

# ТЕЛЕКОММУНИКАЦИИ

УДК 621.39

## ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДВОИЧНОГО ИНФОРМАЦИОННОГО РЕСУРСА НА ОСНОВЕ СТРУКТУРНО-ЭНТРОПИЙНОГО СЛОТИРОВАНИЯ

ПОДЛЕСНЫЙ С.А.

Наводятся примеры использования видеоинформационного ресурса в Вооруженных Силах Украины. Аргументируется необходимость обеспечения категорий информационной безопасности в телекоммуникациях государственных учреждений. Указывается на уязвимость передачи видеоданных при медленных DDoS-атаках. Предлагается применять структурно-энтропийное слотирование в существующих технологиях обработки изображений. Обосновывается обеспечение позиционирования кодового представления в условиях проведения кибератак.

### Введение

В настоящее время в Вооруженных Силах Украины (ВСУ) широко применяются видеоинформационные ресурсы (ВИР) [1]. Одним из примеров использования ВИР являются беспилотные летательные аппараты в зоне проведения антитеррористической операции [2]. Второй областью применения ВИР в ВСУ является видеоконференцсвязь. Необходимость ее применения обусловлена требованием к оперативности принятия решений в кризисных ситуациях [3]. В ходе выполнения передачи видеоинформации противник может влиять на телекоммуникационное оборудование при проведении кибератак [4, 5]. Существенное влияние на передачу ВИР происходит при осуществлении медленной распределенной атаки типа «отказ в обслуживании» (slow DDoS). Эффективность данной кибератаки обусловлена тем, что краткосрочная атака не выявляется существующими системами предупреждения о вторжении, а полученная битовая ошибка в потоке кодов переменной длины сильно влияет на восстановление значений коэффициентов ДКП [6]. Поэтому возникает проблема обеспечения целостности информации в телекоммуникационных системах в условиях действия кибератак.

Для борьбы с такими ошибками в существующую технологию кодирования JPEG добавляют помехоустойчивое кодирование. Принцип работы такого кодирования в том, что к передаваемой информации добавляют проверочные биты [7]. Это позволяет выявить и исправить ошибки. В результате

происходит восстановление информации. Но в такой схеме присутствуют следующие недостатки:

– помехоустойчивое кодирование применяется с использованием аппаратных и временных затрат. Это приводит к увеличению времени обработки;

– при добавлении дополнительных битов увеличивается объем информации. Это приводит к увеличению времени передачи видеоинформации.

Данные недостатки влияют на оперативность передачи видеоинформации, что недопустимо для использования в военной сфере. Поэтому решение проблемы обеспечения целостности ВИР является актуальным.

Целью данного исследования является разработка метода обработки изображений, который обеспечивает позиционирование двоичного представления трансформанты в битовом потоке. Для данного метода выдвигаются условия сохранения временных затрат на передачу в телекоммуникационных системах.

Для достижения данной цели необходимо:

1. Провести модернизацию представления ВИР в существующих технологиях обработки изображений.

2. Разработать метод распределения двоичного представления трансформанты в кодовые конструкции фиксированной длины.

3. Проанализировать обеспечение целостности в условиях проведения кибератак для разработанного метода.

### 1. Разработка метода структурно-энтропийного слотирования

Для уменьшения информационной интенсивности двоичного представления трансформанты предлагается:

– формировать код  $N^{(j)}$  для каждой пары  $\tilde{u}_{i, i+1}$  элементов вектора  $U(\theta)$  линеаризированной трансформанты;

– в процессе формирования кода  $N^{(j)}$  учитывать структурно-статистическую зависимость между элементами  $u_i$  и  $u_{i+1}$ .

Формирование информационной части  $K^{(j)}$  кода  $N^{(j)}$  для элементов  $u_i$  и  $u_{i+1}$  задается следующим функционалом:

$$K^{(j)} := g^{(j)} \times f_{\alpha}(u_i, u_{i+1}) + f_{\beta}(u_i, u_{i+1}), \quad (1)$$

где  $j$  – индекс кода  $N^{(j)}$  пары элементов  $u_i$  и  $u_{i+1}$  линеаризированной трансформанты, который определяется как  $j = 0,5(i+1)$  и изменяется в диапазоне  $j = 1; \frac{\theta}{2}$ ;

$g^{(j)}$  – весовой коэффициент кода  $N^{(j)}$ , который определяется как максимум элементов  $u_i$  и  $u_{i+1}$ , т.е.  $g^{(j)} = \max(u_i; u_{i+1})$ ;  
 $f_\alpha(u_i, u_{i+1})$ ,  $f_\beta(u_i, u_{i+1})$  – функции обработки элементов  $u_i$  и  $u_{i+1}$ .

Для повышения устойчивости к битовым ошибкам используется технология упругого энтропийного кодирования (Error Resilient Entropy Code – EREC). Данная технология задается функцией преобразования  $f_{\text{errec}}$ . Это определяется таким соотношением:

$$\{N^{(j)}\} \xrightarrow{f_{\text{errec}}} S(\Lambda). \quad (2)$$

Здесь  $f_{\text{errec}}$  – функция распределения структурно-энтропийных кодов  $N^{(j)}$  по слотам  $s_\lambda$ ;  $\Lambda$  – количество слотов, в которые распределены структурно-энтропийные коды.

