Experience: The Inspiration for Self". Proc. ECOOP '95, Aarhus, Denmark, 1995. ***23****. T. J. Norman, C. Reed. "Delegation and Responsibility". In Proc. of ATAL '00, 7th International Workshop on Agent Theories, Architectures and Languages, Boston, MA, 2000.*

УДК 681.511.3

ТЕХНОЛОГИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ПРИ ОСНОВНЫХ ПОКРЫВАЮЩИХ СООБЩЕНИЯХ В ВИДЕ БИНАРНЫХ ИЗОБРАЖЕНИЙ

Ирина Маракова
Одесский национальный политехнический университет

Анотація: **Виконано оцінку ефективності систем з прихованими цифровими мітками. Розглянуто систему з прихованими цифровими мітками з використанням бінарних зображень у вигляді головного повідомлення та в умовах адитивної атаки шумом. Одержані формули для P_m та P_{fa} як функцій від числа елементів водяних знаків (ВЗ), постійної перекручень, порогу. Це дозволяє оцінити кількість потрібних біт ВЗ для забезпечення надійності системи в певних умовах.**
Summary: **Watermarking (WM) technology at use as the cover massage of binary images. We consider private (WM) system at use as the cover message of binary images with additive noise attack. The formulas for P_m and P_{fa} are derived as a dependence on the number of WM elements, distortion constraints, chosen threshold. It allows to find out how many bits of WM is necessary to use in order to embed reliable WM for different conditions.**
Ключевые слова: **Водяные знаки, основное покрывающее сообщение, идентификатор.**

I Введение

Цифровые системы с водяными знаками (ВЗ) являются одним из основных приложений сокрытия информации и отличаются от классических стеганографических систем тем, что скрывают не секретное сообщение, а некоторый идентификатор. Параметры систем с ВЗ и требования к ним существенно зависят от их практического применения (защита авторских прав, мониторинг вещания, контроль копирования, сохранение целостности и т. д.). С другой стороны, для идентификации цифровых сообщений используется цифровая подпись (ЦП), которая в итоге является последовательностью цифр, сформированных в зависимости от сообщения в соответствии со специальными стандартными преобразованиями и добавляемых к сообщению. ЦП без труда может быть отделена от сообщения. Погружение же ВЗ в основное покрывающее сообщение (ОПС), которое может быть изображением, аудио, видео подразумевает не только сокрытие ВЗ, но и неотделимость от ОПС, а также одинаковое восприятие ОПС и стегасообщения (ОПС и ВЗ) [1].

Частный случай, когда ОПС является бинарным изображением, весьма важен на практике, например, в электронной диагностике, факсимильной связи и т. д. Кроме того, любое ОПС после квантования можно представить в бинарном виде. Погружение ВЗ при этом представляет собой сложение по модулю 2 содержимого пикселей изображения (0 или 1) и в общем случае кодированного двоичного ВЗ. В качестве критерия верности используется количество ошибочных двоичных пикселей изображения. Другими словами, метрикой верности является вес Хэмминга.

Оценка эффективности бинарных систем с ВЗ осуществляется посредством оценки вероятностей ошибок, а именно, вероятности ложного обнаружения ВЗ P_{fa} и вероятности пропуска ВЗ P_m [2]. Рассмотрены следующие структуры систем с ВЗ: информированный кодер и декодер (используется информация об ОПС как кодером, так и декодером); не информированные кодер и декодер (информация об ОПС не используется ни в декодере, ни при формировании стегасообщения в кодере); информированный кодер и не информированный декодер (информация об ОПС не используется декодером, но учитывается при погружении ВЗ в ОПС) [3]. Не умаляя общности исследований, рассматриваются системы с нулевым битом, когда декодер принимает решение о наличии или отсутствии ВЗ, т. е. по сути является детектором или обнаружителем ВЗ. На выходе такого декодера может быть только два вида сигнала, свидетельствующего либо об отсутствии ВЗ (0), либо о присутствии его в принятом сигнале (1).

