ОБРАБОТКА ИЗОБРАЖЕНИЙ, РАСПОЗНАВАНИЕ ОБРАЗОВ

Реверсивный стеганографический метод сокрытия информации, основанный на интерполяции изображений

А.Ф. Нагиева [1], С.Г. Вердиев [1]
[1] Азербайджанский технологический университет, AZ2011, Азербайджан, г. Гянджа, пр. Хатаи, 103

Аннотация

Обмен информацией посредством открытых компьютерных и коммуникационных сетей подвержен вероятному перехвату передаваемой информации третьей стороной. Для предотвращения этого разработаны и применяются различные методы защиты информации. В настоящей работе поставлена и решена задача разработки нового стенографического реверсивного метода сокрытия информации, основанного на интерполяции изображения. Разработанный алгоритм обладает более высоким объёмом внедряемой секретной информации при одновременном сохранении высокого визуального качества изображения со встроенной информацией. Результаты экспериментальных исследований, приведённые в статье, подтверждают вышесказанное.

Ключевые слова: защита информации, стеганография, интерполяция изображения, сокрытие данных, большой объём внедрения.

Цитирование: **Нагиева, А.Ф.** Реверсивный стеганографический метод сокрытия информации, основанный на интерполяции изображений/ А.Ф. Нагиева, С.Г. Вердиев //Компьютерная оптика. – 2022. – Т 46, №3. – С.465-472. – DOI: 10.18287/2412-6179-CO-1019.

Citation: Nagiyeva AF,Verdiyev SG. Reversible steganographic method of hiding information based on image interpolation. Computer Optics 2022; 46(3): 465-472. DOI: 10.18287/2412-6179-CO-1019.

Введение

В последнее десятилетие методы сокрытия данных превратились в важное направление исследований в области информационных технологий. Широкое распространение Интернета и развитие цифровой коммуникации породили проблему обеспечения безопасности передачи информации по открытым каналам связи. Для решения проблемы были разработаны новые методы безопасности секретной коммуникации. Параллельно с развитием цифровой техники получила развитие и цифровая стеганография – наука о сокрытии информации [8, 9, 11, 12].

Обычно секретная информация внедряется в такие цифровые носители, как цифровые файлы, изображения, видео, тексты, аудио, которые передаются по открытым каналам связи без предварительной шифровки. Стеганография успешно применяется в различных направлениях, таких как медицина, военное дело, надзор над сохранением авторских прав на используемые материалы и циркуляция секретных данных и т.д. По типу решения задачи различают алгоритмы встраивания и извлечения секретных данных.

Наиболее популярным является стеганография изображения, в котором информация внедряется в изображение-контейнер. Термин «контейнер» означает цифровое медиа, используемое для внедрения секретного сообщения. Внедряемая информация называется «секретное сообщение». Изображение, в которое уже внедрено секретное сообщение, называется «изображение со встроенной информацией». Для внедрения секретного сообщения в контейнер разработано множество процедур и алгоритмов, отличающихся своими показателями. Изображение со встроенной информацией, передаваясь по открытым каналам связи, доходит до получателя и подлежит извлечению из него секретного сообщения. Для этой цели разрабатываются и используются соответствующие методы и алгоритмы [12 – 16]. Все методы и алгоритмы характеризуются следующими характеристиками:

- Объём внедрения – это максимально возможная величина внедрения.
- Визуальное качество изображения – это то, насколько изображение со встроенной информацией идентично пустому изображению.
- Безопасность алгоритма – это способность изображения со встроенной информацией противостоять всевозможным атакам, направленным на обнаружение секретного сообщения.

Все разработанные алгоритмы отличаются друг от друга по области внедрения даты в изображение, типу контейнера и методу внедрения. Таким образом, идеальный стеганографический метод должен обладать максимальным объёмом внедрения, высоким визуальном качеством. Недостатком стеганографических методов является относительно низкий объём внедряемой даты и вызванные этим внедрением искажения исходного изображения. В свете сказанного

в этой области есть ещё много проблем, требующих своего решения. Вышеупомянутое вдохновляет сообщество исследователей на разработку новых стеганографических технологий для передачи секретных сообщений и более безопасного обмена секретными данными.

Схожие работы

В стеганографии изображения для повышения качества контейнера, т.е. увеличения его разрешения, используется метод интерполяции. В 2009 году Jung и Yoo [2] предложили использование этого метода в стеганографии изображений. Суть этого метода заключается в уменьшении исходного изображения размером M × N до двух изображений размером

$$\left(\frac{M}{2}+1\right)\times\left(\frac{N}{2}+1\right).$$

Метод Jung состоит из двух основных шагов: интерполяции изображения и сокрытия секретных данных. На первом этапе исходное изображение делится на блоки 3 × 3, а затем расширяется до первоначального размера с использованием алгоритма интерполяции. На втором этапе секретная дата вставляется в сгенерированный на первом этапе контейнер с использованием алгоритма сокрытия секретных данных. Процесс сокрытия информации реализуется по схеме (рис. 1).