Технология EREC характеризуется следующими этапами:

- 1) размещение содержимого кодовых конструкций  $N^{(j)}$ ;
- 2) перераспределение содержимого кодовых конструкций  $N^{(j)}$ .

Данная технология размещает структурно-энтропийные коды  $N^{(j)}$  в слоты пакета EREC  $S(\Lambda)$  на основе перестройки битовой структуры. Здесь учитывается, что слотами являются кодовые слова равномерной длины, т.е.:

$$|s_a|_2 = |s_b|_2 = v, \text{ при } a \neq b. \quad (3)$$

В результате преобразования последовательности  $\{N^{(j)}\}$  структурно-энтропийных кодов  $N^{(j)}$  образуется пакет  $S(\Lambda)$  слотов. Вектор слотов (пакет) записывается следующим образом:

$$S(\Lambda) = \{s_1; \dots; s_\lambda; \dots; s_\Lambda\}.$$

Здесь  $s_1$  – начальный слот в пакете;  $s_\Lambda$  – последний слот в пакете.

Схематическое распределение структурно-энтропийных кодов  $N^{(j)}$  по слотам  $s_\xi$ , т.е.:

$$N^{(1)} \rightarrow s_\xi^{(1)}$$

в соответствии с технологией EREC, показано на рис. 1.

В данной формуле  $s_\xi^{(1)}$  – слот, сформированный при размещении кода  $N^{(1)}$ ; (1) – индекс начального этапа, соответствующий первичному размещению структурно-энтропийных кодов  $N^{(j)}$  по слотам.

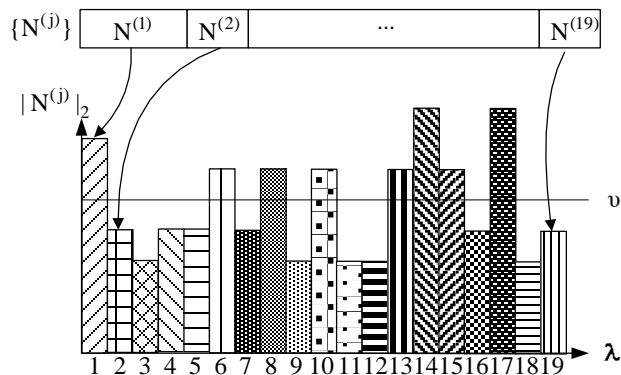


Рис. 1. Первичный этап размещения битовых составляющих кодовых конструкций при формировании пакета слотов

На данном рисунке представлено распределение кодового потока  $\{N^{(j)}\}$ , состоящего из  $\Lambda = 19$  структурно-энтропийных кодов  $N^{(j)}$  по 19 слотам. Различные структурно-энтропийные коды  $N^{(j)}$  представлены схематично в виде разных по окраске и размеру прямоугольников.

На первичном этапе рассматривается размещение структурно-энтропийных кодов  $N^{(j)}$  по слотам  $s_\xi$  без учета их выравнивания по длине  $v$ . Порядок заполнения слотов  $s_\xi$  определяется следующими правилами:

1) первое правило состоит в установлении порядка расстановки структурно-энтропийных кодов  $N^{(j)}$  по слотам пакета. Согласно этому правилу 1-й код  $N^{(1)}$  размещается в слоте  $s_1$  (как показано на рис. 1);

2) второе правило заключается в установке порядка заполнения слотов рядами структурно-энтропийных кодов  $N^{(j)}$ . Согласно этому правилу старшие разряды  $q_{\xi,\gamma}$ ;  $\gamma \rightarrow 1$  кодовой конструкции

$N^{(j)}$  размещаются в нижних битовых позициях слота  $s_\xi$ . Наоборот, младшие разряды  $q_{\xi,\gamma}$ ;  $\gamma \rightarrow |N^{(\xi)}|_2$  кодовой конструкции  $N^{(\xi)}$  размещаются в верхних битовых позициях слота  $s_\xi$ .

Следующим этапом формирования пакета слота является выравнивание длин кодовых слов  $s_\xi$  для выполнения условия (2) в случае, когда известно количество  $\Lambda$  слотов в пакете. Для этого сначала требуется определить длину  $v$  слота.

Длина  $v$  слота определяется как отношение суммарной длины  $|\{N^{(j)}\}|_2$  последовательности

$\{N^{(j)}\}$  кодов к количеству  $\Lambda$  слотов. Формула расчета длины указана в следующем выражении:

$$v = \frac{|\{N^{(j)}\}|_2}{\Lambda} = \left\lceil \frac{1}{\Lambda} \sum_{i=1}^{\theta} |N^{(i)}|_2 \right\rceil. \quad (4)$$

Здесь  $\lceil x \rceil$  – оператор округления значения  $X$  до большего натурального числа.

