3. Бокуть Л.В., Кулешов А.Я. Корреляционный анализ весовых значений векторов направлений //Теоретическая и прикладная механика.-2007.-№22.-С.187-196.
4. T. F. Cootes. Face recognition using Active Appearance Models. University of Manchester, 2000, http: //www.wiau.man.ac.uk.
5. Абламейко С.В., Боричев С.П. и др. Алгоритм фильтрации ПТИ, на основе параллельных операций сдвига и сложения при свертке изображений с масками преобразования// Анализ цифровых изображений. Минск:ОИПИ НАН Беларуси.2002.Вып1.С.7-13.

УДК 004.056

ОЦЕНИВАНИЕ СЛОЖНОСТИ «ВЗЛАМЫВАНИЯ» КОМБИНИРОВАННОГО АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ ЧАСТОТНЫМ МЕТОДОМ

Буснюк Н.Н., Литовко А.А.

Белорусский национальный технический университет, Минск, Республика Беларусь

Две главные задачи, рассматриваемые в криптологии – это 1) создание надежных алгоритмов шифрования информации и 2) разработка инструментов, позволяющих раскодировать закрытый текст с неизвестным ключом.

Основным показателем качества алгоритма шифрования является его криптостойкость, т.е устойчивость к «взламыванию» шифра (подбора ключа). Универсальным, и в то же время наиболее трудоемким методом криптоанализа является метод полного перебора всевозможных вариантов ключей. Его трудоемкость пропорциональна мощности пространства ключей.

Говоря о криптостойкости алгоритмов шифрования, делают оговорку, что они не раскрываемы при существующих возможностях вычислительной техники. С другой стороны, поскольку засекречивание информации всегда имеет за собой коммерческую ценность, говорят о соизмеримости ценности раскрываемой информации и ресурсов, затрачиваемых на ее расшифровывание. Т.е. алгоритм считается вычислительно безопасным, если он не может быть взломан с использованием доступных ресурсов [2].

Целью данной работы, как и последующих по этой тематике, является получение оценок криптоустойчивости шифров, не обладающих совершенной криптостойкостью. В качестве такого шифра в данной работе рассматривается алгоритм, предложенный в [1].

Известно статистическое распределение вероятностей символов русского алфавита. Авторами на языке Delphi была написана программа, с помощью которой подсчитывалось эмпирическое распределение вероятностей символов русскоязычных текстов различного содержания (художественных, научно-популярных, публицистических) и исследовалась зависимость близости эмпирического распределения вероятностей и статистического от длины шифруемого текста. Выяснилось, что угадывание содержания зашифрованного текста возможно вручную криптоаналитиком уже для текстов объемом всего в несколько раз превышающим мощность алфавита A исходного текста. Затем с помощью программы подсчитывалась частота символов закрытого текста в случае, если одному символу алфавита A соответствовало несколько символов алфавита B шифртекста и каждый раз при замене символа открытого текста такое соответствие устанавливалось псевдослучайным образом. В этом случае уже невозможно визуально распознать содержание зашифрованного текста; компьютеры, действующие по принципу «грубой силы», отыскивают шифр путем изучения открытого текста на предмет наличия в нем узнаваемых словосочетаний.

Считается, что криптоаналитик может расшифровать шифртекст, если некоторые из символов повторяются хотя бы пару раз [2]. Однако каких это требует ресурсов (временных и финансовых) однозначно сказать трудно. На практике применение совершенно криптостойких алгоритмов шифрования (т.е. таких, что символы в шифртексте не повторяются) экономически нецелесообразно.

В алгоритме поточного шифрования, предложенном в [1], каждый символ a_i алфавита A открытого текста кодируется v_i символами алфавита B шифртекста. Мощность алфавита A равна n, мощность алфавита B шифротектса равна

$$m = \sum_{i=1}^{n} v_i .$$

Устанавливается длина l символа шифротекста и генерируется шифр длины $l \cdot m$.

Задается параметр L количества символов шифртекста, после получения которых меняются некоторые либо все параметры функции шифрования.

Количество замен алфавита шифротекста

$$N = \frac{M}{L},$$

где M – мощность открытого (шифрованного текста). Если увеличить m, т.е. задаваемую частотность знаков открытого текста приблизить к статистической, то в такой же пропорции можно увеличить параметр L, не ослабляя криптостойкости алгоритма. При этом количество замен последовательности шифра уменьшится во столько же раз, но в итоге длина генерируемой последовательности для шифрования всего текста останется прежней. Если положить $L=m$, то генерируемая последовательность будет равна длине шифртекста .

Оценим количество операций, затрачиваемых криптоаналитиком на раскодирование текста с помощью частотного метода в случае, если проводится криптоатака с использованием только шифртекстов.