В канале атакующего, целью которого является удаление или искажение ВЗ при сохранении неизменным ОПС, рассматривается только аддитивная помеха. Несомненно, современные алгоритмы канала атакующего значительно сложнее (сжатие, геометрические преобразования, фильтрация и т. д.). С другой стороны, исследование системы с ВЗ в условиях воздействия только аддитивного шума атаки позволит получить

нижнюю оценку эффективности. Кроме того, в дальнейшем исследования можно продолжить и для более искусных атакующих преобразований.

II Аналитическая оценка эффективности бинарных систем с ВЗ

Модель ОПС – дискретная во времени случайная стационарная последовательность $C(n)$, $n \in A_N=(1, \ldots, N)$, где N – длина ОПС. Кроме того, случайные последовательности $C(n)$ и $C(n')$, $n' \in A_N=(1, \ldots, N)$ полагаются статистически независимыми, если $n' \neq n$.

При рассмотрении модели системы с ВЗ с точки зрения классической теории связи оптимальным кодированием (погружением ВЗ) в асимптотике является суммирование ОПС с ВЗ. Рассчитаем вероятности P_m и P_{fa}, предполагая, что последовательности ВЗ и аддитивной шумовой атаки являются последовательностями Бернулли. Ограничение на верность ОПС в относительной метрике Хэмминга

$$\frac{1}{N} D_w \leq d_{w,} \tag{1}$$

где D_w – вес Хэмминга для последовательности ВЗ $w(n)$.

Стегасообщение, т. е. ОПС с погруженным ВЗ

$$S(n)=C(n) \oplus w(n),\ n=1, 2, 3, \ldots N\,. \tag{2}$$

Тогда атака на стегасообщение в виде аддитивного шума

$$S'(n)=S(n) \oplus \varepsilon(n),\ n=1, 2, 3, \ldots N\,, \tag{3}$$

где $\varepsilon(n)$ – двоичная последовательность шума атаки, $\oplus$ – операция суммирования по модулю 2.

Если в качестве ОПС используется изображение, в частности, бинарное, то ОПС является двумерным массивом $C(\bar{n}) = C(n_1, n_2)$, $n_1=1, \ldots, N_1$, $n_2=1, \ldots, N_2$, $N=N_1N_2$. Далее, не умаляя общности исследований, будем для простоты использовать одномерные массивы.

Ограничение на верность бинарного ОПС после атаки

$$\frac{1}{N} D_\alpha \leq d_\alpha\,, \tag{4}$$

где D_α вес Хэмминга для последовательности ВЗ после атаки.

Таким образом, последовательности $C(n)$, $w(n)$, $\varepsilon(n)$ являются последовательностями Бернулли, определяемые параметрами d_c , d_w, , d_α, соответственно.