Используя метод NMI (Neıgnbour Mean Interpolation), сокращённые изображения преобразуются в контейнер размером M × N. Затем это изображение делится на несколько блоков. Контейнер и пиксели каждого из его блоков, за исключением первого, могут быть использованы для внедрения информации. Объём внедрения в каждый пиксель зависит от разницы между этим и первым. Для увеличения объёма внедрения метод интерполяции комбинируется с методом LSB.

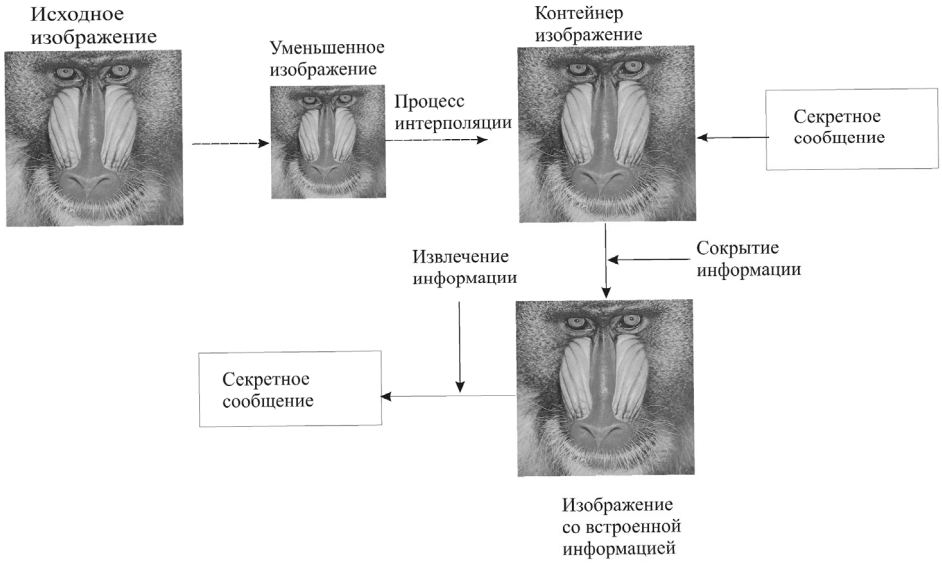


Рис. 1. Схема сокрытия информации

Впоследствии были разработаны несколько разновидностей метода интерполяции изображения, которые в настоящее время применяются в стеганографии. В литературе описаны наиболее успешные методы: NMI (Neighbor Mean Interpolation) [2], INP (Interpolation by Neighboring Pixel [3] и NIE (New Interpolation Expansion) [1]. Все эти методы направлены на разработку новых методов интерполяции и являются модификациями метода Jung. Несмотря на некоторые преимущества, после внедрения секретной даты качество изображения со встроенной информацией становится хуже, чем качество интерполированного изображения. В работе [3] контейнер разделён на блоки 2 × 2, четыре соседних пикселя используются для определения максимального значения четырёх соседних пикселей каждого блока, которые, в свою очередь, используются для вычисления наибольшей разницы между готовыми к внедрению пикселями. Однако несмотря на увеличение объёма внедрения, качество изображения снижается. Sabeen Govind и др. [5] разработали двухэтапную схему сокрытия данных, обеспечивающую большой объём внедрения. На первой стадии интерполяции исходное цифровое изображение превращается в изображение-контейнер с использованием техники ENMI (Enhansed Neighbour Mean Interpolation) алгоритма. Разницы между значениями исходного изображения и контейнера складываются, а полученная сумма делится на число слагаемых. Полученный результат записывается в среднюю ячейку блока контейнера. Однако несмотря на более высокое значение объёма внедрения, визуальное качество изображения со встроенной информацией не слишком высокое, а сам алгоритм сложен для вычислений. Ahmad. A. Mohammad и др., преследуя цель повышения объёма внедрения и качества изображения, достигнутые в работе Jung, разработали новый метод сокрытия данных, основанный на интерполяции изображения, для обеспечения высокого объёма

внедрения. Декларируется, что предлагаемый метод отличается относительной простотой расчетов. Другим достижением является весьма малое искажение изображения. Эти искажения при использовании методов интерполяции возникают на этапах уменьшения и увеличения размеров изображения и сокрытия данных. Для уменьшения искажений изображения при вышеприведённых процедурах разработан алгоритм интерполяции изображений. Но следовало бы отметить, что их метод фактически был модификаций метода Junga.

Jana B.I. и др. [4] предложили новый реверсивный метод сокрытия данных, основанный на методе Weight matrix и отличающийся большим объёмом внедряемой даты. Согласно этому методу исходное изображение размером M (высота), N (ширина) увеличивается дважды путём интерполяций. В результате с использованием разработанных авторами специальных преобразований получается изображение с высотой (2XM-1) и шириной (2XN-1). Затем исходное изображение делится на блоки (3 × 3), а изображение-контейнер – на блоки (5 × 5). Секретная информация внедряется в вычисленную позицию блока изображения-контейнера с (5 × 5). Этим путём достигается большой объём внедрения и реверсивность алгоритма. Однако несмотря на теоретические преимущества, сложность алгоритма усложняет его вычислительные способности, что, в свою очередь, ограничивает практическое использование метода.