После определения длины  $v$  слота возможны случаи, когда длина  $|N^{(j)}|_2$  структурно-энтропийного кода  $N^{(j)}$  не будет равна длине  $v$  слота.

В общем случае избыточная составляющая  $\Delta N^{(\xi)}$  структурно-энтропийного кода  $N^{(\xi)}$  будет размещена по нескольким слотам  $s_i$  (рис. 2).

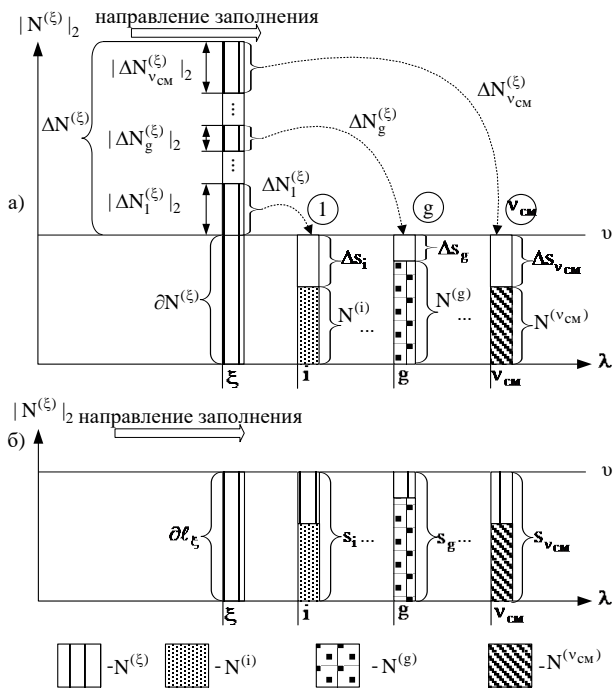


Рис. 2. Структурная схема многослового распределения структурно-энтропийного кода  $N^{(\xi)}$ :  
а – до распределения; б – после распределения

Процесс перераспределения избыточных составляющих  $\Delta N^{(\xi)}$  структурно-энтропийных кодов  $N^{(\xi)}$ , с учетом размещения по нескольким слотам  $s_i$ , включает в себя следующие этапы:

1) определение позиций  $i$  избыточных составляющих  $\Delta s_i$

$$i = \begin{cases} \xi + 1; \Lambda & \text{при } i > \xi; \\ 1; \xi - 1 & \text{при } i < \xi \end{cases}$$

слотов  $s_i$  относительно перераспределяемой избыточной составляющей  $\Delta N^{(\xi)}$  структурно-энтропийного кода  $N^{(\xi)}$ ;

2) определение количества  $v_{cm}$  и размеров  $|\Delta s_i|_2$  избыточных составляющих  $\Delta s_i$  слотов  $s_i$ , в которые будут распределены избыточные составляющие  $\Delta s_i$  слотов  $s_i$  образуют подпоследовательность  $\Delta S(v_{cm})$ , которая записывается следующим образом:

$$\Delta S(v_{cm}) = \{\Delta s_i; \dots; \Delta s_g; \dots; \Delta s_{v_{cm}}\}. \quad (5)$$

Здесь  $v_{cm}$  – количество слотов (этапов), в которые происходит перераспределение всей избыточной составляющей  $\Delta N^{(\xi)}$ , длиной  $|\Delta N^{(\xi)}|_2$ ;  $\Delta s_g$  – избыточная составляющая слота  $s_g$  при  $g$ -м этапе его заполнения.

При этом формула, определяющая распределение избыточной составляющей  $\Delta N^{(\xi)}$  структурно-энтропийного кода  $N^{(\xi)}$  по слотам, следующая:

$$|N^{(\xi)}|_2 = \sum_{g=1}^{v_{cm}} |\Delta s_{\xi+d_g}|_2, \quad d_g = \overline{1; \Lambda - 1}. \quad (6)$$

Для  $g$ -го этапа распределения избыточной составляющей  $\Delta N^{(\xi)}$  структурно-энтропийного кода

$N^{(\xi)}$  с позицией  $\xi$  проверяется остаток слота  $\Delta s_{\xi+d_g}^{(\gamma)}$  с позицией  $\xi+d_g$ . Данный остаток слота  $\Delta s_{\xi+d_g}^{(\gamma)}$  образовался в результате заполнения слота  $s_{\xi+d_g}$  с позицией  $\xi+d_g$  структурно-энтропийным

кодом  $N^{(\xi+d_g)}$  и некоторым количеством  $\gamma$  избыточных составляющих  $\Delta N^{(i)}$  кодов  $N^{(i)}$  с позицией  $i \neq \xi$ .

Старшие разряды избыточной составляющей  $\Delta N^{(\xi)}$  структурно-энтропийного кода  $N^{(\xi)}$  при этом заполняют избыточную составляющую  $\Delta s_{\xi+d_g}^{(\gamma)}$  слота  $s_{\xi+d_g}$ . Схематически результат заполнения показан на рис. 3.

