Абабиль Нагиева

Азербайджанский Технологический Университет

ababil.nagiyeva@mail.ru

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ АЛГОРИТМА СОКРЫТИЯ СЕКРЕТНОЙ ИНФОРМАЦИИ НА ОСНОВЕ МЕТОДА ЗАМЕНЫ НАИМЕНЕЕ ЗНАЧИМЫХ БИТОВ

Аннотация: В данной статье представлены экспериментальные результаты алгоритма сокрытия секретной информации, основанного на методе замены наименее значимых битов. Данный алгоритм позволяет увеличить количество скрываемых бит секретной информации при сохранении визуального сходства между стегоизображением и изображением-контейнером. В реализации алгоритма в качестве входного изображения использовалось цифровое изображение.

Ключевые слова: стегоизображение, LSB, секретная информация, стеганография, стеганография изображений.

Abstract: This article presents experimental results of an algorithm for hiding classified information based on the method of replacing the least significant bits. This algorithm allows you to increase the number of hidden bits of secret information while maintaining the visual similarity between your image and the container image. In the implementation of the algorithm, a digital image was used as the input image.

Keywords: stego image, LSB, classified information, steganography, image steganography.

Введение

Предлагаемый алгоритм состоит из двух этапов. На первом этапе в выбранном изображении-контейнере с помощью стего-ключа определяются пиксели для сокрытия секретной информации, после чего изображение

разбивается на блоки размером 2×2. Затем вычисляется разность между пикселем с минимальным значением и остальными пикселями блока. Секретные биты внедряются в пиксели, отличные от минимального, с использованием алгоритма LSB.

Экспериментальные исследования предложенного алгоритма были сопоставлены с экспериментальными данными нескольких алгоритмов, представленных в литературе. Преимуществами разработанного алгоритма являются: возможность сокрытия большего количества секретной информации, сохранение высокого визуального качества, простота вычислений и способность скрывать данные за короткое время, а также устойчивость к стего-атакам.

Исследование степени схожести контейнера и стего-изображения и объема скрытой информации

Независимо от используемых стандартных изображений, в предложенном алгоритме визуальное сходство между двумя изображениями (то есть PSNR) превышает 50 дБ. Как видно из таблицы 1, предложенный алгоритм имеет более высокие качественные показатели по сравнению с другими алгоритмами. Результаты испытаний создают основу для увеличения количества скрываемых бит секретной информации в дальнейших исследованиях.

Для проверки достоверности полученных результатов были проведены эксперименты на 50 изображениях из базы данных USC-SIPI (США) [104], из которых 4 приведены в таблице 1. Эксперименты проводились с использованием программного обеспечения MATLAB \ R2014b.

Человеческая зрительная система (ЧЗС) не воспринимает разницу выше 36 дБ.Значение PSNR напрямую связано с визуальным качеством стегоизображения. Чем выше PSNR, тем больше сходство между исходным и

стегоизображением. Средние значения качества тестируемых изображений следующие: НС — 435202 бит, PSNR — 38.8096 дБ.

В таблице 1 приведены результаты 4 из 50 тестируемых изображений, включая значения PSNR между изображением-контейнером и стегоизображением. Также представлено сравнение PSNR, времени выполнения алгоритма и объема скрытой информации (НС) с новейшими алгоритмами последних лет.

Для более широкой картины и выхода за рамки алгоритмов, рассмотренных во второй главе, в таблицу также включены показатели алгоритмов, предложенных Malik A. [4, с. 2454–7190] и Wahed M. [6, с. 10795–10819], которые показали успешные результаты в литературе (см. таблицу 1).

Таблица 1.

Сравнительный анализ качественных показателей стегоизображения

Входные изображения	**Качественные показатели**	**Malik A., Sikka G.** . [4, s. 2454-7190], **2018**	**Wahed M.A., Nyeem, H** [6, s. 10795-10819], **2019**	**Ahmad A.M., [1. s. 7181-7205], 2019**	**Yong-qing C.** **[2, s. 271 - 350]** **2020**	**Jana B., Giri D.,** **[3, s.239-248]** **2015**	**Предлагаемый алгоритм**
Lena	**НС (bit)**	177777	198902	224528	226085	223031	240962
	PSNR (dB)	31,67	31,14	33,60	33,27	38,25	51,73
Baboon	**НС (bit)**	262272	125562	259737	231401	273235	277492
	PSNR (dB)	22,57	22,29	28,77	23,70	35,85	50,62
Airplane	**НС (bit)**	185676	179961	228863	213460	211321	208392
	PSNR (dB)	30,01	29,66	31,67	31,43	42,34	52,74
Peppers	**НС (bit)**	175669	195490	223295	227493	232563	247864
	PSNR (dB)	29,78	29,78	33,18	31,13	35,12	51,53