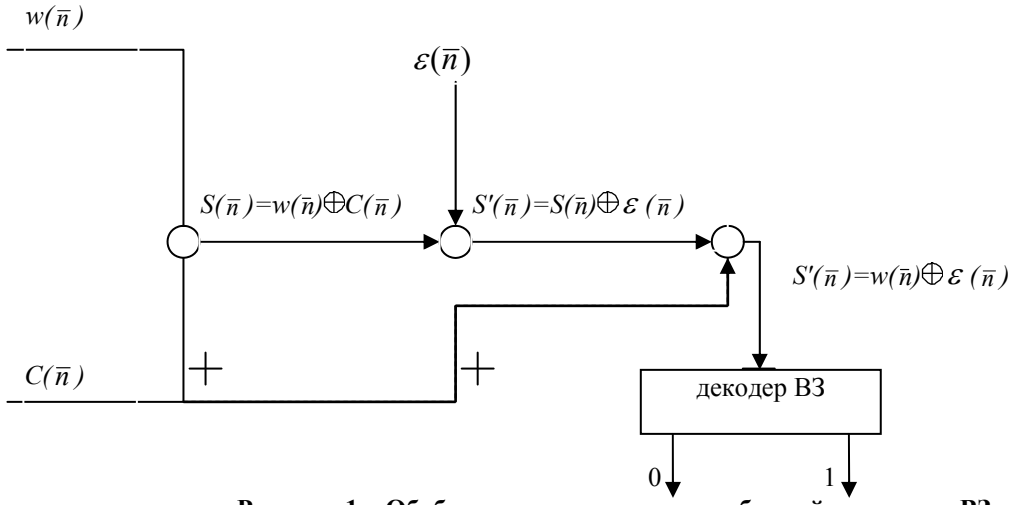

Рисунок 1 – Обобщенная структура двухбитной системы с ВЗ

Рассмотрим структуру системы с ВЗ при информированных кодере и декодере, когда ОПС и ВЗ являются секретным ключом легальных пользователей. Для декодера системы ВЗ с нулевым битом возможны два вида ошибок: пропуск ВЗ, характеризуемое вероятностью пропуска ВЗ P_m, и ложное обнаружение ВЗ, характеризуемое вероятностью ложного обнаружения P_{fa}.

Оценки вероятностей P_m и P_{fa} могут быть получены из следующих соображений. Если $w(n)$ и $\varepsilon(n)$ – последовательности Бернулли, то вероятность того, что именно на позициях погружения ВЗ $w(n)$ в ОПС $C(n)$ появится более $Nd_w - \lambda$ единиц, что приведет к их пропуску, составит

$$P_m = \sum_{i=Nd_\alpha-\lambda}^{Nd_\alpha} \binom{i}{Nd_w} d_\varepsilon^{\,i} (1-d_\varepsilon)^{Nd_w-1}. \tag{5}$$

Отметим, что в среднем на этих позициях будет появляться $Nd_w d_\varepsilon$ единиц. В декодере будет в среднем $N(1- d_w d_\varepsilon)$ единиц. Предположим, что последовательность $w(n)$, являющаяся секретным ключом легальных пользователей, выбирается как последовательность независимых бит, причем вероятности появления единиц и нулей, соответственно

$$P_r\,(w(n)=1)= d_w,$$
$$P_r\,(w(n)=0)=1- d_w. \tag{6}$$

С учетом того, что шум атаки $\varepsilon(n)$ является последовательностью независимых бит с вероятностью единиц d_ε и с вероятностью нулей $1-d_\varepsilon$, то для выполнения (6) относительно d_ε должно выполняться:

$$d_w\,(1- d_\varepsilon)+(1- d_w)\,d_\varepsilon \geq d_\alpha. \tag{7}$$

Рассмотрим вероятность ложного обнаружения, т. е оценку ситуации, когда на известных позициях единиц ВЗ появится более, чем λ

$$P_{fa} = \sum_{i=\lambda}^{Nd_w} \binom{i}{Nd_w} d_\varepsilon^{\,i} (1-d_\varepsilon)^{Nd_w-i}. \tag{8}$$

На выходе оптимального декодера ВЗ формируется величина, пропорциональная

$$\Lambda = \sum_{n=1}^{N} w(n)\{s'(n) \oplus c(n)\} = \sum_{n=1}^{N} w(n)\{c(n) \oplus w(n) \oplus \varepsilon(n) \oplus c(n)\} = \sum_{n=1}^{N} w(n)\{w(n) \oplus \varepsilon(n)\}, \tag{9}$$

которая сравнивается с порогом λ и если $\Lambda \geq \lambda$, то принимается решение об обнаружении ВЗ, в противном случае – об отсутствие ВЗ. Поскольку выполняется условие $1 - d_w d_\alpha > d_w d_\alpha$ во всех случаях, кроме тривиального, когда $d_w d_\alpha$=0,5, то это означает, что при любых d_w, d_α при больших N можно рассчитывать на то, что P_{fa} и P_m будут весьма малы.

