

МЕТОД КРИПТОКОМПРЕССИОННОГО ПРЕДСТАВЛЕНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ АДАПТИВНОГО ОБОБЩЕННОГО ПОЗИЦИОННОГО КОДИРОВАНИЯ ДЛЯ БИНОМИНАЛЬНОГО ПРОСТРАНСТВА

Баранник В.В., Сидченко С.А.

Введение

Современное развитие государства в различных сферах деятельности (политическая, социальная, экономическая, управленческая) неразрывно связано с обеспечением должного уровня информатизации. В последнее время наибольшее применение получили системы сбора информации с использованием дистанционных инфокоммуникационных технологий (системы видеонаблюдения и мониторинга); корпоративные и локальные информационно-коммуникационные системы и сети кризисной инфраструктуры государства; телевизионные системы и системы видеоконференцсвязи; системы связи и передачи информации, в особенности мобильной радиосвязи и космические телекоммуникационные системы.

Видеоинформация приобретает значение важного ресурса, влияющего на национальную безопасность, безопасность коммерческих структур и соблюдения прав личности, и определяет уровень экономического развития государства, его оборонный потенциал, формирование общественного мнения. По данным компании Cisco доминирующими приложениями останутся видеосервисы и передача мультимедийных файлов. Так только по прогнозам в мировом Интернет-трафике к 2020 г. доля видео составит 79 % (в 2015 г. этот показатель составлял 63 %). В мире ежемесячно будет транслироваться три триллиона минут видео, что эквивалентно пяти миллионам лет видео в месяц.

В тоже время для внедрения видеоинформационного ресурса (ВИР) в жизнедеятельность общества и государства присутствуют следующие проблемные ограничения: *Первое проблемное ограничение (на законодательном уровне)*. Любое видеонаблюдение приводит к получению персональных данных [1], как непосредственно, так и опосредованно. А любые персональные данные могут быть отнесены к конфиденциальной информации на основании законов или человеком, о котором эти данные собираются. При этом законодательством Украины не установлен четкий перечень сведений о физическом лице, которые являются персональными данными [1]. Современное состояние правового регулирования видеонаблюдения в Украине является ненадлежащим, многие вопросы регулируются подзаконными нормативными актами (внутренними приказами), которые должны детализировать отдельные положения закона, а в законе в свою очередь они не отражены [1]. Способы и методы защиты видео- и фотоматериалов на законодательном уровне не определены, хотя

необходимость обеспечения надлежащего хранения закреплена в ряде нормативно-правовых актов, в которых затрагиваются вопросы применения систем видеонаблюдения. При этом, резолюция Парламентской Ассамблеи Совета Европы по осуществлению видеонаблюдения в общественных местах рекомендует на законодательном уровне закрепить практику кодирования (шифрования) данных видеонаблюдения для защиты их от несанкционированного доступа и модификации, что может помочь гарантировать их достоверность для уголовных расследований [2].

Сейчас в Украине обеспечение защиты ВИР с длительной актуальностью по времени проводится в основном на основе организационных мероприятий, а для ВИР с ограниченной актуальностью по времени либо отсутствует, либо проводится на основе механизмов разграничения доступа.

Второе проблемное ограничение. Присутствие антропогенных и техногенных угроз требует обеспечение конфиденциальности ВИР, которое приводит к увеличению временных затрат на обработку и доставку видеоданных, т.е. происходит снижение их доступности. В свою очередь, поддержание доступности ВИР обеспечивается при снижении ее конфиденциальности.

Третье проблемное ограничение связано с ограниченностью пропускной способности телекоммуникационных систем, в особенности построенных на основе дистанционных средств. При этом для обеспечения конфиденциальности при поддержании заданной оперативности необходимо снизить объем полезной информации, что приведет к уменьшению достоверности, т.е. потере целостности.

Отсюда **актуальной научно-прикладной проблемой** является повышение категорий информационной безопасности видеоинформации, которая обрабатывается и передается с использованием беспроводных телекоммуникационных технологий в условиях реального времени.