Средние значения	**HC (bit)** **PSNR (dB)**	205349 28,50	249979 28,22	234106 31,8	237110 29,88	235037 38,39	**243677** **51,65**

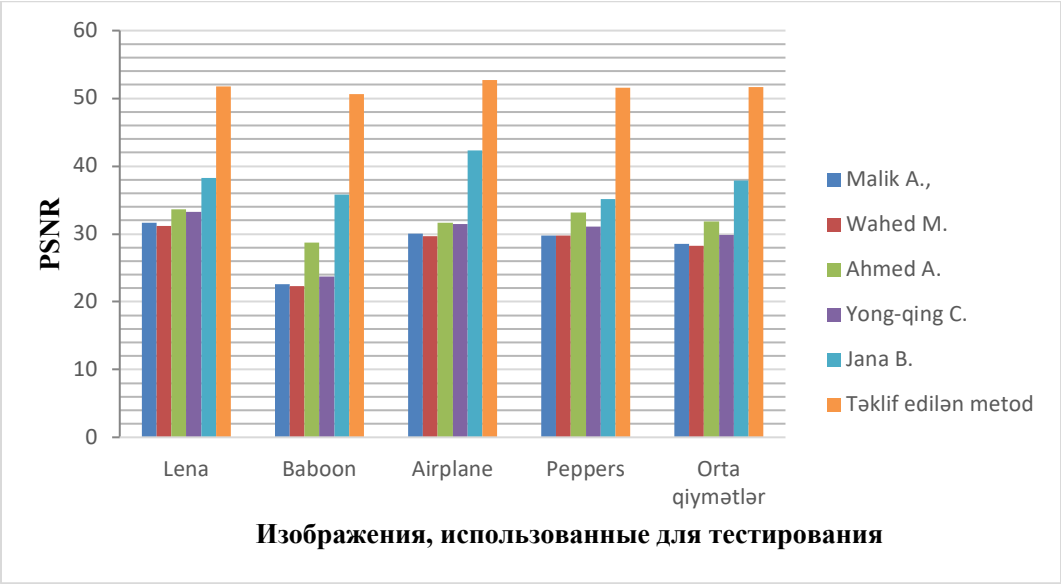

Рисунок 1. Зависимость показателей PSNR от различных изображений

Как видно из рисунка 1, в экспериментах, проведённых с пятью изображениями из базы данных, предложенный в данной главе алгоритм превосходит сравниваемые алгоритмы по своим показателям.

