*42. **6.** Панин О. А., Журин С. И. Оптимизация параметров систем охранной сигнализации как задача многокритериального выбора. // Защита информации. Конфидент № 1, 2004. – С. 84-87. **7.** Кононович В. Г. Тардаскін М. Ф., Тардаскіна Т. М. Аналіз проблеми розподілу витрат на інформаційну безпеку інформаційно-телекомунікаційних систем. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С 62-68. **8.** Черноруцкий И. Г. Методы оптимизации и принятия решений. С.-Пб, 2001, С. 248. **9.** Гафт М. Г. Методы оценки технического уровня, Интерактивный подход. //Проблемы информационных систем. – М.: № 2, 1987. – С. 1–21. **10.** Бельфер Р. А. Анализ систем связи в аспекте проектирования информационной безопасности. // "Электросвязь", № 3, 2004. – С 22 – 24. **11.** Додонов О. Г., Горбачик О. С., Кузнєцова М. Г. Захист інформації в інформаційно-аналітичних системах державних органів управління // Реєстрація, зберігання і обробка даних, 2000, Т. 2, № 2, – С. 66-72. **12.** Гайкович В., Першин А. Безопасность электронных банковских систем. –М. Единая Европа, 1994. – 351 с. **13.** Яновский Г. Г. Применение устойчивых пакетных колец в сетях следующего поколения // "Вестник связи", № 7, 2003, - с 54- 56. **14.** Recomendation CCITT X.800. Security architecture for open systems interconnection for CCITT applications. Geneva.1991; (Стандарт ISO 7498-2:1989. Архітектура безпеки ВВС). **15.** "Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах". Затверджений наказом ДСТСЗІ СБУ № 76 від 24. 12. 2001 р.*

УДК 681.5.015: 004.056.57

АЛГОРИТМЫ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ С ТОЧНЫМ ВОССТАНОВЛЕНИЕМ ОСНОВНЫХ ПОКРЫВАЮЩИХ СООБЩЕНИЙ

Ирина Маракова
Одесский национальный политехнический университет

Анотація: **Розглянуто використання цифрових водяних знаків (ЦВЗ) для ідентифікації та підтвердження цілісності зображень. На відміну від інших технології, наприклад, цифрового підпису, ЦВЗ не потребує додаткового простору та є невіддільними від основного повідомлення. Фундаментальна проблема створення таких систем — відновлювання основного повідомлення без втрат після детектування ЦВЗ. Розглянуто модульний спосіб занурення та адаптивне детектування ЦВЗ, отримані аналітичні оцінки ймовірності помилок, виконано імітаційне та аналітичне моделювання**.

Summary: **A watermark (WM) application to assist in the integrity maintenance and verification of the associated images is considered. There is a great benefit of WM use in context authentication since WM is inseparable from cover message and it does not require additional storage space for supplementary meta-data, as cryptographic signatures for instance. However there is a fundamental problem: the restoration of cover message without any error after WM detection. The modulo addition of a mark and advanced WM detection are used. The formulas for the probabilities of errors are proposed. The analectic and imitation simulations are done.**

Ключевые слова: **Цифровые водяные знаки, основное покрывающее сообщение, верификация, цифровая подпись, модульное сложение.**

I Введение

Технологии цифровых водяных знаков (ЦВЗ) могут использоваться не только для идентификации, но и для подтверждения целостности (верификации) сообщений [1]. В отличие от решающих аналогичные задачи криптографических методов, а именно, формирования цифровой подписи (ЦП), ЦВЗ не увеличивают размер сообщения и не могут быть удалены из стегасообщения (сообщения и ЦВЗ) без существенной потери надежности восприятия. С другой стороны, в качестве ЦВЗ можно использовать ЦП некоторого сообщения при выполнении требований по надежности восприятия стегасообщения (сообщения и ЦВЗ) и устойчивости к преобразованиям канала атаки. Основная проблема верификации на основе ЦП, заключающаяся в несанкционированном удалении ЦП, для ЦВЗ не актуальна. Однако возникает другая проблема: ЦВЗ должны быть инвертируемы, т. е. необходимо точное восстановление исходного основного покрывающего сообщения (ОПС) после детектирования ЦВЗ. Для решения данной проблемы представляется интересным использовать модульный способ погружения ЦВЗ.

