як ключі шифрування;

мінімізація часу, необхідного для реалізації шифрувальних функцій;

доведення необхідної межі стійкості розроблених алгоритмів і методів шифрування щодо атак на системи шифрування, що гарантує безпечність кожної окремої криптосистеми.

Інтегральність інформації, котра передається, означає, що в отриманих адресатом відомостях немає частин, які не відповідають оригіналу. Найактуальнішим є забезпечення інтегральності в сферах фінансової діяльності, де зміна одного фрагмента даних може призвести до катастрофічних для легальних абонентів наслідків. До методів забезпечення інтегральності слід віднести метод, що базується на використанні вже згадуваного MAC.

Другим методом забезпечення інтегральності є метод, що полягає у використанні цифрового підпису. Цифровий підпис створюється шляхом редукції тексту, який передбачається передавати за допомогою односпрямованих функцій (типу Н-функцій) та шифрування Н-образу тексту з допомогою несиметричних алгоритмів. При шифруванні абонент використовує приватний ключ, який є таємним, і скорочений зашифрований текст, котрий являє собою цифровий підпис, що разом з текстом, який може бути зашифрований за допомогою симетричного шифру або бути відкритим, передається адресату. Адресат, використовуючи публічний ключ, розшифровує Н-образ тексту повідомлення, через прийнятий каналом зв'язку тексту формує його скорочений образ. Якщо цей образ збігається зі скороченим образом, отриманим з цифрового підпису, то це є гарантією, що текст повідомлення не було модифіковано.

Доступність означає можливість управління доступом до засобів масової інформації, до інформації, котра знаходиться в системі масової інформації, до засобів шифрування даних, що передаються, та інших компонент, несанкціонований доступ до яких може призвести до порушення роботи системи масової інформації та неможливості надання послуг легальним користувачам. Таким чином, небезпека, що пов'язана з несанкціонованим доступом до системи масової інформації, є досить багатогранною за способами взаємодії з нею.

Компонентами, що протидіють такій небезпеці, є паролі та ідентифікаційні номери PIN. Розвиток електронно-апаратних засобів дозволяє застосовувати для контролю доступу більш складні методи. Сьогодні для ідентифікації споживачів послуг використовують цілий ряд біометричних засобів. До них, зокрема, належать:

ідентифікація за райдужною оболонкою ока;

ідентифікація за відбитком долоні;

ідентифікація за відбитком пальців;

ідентифікація за голосом.

Одним з базових методів захисту даних у засобах масової інформації є скремблювання мови. Методи скремблювання використовуються для аналогових систем і являють собою методи шифрування аналогового сигналу. Для того щоб шифрувати сигнал мови, необхідно поміняти кореляцію між параметрами, що визначають аналоговий сигнал: часом, частотою, амплітудою.

Скремблювання частоти полягає у виділенні окремих частотних смуг у сигналі і переставлянні фрагментів сигналів цих частотних смуг у зміненому порядку. Скремблювання в часі має своєю суттю перестановку виділених фрагментів сигналу з однієї часової послідовності в іншу. Скремблювання аналогового сигналу за одним параметром називається однопараметричним. Якщо воно реалізується за кількома параметрами, то іменується багатопарометричним.

1. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. — М.: Яхтсмен, 1996, — 187 с. 2. Коутинхо С. Введение в теорию чисел. Алгоритм RSA / Коутинхо С. — М.: Постмаркет, 2001. — 328 с.

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

Описываются наиболее распространённые методы защиты данных в средствах массовой информации.

PROTECTION METHODS OF INFORMATION IN MEDIA

Outlines the most common methods of data protection in the media.

Стаття надійшла 13.05.10

УДК 681.5

В. М. Сеньківський
Українська академія друкарства
Р. О. Козак
Тернопільський національний технічний університет ім. Івана Пулюя

КРИТЕРІЇ ОПТИМАЛЬНОСТІ ПРОЦЕДУРИ ПАРАМЕТРИЧНОГО СИНТЕЗУ ПРОЕКТНИХ РІШЕНЬ

Окреслено суть критеріїв оптимальності та постановку задачі багатокритеріальної оптимізації для випадку згортання часткових критеріїв в узагальнений і нормалізації вагових коефіцієнтів у процедурах параметричного синтезу.

Критерії оптимальності, постановка задачі, багатокритеріальна оптимізація, параметричний синтез

Основою будь-якого проектування є процедура синтезу проектних пропозицій, від успішного виконання котрої значною мірою залежать властивості майбутньої продукції [5]. Зазвичай проектування розпочинають із структурного синтезу, результатом якого є продукування концептуальних пропозицій проекту: фізичний принцип дії механізму, функціональна схема пристрою, типова конструкція вузла системи. Однак ці конструкції й схеми обирають у параметричному вигляді без наведення числових значень параметрів елементів.