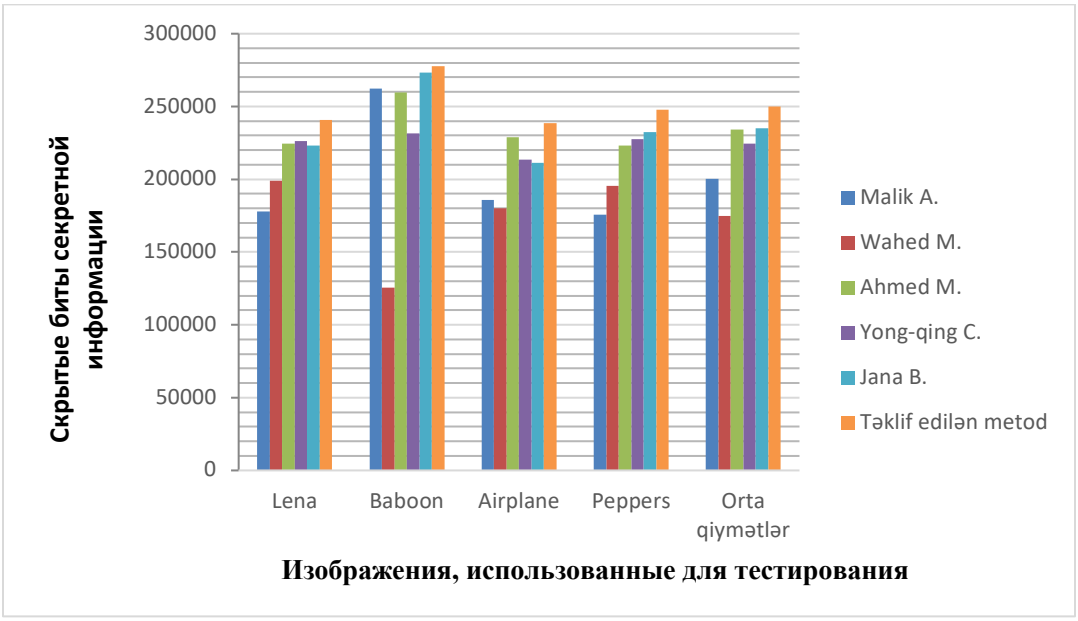

Рисунок 2. Зависимость количества скрытых битов секретной информации от различных изображений

На рисунке 2 показано, какое количество секретной информации может быть скрыто на различных изображениях с использованием предложенного алгоритма и алгоритмов, представленных в литературе. Из рисунка видно, что предложенный алгоритм обеспечивает сокрытие большего количества секретных битов по сравнению с другими сравниваемыми алгоритмами.

Исследование алгоритма с использованием гистограммного стегоанализа

Для проверки надёжности показателей алгоритма вновь использовались стандартные изображения, применяемые в алгоритмах сокрытия, в качестве исходных изображений. Гистограммы исходных изображений и соответствующих им стегоизображений приведены на рисунках 3 и 4. Из этих рисунков видно, что сравниваемые изображения в основном имеют одинаковые гистограммы. Это, в свою очередь, означает высокую степень сходства между сравниваемыми изображениями.

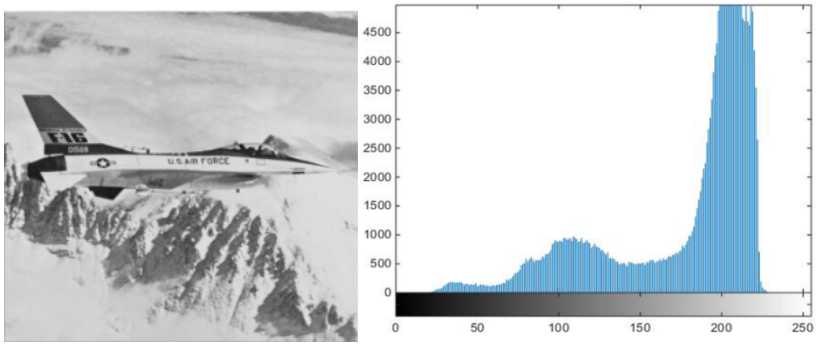

Рисунок 3. Изображение контейнера и его гистограмма

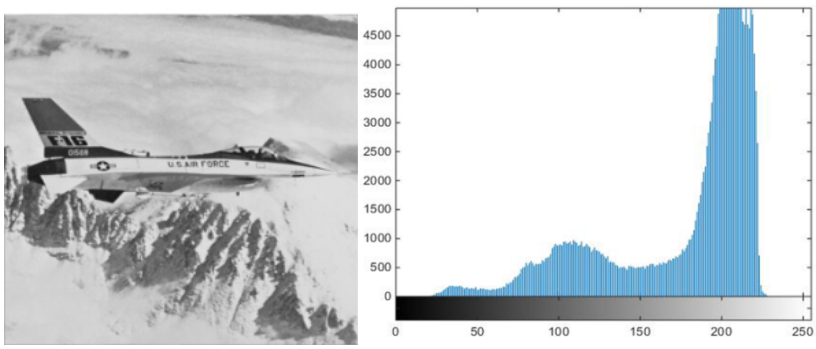

Рисунок 4. Стего-изображение и его гистограмма

Исследование предлагаемого алгоритма с помощью двоичного статистического стегоанализа.

Устойчивость предлагаемого алгоритма была проверена не только методом гистограммного стегоанализа, но и более широко — методом RS-стегоанализа.

Данный анализ использует чувствительную двоичную статистику, основанную на пространственной корреляции изображений. RS-стегоанализ применяется к 24-битным цветным и 8-битным оттенкам серого изображениям.

RS-стегоанализ используется для обнаружения наличия скрытой информации на основе замены наименее значимого бита в файлах изображений (методы вставки LSB). Этот вид стегоанализа был проведён следующим образом. Сначала к четырём исходным изображениям-контейнерам (Lena, baboon, airplane, peppers) был применён RS-стегоанализ, результаты которого приведены в таблице 2.