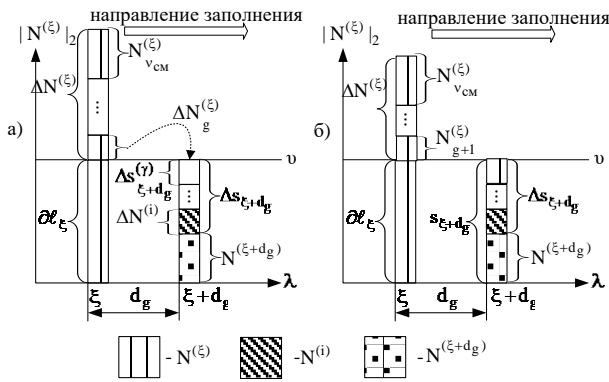


Рис. 3. Распределение структурно-энтропийного кода  $N^{(\xi)}$  на  $g$ -м этапе:  
а – до распределения; б – после распределения

Этапы перераспределения структурно-энтропийного кода  $N^{(\xi)}$  повторяются до устранения в позиции  $\xi$  положительной избыточности, вызванной перегрузкой слота. Результат окончательного распределения структурно-энтропийного кода  $N^{(\xi)}$  с позицией  $\xi$  за  $v_{\text{см}}$  этапов представлен на рис. 4.

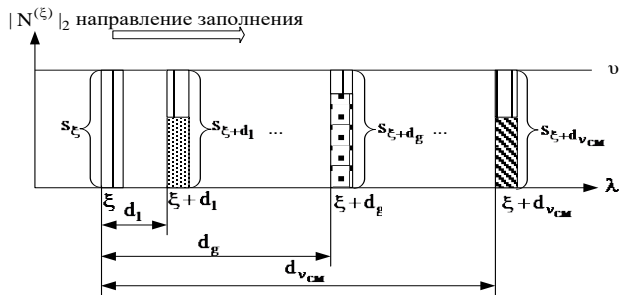


Рис. 4. Результат распределения структурно-энтропийного кода  $N^{(\xi)}$

Различные структурно-энтропийные коды  $N^{(\xi)}$  представлены схематично в виде различных по окрасу и размеру прямоугольников.

Распределение всей последовательности  $\{N^{(\xi)}\}$  структурно-энтропийных кодов  $N^{(\xi)}$  происходит по аналогичному сценарию. Результат распределения всей последовательности  $\{N^{(\xi)}\}$  структурно-энтропийных кодов  $N^{(\xi)}$ , представленной на рис. 1, по пакету  $S(\Lambda)$  слотов  $s_{\xi}$ , в соответствии с технологией EREC, показан на рис. 5.

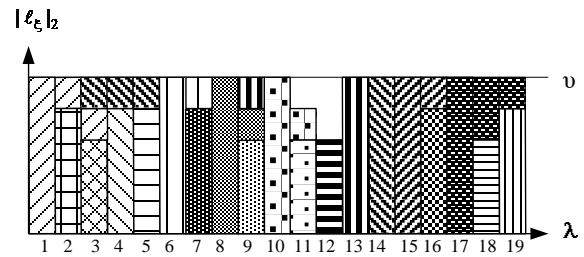


Рис. 5. Результат размещения битовых составляющих кодовых конструкций в сформированном пакете слотов

## 2. Разработка метода структурно-энтропийного деслотирования

Имея информацию о данном алгоритме при отсутствии ошибок в канале, на приемной стороне кодовую последовательность  $\{N^{(\xi)}\}$  структурно-энтропийных кодов  $N^{(\xi)}$  можно взаимнооднозначно восстановить и декодировать. Рассмотрим процесс декодирования распределенных структурно-энтропийных кодов  $N^{(\xi)}$  и восстановления компонент  $u_{\xi}$  трансформанты на приемной стороне.

По условиям предлагаемого алгоритма необходимо идентифицировать структурно-энтропийные коды  $N^{(\xi)}$ , полностью вошедшие в соответствующие слоты  $S_{\xi}$  при первичном заполнении, и определить номер  $i$ -х позиций слотов  $S_i$ , которые имеют избыточность  $|s_i|_2$ . Номер позиции необходим для сборки структурно-энтропийных кодов  $N^{(\xi)}$ , которые были распределены по нескольким слотам  $S_i$ .

В предлагаемом алгоритме количество слотов  $s_{\lambda}$  составляет фиксированное значение  $\Lambda$ . При этом информация о длине  $|S(\Lambda)|_2$  пакета слотов предоставляется декодеру. Используя длину  $|S(\Lambda)|_2$  пакета  $S(\Lambda)$  слотов и количество  $\Lambda$  слотов, декодер определяет длину  $v$  слота:

$$v = \frac{|S(\Lambda)|_2}{\Lambda}.$$

Информация о длине слота позволяет определить позиционирование всех слотов  $S_{\lambda}$  в пакете  $S(\Lambda)$ . Порядок заполнения слотов  $s_{\xi}$  предоставляет возможность идентифицировать начало  $\alpha_{\xi}$  каждого структурно-энтропийного кода  $N^{(\xi)}$ , как указано на рис. 6.

