УДК 004.056

МЕТОД ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКОГО ХАОСА

А.В. Сидоренко, И.В. Шакинко

Предложен метод встраивания цифровых водяных знаков в изображения на основе динамического хаоса. Тестирование предлагаемого алгоритма показало его стойкость к атакам копирования, потере фрагмента изображения, наличию шумов в канале связи, что свидетельствует о возможности его применения в реальных задачах, связанных с защитой авторских прав.

Введение

На современном этапе развития информационных технологий особое место занимает область защиты информации. При этом достаточно важными являются вопросы защиты авторских прав, связанные с мультимедиа файлами. Одним из подходов, используемым для этого, является применение цифровых водяных знаков [1]. Например, для изображений существуют разнообразные схемы встраивания цифровых водяных знаков [2]. И в то же время, постоянно разрабатываются новые типы атак, большинство из которых направлены на уничтожение цифрового водяного знака, присутствующего в изображении. Особое место занимает атака копирования, целью которой является копирование цифрового водяного знака из одного изображения и добавления его к другому [3]. Это может привести к неработоспособности протоколов, использующих цифровые водяные знаки для решения задач идентификации. Для того, что бы повысить стойкость цифрового водяного знака к данному типу атак, предлагается осуществлять его формирование с учетом изображения, в которое он встраивается [3]. Однако, в результате наличия помех в канале связи, часть информации об исходном изображении может быть утеряна либо искажена. Это может привести к невозможности обнаружения цифрового водяного знака в изображении.

В данной работе предложен метод встраивания цифровых водяных знаков в изображения, стойкий к атакам копирования и учитывающий возможность искажений изображения в канале связи.

Восстановление начальных условий

В основе предлагаемого алгоритма встраивания цифровых водяных знаков в изображения положена возможность нахождения таких начальных условий, при использовании которых формируемая последовательность значений с использованием хаотических отображений совпадает с наблюдаемой последовательностью.

Рассмотрим процесс формирования последовательности Y длиной n элементов с использованием одномерного дискретного хаотического отображения f. Дискретное хаотическое отображение записывается в итерационной форме:

$$x_{i+1} = f(x_i) \tag{1}$$

где x_i – значение переменной x на i-ой итерации.

Разделим интервал значений, которые может принимать переменная x, на m равных частей. При этом i-ому элементу последовательности Y присвоим значение, равное номеру интервала, которому принадлежит значение x_i . Стоит отметить, что большинство дискретных хаотических отображений позволяют по значению x_{i+1} определить возможные значения x_i. В качестве примера рассмотрим логистическое отображение

$$x_{i+1} = x_i \cdot (1 - x_i) \cdot \lambda \tag{2}$$

где λ – параметр отображения.

Выражая из (2) переменную x_i через x_{i+1} получаем два возможных решения:

$$x_{i,1} = \frac{-\lambda + \sqrt{\lambda^2 - 4\lambda x_{i+1}}}{2\lambda}, \tag{3}$$

$$x_{i,2} = \frac{-\lambda - \sqrt{\lambda^2 - 4\lambda x_{i+1}}}{2\lambda}. \tag{4}$$

Подходящее решение x_i можно выбрать, зная значение i-ого элемента последовательности Y. Таким образом, оказывается возможным найти начальное значение x_0, при использовании которого формируется наблюдаемая последовательность Y.

Следует отметить, что точное значение x_{i+1} остается неизвестным при известных значениях элементов последовательности Y. Возможным оказывается определение только в каких пределах оно находится.

В реальных задачах существующие значения элементов последовательности Y могут быть искажены вследствие шума. Для восстановления начальных условий в данном случае предлагается следующая последовательность действий.

1. Формирование таблицы T, j-ая строка которой содержит все возможные значения (i+1)-ого элемента последовательности Y в случае, если значение i-ого элемента равно j, где $j = 1 \ldots m$.

2. Формирование матрицы E, содержащей m строк и n столбцов. При этом ij-ый элемент матрицы e_{ij} равен единице, если представление значения i-ого элемента последовательности Y в двоичном виде не отличается от двоичного представления числа j не более чем в r любых разрядах. В противном случае $e_{ij} = 0$.

3. Формирование массива пар B. Если $e_{ij} = 1$, $e_{i+1,k} = 1$ и в j-ой строке матрицы T присутствует значение k, то пара (e_{ij}, $e_{i+1,k}$) добавляется в массив B.

