данная мера не приводит к заметному улучшению качества связи, но может быть причиной повышенной интенсивности электромагнитного фона в местах с высокой плотностью населения, что является небезопасным с точки зрения электромагнитной безопасности.

ПОРОГОВАЯ СХЕМА ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ С РАЗДЕЛЕННЫМ СЕКРЕТОМ

О.А. Селеня, С.Б. Саломатин

Защита с помощью использования пороговой электронно-цифровой подписи с разделенным секретом включает в себя задачи разделения доступа, подтверждения авторства, контроль целостности, конфиденциальность, обеспечение юридической значимости электронного документа.

Существует большое количество схем ЭЦП на основе разделения секрета, одна из них приведена в [1]. В ходе анализа этой схемы было выявлено, что возникают проблемы при использовании описанного алгоритма для нечетного числа участников так как количество долей в ключевом наборе является четным, а следовательно при собирании общей подписи одной доли либо будет недоставать, либо она будет дублироваться, что приведет к неправильному значению общей подписи. Наборы, отсылаемые одному участнику, содержат все разделенные доли секрета, что снижает надежность алгоритма. Кроме того, по этой схеме генерируются и отсылаются каждому участнику наборы для каждого порога, что увеличивает размер хранимой информации на стороне клиентов и сервера. В модифицированном алгоритме эти недостатки устраняются путем генерации количества наборов равного количеству участников. При этом для работы с порогами выше минимального не требуется вычислять свои наборы, достаточно сгенерированных наборов для минимального порога.

Литература

1. *Джунковский П.О., Дитенкова А.С.* Пороговая схема цифровой подписи с разделенным секретом на базе ГОСТ Р 34.10-2001. Журнал «Безопасность информационных технологий». Выпуск №3, 2010.

ОБ ИСПОЛЬЗОВАНИИ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ ПРИ ФОРМИРОВАНИИ ХРУПКИХ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

А.В. Сидоренко, И.В. Шакинко

Значительные достижения в области мультимедиа и веб-технологий за последнее время привели к широкому распространению изображений в цифровом виде. При этом возникает необходимость в решении задач, связанных с аутентификацией цифровых изображений [1]. Для решения данных задач применяется метод, связанный с хрупкими цифровыми водяными знаками. Хрупкие цифровые водяные знаки используются для выявления изменений в изображении при его передаче [2].

В данной работе при формировании хрупких цифровых водяных знаков применяются хаотические отображения. На каждой итерации значения интенсивности элементов передаваемого изображения добавляются к значениям параметров с учетом переменных выбранного отображения. При этом через некоторое количество итераций выявляются существенные отличия в значениях переменных отображения.

Нами предложена схема встраивания хрупких цифровых водяных знаков в изображения. Проведенное тестирование этой схемы подтверждает способность выявления искажений, возникающих при передаче по каналу связи. Полученные данные свидетельствуют о возможности использования предлагаемой схемы встраивания хрупких цифровых водяных знаков при решении задач, связанных с аутентификацией.

Литература

1. Sidiropoulos P. Invertible chaotic fragile watermarking for robust image authentication / P. Sidiropoulos, N. Nikolaidis, I. Pitas // Chaos, Solitons and Fractals. 2009. Vol. 42. P. 2667–2674.

2. Vartak R. Survey of Digital Image Authentication Techniques / R. Vartak, S. Deshmukh // International Journal of Research in Advent Technology. 2014. Vol. 2, № 7. P. 176–179.