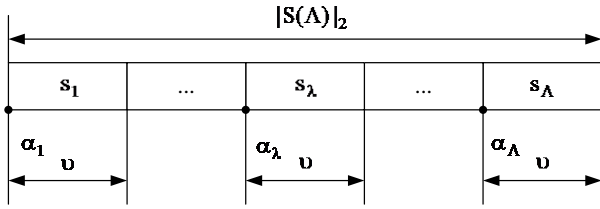


Рис. 6. Процесс разделения пакета  $S(\Lambda)$  слотов  $s_\lambda$  и определения начала  $\alpha_\lambda$  кодов  $N^{(\xi)}$

Это позволяет декодеру синхронизироваться с потоком битов в начале каждого слота.

Выделив из пакета  $S(\Lambda)$  отдельный слот  $s_\xi$ , производим процесс поразрядной сборки структурно-энтропийного кода  $N^{(\xi)}$ . При поразрядной сборке первого структурно-энтропийного кода  $N^{(1)}$  индекс позиции структурно-энтропийного кода  $N^{(\xi)}$  в кодовом потоке принимается равным  $\xi = 1$ .

На первоначальном этапе  $g = 1$  старшему разряду  $q_{\xi,1}$  структурно-энтропийного кода  $N^{(\xi)}$  приводится в соответствие значение двоичного разряда  $h_{\xi,1}$  нижней битовой позиции слота  $s_\xi$ , т.е.:

$$q_{\xi,1} := h_{\xi,1}. \quad (7)$$

При этом данный разряд формирует содержимое части кода  $\partial N^{(\xi)}$ :

$$[\partial N^{(\xi)}]_2 = \{q_{\xi,1}\}.$$

В результате этого длина  $|\partial N^{(\xi)}|_2$  части кода  $\partial N^{(\xi)}$  равняется:

$$|\partial N^{(\xi)}|_2 = 1.$$

После этого декодер на основе функции  $f_{\text{vlc}}^{-1}(\partial N^{(\xi)}, P_{\text{сл}})$  идентифицирует окончания  $\xi$ -й кодовой комбинации  $N^{(\xi)}$ .

Успешная идентификация приводит к следующим последствиям:

а) кодовой комбинации  $N^{(\xi)}$  приводится в соответствие часть кода  $\partial N^{(\xi)}$ :

$$N^{(\xi)} := \partial N^{(\xi)};$$

б) восстанавливается соответствующая компонента  $u_\xi$ ;

в) фиксируется длина  $|\partial N^{(\xi)}|_2$  части кода  $\partial N^{(\xi)}$ ;

г) дальнейшая сборка структурно-энтропийного кода  $N^{(\xi)}$  прекращается.

Если идентификация окончания  $\xi$ -й кодовой комбинации  $N^{(\xi)}$  не удалась, то разряду  $q_{\xi,2}$  струк-

турно-энтропийного кода  $N^{(\xi)}$  приводится в соответствие двоичный разряд  $h_{\xi,2}$  следующей битовой позиции слота  $s_\xi$ , т.е.:

$$q_{\xi,2} := h_{\xi,2}. \quad (8)$$

При этом изменяется содержимое  $[\partial N^{(\xi)}]_2$  части кода  $\partial N^{(\xi)}$ :

$$[\partial N^{(\xi)}]_2 = \{q_{\xi,1}; q_{\xi,2}\}.$$

Соответственно длина  $|\partial N^{(\xi)}|_2$  части кода  $\partial N^{(\xi)}$  при этом увеличивается:

$$|\partial N^{(\xi)}|_2 := |\partial N^{(\xi)}|_2 + 1.$$

После этого декодер на основе функции  $f_{\text{vlc}}^{-1}(\partial N^{(\xi)}, P_{\text{сл}})$  повторно производит идентификацию окончания  $\xi$ -й кодовой комбинации  $N^{(\xi)}$ .

Данные операции первоначального этапа побитного внесения двоичных разрядов  $h_{\xi,\mu}$  слота  $s_\xi$  в содержимое части кода  $\partial N^{(\xi)}$  продолжают до момента:

- 1) идентификации окончания  $\xi$ -й кодовой комбинации  $N^{(\xi)}$ ;
- 2) использования всех двоичных разрядов  $h_{\xi,\mu}$  слота  $s_\xi$ .

В первом случае декодер восстанавливает соответствующую компоненту  $u_\xi$ . Также при этом формируется избыточная составляющая  $\Delta s_\xi$  слота  $s_\xi$ .

Она задается следующим образом:

$$[\Delta s_\xi]_2 = \{h_{\xi,|\ell_\xi|_2+1}; \dots; h_{\xi,\nu}\}. \quad (9)$$

В данной формуле  $h_{\xi,\mu} - \mu$ -й разряд слота  $s_\xi$ .

