3. Weller, M. "The Digital Scholar: How Technology is Transforming Scholarly Practice". Bloomsbury Academic, 2011.
4. Аникеев, Д. В. "Цифровизация образования в России и за рубежом". Российский научный журнал, 2020, № 8, с. 21-27.
5. Соловьева, А. В. "Перспективы и вызовы цифровой трансформации образования". Вестник высшей школы, 2022, № 4, с. 36-44.

УДК 004.56+003.26

М. Г. Савельева
Белорусский государственный технологический университет
Минск, Беларусь

СРАВНИТЕЛЬНЫЙ АНАЛИЗ УСТОЙЧИВОСТИ МЕТОДОВ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ К РАЗЛИЧНЫМ МЕТОДАМ СТЕГОАНАЛИЗА

Аннотация. *Стегоанализ представляет собой важный процесс обнаружения, извлечения и анализа скрытой информации, которая может быть внедрена в изображение-контейнер. Для углубленного исследования были выбраны несколько методов стегоанализа: Regular-Singular (RS), Sample Pair Analysis (SPA) и атака χ^2, и несколько методов стеганографитческих преобразований: DCT, DWT, LSB, GML и MPV.*

M. G. Saveleva
Belarusian State Technological University
Minsk, Belarus

COMPARATIVE ANALYSIS OF THE STABILITY OF TEGANOGRAPHIC TRANSFORMATION METHODS TO VARIOUS STEGOANALYSIS METHODS

Abstract. *Steganalysis is an important process of detecting, extracting and analyzing hidden information that may be embedded in a container image. Several steganalysis methods were selected for in-depth study: Regular-Singular (RS), Sample Pair Analysis (SPA) and χ^2 attack, and several steganographic transformation methods: DCT, DWT, LSB, GML and MPV.*

Основная задача стеганографических систем заключается в скрытии секретной информации внутри других данных (например, изображений, аудиофайлов, текстов и т.д.) таким образом, чтобы визуально не было заметно, что в носителе данных содержится скрытая информация [1]. Однако система также должна обеспечивать

устойчивость скрытой информации к различным видам атак, таким как сжатие данных, фильтрация, изменение формата файла и другие виды обработки данных. Даже при оптимальных условиях для атаки задача извлечения скрытого сообщения из контейнера может оказаться очень сложной. Однозначно утверждать о факте существования скрытой информации можно только после ее выделения в явном виде.

Для исследования устойчивости методов стеганографических преобразований использованы 3 изображения-контейнера формата PNG (I, II, III), а также сообщения на 15000 и на 30000 символов. Все файлы-контейнеры имеют разрешение 1920×1080, соответственно, содержат в себе 2 073 600 пикселей.

В качестве атак на стегосистемы рассмотрены RS, SPA (Sample Pair Analysis) и χ^2. Метод RS использует анализ пикселей изображения-контейнера, основанный на оценке регулярности групп пикселей [2]. Высокая степень регулярности в определенных областях изображения может указывать на наличие скрытой информации. Метод SPA анализа основан на статистических отношениях между парами соседних пикселей изображений. SPA анализирует отношения между яркостными значениями соседних пикселей в изображении [3]. Идея атаки χ^2 заключается в поиске этих близких значений и подсчете вероятности встраивания на основе того, как близко располагаются значения частот четных и нечетных элементов анализируемого контейнера [4].

В целях исследования работы атак были проведены атаки на незаполненные контейнеры. Результат представлен в таблице 1.

Таблица 1 – Относительная стеганографическая емкость, полученная при различных атаках на контейнер

Контейнер	Относительная стеганографическая емкость, полученная при атаке на контейнер		
	RS	SPA	χ^2
I	0,021	0,027	0,356
II	0,245	0,252	0,201
III	0,053	0,035	0,904

Для внедрения сообщений были выбраны следующие методы: DCT (Discrete Cosine Transform – дискретное косинусное преобразование), DWT (Discrete Wavelet Transform – дискретное вейвлет-преобразование), LSB (Least Significant Bit – наименьший значащий бит), GML (Grey Level Modification – изменение уровня серого) и MPV (Mid Position Value – значение средней позиции). С помощью методов DCT и DWT максимально можно внедрить один символ в блок 8□8, тем самым для 15000 символов контейнер будет заполнен на 0,46 от общего размера контейнера, для 30000 символов –

на 0,93. Используя классический метод LSB при псевдослучайном выборе младших бит можно максимально внедрить один символ в 3 пикселя, тем самым для 15000 символов контейнер будет заполнен на 0,02 от общего размера контейнера, для 30000 символов – на 0,04. При применении метода GML можно осадить один символ в один пиксель, тем самым для 15000 символов контейнер будет заполнен на примерно 0,007 от общего размера контейнера, для 30000 символов – на 0,014. При использовании метода MPV можно внедрить один символ в блок 2□2 пикселя, тем самым для 15000 символов контейнер будет заполнен на примерно 0,028 от общего размера контейнера, для 30000 символов – на 0,058. Результат проведения атак приведен в таблице 2.