Предлагаемый метод сокрытия даты

В этом параграфе предлагается новый реверсивный метод сокрытия секретной информации, основанный на интерполяции изображения.

Преимуществом метода является обеспечение большого объёма внедряемых секретных бит при более высоких значениях визуального качества изображения со встроенной информацией.

Предлагаемый метод сокрытия информации реализуется по схеме сокрытия информации (рис. 1.), который, в свою очередь, состоит из следующих этапов:

- уменьшение изображения;
- расширение изображения;
- сокрытие информации;
- извлечение информации.

Реверсивность достигается по отношению к «уменьшенному изображению», но не к исходному полноразмерному.

Поэтапное выполнение операций по цифровой реализации метода и обработке изображений, в которые внедряются секретные биты, приводится ниже.

Последовательность шагов на этапе внедрения.

Шаг 1. Оригинальное изображение, разделяясь на блоки 3 × 3, подвергается интерполяции. Для этой цели используется формула (1).

$$\begin{aligned} &C(0,0)=O(0,0),\\ &C(0,1)=\big(C(0,0)+C(0,2)\big)/3+\big(C(2,0)+C(2,2)\big)/6,\\ &C(1,0)=\big(C(0,0)+C(2,0)\big)/3+\big(C(0,2)+C(2,2)\big)/6,\\ &C(1,1)=\big(C(0,0)+C(0,2)+C(2,0)+C(2,2)\big)/4. \end{aligned} \quad (1)$$

Шаг 2. Путём интерполяции генерируется контейнер. Полученное изображение делится на блоки 2 × 2. В предлагаемом алгоритме сокрытия информации пиксели, находящиеся в верхней правой части блока, в нижней части слева и в нижней части справа, пригодны для внедрения секретного сообщения. Используя координаты (2), обозначим пиксели блоков как d_1, d_2, d_3:

$$\begin{aligned} &d_1 = ma\big(\big|C_1(0,1)-C_1(0,0)\big|,\big|C_1(0,1)-C_2(0,0)\big|\big),\\ &d_2 = ma\big(\big|C_1(1,0)-C_1(0,0)\big|,\big|C_1(1,0)-C_3(0,0)\big|\big),\\ &d_3 = ma(\big|C_1(1,1)-C_1(0,0)\big|,\big|C_1(1,1)-C_2(0,0)\big|,\\ &\big|C_1(1,1)-C_3(0,0)\big|,\big|C_1(1,1)-C_4(0,0)\big|). \end{aligned} \quad (2)$$

Шаг 3. После нахождения трёх значений разниц для определения количества секретных бит, подлежащих внедрению в каждый пиксель, десятичные значения результатов, полученных от вычислений по формуле (2), переводятся в двоичную систему. В цифровом ряде, полученном от этого системного преобразования, количество бит равняется количеству бит, подлежащих внедрению.

Шаг 4. Если принять секретную дату как b_1, b_2, b_3, то они могут быть внедрены с помощью (3):

$$\begin{aligned} &S_1(0,1)=\begin{cases} C_1(0,1)+b_1,\ if\ C_1(0,1)\le O_1(0,1),\\ C_1(0,1)-b_1,\ иначе; \end{cases}\\ &S_2(1,0)=\begin{cases} C_1(1,0)+b_2,\ if\ C_1(1,0)\le O_1(1,0),\\ C_1(1,0)-b_2\ иначе; \end{cases}\\ &S_3(1,1)=\begin{cases} C_1(1,1)+b_3, if\ C_1(1,1)\le O_1(1,1),\\ C_1(1,1)-b_3\ иначе. \end{cases} \end{aligned} \quad (3)$$

Здесь $C(i,j)$ представляет собой пиксели контейнера, а с $S(i,j)$ являются пикселями изображения со встроенной информацией, в которые внедрена секретная дата.

Полученные пиксели выглядят как на рис. 2.

а)

C(0,0)	C(0,1)
C(1,0)	C(1,1)

б)

S(0,0)	S(0,1)
S(1,0)	S(1,1)

Рис. 2. Блоки: контейнера (а) и изображения со встроенной информацией (б)

Сравнивая пиксели контейнера и изображения со встроенной информацией, заметим, что изменения в

пикселях незначительны. При замене процедуры логарифмирования преобразованием десятичной системы в двоичную, количество бит секретной даты становится больше, что, в свою очередь, означает увеличение объёма внедрения. Кроме того, из-за уменьшения изменений в пикселях значение PSNR получается высоким.

Цифровой пример встраивания

Исходное изображение путём интерполяции по формуле (1) преобразуется в контейнер. По формуле (2) вычисляются разницы d_1, d_2, d_3.