4. Выбор из пар, содержащихся в массиве B, тех, которые позволяют установить непрерывную связь между первым и последним ненулевыми элементами матрицы E. Результатом являются возможные варианты значений элементов последовательности Y. Следует отметить, что при $r = 2$ и $m = 256$ количество возможных значений для большинства элементов

последовательности Y равно 1. После данных шагов задача восстановления начальных значений сводится к рассмотренной ранее.

Предлагаемый метод встраивания цифровых водяных знаков

Предлагаемый метод встраивания цифровых водяных знаков сводится к следующей последовательности действий:

1) формирование начального значение x_0;

2) формирование элементов последовательности W;

3) перестановка элементов последовательности W;

4) создание связи между значениями элементов последовательности W и элементов изображения;

5) добавление к изображению последовательности, полученной на предыдущем шаге.

Расмотрим каждый этап более подробно.

1. На первом этапе формируется начальное значение x_0 для создаваемой последовательности. Стоит отметить, что если для двух одинаковых изображений формируются разные значения x_0, то злоумышленник, сравнивая данные изображения, может сделать некоторые выводы об используемом алгоритме. Для того, что бы усложнить задачу злоумышленнику, предлагается выбирать начальные условия для одинаковых изображений одинаковыми. Это может быть достигнуто, например, получая начальные условия на основе значения хэш-значения, вычисленного с учетом всего изображения.

2. Формирование последовательности W. Используя полученное на предыдущем этапе значение x_0 формируется последовательность целых чисел Y с использованием выбранного хаотического отображения. Разряды полученных значений в двоичном виде являются элементами последовательности W.

3. Для сформированной на предыдущем этапе последовательности W характерно наличие связи между значениями соседних элементов. Для уменьшения величины данной связи применяется процедура перестановки элементов. Перестановка может осуществляться любым способом, однако должна быть обратимой и выглядеть как случайная.

Стоит отметить, что если разбить последовательность на фрагменты и осуществлять перестановку каждого фрагмента отдельно от другого, то повысится стойкость цифрового водяного знака к потере фрагментов изображения. В данном случае для обнаружения цифрового водяного знака будет достаточно получить только один из фрагментов.

4. Каждому значению элемента изображения ставится в соответствие единица либо ноль. Для этого формируется массив S, половина элементов которого равна единице, другая – нулю, при этом связь между индексом элемента массива S и значением должна быть похожа на случайную. Значение элемента изображения выступает в качестве номера элемента массива S, а значение, которое ставится в соответствие есть значение соответствующего элемента массива S. После этого к полученной последовательности нулей и единиц добавляется последовательность W. В качестве функции объединения

последовательностей предлагается использовать поэлементное сложения по модулю два. Обозначим полученную последовательность как W_I.

5. Каждый наименьший значащий разряд двоичного представления элемента изображения заменяется значением соответствующего элемента сформированной на этапе 4 последовательности W_I.

Данный способ встраивания не является единственно возможным. Например, может использоваться подход на основе вейвлет-преобразования [4].

В результате проведения атаки копирования восстановить начальные условия оказывается невозможным, поскольку использование других значений элементов изображения на этапе 4 приведет к существенным изменениям в значениях элементов последовательности W.

Для обнаружения цифрового водяного знака в изображении, а также определения искажений, которым подверглось изображение в канале связи, требуется выполнение следующих действий:

1. Извлечение из изображения последовательности W_I'. Штрих в данном случае указывает на то, что полученная последовательность W_I' может отличаться от передаваемой W_I вследствие помех в канале связи. В случае, если использовался метод встраивания на основе наименьшего значащего разряда, значение элемента последовательности равно значению наименьшего разряда в двоичном представлении значения элемента изображения.

2. Определение значений элементов последовательности W'. Данный этап аналогичен этапу 4 алгоритма встраивания цифрового водяного знака.

3. Обратная перестановка элементов последовательности W'.

4. Восстановление начального условия. Осуществляется по алгоритму, рассмотренному в предыдущем разделе.

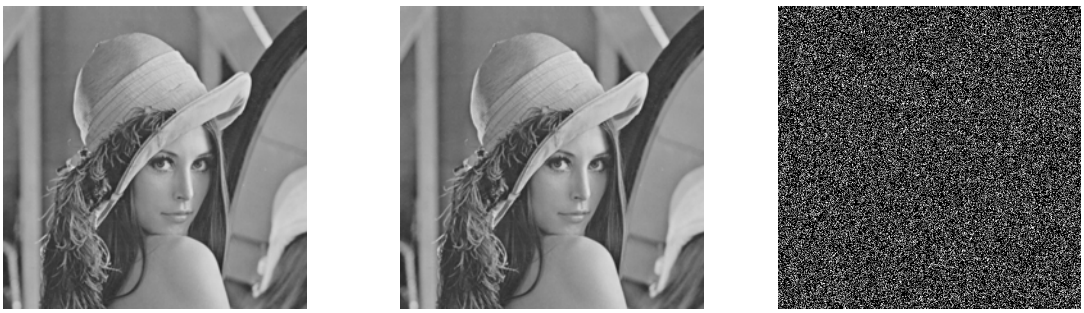
5. Формирование последовательности W''. Используя найденное на предыдущем этапе начальное условие, формируется последовательность W'' Данный этап аналогичен этапу 2 алгоритма встраивания цифрового водяного знака.