Для упрощения численных исследований эффективности для больших N (5), (8) можно преобразовать

$$P_m \leq \left(\frac{d_\varepsilon}{1-\lambda/Nd_w}\right)^{Nd_w-\lambda} \left(\frac{(1-d_\varepsilon)Nd_w}{\lambda}\right)^{\lambda}, \tag{10}$$

$$P_{fa} \leq \left(\frac{1-d_\varepsilon}{1-\lambda/Nd_w}\right)^{Nd_w-\lambda} \left(\frac{d_\varepsilon Nd_w}{\lambda}\right)^{\lambda}. \tag{11}$$

Рассмотрим практически более важную структуру построения системы с ВЗ, когда ОПС не известно в декодере и не используется в кодере при формировании стеганографического сообщения. Если ОПС также представить последовательностью Бернулли, то, по существу, ОПС является дополнительной помехой. Вероятность ошибки на входе декодера ВЗ будет уже не d_ε, а

$$d_\varepsilon' = d_c\,(1-d_\varepsilon)+(1-d_c)\,d_\varepsilon. \tag{12}$$

При этом для оценки вероятностей ошибок в (5), (8) нужно d_ε заменить на d_ε' (12).

Поскольку $(1- d_\alpha d_\varepsilon) > d_\alpha d_\varepsilon$, то при вероятности единиц в ОПС, близкой к d_c=0,5, что наиболее вероятно для реальных ОПС, эффективность систем с ВЗ будет существенно ухудшаться.

Для структуры системы с ВЗ, когда информация об ОПС не используется декодером, но учитывается в кодере при погружении ВЗ в ОПС, по-прежнему, полагаем, что ОПС описывается моделью Бернулли (d_c) и используем следующую схему кодирования.

Последовательность ВЗ $w(n)$ выбирается из множества W, $w(n) \in \mathbf{W}$, где $|W| = L$ достаточно велико. Множество последовательностей ВЗ является секретной «кодовой книгой» и используется декодером. Когда поступает конкретное ОПС $C_o(n)$, то выбирается та последовательность $w_o(n)$ из кодовой книги $\mathbf{W}$, которая ортогональна с $C_o(n)$, т. е.

$$\sum_{n}^{N} C_o(n) w_o(n) \le \delta \tag{13}$$

Фактически, для рассматриваемой структуры последовательность $w_o(n)$ имеет единицы в основном там, где $C_o(n)$ имеет нули. Другими словами, $C_o(n)$ – это такое ОПС, которое наилучшим образом соответствует передаче ВЗ $w_o(n)$.

При оценке вероятностей P_m, P_{fa} для данной структуры предполагается, что ОПС $C_o(n)$ задано, а количество последовательностей ВЗ $w(n) \in W$ генерируется каждый раз случайно. Данное предположение не умаляет общности исследований. Тогда, если полагать, что каждая посылка ВЗ есть последовательность Бернулли (d_w), и что в последовательности $C_o(n)$ содержится в среднем N единиц, то вероятность выполнения неравенства (11) для каждой выбранной последовательности ВЗ

$$P(l, \delta) = \sum_{i=0}^{\delta} \binom{Nd_c}{i} d_\alpha^{\,i} (1 - d_\alpha)^{Nd_c - i}. \tag{14}$$

Вероятность же того, что условие (11) выполняется хотя бы для одной из L последовательностей, будет иметь границу

$$P(L, \delta) \ge 1 - (1 - P(l, \delta))^L. \tag{15}$$

Нижняя граница вероятности пропуска ВЗ

$$P_m \le 1 - (1 - P(1, \delta)) \sum_{i=Nd_\alpha - \lambda}^{Nd_\alpha} \binom{Nd_\alpha}{i} (d'_\varepsilon)^i (1 - d'_\varepsilon)^{Nd'_\varepsilon - i} + P(L, \delta) \sum_{i=Nd_\alpha - \lambda}^{Nd_\alpha} \binom{Nd_\alpha}{i} (d_\varepsilon)^i (1 - d_\varepsilon)^{Nd_\varepsilon - i}. \tag{16}$$

Вероятность ложного обнаружения ВЗ будет ограничена неравенством

$$P_{fa} \le 1 - (1 - \sum_{i=ND_1 - \lambda}^{ND_1} \binom{Nd_{w1}}{i} (d'_\varepsilon)^i (1 - d'_\varepsilon)^{d_w + 1})^L. \tag{17}$$

Становится возможным решить численную задачу оптимизации параметра L, чтобы получить наилучшую пару вероятностей P_m, P_{fa}.