Анализ последних исследований и публикаций. На сегодняшний день наиболее популярным решением для обеспечения конфиденциальности информации является шифрование. Однако существенным недостатком криптографических алгоритмов является то, что подавляющее большинство методов являются универсальными, т.е. не учитывают особенности источников информации. За последние годы было предложено множество специализированных алгоритмов шифрования для решения проблемы защиты цифровых изображений и потока видеоинформации. Один из первых широко распространенных подходов заключался в перестановке строк или столбцов кадров видеопотока [3]. Большинство таких алгоритмов не обеспечивают достаточную криптостойкость и были подвергнуты вскрытию. Вместе с тем, в настоящее время активно ведутся разработки в области визуальной

криптографии, впервые предложенные М. Наором и А. Шамиром [4]. Однако предложенные подходы применяются к исходным видеоданным, но на практике исходный объем ВИР может быть большим, что приведет к потере оперативности при обработке данных в реальном режиме времени.

В случае обеспечения конфиденциальности изображений следует учитывать, что:

1) для видеоинформации кардинально меняется вопрос, связанный с ее защитой, а именно встает вопрос с резким разделением информационной защиты на семантический и синтаксический уровень;

2) видеоинформация – особый источник информации, имеющий аналоговую природу и до 90 % обусловленный психофизическими особенностями ее восприятия зрительной системой;

3) наличие многомерных связей;

4) отсутствие методологически обоснованного математического аппарата позволяющего устанавливать взаимосвязи между качественной и количественной сторонами видеоинформации;

5) наличие значительного количества показателей оценки качества и количества видеоинформации и видеоданных.

Поэтому возникла необходимость в разработке принципиально новой технологии, которая одновременно обеспечивает повышение оперативности доведения видеоинформации и ее защиту на основе методов семантической и синтаксической обработки изображений. В работах [5–9] была предложена технология криптокомпрессионного представления (ККП) изображений, предназначенная для сокрытия семантического содержания изображения с учетом как статистических, так и структурных особенностей источника информации. На основе разработанной технологии в работах [10, 11] предложен метод ККП изображений на основе статической схемы обобщенного позиционного кодирования в двумерном базисе. Одним из недостатков такого подхода является построение информационной составляющей (ИС) ККП на основе одинакового количества исходных элементов фрагмента видеоданных. Длина большинства кодограмм ИС ККП в битном представлении при таком подходе является значительно меньшей, чем выделяется для хранения кодового слова. Это приводит к появлению большого количества незначимых нулевых элементов в битных последовательностях ИС ККП [12, 13]. Этот недостаток влияет на объем ИС ККП и на выходные статистические характеристики ИС ККП. Поэтому в [12–16] был предложен метод ККП изображений на основе плавающей схемы в базисе по верхним границам. Для дополнительного сокращения избыточности и повышения криптостойкости представления кода ИС ККП предлагается внести изменение в структурную схему построения систем ККП изображений.

Целью исследований является разработка метода криптокомпрессионного представления изображений на основе адаптивного обобщенного позиционного кодирования для биномиального пространства для дополнительного сокращения избыточности и повышения криптостойкости видеоинформационных ресурсов.

Основной материал

Особенностью метода является выполнение двухкаскадного обобщенного позиционного кодирования в двоичном структурном пространстве, которое заключается в:

1) кодировании двоичного представления элементов фрагмента изображения;

2) формировании кода с учетом структурных особенностей исходного фрагмента изображения.

Рассмотрим подробнее этапы двухкаскадного обобщенного позиционного кодирования.

Первоначально кадр изображения представляет собой массив пикселей размерностью $I^{(\text{row})} \times I^{(\text{col})}$, где $I^{(\text{row})}$ – количество строк в изображении, а $I^{(\text{col})}$ – количество столбцов. Количество δ градаций яркости элементов цветовой компоненты изображения характеризует максимально возможное значение яркости A . Исходный кадр изображения перед обработкой разбивается на сегменты A_φ размерностью $m \times n$, где m – количество строк фрагмента изображения, а n – количество столбцов.