При использовании технологий ЦВЗ для контроля копирования, предотвращения несанкционированного копирования, мониторинга рекламного вещания, электронного делопроизводства и т. д. полагается, что

некоторые изменения ОПС в результате погружения ЦВЗ являются допустимыми и на приемной части восстановление ОПС не требуется. Однако для подтверждения целостности, например, в медицинском менеджменте, криминалистике, требуется точное восстановление исходного ОПС. С другой стороны, если ОПС содержит N бит и после процедуры сжатия останется только L бит, то в $N - L$ бит ОПС допустимо погружать ЦВЗ, которые, однако, будут утрачены при сжатии (хрупкие системы с ЦВЗ). Практическое применение такого подхода ограничено [2].

Без потери общности исследований в качестве ОПС рассматриваются монохромные изображения. Стеганографическое сообщение S в случае одномерного представления ОПС

$$s(n) = (c(n) + w(n)) \bmod 256, \quad (1)$$

где $C = c(1), \ldots, c(n), \ldots c(N)$ — ОПС, $n = \in A_N = 1, \ldots, N$, N — число пикселей, $N = N_1 N_2$, N_1 — число строк, N_2 — число столбцов; $S = s(1), s(n), s(N)$ — стегасообщение; $W = w(1), \ldots w(n), \ldots w(N_{\text{ЦВЗ}})$ — ЦВЗ, $N_{\text{ЦВЗ}}$ — число элементов ЦВЗ, $N > N_{\text{ЦВЗ}}$, но для простоты полагается $N = N_{\text{ЦВЗ}}$ с обнулением несуществующих элементов последовательности ЦВЗ.

Для восстановления ОПС на приемной части системы с ЦВЗ выполняется модульное сложение стегаобраза с секретным ключом в виде ЦВЗ

$$c(n) = (s(n) + w(n)) \bmod 256. \quad (2)$$

В отличие от обычной арифметики при модульном сложении исключается эффект усечения при превышении порога яркости. Однако погружение на основе (1) характеризуется следующими недостатками. Во-первых, появляется мелкоструктурный шум на фрагментах стегаобраза. Искажения указанного рода зависят от типа ОПС и могут быть устранены соответствующими преобразованиями гистограммы яркости ОПС. Вторым недостатком является непригодность преобразований (1), (2) для изображений, чьи гистограммы яркости близки к равномерным.

В разделе 2 описаны адаптивные методы погружения и детектирования ЦВЗ, для которых выполнена аналитическая оценка вероятностей ошибок. В разделе 3 полученные результаты проверены посредством имитационного и аналитического моделирования. Выводы изложены в разделе 4.

II Алгоритм аутентификации

Для ОПС в виде монохромного изображения, каждый пиксель которого представлен 8 битами с градацией яркости в диапазоне от 0 до 255 можно сформировать ЦП, используя произвольные стандарты хеширования и криптографической обработки. Формирование ЦВЗ в виде ЦП ОПС производится с использованием какого либо асимметричного стандарта, например, RSA [3]. Пусть $\{K, G\}$ являются открытыми ключами, а k— секретный ключ. После хеширования дайджест ОПС $h(C)$ определен на пространстве P битовых слов, т. е. $\{0, 1\}^P$. Некоторая функция F реализует преобразование пространства полученного дайджеста ОПС в бинарное, а функция T — инверсное преобразование. Тогда формирование ЦП SA включает следующие шаги $H_c = h(C), \quad f = F(H_c), \quad C_e = (f^k) \bmod G, \quad SA = T(C_e)$ или в целом $SA = (T(F(h(C))^k) \bmod G$. Для подтверждения целостности и идентификации ОПС по полученной паре $\{C, SA\}$ необходимо вычислить дайджест восстановленного ОПС $h(\hat{C})$, где $\hat{C}$ — оценка ОПС, сформировать $S\hat{A}$ полученной оценки ОПС и сравнить с SA. Совпадение $S\hat{A}$ и SA подтверждает целостность сообщения. Таким образом, для процедуры идентификации и верификации на основе ЦП, погруженной в ОПС как ЦВЗ, необходимо выполнение следующих требований:

— отличие стегасообщения и ОПС не должно превышать заданный уровень в соответствии с требуемой надежностью восприятия;

— на основе стегасообщения при наличии секретного ключа в виде ЦВЗ восстановление ОПС должно характеризоваться очень высокой вероятностью.