III Иллюстрация результатов и выводы

Полученные аналитические выражения для оценки вероятностей ошибок бинарных систем с ВЗ в условиях атакующего воздействия только в виде аддитивного шума могут быть весьма полезны для оценки нижней границы эффективности. На рис. 2 приведены графики зависимости длины ВЗ от параметра d_α при зафиксированных d_w и вероятностях ошибок $P_m = P_{fa} = 10^{-3}$ для структуры, когда информация об ОПС используется как кодером, так и декодером (сплошная линия) и когда информация об ОПС не используется декодером, но учитывается при погружении ВЗ в ОПС (пунктирная линия). Как видно из полученных результатов, при не информированном декодере для обеспечения того же уровня эффективности обнаружения ВЗ требуется в полтора и более раза увеличить длину ВЗ, что, несомненно, приведет к ухудшению визуального восприятия сообщения с ВЗ.

На рис. 3 приведены графики зависимости длины ВЗ от параметра d_α при зафиксированных d_w и вероятностях ошибок $P_m = P_{fa} = 10^{-3}$ для структуры системы, когда информация об ОПС не используется ни кодером, ни декодером. В данном случае для обеспечения $P_m = P_{fa} = 10^{-3}$ требуется на два порядка увеличить длину ВЗ, что, несомненно, будет иметь трудности при практической реализации.

На рис. 4 приведены результаты визуальной оценки стегасообщений при различных параметрах «рассеянного» погружения ВЗ (по всему ОПС случайным образом, т. е. с использованием секретного ключа) и шумовой атаки. Для улучшения визуальной оценки необходимо осуществлять погружение ВЗ адаптивно к конкретному ОПС. Например, предварительно выделять контур, изменение пикселей которого в результате

погружения ВЗ будет менее заметным. Результаты таких исследований будут приведены в последующих публикациях.

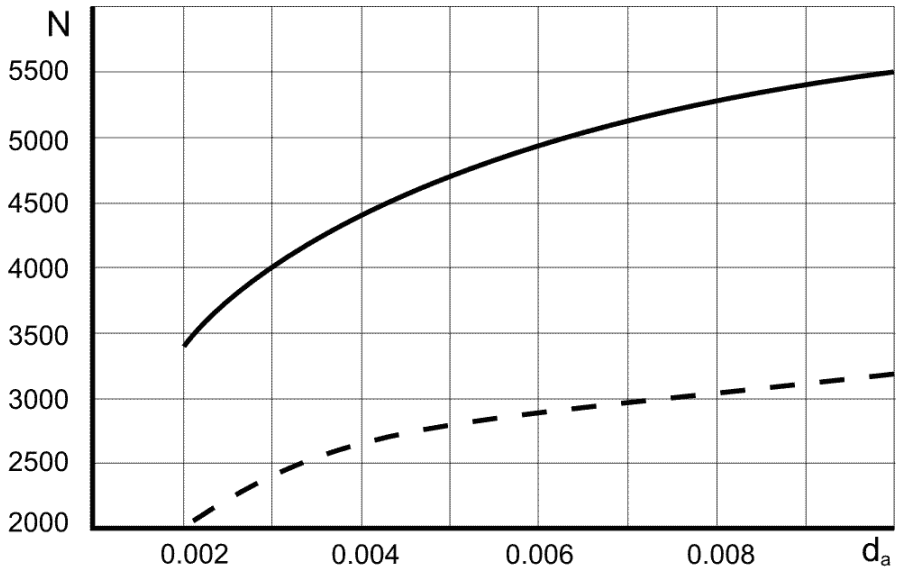

Рисунок 2 – Зависимость длины ВЗ от d_α при $d_w = 10^{-3}$ и обеспечении $P_m = P_{fa} = 10^{-3}$; информированные кодер и декодер – сплошная кривая; информированный кодер и не информированный декодер, $d'_\varepsilon = 10^{-1}$ – пунктирная кривая