Длина  $[\Delta s_\xi]_2$  избыточной составляющей слота  $\Delta s_\xi$  находится как разница длины  $\nu$  слота  $s_\xi$  и длины  $|\ell_\xi|_2$  идентифицированного структурно-энтропийного кода  $N^{(\xi)}$ :

$$|\Delta s_\xi|_2 = \nu - |\ell_\xi|_2.$$

Во втором случае процесс дальнейшей поразрядной сборки структурно-энтропийных кодов  $N^{(\xi)}$  требует обращения к содержимому избыточных составляющих  $\Delta s_i$  других слотов  $s_i$ ,  $i \neq \xi$ . Это обращение производится только после идентификации других структурно-энтропийных кодов  $N^{(i)}$ ,  $i \neq \xi$ , т.е. выполнения этапа  $g = 1$  на позициях всех слотов  $s_i$ .

Значения позиций данных избыточных составляющих  $\Delta s_i$  слотов  $s_i$  в последовательности  $S(\Lambda)$

задаются индексом структурно-энтропийного кода  $N^{(\xi)}$  и вектором смещения  $D(v_{cm})$ .

При этом внесении двоичных разрядов  $h_{\xi+d_g, \mu}$  избыточных составляющих  $\Delta s_{\xi+d_g}^{(\gamma)}$  слота  $s_{\xi+d_g}$  в содержимое части кода  $\partial N^{(\xi)}$  продолжаются до идентификации окончания  $\xi$ -й кодовой комбинации  $N^{(\xi)}$ . Следует заметить, что каждый этап сборки структурно-энтропийных кодов  $N^{(\xi)}$  должен происходить после завершения предыдущего на позициях всех слотов  $s_i$ .

Результат формирования структурно-энтропийного кода  $N^{(\xi)}$  при обращении к битовым составляющим нескольких слотов представлен на рис. 7.

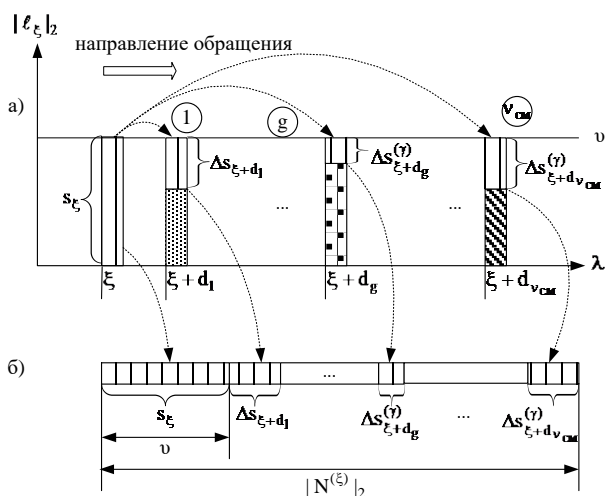


Рис. 7. Сборка структурно-энтропийного кода  $N^{(\xi)}$  по подпоследовательности  $\Delta s(v_{cm})$  до идентификации окончания кодовой комбинации  $N^{(\xi)}$ : а – изъятие битовых составляющих других слотов  $s_{\xi+d_g}$ ; б – результат формирования кода  $N^{(\xi)}$

Остаточная избыточность битов, которые использовались при формировании пакета  $S(\Lambda)$  слотов  $s_{\xi}$ , на результат декодирования не влияет. Результатом обработки всех слотов  $s_{\xi}$  в пакете  $S(\Lambda)$  является восстановление всех компонент  $u_{\xi}$  линейаризованной трансформанты.

### 3. Оценка целостности данных для метода структурно-энтропийной обработки

В условиях отсутствия ошибок в процессе передачи слотов  $s_{\xi}$ , обработки и сборки структурно-

энтропийных кодов  $N^{(\xi)}$  декодирование производится взаимно-однозначно. Тогда квантованные значения компонент  $u_{\xi}$  линейаризованной трансформанты восстанавливаются без ошибок.

Псевдо-случайное смещение последовательности  $d_g$  обеспечивает лучшие свойства отказоустойчивости из-за его некоррелированной характеристики, так как  $d_{g+i}$  от  $d_g$ . Таким образом, два структурно-энтропийных блока  $\lambda$ -го слота не будут искажаться в том же порядке, что может быть использовано для повышения устойчивости к ошибкам.

Алгоритм обратного перераспределения будет продолжаться до окончательной идентификации всех компонент  $u_{\xi}$  линейаризованной трансформанты. При этом процесс идентификации выполняется параллельно.

В случае наличия битовой ошибки в  $\mu$ -м разряде  $h'_{\lambda, \mu}$   $\lambda$ -го слота  $s_{\lambda}$

$$h'_{\lambda, \mu} \neq h_{\lambda, \mu}$$

процесс декодирования будет зависеть от битового положения в слоте:

- 1) Если идентификация  $\lambda$ -й кодовой комбинации  $N^{(\lambda)}$  до считывания разряда  $h_{\lambda, \mu}$  слота  $s_{\lambda}$  не была произведена, то возможна неверная идентификация окончания  $\lambda$ -й кодовой комбинации  $N^{(\lambda)}$ .
- 2) При идентификации  $\lambda$ -й кодовой комбинации  $N^{(\lambda)}$  ошибка затрагивает избыточную составляющую  $\Delta s_{\lambda}^{(\gamma)}$  слота  $s_{\lambda}$ , к которой идет обращение при сборке на  $g$ -м этапе  $\xi$ -го структурно-энтропийного кода  $N^{(\xi)}$ ,  $\xi = \lambda - d_g$ . При этом также возможна неверная идентификация окончания  $\xi$ -й кодовой комбинации  $N^{(\xi)}$ . Идентификация кода  $N^{(\lambda)}$  и кодов  $N^{(i)}$ , избыточные составляющие которых входят в избыточные составляющие  $\Delta s_{\lambda}^{(j)}$ ,  $j < \gamma$  слота  $s_{\lambda}$ , будет произведена верно.