Использование кодов, исправляющих ошибки, позволит повысить эффективность системы с ЦВЗ. Для некоторого бинарного систематического исправляющего ошибки кода $Z \in (m, L, d)$, где m— размер блока, L—число символов в алфавите, d — минимальное кодовое расстояние, b_{ij} является i–ым битом j–го блока кода, причем $i = 1, \ldots, m$, $j = 1, \ldots, 2^L$. Если в ЦП всего R бит, то размер кодового блока должен быть $R_o = R / L$. Каждый кодовый блок содержит m символов, причем для погружения одного кодового символа ЦВЗ, сформированного как ЦП ОПС, потребуется $n_o = N / R_o m = NL / Rm$ пикселей ОПС. Правило погружения j –ого кодового блока:

$$s(n) = (c(n) + \alpha(-1)^{b\left\lfloor \frac{n}{n_o} \right\rfloor + 1, j} w_r(n)) \bmod 256, \tag{3}$$

где $1 \le j \le 2^l$; α — целое число, $0 \le \alpha \le 255$, $w_r(n) = \{\pm 1\}$ — псевдослучайная последовательность (ПСП), полученная, например, с помощью линейного рекуррентного регистра сдвига.

Предположим, что сложение в (3) выполняется не в модульной, а в обычной арифметике и без потери общности, что для передачи и приема каждого символа ЦВЗ в виде ЦП требуется *R/L* бит. В структуре секретной системы с неинформированным детектором, т.е. не использующим при детектировании ОПС, предполагается синхронизированность приемной и передающей частей. Корреляционный детектор принимает решение о том, какое кодовое *j*-ое кодовое слово принято на основании определения максимального значения функционала детектора

$$\Lambda_j = \max_{0 \le j \le 2^L} \sum_{n=1}^{\frac{N}{R_0}} (s(n) - E\{C\}) \alpha(-1)^{b\left\lfloor \frac{n}{n_o} \right\rfloor + 1, j} w_r(n), \tag{4}$$

где ОПС или рассматриваемый фрагмент ОПС предполагается стационарным процессом в широком смысле.

При погружении ЦВЗ по правилу (3) линейный корреляционный детектор (ЛКД) не обеспечивает оптимальное детектирование. Однако для частного случая ОПС в виде стационарного гауссова процесса и при обычном аддитивном погружении ЛКД является оптимальным. Используя аналогию с теорией широкополосных систем связи, на основе центральной предельной теоремы верхняя граница вероятности ложного обнаружения кодового блока

$$P_{fd} \le (2^L - 1) \mathrm{Q}\left(\frac{\alpha}{\sigma_c} \sqrt{\frac{NLd}{Rm}} \right) = (2^L - 1) \mathrm{Q}\left(\frac{\alpha}{\sigma_c} \sqrt{\frac{NL}{R} Vd} \right), \tag{5}$$

где σ_c^2 — дисперсия ОПС;

$V = L/m$ — скорость кодирования для кода *Z*;

$$\mathrm{Q(x)} = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{t^2}{2} \right) dt .$$

Для ЛКД значение (5) не зависит от гистограммы яркости ОПС, но зависит от значения дисперсии ОПС σ_c^2. С другой стороны, анализ (5) позволяет сделать вывод о том, что эффективность детектирования ЦВЗ для выбранного кода *Z* в первом приближении определяется произведением Vd. Например, если число пикселей ОПС $N = 64 \times 10^3$, число бит для ЦП *R*=64, вероятность ошибки $P_{fd} \le 10^{-3}$, то для тривиального кода $\mathrm{Z}: \{m,\ m,\ 1\}$, т. е. $Vd = 1$, необходимо 64 блока с 10^3 пикселями ОПС для каждого. Тогда вероятность неправильного приема каждого блока будет не выше $1{,}56 \times 10^{-5}$ и отношение сигнал/шум после погружения ЦВЗ в ОПС $\eta = \sigma_c^2 / \alpha^2$ составит 55,5. При использовании кода Голея $\mathrm{Z}: \{m,\ m,\ 1\} = \{24,\ 12,\ 8\}$, $Vd = 4$ для обеспечения той же вероятности ошибки отношение сигнал/шум после погружения ЦВЗ составит $\eta = 160$, что значительно лучше с точки зрения надежности восприятия стегасообщения, чем для системы с ЦВЗ без использования исправляющих ошибки кодов.

Если при формировании стегасообщения используется оператор модульного сложения (3), то выражение (5) не корректно, поскольку процедура обнаружения по правилу (4) при переходе в модульную арифметику в общем случае ухудшается. С другой стороны, только использование модульных операций позволяет точно восстанавливать ОПС при правильном декодировании кодового слова $b_{1j} b_{2j} \ldots b_{Lj}$. Для разрешения данного противоречия необходимо адаптировать алгоритм детектирования системы с ЦВЗ при аддитивном модульном погружении ЦВЗ (3).