Индекс φ сегмента A_φ в кадре определяется с помощью координатных переменных ψ и ζ , что задается таким выражением:

$$\varphi = (\psi - 1) \times \zeta_{\max} + \zeta, \quad \varphi = \overline{1, \Phi},$$

где ψ – координата сегмента A_φ в кадре по вертикали;

ζ – координата сегмента A_φ в кадре по горизонтали;

$\zeta_{\max}$ – максимальное значение координатной переменной по горизонтали;

Φ – количество сегментов A_φ в кадре.

Максимальное значение координатной переменной по вертикали $\psi_{\max}$ и по горизонтали $\zeta_{\max}$ определяется из соотношения размера кадра и сегмента:

$$\psi_{\max} = \frac{I^{(\text{row})}}{m}, \quad \zeta_{\max} = \frac{I^{(\text{col})}}{n}.$$

Сегмент A_φ представляет собой двумерный массив. Данный массив содержит элементы $a(i, j)_\varphi$, $i = \overline{1, m}$, $j = \overline{1, n}$, которые содержат информацию о яркости. Размеры $m \times n$ массива выбираются кратными степени 2, т.е

$m, n \in 2, 4, 8, 16$. Обычно значения сторон массива принимаются равными $m = n$. В кадре исходные элементы $a(i, j)_\phi$ в i -й строке j -го столбца сегмента A_ϕ могут принимать значение в диапазоне $[0; 255]$, т.е. $\delta = 255 = 2^8 - 1$.

На **первом** этапе для учета структурных особенностей исходного фрагмента изображения определяются максимальные значения g_i для каждой строки и максимальные значения g_j для каждого столбца на основе формул:

$$g_i = \max(a_{i, j}) + 1, j = \overline{1; n}, \quad (1)$$

$$g_j = \max(a_{i, j}) + 1, i = \overline{1; m}. \quad (2)$$

Последовательность максимальных значений g_i для каждой строки и максимальных значений g_j для каждого столбца образуют вектора $G^{(row)} = \{g_i\}$ и $G^{(col)} = \{g_j\}$ соответственно. После вычисления максимальных значений g_i для каждой строки и максимальных значений g_j для каждого столбца фрагмента изображения A_ϕ происходит определение необходимости формирования структурного кода N_ℓ по значениям яркости $a(i, j)_\phi$ и минимаксной системе оснований на базе плавающей схемы обобщенного позиционного кодирования. Для этого предлагается ввести двоичный признак G_ϕ , который указывает на проведение дополнительного преобразования двоичного представления отдельного элемента $a_{i, j}$ фрагмента изображения согласно функционала:

$$G_\phi = F_G(g_i, g_j), i = \overline{1; m}, j = \overline{1; n}. \quad (3)$$

При значении двоичного признака $G_\phi = 1$ на втором этапе будет осуществляться биномиальное кодирование двоичного представления отдельного элемента $a_{i, j}$ фрагмента изображения.

При значении двоичного признака $G_\phi = 0$ второй этап проводится не будет. В этом случае процесс формирования ИС ККП изображений в двумерном базисе на основе плавающей схемы задается выражением:

$$N = \sum_{\tau=1}^Q a_\tau V_\tau, \quad (4)$$

где V_τ – значение весового коэффициента, которое определяется формулой:

$$V_\tau = \begin{cases} \prod_{\xi=\tau+1}^Q s'_\xi = \prod_{\xi=\tau+1}^Q \min(G^{(row)}(\xi - m \frac{\xi-1}{m}), G^{(col)}(\frac{\xi-1}{m} + 1)), & \tau < Q; \\ 1, & \tau = Q, \end{cases} \quad (5)$$

где Q – плавающее количество элементов исходного фрагмента изображения, принимающих участие в формировании кода в двухмерном базисе на основе плавающей схемы с учетом проверки на переполнение кодового слова;

ξ – линейная координата элемента $a_{i,j}$ при сканировании столбцов фрагмента изображения сверху вниз, начиная с левого столбца. Переход от двухмерной координаты элемента $a_{i,j}$ к линейной определяется зависимостью:

$$\xi = i + (j-1) \times m. \quad (6)$$

Обратное преобразование координат задается формулами:

$$i = \xi - m \left\lfloor \frac{\xi - 1}{m} \right\rfloor, \quad j = \left\lfloor \frac{\xi - 1}{m} \right\rfloor + 1. \quad (7)$$