Для первого варианта положения ошибочного разряда  $h'_{\lambda, \mu}$  при изменении длины  $|N^{(\lambda)}|_2$  кодовой комбинации  $N^{(\lambda)}$ :

- а) в сторону увеличения  $|N^{(\lambda)}|_2 > |N^{(\lambda)}|_2$  ошибка распространяется на коды  $N^{(i)}$ , которые при сборке должны были использовать разряды слотов  $s_i$  с позицией  $i \in \{\lambda + d_{v_{cm}}; \dots; \lambda + d_{v'_{cm}}\}$  и битовое по-

ложение в слоте после избыточной составляющей  $N'_{v_{cm}}^{(\lambda)}$  кода  $N^{(\lambda)}$ ;

б) в сторону уменьшения  $|N^{(\lambda)}|_2 > |N'^{(\lambda)}|_2$  ошибка распространяется на коды  $N^{(i)}$ , которые при сборке будут использовать разряды слотов  $s_i$  с позицией  $i \in \{\lambda + d_{v_{cm}}; \dots; \lambda + d_{v_{cm}}\}$  и битовое положение в слоте после избыточной составляющей  $N'_{v_{cm}}^{(\lambda)}$  кода  $N^{(\lambda)}$ .

При втором варианте положения ошибочного разряда  $h'_{\lambda, \mu}$  ситуация повторяется для кода  $N^{(\xi)}$ .

Наглядное представление неверного декодирования пакета слотов с рис. 1 при ошибке разряда 5 в слоте 1 показано на рис. 8.

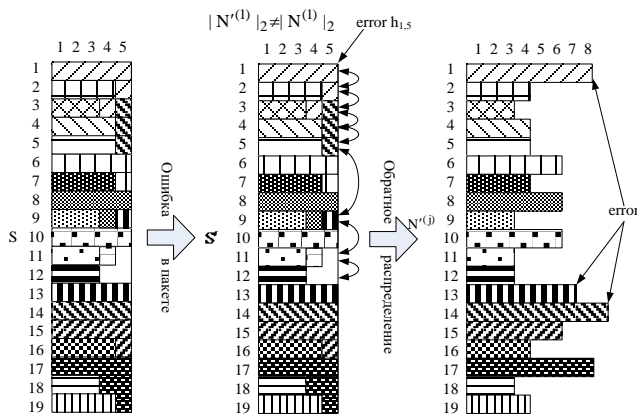


Рис. 8. Влияние ошибки в разряде  $h_{1,5}$  слота  $s_1$  на определение длин  $|N^{(i)}|_2$  кодов  $N^{(i)}$  последовательности  $\{N^{(j)}\}$

В случае ошибочного декодирования первого структурно-энтропийного кода  $N^{(1)}$  декодер неверно определит длину первого кода. В результате искажения слота 1 распространение ошибки позиционирования будет локализовано областью слотов 1, 13 и 14. Для обратного распределения коды с 2 по 12 и с 15 по 19 останутся незатронутыми.

Из количества затронутых ошибкой кодовых слов видно достоинство использования технологии структурно-энтропийного слотирования.

Для восстановления кодов 1, 13 и 14 декодер может использовать как предыдущие, так и следующие значения разрядов, определенных алгоритмом распределения. Ошибка на этапе обработки величины  $K^{(j)}$ , которая соответствует кодовому

представлению пары  $\tilde{u}_{i, i+1}$  элементов вектора  $U(\theta)$  линейризованной трансформанты, на позиционирование кодов  $N^{(\xi)}$ ,  $\xi \neq j$  остальных пар компонент не влияет.

В общем случае при неискаженном значении энтропийного кода  $\Gamma_g^{(j)}$ , который соответствует  $\gamma$ -му диапазону величины  $g^{(j)}$  кода  $N^{(j)}$ , ошибка восстановления пары  $\tilde{u}_{i, i+1}$  элементов вектора  $U(\theta)$  будет локализована в области величины  $g^{(j)}$ . Технология структурно-энтропийного слотирования позволяет увеличить скорость восстановления компонент изображения. Данная технология также обеспечивает локализацию ошибки восстановления для НЧ компонент изображения и позиционирования для ВЧ компонент изображения. Этим обеспечивается целостность двоичного представления трансформанты изображения.