Найденные десятичные значения разниц между пикселями переводятся в двоичную систему исчисления

$$\begin{aligned} n_1 &= 7 = 111, \\ n_2 &= 6 = 110, \\ n_3 &= 16 = 10000. \end{aligned} \tag{4}$$

После перевода значений d в двоичную систему выбираются биты секретной даты, количество которых равняется количеству нулей (0) и единиц (1) двоичных чисел. Например, если заданы биты секретной даты $b_1 = 11001100111100011$, то при $n_1 = 7 = 111$ первые 3 бита секретной даты $b_1 = 110$. После перевода этого значения в десятичную систему исчисления $b_1 = 6$. На очередном этапе сравниваются пиксели контейнера и изображения со встроенной информацией.

Если пиксели контейнера меньше, чем пиксели исходного изображения, то выбранные секретные биты добавляются к пикселю контейнера. В противном случае выбранные секретные биты вычитаются из пикселя контейнера. Таким образом, уменьшается разница между контейнером и изображением со встроенной информацией. А это означает повышение PSNR.

$$\begin{aligned} S_1 &= 75 + 6 = 81, \\ S_2 &= 75 + 3 = 78, \\ S_3 &= 77 + 7 = 84. \end{aligned} \tag{5}$$

Таким образом, формируются пиксели изображения со встроенной информацией.

73	81
78	84

Рис. 3. Пиксели блока изображения со встроенной информацией

Если сравнить пиксели контейнера и изображения со встроенной информацией, заметим, что разница между пикселями очень небольшая. В результате замены процедуры логарифмирования на процедуру перевода разницы значений пикселей контейнера n из десятичной системы в двоичную количество бит секретной даты, подлежащих внедрению в ковер-изображение, возрастает. Это, в свою очередь, означает увеличение объёма внедрения секретной даты и является преимуществом предлагаемой схемы по сравнению с другими методами, что и является основной задачей настоящего исследования.

Шаги фазы извлечения

Алгоритм извлечения секретного сообщения из изображения со встроенной информацией, будучи противоположностью алгоритма внедрения, используется для выделения скрытой даты и восстановления исходного изображения.

Шаг 1. Изображение со встроенной информацией делится на блоки 2×2, а интерполированное изображение-контейнер вновь восстанавливается. Полученные результаты используются для извлечения секретного сообщения.

а)

C(1,1)	C(1,2)	C(1,3)
C(2,1)	C(2,2)	C(2,3)
C(3,1)	C(3,2)	C(3,3)

б)

S(1,1)	S(1,2)
S(2,1)	S(2,2)

Рис. 4. Блоки: контейнера (а) и изображения со встроенной информацией (б)

Затем из пикселей изображения со встроенной информацией вычитаются пиксели изображения-контейнера.

$$\begin{aligned} De1 &= C(1,2) - S(1,2), \\ De2 &= C(2,1) - S(2,1), \\ De3 &= C(2,2) - S(2,2). \end{aligned} \tag{6}$$

Из полученных значений разниц изображения со встроенной информацией и контейнера восстанавливаются биты секретной даты.

Цифровой пример фазы извлечения

Изображение со встроенной информацией делится на блоки 2×2, а интерполированное изображение-контейнер вновь восстанавливается и используется в процессе извлечения.

а)

73	75	70
5	77	93
71		

б)

73	81
78	84

Рис. 5. Блоки: интерполированного изображения (а) и изображения со встроенной информацией (б) Из пикселей изображения со встроенной информацией вычисляются пиксели контейнера

$$\begin{aligned} 81 - 75 &= 6 = 110, \\ 78 - 75 &= 3 = 11, \\ 84 - 77 &= 7 = 111. \end{aligned}$$

Из полученных значений вычисленных разниц формируются биты секретных данных, которые передаются по открытому каналу связи.

Результаты экспериментальных исследований

С целью проверки достоверности полученных результатов исследования были проведены эксперименты на стандартных серых снимках размером 512×512, взятых из базы данных изображений USC-SIPI, 8 из которых показаны на рис. 2. Эксперименты были проведены с использованием MATLAB \ R2014b.

Для оценки качества изображения со встроенной информацией использовалась метрика RSNR, значение которой вычислялось методом Peak Signal to Noise Ratio (RSNR) по формуле:

$$PSNR = 10\log_{10}\left[\frac{255\times 255}{\frac{1}{P*Q}\sum_{n-1}^{P}\left[CI(m,n)-SI(m,n)\right]^2}\right], \quad (7)$$

которая определяет степень схожести двух сравниваемых снимков. Зрительная система человека не способна улавливать разницу свыше 36 dB. Значение PSNR прямо связано с визуальным качеством изображения со встроенной информацией. Чем больше его значение, тем больше сходство сравниваемых изображений. *P* и *Q* обозначают размер изображения, а *CI* и *SI* – вид изображения. Заранее отметим высокие средние значения показателей тестированных изображений, которые равняются по сокрытию данных – 435202; PSNR – 38,8096.

Затем рассчитывались величины PNSR между контейнером и изображением со встроенной информацией, которые приводятся в табл. 1. В таблице приведены данные сравнения PSNR предлагаемого метода с новыми методами, разработанными в последние годы.