Таблица 2. RS-стегоанализ контейнерных изображений

Контейнерное изображение	$\lvert R_m - R_{-m} \rvert$ (dB)	$\lvert S_m - S_{-m} \rvert$ (dB)
Lena	0,0078	0,0088
Baboon	0,0057	0,0067
Airplane	0,0063	0,0065
Peppers	0,0093	0,0083

Далее для контейнерного изображения, после скрытия различного объёма секретных информационных битов (в этом случае контейнерное изображение становится стегоизображением) $\lvert R_m - R_{-m} \rvert$, были вычислены значения и $\lvert S_m - S_{-m} \rvert$, результаты представлены в таблице 3.

Таблица 3. Результаты RS-стегоанализа стегоизображений

стегоизображение	**RS-стегоанализ (дБ)**	**Объём скрытой секретной информации (байты)**			
		1000	5000	10000	15000
Lena	$\lvert R_m - R_{-m} \rvert$	0,0080	0,0087	0,0093	0,0099
	$\lvert S_m - S_{-m} \rvert$	0,0091	0,0095	0,0097	0,0099
Baboon	$\lvert R_m - R_{-m} \rvert$	0,0064	0,0079	0,0093	0,0052
	$\lvert S_m - S_{-m} \rvert$	0,0073	0,0163	0,0031	0,0043
Airplane	$\lvert R_m - R_{-m} \rvert$	0,0093	0,0095	0,0099	0,0103
	$\lvert S_m - S_{-m} \rvert$	0,0082	0,0086	0,0025	0,0026
Peppers	$\lvert R_m - R_{-m} \rvert$	0,0097	0,0098	0,0086	0,0093
	$\lvert S_m - S_{-m} \rvert$	0,0085	0,0085	0,0092	0,0098

В приведённой выше таблице полученные в результате RS-стегоанализа $|R_m - R_{-m}|$ и $|S_m - S_{-m}|$ различия, близкие к нулю, подтверждают устойчивость алгоритма.

Из результатов, приведённых в таблице 3, ясно, что при применении исследуемого алгоритма ни один стегоаналитик (злоумышленник) не сможет извлечь секретную информацию, скрытую с помощью данного алгоритма и известных на сегодняшний день алгоритмов стегоанализа. Это связано с тем, что показатели устойчивости, независимо от объёма скрытой секретной информации, спрятанной в различных изображениях, не превышают критический уровень и стабильно принимают значения, очень близкие к нулю.

Экспериментальное исследование вычислительной сложности алгоритма.

Важным аспектом является вычислительная сложность предлагаемого алгоритма, то есть время, затрачиваемое на выполнение всех процедур, используемых в алгоритме. Даже при высоких показателях устойчивости время вычислений считается одним из решающих параметров, и при выборе из двух или трёх алгоритмов предпочтение отдаётся тому, который требует меньше времени. Учитывая это, данный показатель был исследован экспериментально. Для экспериментов использовалась международная база изображений [5].

Для проверки вычислительной сложности алгоритма (времени выполнения) был проведён следующий эксперимент. Для этого использовалась программа MATLAB/R2014b. В различные контейнерные изображения была скрыта секретная информация, и измерялось время скрытия информации и её извлечения из полученного стегоизображения. В экспериментах использовались различные стандартные изображения, в которые скрывался секретный информационный объём различного размера.

Время измерялось как для процедуры скрытия, так и для процедуры извлечения информации из стегоизображения. Полученные результаты приведены в таблице 4.

Таблица 4. Время выполнения алгоритма

Контейнерное изображение	Объём секретной информации (байты)	Время скрытия информации (секунды)	Время извлечения информации (секунды)
Lena	5000	0,024	0,0204
	10000	0,029	0,0205
	15000	0,029	0,0209
Baboon	5000	0,027	0,0212
	10000	0,026	0,0211
	15000	0,0295	0,0230
	15000	0,0275	0,0232
Peppers	5000	0,0230	0,0213
	10000	0,0263	0,0233
	15000	0,0293	0,0252

Из результатов таблицы видно, что при выполнении обеих процедур время вычислений варьируется около 0,02 секунды и не достигает 0,03 секунды. Это меньше, чем время выполнения алгоритмов, приведённых в литературе, и может считаться хорошим показателем. Наблюдаются определённые различия от изображения к изображению, однако это приемлемо, поскольку структура и характеристики используемых изображений различны. Аналогичная ситуация наблюдается и в зависимости от объёма скрываемой информации.