Количество Q элементов исходного фрагмента изображения, принимающих участие в формировании кода в двухмерном базисе на основе плавающей схемы с учетом проверки на переполнение кодового слова, не превышает общее количество элементов в фрагменте изображения:

$$Q \leq mn. \quad (8)$$

Для контроля переполнения кодового слова при формировании кода ИС ККП N введем дополнительную величину T_Q , равную накопленному произведению оснований для Q элементов, принимающих участие в формировании кода, которая определяется по формуле:

$$T_Q = \prod_{\xi=1}^Q s_{\xi} = \prod_{\xi=1}^Q \min \left(G^{(\text{row})} \left(\xi - m \frac{\xi - 1}{m} \right), G^{(\text{col})} \left(\frac{\xi - 1}{m} + 1 \right) \right). \quad (9)$$

Переполнения кодового слова не произойдет, если выполняется неравенство

$$T_Q \leq 2^M - 1, \quad (10)$$

где $2^M - 1$ – наибольшее число, которое может храниться в кодовом слове длиной m элементов.

Действительно, поскольку выполняется неравенство $T_Q \geq N$, тогда

$$N \leq 2^M - 1.$$

Максимальное количество элементов $Q_{\text{пр}}$, принимающих участие в формировании кода ИС ККП, определяется как значение аргумента, при котором величина T_Q достигает максимума при условии выполнения неравенства (10) и рассчитывается по формуле

$$Q_{\text{пр}} = \arg \max_Q (T_Q) = \arg \max_Q \left(\prod_{\xi=1}^Q s'_\xi \right) =$$

$$= \arg \max_Q \left(\prod_{\xi=1}^Q \min \left(G^{(\text{row})} \left(\xi - m \frac{\xi-1}{m} \right), G^{(\text{col})} \left(\frac{\xi-1}{m} + 1 \right) \right) \right) \quad (11)$$

С учетом соотношения (11) выражение (4) для определения кода принимает вид

$$N = \sum_{\tau=1}^{Q_{\text{пр}}} a_\tau V_\tau, \quad (12)$$

и выражение (5) для определения весового коэффициента преобразуется в

$$V_\tau = \begin{cases} \prod_{\xi=\tau+1}^{Q_{\text{пр}}} \min \left(G^{(\text{row})} \left(\xi - m \frac{\xi-1}{m} \right), G^{(\text{col})} \left(\frac{\xi-1}{m} + 1 \right) \right), & \tau < Q_{\text{пр}} < mn; \\ 1, & \tau = Q_{\text{пр}} \leq mn. \end{cases} \quad (13)$$

Из анализа выражений (11) – (13) при условии, что каждый элемент фрагмента изображения a_τ принимает максимальное значение равно 255, а его основание s_τ соответственно равно 256, с учетом соотношений (9) и (10) при длине кодового слова M , равной 64 бита, максимальное количество элементов $Q_{\text{пр}}$, которые могут принимать в формировании кода ИС ККП, равно 8. Это значение и есть минимальным количеством элементов, принимающих участие в формировании кода-номера.

Информационная составляющая кодограммы изображений на основе плавающей схемы системы обобщенного позиционного кодирования вычисляется за три шага, так, что:

1. На первом шаге (закключающемся в подготовке исходных данных и определении служебных составляющих):

– исходное изображение разбивается на фрагменты размерностью $m \times n$;

– определяется система оснований $S'(m \times n) = \min (G^{(\text{row})}(i), G^{(\text{col})}(j))$, $i = \overline{1, m}$, $j = \overline{1, n}$, исходного фрагмента изображения на основе выражений (1) и (2);

– преобразовывается исходный фрагмент изображения на основе выражения (6) из двумерной матрицы $A = \{a_{i,j}\}$, $i = \overline{1, m}$, $j = \overline{1, n}$, в одномерный вектор $A = \{a_\tau\}$, который в дальнейшем будет рассматриваться, как одномерное структурное число;