Табл. 1. Сравнение показателей алгоритмов

Исходное изображение	Метрики	Yong-qing Chen и др.[17]	Malik A.и др. [18]	Предлагаемый метод
Lena	PSNR Capacity	34,18 369,715	31,93 144,887	38,56 564,744
Baboon	PSNR Capacity	24,69 651,710	22,85 187,141	36,47 546,791
Airplane	PSNR Capacity	32,84 334,328	30,26 151,269	35,88 524,719
Peppers	PSNR Capacity	32,82 374,589	30,42 144,177	39,32 656,611
Sailboat	PSNR Capacity	31,80 364,589	29,04 175,183	33,36 378,123
Boat	PSNR Capacity	29,82 343,589	32,22 124,236	35,93 369,563
Couple	PSNR Capacity	26,82 381,589	24,36 354,137	29,68 400,021
House	PSNR Capacity	32,02 236,589	31,32 235,325	36,21 282,753
Средние значения	PSNR Ёмкость встраивания	30,26 382,087	29,05 189,544	35,60 465,415

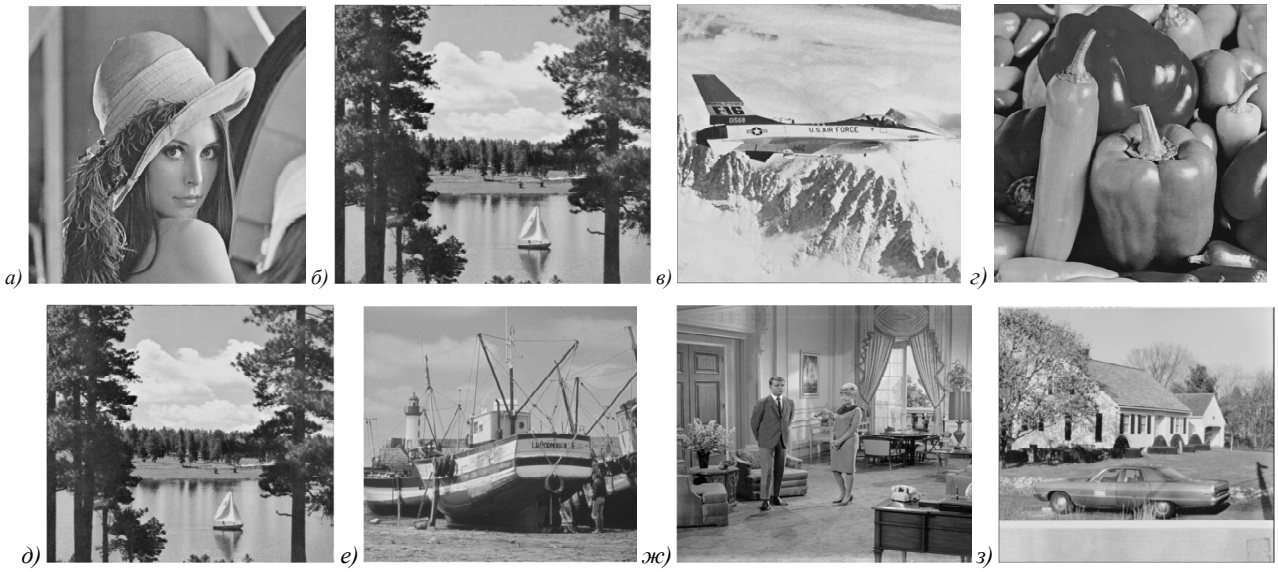


Рис. 6. Контрольные изображения

Более высокие значения PSNR и объёма внедрения указывают на превосходство предлагаемого метода над другими сравниваемыми. Все изображения имеют PSNR свыше 36 dB, что говорит о том, что неизбежные и связанные с внедрением секретных данных искажения остаются незаметными для человеческого глаза. Кроме PSNR, для получения более точных результатов сравнения исходного и изображений со встроенной информацией нами был использован также графический метод гистограмм.

В табл. 2 приведены гистограммы исходных и соответствующих им изображений со встроенной информацией. Из таблицы видно, что все сравниваемые изображения имеют почти одинаковые гистограммы. Это свидетельствует о высокой степени идентичности сравниваемых изображений, из-за чего обнаружение наличия секретной информации становится невозможным.