2.1 Прореженное детектирование ЦВЗ

Идея прореженного детектирования (ПД) основана на том, что для *n* пикселей ОПС результаты модульных и обычных операций будут совпадать:

$$F_\alpha = \{n \le N \,|\, (s(n) - \alpha) \bmod 256 \le 255 - \alpha;\ \ (s(n) + \alpha) \bmod 256 \ge \alpha\}$$

и правило обнаружения

$$\Lambda^{ПД} = \sum_{n \in F_\alpha} (s(n) - C_0) w(n) \;\Rightarrow\; b = \begin{cases} 0, & \text{если } \Lambda \geq 0, \\ 1, & \text{если } \Lambda \leq 0, \end{cases} \tag{6}$$

где $C_0 = E\{C\}$ является средним значением ОПС $c(n),\ n \in F_\alpha$.

С учетом центральной предельной теоремы оценка вероятности ошибки такого обнаружителя

$$P_e = \mathrm{Q}\left(\frac{\alpha}{\sigma_c}\sqrt{N\mu}\right), \tag{7}$$

где $\mu = \frac{N_o}{N}$, $N_o = |F_\alpha|$.

В частном случае изображения с равномерной гистограммой яркости в диапазоне 0…255, т. е. когда

$$\forall \Delta = 0,\ 1,\ ....,\ 255,\ n = 1,\ ...,\ N:\ \Pr ob(c(n) = \Delta) = \frac{1}{256} \tag{8}$$

получим

$$\mu = \frac{256 - 2\alpha}{256} = 1 - \frac{\alpha}{128},\ \sigma_c^2 = \frac{255^2}{12} = 5418. \tag{9}$$

В результате подстановки (9) в (7) можно сделать вывод, что для некоторого приемлемого значения α вероятность ошибки P_e устремится к нулю при увеличении N, т. е. $\lim_{N\to\infty} P_e = 0$. Однако данный факт противоречит известному свойству равномерного распределения на некотором интервале $\{0,... J-1\}$, а именно: если к равномерно распределенной величине добавить или отнять по модулю J константу, то результирующая величина так же характеризуется равномерным распределением. Из данного свойства становится очевидно, что для изображений с равномерной гистограммой яркости гипотезы $b = 1$ и $b = 0$ становятся не различимыми. Для решения данной парадоксальной ситуации и применяется ПД. Вероятность ошибки детектирования ЦВЗ

$$P_e = \mathrm{Q}\left(\frac{E\{\Lambda\}}{\sqrt{Var\{\Lambda\}}}\right), \tag{10}$$

где $E\{\Lambda\}$, $Var\{\Lambda\}$ — математическое ожидание и дисперсия функционала ПД, соответственно,

$$E\{\Lambda_0^{ПД}\} = N\mu\left[\alpha + \frac{\sum_{C\in A_C} CP(C) - \sum_{C\in B_C} CP(C)}{1 + \sum_{C\in D_C} CP(C)}\right]. \tag{11}$$

Для $b = 0$

$$E\{\Lambda_1^{ПД}\} = -E\{\Lambda_0^{ПД}\} \tag{12}$$

$$Var\{\Lambda^{ПД}\} = \frac{N\mu}{1 + \sum_{C\in D_C} CP(C)}\left[\left(\sum_{C=0}^{255} C^2 P(C) + \sum_{C\in D_C}^{255} C^2 P(C)\right) - 2C_o\left(C_o + \sum_{C\in D_C}^{255} C^2 P(C)\right) - \right.$$

$$\left. 2C_o\alpha\left(\sum_{C\in A_C}^{255} P(C) - \sum_{C\in B_C}^{255} P(C)\right) - \frac{\left[\sum_{C\in A_C}^{255} CP(C) - \sum_{C\in B_C}^{255} CP(C)\right]^2}{1 + \sum_{C\in D_C} CP(C)}\right], \tag{13}$$

где $P(C)$ – вероятность распределения (гистограмма) ОПС; $A_C = \{0,\ 1,\ ...,\ 255 - 2\alpha\}$; $B_C = \{2\alpha,\ 2\alpha + 1,\ ...,\ 255 - 2\alpha\}$; $D_C = 2\alpha,\ 2\alpha + 1,\ ...,\ 255\}$.