6. Сравнение последовательностей W'' *и* W'. Сравния поэлементо полученные последовательности W'' *и* W' можно установить факт присутствия цифрового водяного знака в изображении, выявить конкретные элементы изображения, значения которых подверглись изменениям. В случае, если отношение количества различающихся элементов к общему количеству элементов больше порогового значения q, считается, что цифровой знак отсутствует в изображении. Стоит отметить, что при использовании данного алгоритма для проверки наличия цифрового водяного знака не требуется исходное (без встроенного цифрового водяного знака) изображение.

Результаты и их обсуждение

В работе приводятся результаты, полученные при использовании логистического отображения, со значением параметра $\lambda = 3.995142$. Диапазон принимаемых значений переменной x делился на $m = 256$ интервалов. Значение праметра r было выбрано равным 2, значение порогового значения q было выбрано равным 0.4. Результат применения предлагаемого алгоритма к

тестовому изображению «Lena.bmp» представлен на рисунке 1. Исходное изображение (рисунок 1а) и изображение со встроенным цифровым водяным знаком (рисунок 1б) практически совпадают. Разница в значениях яркости данных изображений, увеличенная в 256 раз, представлена на рисунке 1в.



а) б) в)

а) – исходное изображение «Lena.bmp»; б) – изображение со встроенным цифровым водяным знаком; в) – разница между изображениями а) и б), увеличенная в 256 раз

Рис.1. Иллюстрация работы предлагаемого алгоритма

Для проверки стойкости предлагаемого алгоритма к атаке копирования, полученный цифровой водяной знак для изображения «Lena.bmp» был добавлен к другим изображениям. Результат проведения атаки копирования с использованием тестового изображения «peppers.bmp» представлен на рисунке 2. Результат проверки на наличие цифрового водяного знака (риунок 2в) свидетельствует о том, что примерно половина элементов последовательности подверглась изменениям ($q > 0.47$) . Это свидетельствует о том, что соответствующий цифровой водяной знак не был обнаружен в рассматриваемом изображении.

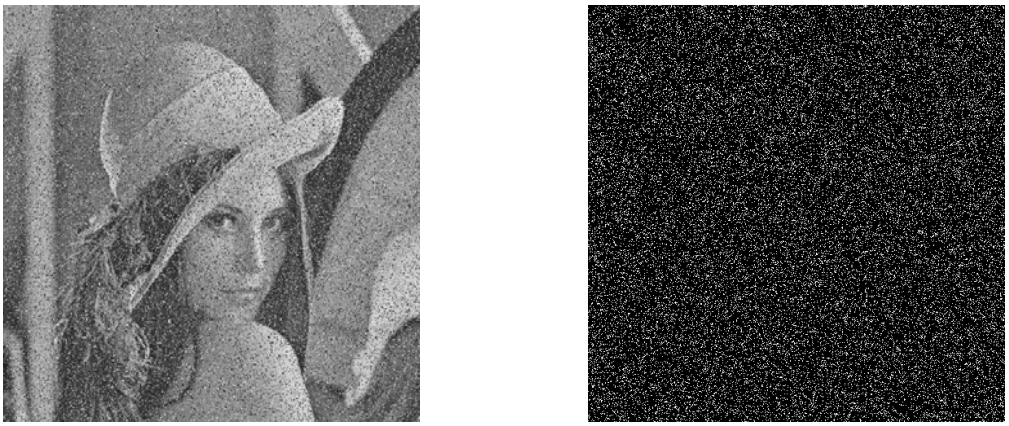
а) б) в)

а) – исходное изображение «peppers.bmp»; б) – изображение со встроенным цифровым водяным знаком, полученным для изображения «lenna.bmp»; в) – результат поверки на наличие цифрового водяного знака

Рис.2. Результат проведения атаки копирования с использованием изображения «peppers.bmp»

Для оценки стойкости алгоритма к шумам каждый четвертый элемент встраиваемой последовательности (до проведения процедуры перестановки) и соответствующее значение элемента изображения были заменены случайным значением. Полученное изображение и результат проверки на присутствие цифрового водяного знака представлены на рисунке 3. Как следует из полученных данных (рисунок 3б), количество элементов с различающимися

значениями составляет около 25% от общего количества элементов, что свидетельствует о сохранении цифрового водяного знака в изображении.