Табл. 2. Гистограммы сравниваемых изображений

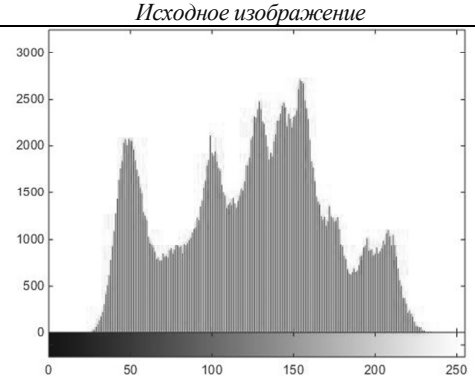
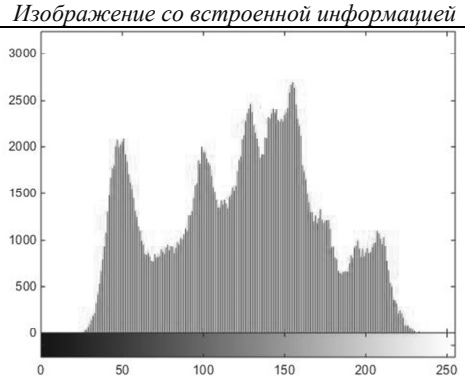
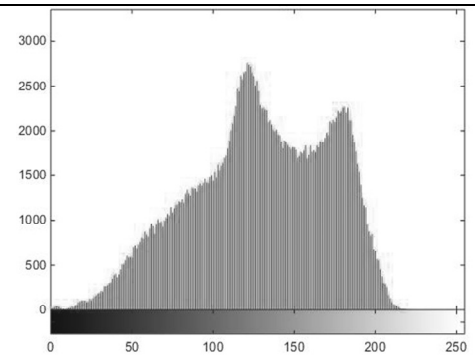
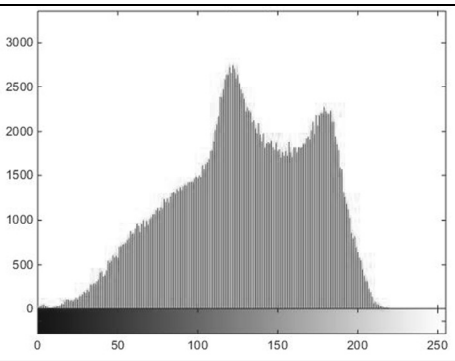
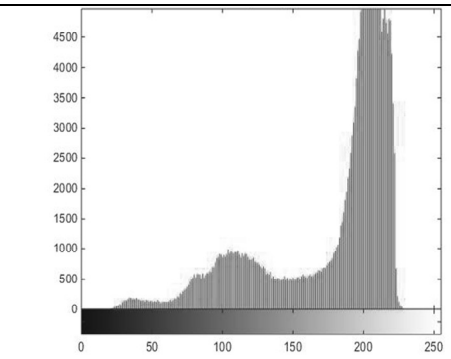
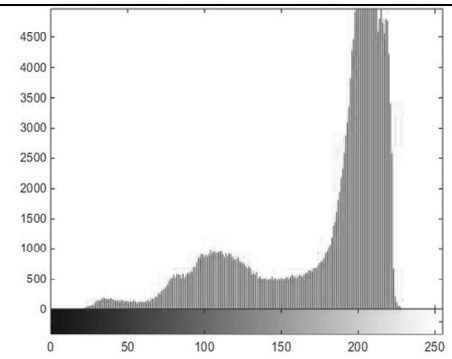
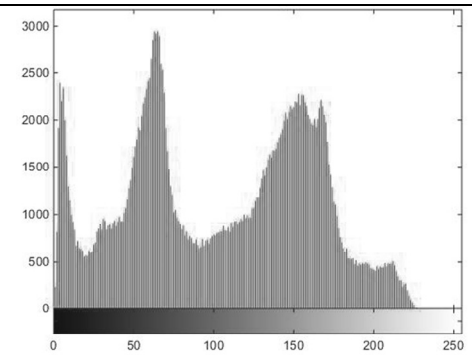
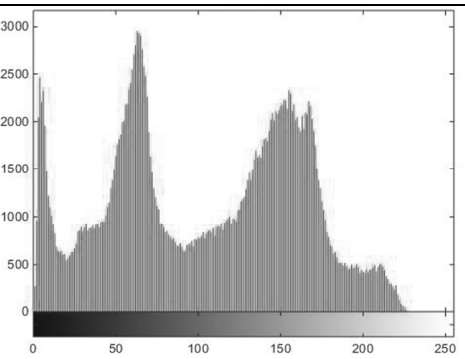
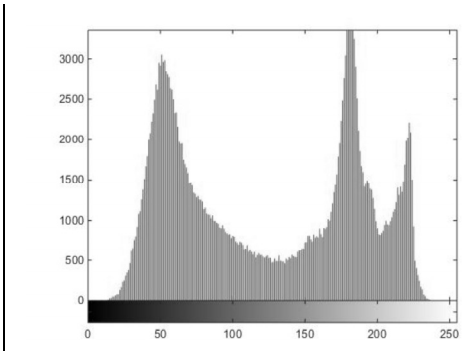
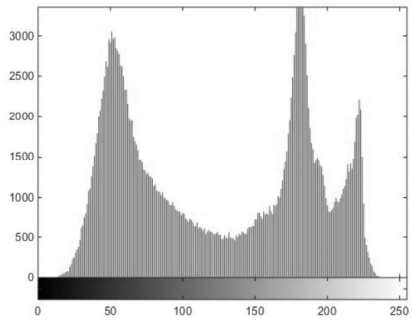
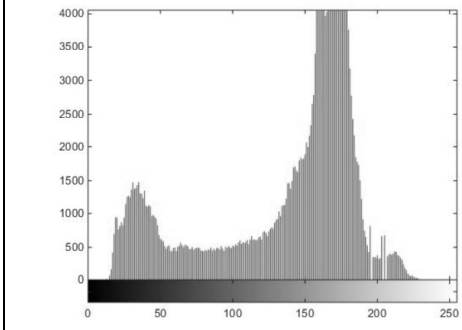
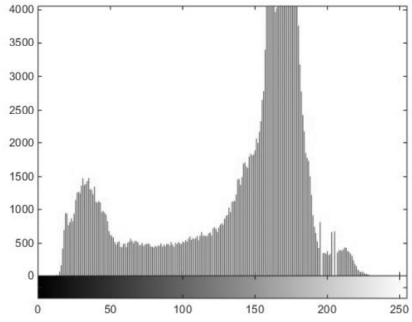
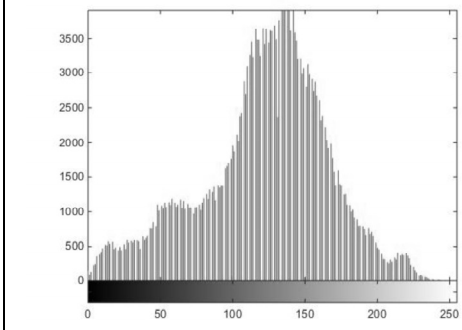
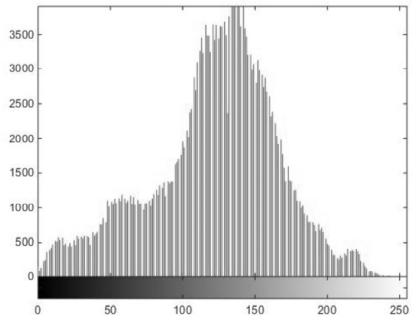
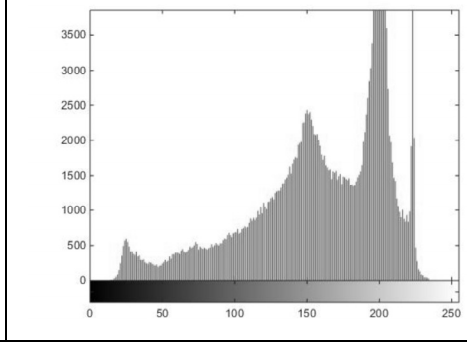
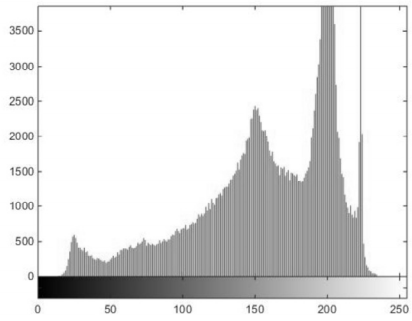
Изображение	*Исходное изображение*	*Изображение со встроенной информацией*
(а)		
(б)		
в)		
г)		