Для ОПС с равномерной гистограммой яркости математические ожидания (11) и (12) будут нулевыми и события $b = 1$ и $b = 0$ не различимы. Но для ОПС с другими типами гистограмм использование ПД будет более эффективным, чем ЛКД, определенного для пространства $I_\alpha = \{1,\ 2,... ,\ N\}$. Для обычного детектора, т. е. ЛКД при $n \in I_\alpha$, оценка вероятности ошибочного детектирования ЦВЗ (10) справедлива, но изменяются аналитические оценки математического ожидания и дисперсии функционала $\Lambda^{ОД}$:

$$E\{\Lambda_0^{ОД}\} = N\left[\alpha\text{-}128\left(\sum_{C\in D_C} P(C) + \sum_{C\in A_C} P(C)\right)\right] \tag{14}$$

для $b = 1$,

$$E\{\Lambda_1^{ОД}\} = -E\{\Lambda_0^{ОД}\}, \tag{15}$$

для $b = 0$,

$$Var\{\Lambda^{ОД}\} = N\Bigg[\ \sigma_c^2 + \frac{256^2}{2}\Big(\sum_{C\in A_C} P(C) + \sum_{C\in D_C} P(C)\Big) - 256\Big(\sum_{C\in A_C} (C - C_0)P(C) - \sum_{C\in D_C} (C - C_0)P(C)\Big) - \\ - 128^2\left[\sum_{C\in A_C} P(C) + \sum_{C\in D_C} P(C)\right]^2\Bigg], \tag{16}$$

где $A_C = \{0,\ 1,\ ...,\ \alpha\text{-}1\}$; $D_C = \{255 - \alpha + 1,\ ...,\ 255\}$.

Для ОПС с гистограммой яркости (8) $E\{\Lambda_0^{ОД}\} = E\{\Lambda_1^{ОД}\} = 0$ и гипотезы $b = 1$ и $b = 0$ не различимы.

2.2 Модульное детектирование ЦВЗ

Описанные алгоритмы прореженного и обычного детектирования не являются оптимальными даже при гауссовом ОПС, если погружение ЦВЗ осуществлено на основе (3). В соответствии с критерием максимального правдоподобия алгоритм принятия решения оптимального модульного детектора (МД) имеет вид

$$\Lambda^{МД} = \sum_{n\le N}(((s(n) - \alpha w(n)) \bmod 256) - C_0)^2 - \sum_{n\le N}(((s(n) + \alpha w(n)) \bmod 256) - C_0)^2 \Rightarrow \begin{cases} 0, & \text{если } \Lambda^{МД} \le 0, \\ 1, & \text{если } \Lambda^{МД} > 0. \end{cases}$$

Для МД справедлива оценка (10), но после коррекции выражений для математического ожидания и дисперсии функционала, а именно:

$$E\{\Lambda_0^{МД}\} = N\Bigg[-4\alpha^2 - \Big(\frac{256^2}{2} - 512\alpha\text{-}256C_0\Big)\sum_{C\in A_C} P(C) - \Big(\frac{256^2}{2} - 512\alpha + 256C_0\Big)\sum_{C\in B_C} P(C) - \\ - 256\Big(\sum_{C\in A_C} CP(C) - \sum_{C\in B_C} CP(C)\Big)\ \Bigg] \tag{17}$$