Таблица 5. Сравнение времени выполнения предлагаемого алгоритма с другими алгоритмами

Изображения	**Время выполнения алгоритма (сек)**	**Malik A., Sikka G.** . [4, s. 2454-7190], **2018**	**Wahed M.A., Nyeem, H** [6, s. 10795-10819], **2019**	**Ahmad A.M., [1. s. 7181-7205], 2019**	**Yong-qing C.** **[2, s. 271 - 350]** **2020**	**Jana B., Giri D.,** **[3, s.239-248]** **2015**	**Предлагаемый алгоритм**
Lena	Скрытие информации	0,031	0,038	0,036	0,033	0,039	0,029
	Извлечение информации	0,031	0,04	0,0039	0,035	0,036	0,021
Baboon	Скрытие информации	0,042	0,046	0,039	0,035	0,041	0,026
	Извлечение информации	0,042	0,043	0,037	0,034	0,039	0,021
Airplane	Скрытие информации	0,037	0,029	0,041	0,038	0,039	0,026
	Извлечение информации	0,037	0,025	0,039	0,035	0,034	0,027
Peppers	Скрытие информации	0,042	0,033	0,036	0,037	0,048	0,028
	Извлечение информации	0,034	0,031	0,033	0,035	0,046	0,023

Результаты, приведённые в таблице 5, показывают, что время выполнения каждого алгоритма и используемого контейнерного изображения различается. Например, максимальное время скрытия информации на этапе вставки в изображение Papper, согласно [3, с. 239-248], достигает 0,048 секунды. Для того же изображения, применяя предлагаемый алгоритм, этот показатель составляет всего 0,028 секунды. Максимальное время извлечения информации равно 0,046 секунды, и опять же максимальное значение наблюдается для изображения Papper, тогда как в работе других авторов время

извлечения секретной информации для изображения Airplane равно 0,034 секунды.

Вывод

В целом, учитывая средние значения, можно отметить, что время вычислений, отражающее вычислительную сложность предлагаемого алгоритма, является минимальным, независимо от алгоритмов, процедур и изображений.

К показателям качества стегоалгоритмов можно добавить время работы алгоритма. Предлагаемый алгоритм требует минимального времени для реализации, что наглядно подтверждается результатами, приведёнными в таблицах 4 и 5.

В данной работе представлен новый стеганографический алгоритм скрытия информации в цифровых изображениях. Обычно авторы используют методы интерполяции для улучшения визуального качества изображения. В отличие от них, в предложенном алгоритме применяется метод определения и использования минимального бита пикселя для скрытия секретной информации.

Список литературы:

1. Ahmad, A. M., Al-Haj, A., Mahmoud, F. An improved capacity data hiding technique based on image interpolation // Multimedia Tools and Applications, Springer, 2019. № 78, pp. 7181-7205.
2. Chen, Y., An efficient general data hiding scheme based on image interpolation / W. Sun, L. Li, X. Chang, C. Wang // Journal of Information Security and Applications, 2020. № 54, pp. 271-350.
3. Jana, B., Giri, D., Mondal, S. K. Weighted Matrix based Reversible Data Hiding Scheme using Image Interpolation // Computational Intelligence in Data Mining, Springer, 2015. № 2, pp. 239-248.

4. Malik, A., Sikka, G., Verm, H. K. Image interpolation based high capacity reversible data hiding scheme // Multimedia Tools Application, 2018. № 76, pp. 2454-7190.
5. Skrypnyk, I., Lowe, D. G. Scene Modelling, Recognition and Tracking with Invariant Image Features // Third IEEE and ACM International Symposium on Mixed and Augmented Reality, Arlington, VA, USA, IEEE, 05 November 2004, pp. 110-119.
6. Wahed, M. A., Nyeem, H. Reversible data hiding with interpolation and adaptive embedding // Multimedia Tools and Applications, 2019. 78(3), pp. 10795-10819.

Experimental study of the algorithm for hiding secret information based on the least significant bit substitution method

Ababil Naghiyeva

Azerbaijan University of Technology

ababil.nagiyeva@mail.ru

Abstract: This article presents experimental results of the proposed algorithm for hiding secret information based on the least significant bit substitution method. This algorithm allows to increase the number of secret information bits to be hidden while maintaining the visual similarity between the stego-image and the container image. A digital image was used as the input image in the implementation of the algorithm.

Keywords: Stego-image, LSB, secret information, steganography, image steganography