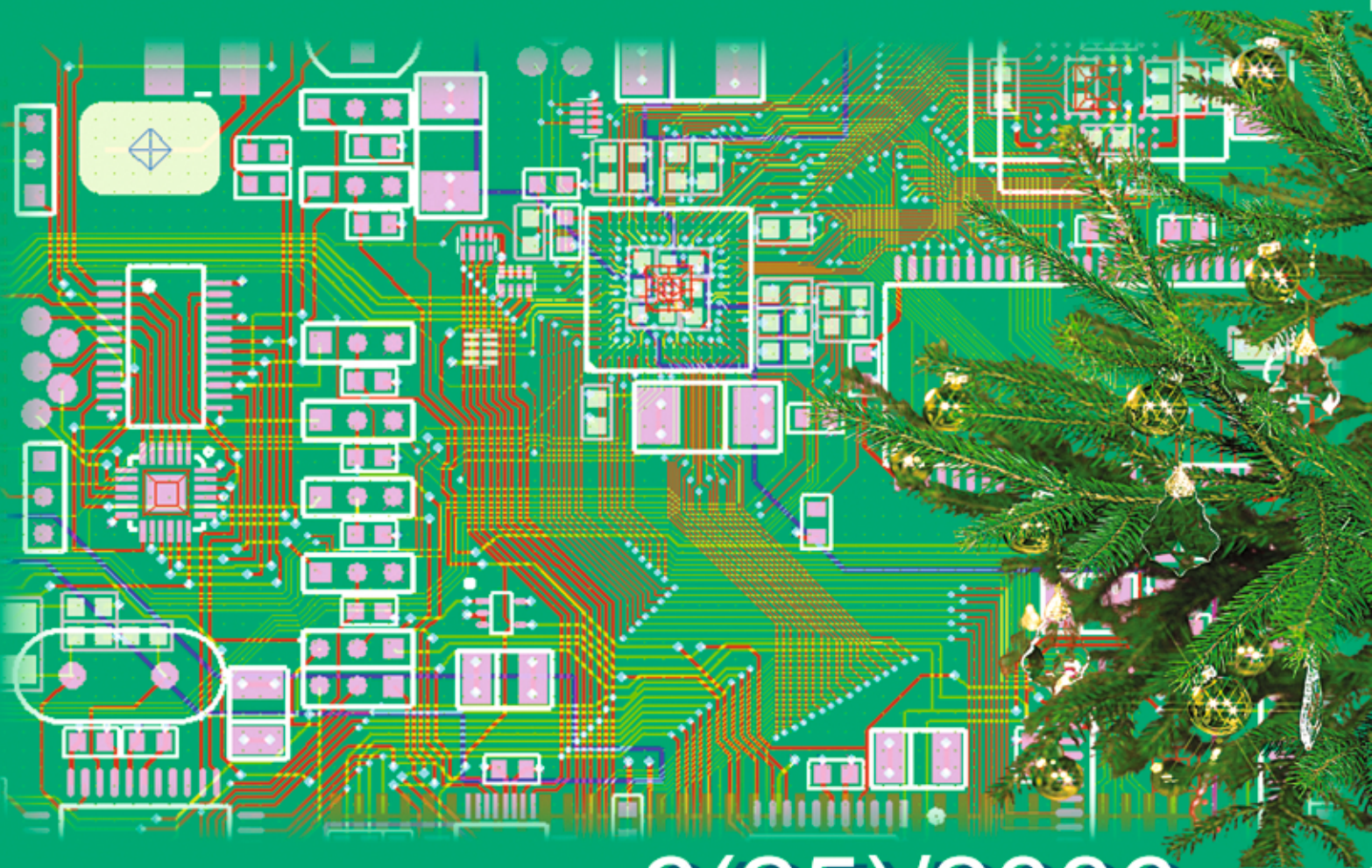


ИНФОРМАЦИОННО- УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ



6(25)/2006

6(25)/2006

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

Главный редактор

М. Б. Сергеев,
доктор технических наук, профессор

Зам. главного редактора

Г. Ф. Мощенко

Редакционный совет:

Председатель А. А. Оводенко,
доктор технических наук, профессор
В. Н. Васильев,
доктор технических наук, профессор
В. Н. Козлов,
доктор технических наук, профессор
Ю. Ф. Подоплекин,
доктор технических наук, профессор
Д. В. Пузанков,
доктор технических наук, профессор
В. В. Симаков,
доктор технических наук, профессор
А. Л. Фрадков,
доктор технических наук, профессор
Л. И. Чубраева,
доктор технических наук, профессор, чл.-корр. РАН
Р. М. Юсупов,
доктор технических наук, профессор, чл.-корр. РАН

Редакционная коллегия:

В. Г. Анисимов,
доктор технических наук, профессор
Е. А. Крук,
доктор технических наук, профессор
В. Ф. Мелехин,
доктор технических наук, профессор
А. В. Смирнов,
доктор технических наук, профессор
В. И. Хименко,
доктор технических наук, профессор
А. А. Шалыто,
доктор технических наук, профессор
А. П. Шепета,
доктор технических наук, профессор
З. М. Юлдашев,
доктор технических наук, профессор

Редактор: А. Г. Ларионова

Корректор: Т. В. Звертановская

Дизайн: М. Л. Черненко

Компьютерная верстка: Т. М. Каргапольцева

Ответственный секретарь: О. В. Муравцова

Адрес редакции: 190000, Санкт-Петербург,

Б. Морская ул., д. 67

Тел.: (812) 494-70-36

Факс: (812) 494-70-18

E-mail: 80x@mail.ru; ius@aanet.ru

Сайт: www.i-us.ru

Журнал зарегистрирован

в Министерстве РФ по делам печати,

телерадиовещания и средств массовых коммуникаций.

Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г.

Журнал распространяется по подписке.

Подписку можно оформить через редакцию, а также

в любом отделении связи по каталогам:

«Пресса России» – № 42476;

«Роспечать» («Газеты и журналы») – № 15385

ОБРАБОТКА ИНФОРМАЦИИ И УПРАВЛЕНИЕ

Беззатеев С. В., Литвинов М. Ю., Трояновский Б. К., Филатов Г. П. Выбор алгоритма преобразования, обеспечивающего изменение структуры изображения 2

Шолохов А. В. Метод оценки достоверности информации при периодической коррекции наземных навигационных систем 7

МОДЕЛИРОВАНИЕ СИСТЕМ И ПРОЦЕССОВ

Нестеренко В. Д. Концепция построения архитектуры моделей процессов управления инфокоммуникационными сетями (Часть 1) 15

ПРОГРАММНЫЕ И АППАРАТНЫЕ СРЕДСТВА

Ронжин А. Л., Карпов А. А., Лобанов Б. М., Цирульник Л. И., Йокиш О. Фонетико-морфологическая разметка речевых корпусов для распознавания и синтеза русской речи 24

Канжелев С. Ю., Шалыто А. А. Автоматическая генерация автоматного кода 35

ИНФОРМАЦИОННЫЕ КАНАЛЫ И СРЕДЫ

Рыжиков Ю. И. Средние времена ожидания и пребывания в многоканальных приоритетных системах 43

КРАТКИЕ СООБЩЕНИЯ

Голландцев Ю. А. Сравнение механических характеристик асинхронных и вентильных индукторно-реактивных двигателей 50

ХРОНИКА И ИНФОРМАЦИЯ

Юсупов Рафаэль Мидхатович. Творческая биография 54

СВЕДЕНИЯ ОБ АВТОРАХ

57

АННОТАЦИИ

СОДЕРЖАНИЕ ЖУРНАЛА «ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ» за 2006 г. [№ 1–6] 62

ЛР № 010292 от 18.08.98.

Сдано в набор 10.10.2006. Подписано в печать 15.12.2006. Формат 60×90/8.

Бумага офсетная. Гарнитура SchoolBookC. Печать офсетная.

Усл. печ. л. 8,0. Уч.-изд. л. 9,0. Тираж 1000 экз. Заказ 658.

Оригинал-макет изготовлен
в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

Отпечатано с готовых диапозитивов
в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

УДК 681.3

ВЫБОР АЛГОРИТМА ПРЕОБРАЗОВАНИЯ, ОБЕСПЕЧИВАЮЩЕГО ИЗМЕНЕНИЕ СТРУКТУРЫ ИЗОБРАЖЕНИЯ

С. В. Беззатеев,

канд. техн. наук, доцент

М. Ю. Литвинов,

соискатель

Б. К. Трояновский,

доцент

Г. П. Филатов,

соискатель

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Рассматривается проблема выбора эффективного алгоритма преобразования видеоинформации в видеосистемах встраиваемого класса, обеспечивающего ее конфиденциальность при передаче и хранении. Предлагается модификация алгоритма VEA, позволяющая повысить защищенность информации в условиях атак по перехваченной преобразованной информации и выбранному исходному изображению и обеспечивающая эффективное уничтожение структуры передаваемой видеоинформации.

The authors study the choice of an effective algorithm for the transformation of video information in embedded video systems that ensures its confidentiality on keeping and transmission. A modification of the VEA algorithm is proposed. This modification increases the protection level of the information against the interception attacks and ensures an efficient destruction of the transmitted information.

Введение

Для решения задачи обеспечения конфиденциальности передаваемой и хранимой информации традиционно используется специальное преобразование, устойчивое к различного типа атакам. В контексте данной задачи наиболее эффективными и опасными являются атаки по парам исходное — преобразованное изображение и по выбранному исходному изображению. Кроме того, следует отметить необходимость предотвращения атак, связанных со спецификой исходной информации, — изображения, которое изначально содержит характерные фрагменты (контуры) и тем самым уже по умолчанию предполагает возможность атаки по парам исходное — преобразованное изображение. Задача выбора алгоритма преобразования осложняется спецификой видеосистем встраиваемого класса — существенными ограничениями на свободные вычислительный ресурс и объем оперативной памяти.

Потоковые и блочные преобразования

Все преобразования условно разделяют на два типа — потоковые и блочные. К потоковым преобразованиям относятся системы, использующие

ключевые последовательности, генерируемые регистрами сдвига, и системы хаотичного преобразования (CVEC). Такие системы обеспечивают высокую скорость обработки информации, однако они неустойчивы к атакам с использованием перехваченных образцов обработанного и исходного изображения [14]. Системы блочного преобразования, в свою очередь, можно разделить на системы полного и частичного преобразования. Системы частичной обработки видеоинформации, использующие так называемые методы селективного преобразования, делятся на системы, учитывающие структуру видеоформата и ориентированные на обработку форматов сжатого изображения [1–6, 8–12], и системы, предназначенные для обработки несжатой информации [13]. Рассмотрим особенности этих подходов на примере нескольких наиболее известных алгоритмов.

1. Video Encryption Algorithm by Okao and Nahrstedt [8]. Основной идеей алгоритма является изменение статистических свойств видеоформата MPEG. Преобразование представляет собой аналог одного раунда сети Фейстейла. Первоначально весь информационный поток разбивается на блоки одинаковой длины (например, на байты), таким