для $b = 0$,

$$E\{\Lambda_1^{МД}\} = -E\{\Lambda_0^{МД}\} \tag{18}$$

для $b = 1$,

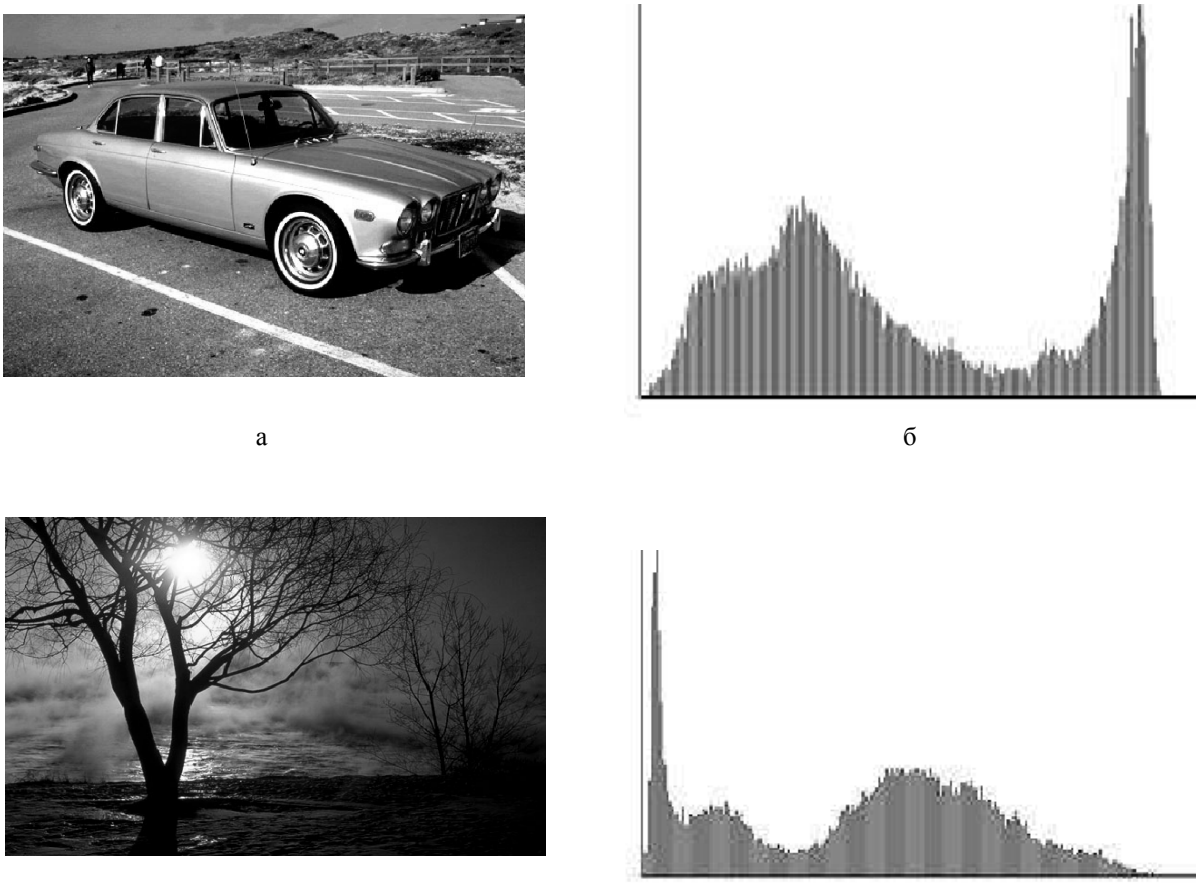
$$Var(\Lambda^{МД}) = \frac{N}{2}\Bigg[\sum_{c=0}^{255}[(c - C_0)^2 - (c + 2\alpha) \bmod 256 - C_0]^2 P(C) + \Bigg[\sum_{c=0}^{255}[(c - C_0)^2 - (c - 2\alpha) \bmod 256 - C_0]^2 P(C)\ \Bigg]^2 - \\ - \frac{1}{N^2}\Big[E\{\Lambda_o^{МД}\}\Big]^2, \tag{19}$$

где $A_C = \{0,\ 1,\ ...,\ 2\alpha\text{-}1\}$; $B_C = \{255 - 2\alpha + 1,\ ...,\ 255\}$.

В отличие от (13) и (16) расчет по (19) возможен численными методами. Подстановка (8) в (17) и (18) приводит к нулевому результату, как и ранее, т. е. для ОПС с плоскими гистограммами яркости различение гипотез $b = 1$ и $b = 0$ невозможно. Но для других типов гистограмм МД демонстрирует более высокую эффективность детектирования ЦВЗ, чем ПД. Весьма важным является вывод, что верификация сообщений на основе технологий ЦВЗ реализуема для различных типов детекторов. Это позволяет при формировании стегасообщения выбирать для каждого конкретного ОПС такой алгоритм погружения ЦВЗ, который наилучшим образом обеспечивает надежность восприятия стегасообщения с учетом особенностей конкретного ОПС. Для восстановления ОПС на приемной части системы в таком случае кроме секретного ключа понадобится некоторая дополнительная информация. Возможен перебор всех рабочих алгоритмов при детектировании стегасигнала и выбора обеспечивающего наилучший результат верификации. Если это допустимо практическим приложением системы с ЦВЗ, то при погружении для достижения наибольшей эффективности процедуры верификации ОПС можно корректировать гистограмму ОПС.

III Результаты моделирования

Для двух ОПС в виде монохромных изображений при N=64000 пикселей были получены гистограммы распределения яркости (рис. 1а, б – ОПС 1 и гистограмма; рис. 1в, г – ОПС 2 и гистограмма). Длина ЦВЗ в эксперименте N=64 бита, для передачи каждого использовалась ПСП длиной 1000. В зависимости от интенсивности ЦВЗ изменяется значение параметра $\mu = N_o / N$ (табл. 1). Исследуемые ОПС характеризуются различной вероятностью ошибки (табл. 2) при использовании рассмотренных трех типов детекторов: ПД, МД и ЛКД.