Табл. 2. Гистограммы сравниваемых изображений (продолжение)

д)		
е)		
ж)		
з)		

Заключение

Предложен реверсивный метод сокрытия секретных данных, отличающийся большим объёмом внедрения секретной информации. Разработанный алгоритм основан на концепции интерполяции изображений. Известно, что высокое качество изображения и объём скрываемой информации прямо противоположны друг другу. Целью настоящей работы была разработка алгоритма, отличающегося большим объёмом внедряемой информации при сохранении высокого качества изображения со встроенной информацией. Это было достигнуто путём использования нового механизма внедрения, путём замены процедуры логарифмирования процедурой перевода данных из десятеричной системы исчисления в двоичную. Эффективность предлагаемого метода была доказана экспериментальными исследованиями, проведённы-

ми на множестве контрольных изображений. Сходство сравниваемых, исходных и изображений со встроенной информацией подтверждалось методами RSNR и гистограмм.

Высокие значения визуального качества изображений не менялись в зависимости от объёма внедрения и вида контрольных изображений. Из сказанного выше можно заключить, что предлагаемый нами реверсивный метод сокрытия информации обеспечивает лучшее визуальное качество изображения со встроенной информацией и более высокий объём сокрытой даты по сравнению с другими приведёнными в литературе.

References

[1] Ahmad AM, Ali AH, Mahmoud F. An improved capacity data hiding technique based on image interpolation. Multimed Tools Appl 2019; 78(6): 7181-7205.

[2] Jung KH, Yoo KY. Data hiding method using image interpolation. Comput Stand Interfaces 2009; 31(2): 465-470.

[3] Lee C-F, Huang Y-L. An efficient image interpolation increasing payload in reversible data hiding. Expert Syst Appl 2012; 39(8): 6712-6719.

[4] Jana B. High payload reversible data hiding scheme using weighted matrix. Optik 2016; 127(3): 3347-3358.

[5] Sabeen PV, Sajila MK, Bindiya MV. A two stage data hiding scheme with high capacity based on interpolation and difference expansion. Procedia Technology 2016; 24(2): 1311-1316.

[6] Chen Y-q, Sun W-j, Li L-y, Chang C-C, Wang X. An effcient general data hiding scheme based on image. J Inf Secur Appl 2020; 54(4): 214-228.