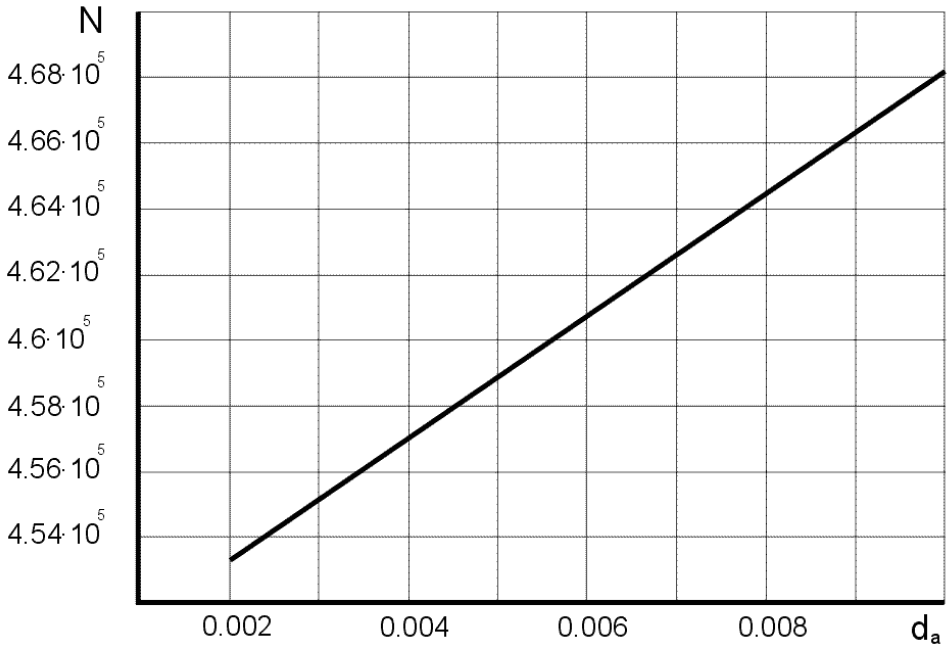

Рисунок 3 – Зависимость длины ВЗ от d_α при $d_w = 10^{-3}$, $d'_\varepsilon = 10^{-1}$