а б

в г

Рисунок 1 – ОПС 1 (а), ОПС 2 (в) и гистограммы распределения яркости (б, г), соответственно

Таблица 1 – Оценка параметра μ

α	1	2	3	5	6	10	20	30	50
ОПС 1	1	1	1	1	0,999	0,998	0,993	0,986	0,962
ОПС 2	1	2	0,998	0,992	0,989	0,985	0,964	-,882	0,644

Анализ полученных результатов (табл. 2) показывает, что для ОПС 2 МД значительно уступает ЛКД и ПД, в то время, как для ОПС 1 все три типа детекторов демонстрируют практически одинаковый уровень эффективности детектирования ЦВЗ, что подтверждает теоретические исследования.

Таблица 2 – Оценка вероятности ошибки детектирования ЦВЗ на основе имитационного моделирования

ОПС	Детектор	Параметр ЦВЗ α					
		3	4	5	6	10	30
ОПС 1	ОД	0,027	0,01	0,004	0,001	0.00003	0,002
	ПД	0,03	0,013	0,004	0,001	0.00001	0,00001
	МД	0,032	0,014	0,005	0,002	0,00002	0,001

Продовження Таблиці 2.

ОПС 2	ОД	0,074	0,128	0,348	0,541	0,592	0,297
	ПД	0,067	0,123	0,353	0,535	0,597	0,301
	МД	0,02	0,04	0,1	0,17	0,13	0,09

Оценка вероятности ошибки при использовании ПД на основе (14), (15), (16) продемонстрировала существенную зависимость α от параметра ЦВЗ (табл. 3). Данный эксперимент выявил существенное отличие модульного погружения от обычного, т. е. при использовании ЛКД. Вероятность ошибки при модульном погружении не является монотонной функцией интенсивности ЦВЗ и существует некоторое пороговое значение α, для которого P_e максимально, что также подтверждает аналитические исследования. Результаты аналитического моделирования (табл. 3) подтверждаются результатами имитационного моделирования (табл. 2).

Таблица 3 – Оценка вероятности ошибки детектирования ЦВЗ на основе аналитического моделирования

α	3	4	5	6	10	20	30
P_e	0,05	0,12	0,33	0,49	0,44	0,35	0,30

В качестве примера рассмотрена система с ЦВЗ при использовании МД, α=3, генерация для каждого информационного бита ЦВЗ 10 ПСП (чипов) длиной 1000. Для простоты эксперимента информационные биты ЦВЗ полагались нулевыми, ошибка соответствовала появлению единицы после декодирования. Повторение ПСП при передаче бита ЦВЗ несколько раз позволяет существенно снизить число ошибочно декодированных бит (табл. 4). Декодер может инвертировать сначала одиночные биты в последовательности после детектирования, на что потребуется при 64 бит ЦВЗ 64 итерации. Если результат верификации будет отрицательным, то потребуется инверитировать 2016 удвоенных бит, далее 41664 утроенных бит и т. д., что, однако, уже существенно удлинит и усложнит процедуру верификации.

Таблица 4 – Оценка ошибочного декодирования

№ теста	Число ошибок	Ошибочное декодирование
1	5	1000000000000001100000000000001000000000000000000000000010000000
2	3	1000000000000000100000000000010000000000000000000000000000000000
3	0	0000000000000000000000000000000000000000000000000000000000000000
4	2	1000000000000000000000000000000000000000000001000000000000000000
5	4	1000000000000001000000000000000000000000000000010000000000000001
6	1	0000000000000001000000000000000000000000000000000000000000000000
7	2	1000000000000000000000000000000000000000000010000000000000000000
8	0	0000000000000000000000000000000000000000000000000000000000000000
9	2	1000000000000000000001000000000000000000000000000000000000000000
10	4	1000000000000001000000000000000000000000000010000000000010000

Конечно, существуют более оптимальные коды с исправлением ошибок [4]. Однако их использование потребует еще большей избыточности относительно числа бит, необходимых для формирования ЦВЗ.