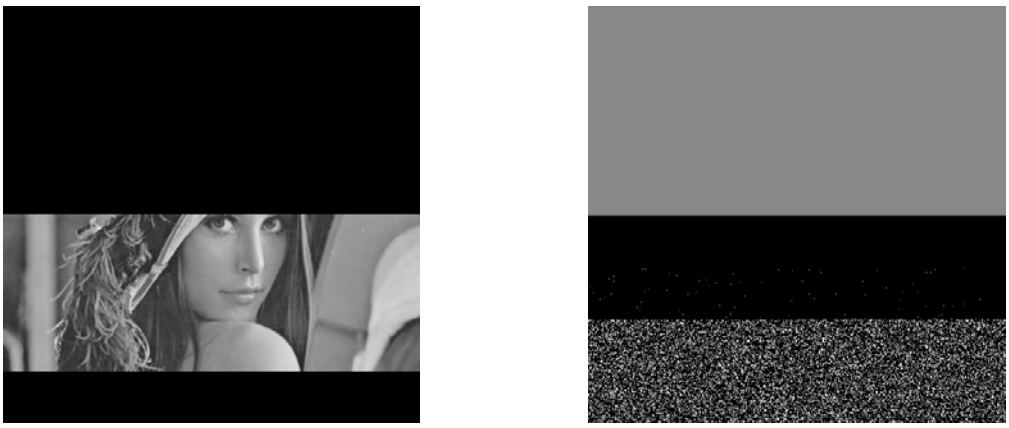


а) б)

а) –изображение «Lena.bmp» с добавленным шумом; б) –результат поверки на наличие цифрового водяного знака

Рис.3. Иллюстрация работы алгоритма при наличии шума в канале связи

Предлагаемый алгоритм также учитывает возможность потери фрагмента изображения. На рисунке 4 представлен результат работы алгоритма в данной ситуации. Как следует из результатов проверки (рисунок 4б), оказывается возможным установить присутствие цифрового водяного знака для переданного фрагмента изображения, несмотря на то, что исходные начальные условия, использующиеся при формировании цифрового водяного знака, были утеряны при передаче.



а) б)

а) –фрагмент переданного изображения «Lena.bmp»; б) –результат поверки алгоритма

Рис.4. Иллюстрация работы алгоритма при потере фрагмента изображения

Заключение

Предложен новый метод встраивания цифровых водяных знаков в изображения на основе динамического хаоса. В основе предлагаемого алгоритма встраивания цифровых водяных знаков в изображения находится возможность нахождения таких начальных условий, при использовании которых формируемая последовательность значений с использованием хаотических отображений совпадает с наблюдаемой последовательностью. Результаты тестирования предлагаемого алгоритма свидетельствуют о том, что

данный алгоритм является стойким к атакам копирования, учитывает возможность потери фрагментов изображения, допускает изменение более чем 25% элементов изображения в результате наличия шумов в канале связи.

Список литературы

1. Tao, H. Robust Image Watermarking Theories and Techniques: A Review / H. Tao [et al.] // Journal of Applied Research and Technology. – 2014. – Vol. 12. – p. 122–138.
2. Pushpa Mala, S. Digital image watermarking techniques: a review / S. Pushpa Mala, D. Jayadevappa, K. Ezhilarasan // International Journal of Computer Science and Security– 2015. – Vol. 9. – p. 140 - 156.
3. Kutter, M. The Watermark Copy Attack / M. Kutter, S. Voloshynovskiy, A. Herrigel // Proceedings of SPIE: Security and Watermarking of Multimedia Content, San Jose, CA, USA, January 2000 – San Jose, 2000. – p. 371–380.
4. Dawei, Zh. A chaos-based robust wavelet-domain watermarking algorithm / Zh. Dawei, Ch. Guanrong, L. Wenbo // Chaos, solitons and fractals – 2004. – № 22. – p. 47–54.

Сидоренко Алевтина Васильевна, профессор кафедры физики и аэрокосмических технологий факультета радиофизики и компьютерных технологий Белорусского государственного университета, доктор технических наук, профессор, sidorenkoa@yandex.ru

Шакинко Иван Владимирович, аспирант кафедры телекоммуникаций и информационных технологий факультета радиофизики и компьютерных технологий Белорусского государственного университета, ivan.rf13@gmail.com