и обеспечении $P_m = P_{fa} = 10^{-3}$; не информированные кодер и декодер

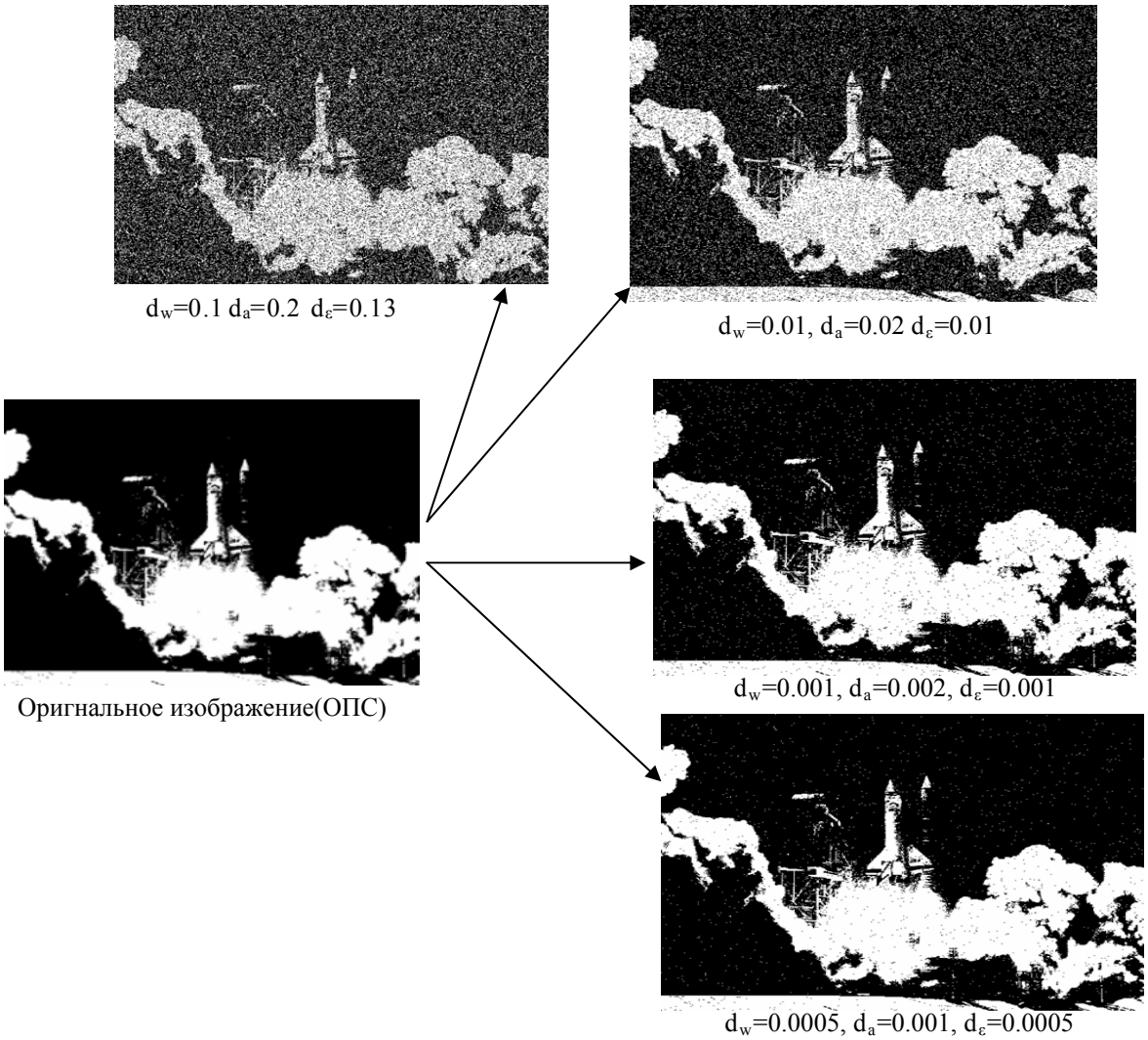

Рисунок 4 – «Рассеянное» погружение ВЗ и атака шумом, размер ОПС 34 кб,

Необходимо отметить, что для зависимых пикселей ОПС даже в виде бинарного изображения не очень подходит метрика Хэмминга. Действительно, если выбирается такое *w(n),* что большинство его единиц попадает на нулевые поля ОПС, то это приводит к значительным качественным искажениям отдельных сегментов изображения, несмотря на то, что условие на верность может выполняется. Потому в этом случае нужно ввести другую метрику верности, например фрагментальную Хэммингову, т. е. скользящую (среднее число ошибочных пикселей в любом скользящем фрагменте не превосходит некоторой заданной величины). Размеры фрагмента необходимо определять предварительно, исходя из конкретноых свойств ОПС. Адаптивные алгоритмы погружения ВЗ при бинарных ОПС несомненно представляют интерес с практической точки зрения и будут рассмотрены в последующих публикациях.

*Литература: **1**. S. Katzenbeisser, F. Petiticolas "Information Hiding", Artech HouseInc., 2000, 270 p. - **2**. Маракова И. И., Мараков Д. А. Методика оценки эффективности систем с цифровыми водяными знаками в рамках заданных ограничении/ Захист інформації. - К., № 2, 2002 , с. 58-65 **3**. J. Linnartz, T. Klaker,*

G Deprovere "Modeling the False Alarm and Missed Defection rate for Electronic Watermarks", Second Intern. Workshop, IH'98/LNCS, N1525, p. 329-343