IV Выводы

Для верификации изображений на основе погружения ЦВЗ, представляющего собой ЦП данного ОПС в виде изображения, использование алгоритма погружения на основе модульного сложения позволяет выполнять восстановление ОПС после детектирования ЦВЗ, но приводит к ухудшению эффективности детектирования ЦВЗ. Получены аналитические выражения оценки вероятности ошибочного декодирования одного информационного бита ЦВЗ при использовании трех типов детекторов: ЛКД и предлагаемых адаптивных (ПД, МД). Выявлено важное свойство модульного аддитивного способа погружения ЦВЗ, заключающееся в том, что вероятность ошибки декодирования не является монотонной функцией интенсивности ЦВЗ и существует некоторое оптимальное значение параметра α, которому соответствует минимальное значение вероятности ошибки. Для всех типов детекторов ОПС в виде изображений с плоской гистограммой яркости не подлежат верификации без специальных мер предварительной обработки. Важным выводом является то, что уже на этапе погружения ЦВЗ в виде ЦП основного сообщения представляется возможным оценить возможность верификации ОПС. Разработчик системы может изменять значение параметра α, реализацию ЦВЗ, гистограмму ОПС [5]. Однако данные преобразования ОПС должны быть обратимыми и известными на приемной части системы. Чтобы не передавать дополнительную информацию возможно на приемной части использовать некоторую «кодовую книгу», задающую типы преобразований

ОПС, значения параметров. При этом процедура верификации потребует проведения тестов до получения наилучшего результата. В настоящей работе были исследованы тесты только для различных реализаций ЦВЗ, полученных в виде линейной или нелинейной функции некоторого секретного ключа.

*Литература **1**. Малахов В. П., Маракова И. И. Исследование секретних систем с цифровими водяными знаками// Труды Одесск. нац. политех. ун-та. — 2004. — вып. 1, С. 123 — 131. **2**. Coppersmith D., Mintzer E., Tresser C., Wu C. W., Yung M. M. Fragile Imperceptible Digital Watermark with Privacy Control // Security and Watermarking of Multimedia Contents. — SPIE-3657. — 1999. — P. 79 — 84. **3**. Schneier B. Applied Cryptography. Protocols, Algorithms and Source Code. —J. Wiley & Sons — N. Y. — 1994. —618 p. **4**. C. Schlegel, Trellis Coding, —IEEE Press, — 1997. — 340 p. **5**. Pratt W. K. Digital Image Processing. — J. Wiley&Sons. — N. Y. — 2001. — 734 p.*

УДК 621.396.6

АЛГОРИТМИЗАЦИЯ И ФОРМАЛИЗАЦИЯ ПРОЦЕССА ДЕФЕКТАЦИИ ОБОРУДОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ С АВАРИЙНЫМИ ПОВРЕЖДЕНИЯМИ

Лев Сакович, Виталий Павлов

Спецфакультет СБ Украины в составе ВИТИ НТУУ «КПИ»

Аннотация: **Встановлено порядок перевірки конструктивних елементів пошкоджених засобів зв'язку систем захисту інформації, обґрунтовано критерій визначення мінімального числа перевірених конструктивних одиниць виробів за заданою ймовірністю оцінки реального технічного стану, формалізовано процес визначення ступеня пошкодження обладнання засобів захисту інформації з апріорно невідомим ступенем пошкодження.**

Summary: **The certain order of the check constructive element damaged meanses of protection information, is motivated criterion of the determination of the minimum number checked constructive units of the product on given probability of the estimation of the real technical condition, formalized process of the determination degree damages of the equipping the meanses of protection information with a priori unknown degree of the damage.**

Ключевые слова: **Радиоэлектронные средства, аварийные повреждения, ремонт, дефектация.**

I Введение

Под дефектацией понимается процесс определения степени повреждения объекта, выявления явных дефектов и устранения вызванных ими неисправностей при восстановлении работоспособности оборудования систем защиты информации (СЗИ) после получения аварийных повреждений. Дефектация проводится для установления реального технического состояния поврежденного объекта и завершается выводом о целесообразности ремонта, его виде и месте проведения [1, 2].

II Постановка задачи

Анализ известных публикаций по дефектации [1 – 3] позволяет сформулировать постановку научной задачи исследований: при повреждении СЗИ известной конструкции необходимо установить за минимальное время с заданной вероятностью степень ее разрушения для принятия обоснованного решения о целесообразности и месте выполнения ремонта или списании и утилизации. С этой целью необходимо решить ряд частных задач:

1. установить порядок проверки технического состояния конструктивных единиц СЗИ;
2. сформировать комплексную оценку технического состояния СЗИ;
3. определить критерий завершения процесса дефектации.

Дефектация СЗИ является составной частью процесса ремонта, существенно влияющей на общее время восстановления их работоспособности. Технология дефектации исследована и разработана не в достаточной мере, что затрудняет работу персонала ремонтных органов по определению степени повреждения СЗИ и принятию обоснованного решения о целесообразности и месте проведения ремонта. Цель настоящей работы – исследование процесса дефектации для алгоритмизации и формализации действий персонала ремонтных органов при определении степени повреждения СЗИ.