Таблица 2 – Относительная стеганографическая емкость, полученная при различных атаках на стегоконтейнер

Атака	Кон-тейнер	Кол-во внедренных символов	Относительная стеганографическая емкость, полученная при атаке на стегоконтейнер				
			DCT	DWT	LSB	GLM	MPV
RS	I	15000	0,021	0,027	0,036	0,059	0,013
	II		0,245	0,836	0,091	0,303	0,181
	III		0,053	0,053	0,048	0,094	0,015
	I	30000	0,027	0,027	0,077	0,095	0,013
	II		0,253	0,851	0,075	0,339	0,183
	III		0,035	0,055	0,048	0,131	0,013
SPA	I	15000	0,021	0,027	0,005	0,056	0,002
	II		0,245	0,358	0,014	0,283	0,022
	III		0,053	0,022	0,007	0,053	0,004
	I	30000	0,027	0,027	0,007	0,085	0,002
	II		0,253	0,348	0,012	0,306	0,013
	III		0,035	0,034	0,005	0,068	0,004
χ^2	I	15000	0,344	0,412	0,357	0,331	0,448
	II		0,116	0,196	0,201	0,110	0,198
	III		0,541	0,888	0,904	0,531	0,889
	I	30000	0,356	0,437	0,363	0,331	0,500
	II		0,121	0,196	0,201	0,110	0,198
	III		0,566	0,887	0,904	0,532	0,887

Исходя из результатов проведенных атак на стегоконтейнеры, можно сделать вывод, что к RS-атаке и SPA-атаке наиболее устойчивы методы DCT, DWT и MPV. К атаке χ^2 самым устойчивым является LSB (результат атак на стегоконтейнеры, полученные в результате применения этого метода, не отличается от атак на исходный контейнер). Таким образом ни один рассмотренный метод нельзя назвать полностью устойчивым к стегоанализу. Кроме того, проведенные атаки назвать полностью эффективными также нельзя, так как они не обнаружили верный объем внедренного сообщения, а лишь указали на наличие изменений.

Список использованных источников

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации / П. П. Урбанович. – Минск : БГТУ, 2016. – 220 с.

2. Fridrich J., Long M. Steganalysis of LSB encoding in color images // 2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No. 00TH8532). – IEEE, 2000. – Т. 3. – С. 1279–1282.

3. Dumitrescu S., Wu X., Wang Z. Detection of LSB steganography via sample pair analysis // Information Hiding: 5th International Workshop, IH 2002 Noordwijkerhout, The Netherlands, October 7-9, 2002 Revised Papers 5. – Springer Berlin Heidelberg, 2003. – С. 355–372.

4. J. Fridrich, G. Miroslav, R. Du Steganalysis Based on JPEG Compatibility. – SUNY Binghamton, New York, 2001. – 6 с.

УДК 004.9:63

D.A. Sahadov, A.A. Mommyyeva, A.M. Jumayeva
State Energy Institute of Turkmenistan,
Mary, Turkmenistan

A DIGITAL SOLUTION FOR THE CARE OF AGRICULTURAL PRODUCTS

Abstract. *In this research paper, the use of artificial intelligence and automated systems in agriculture can overcome various shortcomings and allow farmers to focus on more important issues and land management. Innovative technologies help the agricultural and livestock sectors to collect the necessary information and solve problems that may arise in the production chain on the basis of that information.*

Key words. *Agriculture, agricultural technology, crop monitoring, quality control, logistics, sustainable agriculture.*

Д.А. Сахадов, А.А. Моммыева, А.М. Юмаева
Государственный энергетический институт Туркменистана
Мары, Туркменистан

ЦИФРОВОЕ РЕШЕНИЕ ДЛЯ УХОДА ЗА СЕЛЬСКОХОЗЯЙСТВЕННОЙ ПРОДУКЦИЕЙ

Аннотация. *В этой исследовательской работе говорится, что использование искусственного интеллекта и автоматизированных систем в*