– расширяется система оснований $S'(m \times n) = \min (G^{(\text{row})}(i), G^{(\text{col})}(j))$ до мощности исходного фрагмента изображения в одномерном векторном виде $S'(m \times n) = \{s'_\xi\}$ на основе выражения:

$$s'_\xi = \min (G^{(row)}(\xi - m \frac{\xi - 1}{m}), G^{(col)}(\frac{\xi - 1}{m} + 1)).$$

2. На втором шаге рассчитывается максимальное количество элементов Q_{np} одномерного структурного числа, принимающих участие в формировании ИС ККП, из соотношения

$$\begin{aligned} Q_{np} &= \arg \max_Q (T_Q) = \arg \max_Q (\prod_{\xi=1}^Q s'_\xi) = \\ &= \arg \max_Q (\prod_{\xi=1}^Q \min (G^{(row)}(\xi - m \frac{\xi - 1}{m}), G^{(col)}(\frac{\xi - 1}{m} + 1))) \end{aligned} \quad (14)$$

при котором выполняется следующее условие

$$\prod_{\xi=1}^Q s'_\xi = \prod_{\xi=1}^Q \min (G^{(row)}(\xi - m \frac{\xi - 1}{m}), G^{(col)}(\frac{\xi - 1}{m} + 1)) \leq 2^M - 1. \quad (15)$$

3. На третьем шаге непосредственно формируется ИС ККП на основе выражений (4) и (5). Значение кода ИС является интегрированным, и формируется с учетом служебных данных по оператору $f(A; G)$, где:

$$\begin{aligned} f(A; G) = N &= \sum_{\tau=1}^{Q_{np}} a_\tau V_\tau = \sum_{\tau=1}^{Q_{np}} a_\tau \prod_{\xi=\tau+1}^{Q_{np}} s'_\xi = \\ &= \sum_{\tau=1}^{Q_{np}} (a_\tau \times \min (G^{(row)}(\tau - m \frac{\tau - 1}{m}), G^{(col)}(\frac{\tau - 1}{m} + 1))) \end{aligned} \quad (16)$$

Формирование кода ИС ККП возможно и на основе рекуррентной схемы путем добавления очередного элемента одномерного структурного числа. Первоначальное значение кода N_1 определяется значением первого элемента a_1 , т.е.

$$N_1 = a_1. \quad (17)$$

Процесс формирования кода задается следующими выражениями

$$\begin{aligned} N_\tau &= N_{\tau-1} s'_\tau + a_\tau = \\ &= N_{\tau-1} \times \min (G^{(row)}(\tau - m \frac{\tau - 1}{m}), G^{(col)}(\frac{\tau - 1}{m} + 1)) + a_\tau, \end{aligned} \quad (18)$$

где N_τ , $N_{\tau-1}$ – промежуточное значение кода для τ -го и $(\tau-1)$ -го элементов.

Для исключения переполнения кодового слова перед каждым добавлением к коду ИС ККП $N_{\tau-1}$ очередного элемента a_τ проводится проверка на переполнение кодового слова, которая с учетом соотношения $\tau = Q$, определяется с помощью дополнительной величины T_τ на основе выражения (9) с учетом выполнения неравенства (10).

Действительно, поскольку выполняется неравенство $T_\tau \geq N_\tau$, тогда

$$N_{\tau} \leq 2^M - 1.$$

Процесс формирования кода ИС ККП N заканчивается тогда, когда будет обработан последний Q -й элемент:

$$N = N_Q = N_{Q-1} s'_Q + a_Q = N_{Q-1} \times \min \left(g_{Q-m \left\lfloor \frac{Q-1}{m} \right\rfloor}, g_{\left\lfloor \frac{Q-1}{m} \right\rfloor + 1} \right) + a_Q, \quad (19)$$

$$\text{при } T_Q \leq 2^M - 1 \text{ и } Q \leq mn.$$

В данном случае Q -й элемент будет равен максимальному количеству элементов $Q_{\text{пр}}$ одномерного структурного числа, принимающих участие в формировании кода ИС ККП, рассчитанному по формуле (14).