### Выводы

Разработана технология структурно-энтропийного слотирования кодового представления пар элементов линейризованной трансформанты. Эта технология учитывает как структурную особенность и зависимость между элементами в кодируемой паре, так и статистические характеристики значений элементов в обрабатываемой трансформанте. Разработана технология позиционирования двоичного представления трансформанты при структурно-энтропийном слотировании в условии проведения кибератак.

**Литература:** 1. Баранник В.В., Підлісний С.А. Обґрунтування підходу щодо створення технології кіберзахисту відеоінформаційного ресурсу в інфокомунікаційному просторі // Науковий часопис Національного університету «Київський політехнічний інститут». 2016. №1(29). С. 82 – 86. 2. Barannik V., Podlesny S., Krasnorutskyi A., Musienko A. and Himenko V. The ensuring the integrity of information streams under the cyberattacks action // IEEE East-West Design & Test Symposium (EWDTS), 2016. P. 1-5. 3. Barannik V., Podlesny S. A., Yalivets K. and Bekirov A., The analysis of the use of technologies of error resilient coding at influence of an error in the codeword // 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET). 2016. P. 52-54. 4. Barannik V.V., Akimov R.I., Vlasov A.V. Method of increasing availability and integrity of video information resources // XIIth International Conference "Modern problems of radio engineering, telecommunications and computer science, TCSET"2014. 2014. 532 p. 5. Баранник В.В., Рябуха Ю.Н. Метод повышения информационной безопасности в системах видеомониторинга кризисных ситуаций. Черкассы, 2015. 143 с. 6. Баранник В.В., Власов А.В., Сидченко С.А., Бекіров А.Э. Обоснование значимых угроз безопасности

відеоінформаційного ресурса систем відеоконференцсвязи профільних систем управління // Інформаційно-управляючі системи на ЖД транспорті. 2014. №3. С. 24 – 31. 7. *Бараннік В.В., Власов А.В., Тарнополов Р.В.* Модель загроз безпеки відеоінформаційного ресурсу систем відеоконференцсвязки // Науковий журнал. 2014. № 1 (21). С. 55 – 60. 8. *Бараннік В., Красноруцький А.*, Побудова правила формування позиційних структурно-вагових чисел в умовах кодування за заданою довжиною // Безпека інформації. 2014. Т. 20, №. 1. С. 62-65.

#### **Transliterated bibliography:**

1. *Barannik V.V., Pidlisnyj S.A.*, Obg'runtuvannja pidhodu shhodo stvorennja tehnologii' kiberzahystu videoinformacijnogo resursu v infokomunikacijnomu prostori // Naukojemni tehnologii', 2016, №1(29), S. 82 – 86.
2. *Barannik V., Podlesny S., Krasnorutskyi A., Musienko A. and Himenko V.*, The ensuring the integrity of information streams under the cyberattacks action // IEEE East-West Design & Test Symposium (EWDTS), 2016, pp. 1-5 (in print).
3. *Barannik V., Podlesny S. A., Yalivets K. and Bekirov A.*, The analysis of the use of technologies of error resilient coding at influence of an error in the codeword // 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), 2016, pp. 52-54.
4. *Barannik V.V., Akimov R.I., Vlasov A.V.*, Method of increasing availability and integrity of video information resources // XIIth International Conference "Modern problems of radio engineering, telecommunications and computer science, TCSET'2014, 2014. p. 532.

5. *Barannik V.V., Rjabuha Ju.N.*, Metod povyshenija informacionnoj bezopasnosti v sistemah videomonitoringa krizisnyh situacij, Cherkassy, 2015, 143 s.

6. *Barannik V.V., Vlasov A.V., Sidchenko S.A., Bekirov A.Je.*, Obosnovanie znachimyh ugroz bezopasnosti videoinformaci-onnogo resursa sistem videokonferencsvjazi profil'nyh sistem upravlenija // Informacionno-upravljajushhie sistemy na ZhD transporte, 2014, №3. S. 24 – 31.

7. *Barannik V.V., Vlasov A.V., Tarnopolov R.V.*, Model' zagroz bezpeky videoinformacijnogo resursu system videokonferencsv'jazku // Naukojemni tehnologii', 2014, № 1 (21). S. 55 – 60.

8. *Barannik V., Krasnoruckyj A.*, Pobudova pravyla formuvannja pozycijnyh strukturno-vagovyh chysel v umovah kodoutvorennya za zadanoju dovzhynuju // Bezpeka informacii', 2014, T. 20. №. 1. S. 62-65.

Поступила в редколлегию 18.09.2016

**Рецензент:** д-р техн. наук, проф. Безрук В.М.

**Подлесный Сергей Анатоліевич**, начальник отделения центра Харьковского национального университета Воздушных Сил. Научные интересы: сетевые технологии, обработка информации. Адрес: Украина, 61000, Харьков, ул. Сумская 77/79, тел. 0635653862.

**Podlesny Sergey Anatolievich**, head of the center department in the Kharkiv national university of Air Forces. Scientific interests: network technologies, information processing. Kharkov, Sumskaia st. 77/79, +380635653862.