[7] Witten IH, Neal RM, Cleary JG. Arithmetic coding for data compression. Common ACM 1987; 30(6): 520-540.

[8] Abbas C, Joan C, Kevi C, Paul K. Digital image steganography: Survey and analysis of current methods. Signal Process 2010; 90(3): 727-752. DOI: 10.1016/j.sigpro.2009.08.010.

[9] Mehdi H, Ainuddin WAW, Yamani IBI, Jung KH. Image steganography in spatial domain: A survey. Signal Process Image Commun 2018; 65: 46-66. DOI: 10.1016/j.image.2018.03.012.

[10] Sabeen GPV, Judy MV. A secure framework for remote diagnosis in health care: A high capacity reversible data hiding technique for medical images. Comput Electr Eng 2020; 89(25): 300-314.

[11] Niels P, Peter H. Hide and Seek: an introduction to steganography. IEEE Secur Priv 2003; 99(5): 32-44.

[12] Kriti DN, Dabahdeh DS. A survey on image steganography & its techniques in spatial & frequency domain. Int J Recent Innov Trends Comput Commun 2014; 3(2): 776-779.

[13] Bin Li, Janhui H, Jiwu H, Yun QS. A Survey on Image Steganography and steqanalysis. J Inf Hiding Multimedia Signal Process 2011; 2(2): 142-172.

[14] Nazinder K, Amanjot K. Art of steganography. Int J Adv Trends Comput Appl 2017; 4(2): 30-33.

[15] Neil FJ, Stefan CK. A survey of steganography techniques. In Book: Katzenbeisser S, Petitcolas FA, eds. Information hiding techniques for steganography and digital watermarking. Ch 3. Norwood: Artech House Inc; 1999: 43-78.

[16] Naghiyeva A, Akbarzadeh K, Verdiyev S. New steganography method of reversible data hiding with priority to visual quality of image. 2nd Int Conf on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS) 2021: 329-333.

[17] Chen Y, Sun W, Li L, Chang C, Wang X. An efficient general data hiding scheme based on image interpolation. J Inf Secur Appl 2020; 54(6): 271-350.

[18] Malik A, Sikka G, Verma HK. Image Interpolation based hight capacity reversible data hiding scheme. Multimed Tools Appl 2017; 76(22): 24107-24123.

Сведения об авторах

Нагиева Абабил Фахраддин гызы, 1993 года рождения, в 2014-м году окончила Азербайджанский государственный аграрный университет по специальности «Инженерия информационных технологий и систем. Является докторантом кафедры компьютерной инженерии и телекоммуникации Азербайджанского технологического университета. Область научных интересов: защита информации, стеганография.
E-mail: *nagiyevaababil@gmail.com* .

Вердиев Сакит Гамбай оглы, 1945 года рождения, окончил Азербайджанский государственный аграрный университет по специальности «Электрификация с/х». Работает зав. кафедрой компьютерной инженерии и телекоммуникации Азербайджанского технологического университета. Область научных интересов, защита информации, стеганография. E-mail: *info_tel@inbox.ru* .

ГРНТИ: 81.93.29
Поступила в редакцию 30 июля 2021 г. Окончательный вариант – 17 марта 2022 г.

Reversible steganographic method of hiding information based on image interpolation

A.F. Naghiyeva [1], S.G.Verdiyev [1]
[1] Azerbaijan Technological University, AZ2011, Azerbaijan, Ganja, Khatai ave., 103

Abstract

When information is exchanged through open communication networks, there is a possibility of third-party interception. Various methods of data protection have been developed and applied to eliminate this flaw. In this work, a task of developing a new reversible steganographic method of concealing information based on interpolation of an image is set and solved. The developed algorithm has a higher payload of secret information while preserving the high visual quality of the stego image. Results of the pilot studies confirm this and are presented in this article.

Keywords: information security, steganography, image interpolation, data hiding, high capacity of embedding.

Citation: Nagiyeva AF,Verdiyev SG. Reversible steganographic method of hiding information based on image interpolation. Computer Optics 2022; 46(3): 465-472. DOI: 10.18287/2412-6179-CO-1019.

Authors' information

Ababil Faxraddin gizi Naghiyeva (b. 1993), graduated from Azerbaijan State Agrarian University in 2014, majoring in Information Systems and Technologies and Azerbaijan State Pedagogical University in 2016, majoring in Computer Science. Currently she works as the doctoral student of PhD. Computer Engineering and Telecommunication department of Azerbaijan Technological University. Research interests are information security, data hiding, image steganography. E-mail: *nagiyevaababil@gmail.com* .

Sakit Gambai oglu Verdiyev (b. 1945), graduated from Azerbaijan State Agrarian University in 1968, majoring in Electronic Engineering. Currently he works as the head of Computer Engineering and Telecommunication department of Azerbaijan Technological University. Research interests are information security, steganography.
E-mail: *info_tel@inbox.ru* .

Received July 30, 2021. The final version – March 17, 2022.