Далее на *втором* этапе при значении двоичного признака $G_{\phi} = 1$, выполняется биномиальное кодирование двоичного представления отдельного элемента $a_{i,j}$ фрагмента изображения. Для чего элемент фрагмента изображения рассматривается как одномерное плавающее структурное число. Плавающая схема формирования структурного кода подразумевает переменное количество v кодируемых разрядов $b(a_{i,j})^{(\gamma)}$ двоичной последовательности элемента $a_{i,j}$.

Вычисление количества серий единиц $\eta_{i,j}$ для v кодируемых разрядов $b(a_{i,j})^{(\gamma)}$ двоичной последовательности элемента $a_{i,j}$ выполняется, начиная со старшего разряда согласно следующему алгоритму:

– на нулевом шаге $\gamma = 0$ начальные значения разряда и длины серии приравнивают нулю: $b(a_{i,j})^{(0)} = 0$, $\eta_{i,j}^{(0)} = 0$;

– на γ -м шаге число серий увеличивается на 1:

$$\eta_{i,j}^{(\gamma)} = \eta_{i,j}^{(\gamma-1)} + 1, \text{ если } b(a_{i,j})^{(\gamma)} > b(a_{i,j})^{(\gamma-1)};$$

– в противном случае $\eta_{i,j}^{(\gamma)} = \eta_{i,j}^{(\gamma-1)}$, если $b(a_{i,j})^{(\gamma)} \leq b(a_{i,j})^{(\gamma-1)}$;

– для конечного шага при $\gamma = v$ получаем искомое значение количества серий единиц $\eta_{i,j} = \eta_{i,j}^{(v)}$ для элемента $a_{i,j}$.

Формирование структурного представления $y_{i,j}$ двоичных данных для отдельного элемента $a_{i,j}$ задается функционалом $f_{\text{bin}}(a_{i,j}, v, \eta_{i,j})$:

$$y_{i,j} = f_{\text{bin}}(a_{i,j}, v, \eta_{i,j}), \quad (20)$$

где v – количество кодируемых разрядов отдельного элемента $a_{i,j}$ фрагмента изображения,

$\eta_{i,j}$ – количество серий единиц отдельного элемента $a_{i,j}$ фрагмента изображения.

Полученное структурное представление $y_{i,j}$ характеризуется количеством $W_{i,j}$ допустимых структурных чисел для элемента фрагмента изображения, которое определяется по формуле:

$$W_{i,j} = \frac{(v+1)!}{(2\eta_{i,j})!(v+1-2\eta_{i,j})!}.$$

Формирование структурного представления $y_{i,j}$ двоичных данных для отдельного элемента $a_{i,j}$ фрагмента изображения производится на основе выражения:

$$y_{i,j} = \sum_{\gamma=1}^v b(a_{i,j})^{(\gamma)} \times p_{i,j}^{(\gamma)}, \quad (21)$$

где $b(a_{i,j})^{(\gamma)}$ – значение γ -го разряда элемента $a_{i,j}$;

$p_{i,j}^{(\gamma)}$ – весовой коэффициент отдельного элемента $a_{i,j}$ фрагмента изображения, зависящий от значений γ и $\eta_{i,j}$.

Расчет весовых коэффициентов проводится на основе рекуррентных выражений [17], позволяющих вычислить значение весового коэффициента $p_{i,j}^{(\gamma)}$ разряда $b(a_{i,j})^{(\gamma)}$ для элемента $a_{i,j}$ через весовой коэффициент $p_{i,j}^{(\gamma-1)}$ предыдущего разряда $b(a_{i,j})^{(\gamma-1)}$ элемента $a_{i,j}$. При этом возможны четыре варианта зависимости между разрядами отдельного элемента $a_{i,j}$ фрагмента изображения:

$$1) |b(a_{i,j})^{(\gamma-2)} - b(a_{i,j})^{(\gamma-1)}| = 1 \text{ и } |b(a_{i,j})^{(\gamma-1)} - b(a_{i,j})^{(\gamma)}| = 1:$$

$$p_{i,j}^{(\gamma)} = p_{i,j}^{(\gamma-1)} \frac{\beta_{i,j}^{(\gamma-1)} + 1}{v - \gamma + 2}; \quad (22)$$