Длина вектора инициализации, устанавливаемого вначале текста, не может быть больше l. Не зная величины l, компьютер должен перебрать комбинации групп битов от 8 до l .Таким образом для

подсчета эмпирических частот встречаемости одинаковых комбинаций последовательно стоящих битов в закрытом тексте компьютером будет затрачено порядка $O(l^2M)$ операций. Криптоаналитику следует распознать l^2 закрытых текстов. При этом значение параметра m неизвестно. Устанавливая соответствие между выделенными комбинациями бит шифртекста и символами алфавита открытого текста компьютер должен распознать в расшифровываемом сообщении смысловое содержание. Количество таких замен в случае полного перебора равно числу подстановок n^m. Учитывая тот факт, что отображение $A \to B$ неоднозначно, i-тый символ алфавита А имеет v_i образов, количество таких подстановок будет равно произведению сочетаний

$$\prod_{i=1}^{n} C_{\sum_{j=i}^{n} v_j}^{v_i} = \frac{m!}{\prod_{i=1}^{n}(v_i!)}.$$

Оценка снизу для этой величины, используя приближенную формулу Стирлинга, будет равна

$$\frac{m^m}{\prod_{i=1}^{n} v_i}.$$

Программой на языке Delphi подсчитывалась эмпирическая статистика для случая, когда $m=114$ (вероятность появления каждого символа алфавита B равна около 0,009). При этом замена символа a_i (пары символов) символом алфавита B каждый раз в случае, если

$v_i > 1$, осуществлялась псевдослучайным образом. Оценка для количества способов расшифровки закодированного с помощью алгоритма [1] текста оказалась равна порядка $O(10^{130})$.

1. Буснюк Н.Н. Пример комбинированного алгоритма поточного шифрования с ограниченными ресурсами // Материалы X1У Международной конференции «Комплексная защита информации» 19-22 мая 2009 г., Могилев,2009, с. 64-65.
2. Математические и компьютерные основы криптологии: Учебное пособие / Ю.С.Харин и др. – Мн.: Новое знание, 2003, 382с.

УДК 658.512

ТЕХНОЛОГИЧЕСКОЕ ОБОРУДОВАНИЕ С ЧПУ ДЛЯ ОБРАБОТКИ ВЫПУКЛЫХ АСФЕРИЧЕСКИХ ПОВЕРХНОСТЕЙ

Атрашкевич Р.В.[1], Кузнечик В.О.[1], Хохленков Л.Н.[2]

[1]Белорусский национальный технический университет, Минск, Республика Беларусь
[2] НП ЧУП «ЛЭМТ», Минск, Республика Беларусь

Использование асферических поверхностей в оптических приборах позволяет обеспечить их высокие эксплуатационных характеристики при простейшей конструкции систем.

Асферическая оптика может быть грубой, средней и высокой точности, что и предопределяет выбор метода формообразования ее поверхностей.

Наивысшее качество достигается, по сравнению с другими методами, посредством механического съема припуска с исходной поверхности оптической детали.

Схема устройства для реализации данного способа приведена на рис. 1. Устройство содержит: бабку изделия 1, шлифовальную бабку 2 инструмента, поворотный стол 3 и редуктор подачи 4, которые базируются на станине 5 (рис. 1).

В бабке изделия 1 на подшипниках 6 смонтирован шпиндель изделия 7. Подшипники расположены в пиноли 8, на левом конце которой закреплена червячно-косозубая пара 9 с маховиком 10.

Бабка изделия 1 соединена с верхней плитой поворотного стола 3, который крепится к станине 5. В поворотном столе размещены червяк 11 и вал 12 червячного колеса, являющийся осью поворота стола, смонтированной на подшипниках 13.

Шлифовальная бабка 2 инструмента, с расположенным внутри нее валом 14 шпинделя инструмента, базирующимся на аэростатических подшипниках 15, 16 и 17, крепится к плите 18, имеющей возможность перемещения вдоль оси шпинделя 7. На левом конце вала 14 шпинделя инструмента закреплен шлифовальный инструмент 19, а 30-92 на правом – ротор встроенного электродвигателя 20. Плита 18 с закрепленной на ней шлифовальной бабкой инструмента 2 имеет возможность перемещения относительно плиты 21 с целью обеспечения установки режущей кромки инструмента 19 относительно обрабатываемой детали 22. Редуктор подачи 4, с расположенными внутри его червячными парами 23, 24 и шариковой винтовой передачей 25, закреплен, как и шлифовальная бабка инструмента 2, на плите 18, при этом винт шариковой винтовой передачи установлен соосно с валом 14 шпинделя инструмента. Система ЧПУ 26 обеспечивает включение привода поворота стола, привода шпинделя инструмента, вращение инструмента и детали.

Для шлифования криволинейной поверхности вращающейся детали 22 коническим алмазным инструментом 19 инструмент закрепляют на горизонтальном вращающемся шпинделе. Центр ближайшей сферы обрабатываемой криволинейной поверхности детали совмещают с вертикальной осью качания шпинделя детали. Точку взаимного контакта инструмента и детали размещают от оси инструмента в вертикальной плоскости на расстоянии, равном радиусу средней окружности рабочей поверхности инструмента.