$$2) |b(a_{i,j})^{(\gamma-2)} - b(a_{i,j})^{(\gamma-1)}| = 1 \text{ и } |b(a_{i,j})^{(\gamma-1)} - b(a_{i,j})^{(\gamma)}| = 0:$$

$$p_{i,j}^{(\gamma)} = p_{i,j}^{(\gamma-1)} \left(\frac{(\beta_{i,j}^{(\gamma-1)} + 1)\beta_{i,j}^{(\gamma)}}{(v - \gamma + 2 - \beta_{i,j}^{(\gamma-1)})(v - \gamma + 2)} \right); \quad (23)$$

$$3) |b(a_{i,j})^{(\gamma-2)} - b(a_{i,j})^{(\gamma-1)}| = 0 \text{ и } |b(a_{i,j})^{(\gamma-1)} - b(a_{i,j})^{(\gamma)}| = 1:$$

$$p_{i,j}^{(\gamma)} = p_{i,j}^{(\gamma-1)} \frac{(v - \gamma - \beta_{i,j}^{(\gamma-1)} + 3)(v - \gamma + 2 - \beta_{i,j}^{(\gamma-1)})}{(\beta_{i,j}^{(\gamma-1)})(v - \gamma + 2)}; \quad (24)$$

$$4) |b(a_{i,j})^{(\gamma-2)} - b(a_{i,j})^{(\gamma-1)}| = 0 \text{ и } |b(a_{i,j})^{(\gamma-1)} - b(a_{i,j})^{(\gamma)}| = 0:$$

$$p_{i,j}^{(\gamma)} = p_{i,j}^{(\gamma-1)} \frac{v - \gamma - \beta_{i,j}^{(\gamma-1)} + 3}{v - \gamma + 2}, \quad (25)$$

где v – количество разрядов в обрабатываемом отдельном элементе $a_{i,j}$; $\beta_{i,j}^{(\gamma)}$ – рекуррентный параметр, равный количеству двоичных перепадов (переходов между «0» и «1») для последовательности, состоящей из $(v - \gamma + 1)$ необработанных разрядов отдельного элемента $a_{i,j}$ фрагмента изображения:

$$\beta_{i,j}^{(\gamma)} = \beta_{i,j}^{(\gamma-1)} - |b(a_{i,j})^{(\gamma)} - b(a_{i,j})^{(\gamma-1)}|. \quad (26)$$

Для начального шага обработки ($\gamma=1$) принимаются следующие значения разряда $b_{i,j}^{(0)} = 0$ и рекуррентного параметра $\beta_{i,j}^{(0)} = 2\eta_{i,j}$. Весовой коэффициент $p_{i,j}^{(\gamma)}$ на первом шаге обработки для двух случаев значения первого разряда отдельного элемента $a_{i,j}$ фрагмента изображения определяется как:

$$1) b(a_{i,j})^{(1)} = 1:$$

$$p_{i,j}^{(1)} = W_{i,j} \frac{v + 1 - 2\eta_{i,j}}{v + 1}; \quad (27)$$

$$2) b(a_{i,j})^{(1)} = 0:$$

$$p_{i,j}^{(1)} = W_{i,j} \frac{2\eta_{i,j}}{v + 1}. \quad (28)$$

С учетом выражений (27) и (28) выражение (21) для вычисления структурного представления $y_{i,j}$ двоичных данных для отдельного элемента $a_{i,j}$ фрагмента изображения принимает вид:

$$y_{i,j} = b(a_{i,j})^{(1)} \times W_{i,j} \times \frac{v + 1 - 2\eta_{i,j}}{v + 1} + \overline{b(a_{i,j})^{(1)}} \times W_{i,j} \times \frac{2\eta_{i,j}}{v + 1} + (b(a_{i,j})^{(2)}; \dots; b(a_{i,j})^{(v)}) \cdot (p_{i,j}^{(2)}; \dots; p_{i,j}^{(v)}), \quad (29)$$

где $\overline{b(a_{i,j})^{(\gamma)}}$ – инвертированное значение γ -го разряда элемента $a_{i,j}$;

$B \cdot P$ – выполнение скалярного умножения вектора $B = \{b(a_{i,j})^{(2)}; \dots; b(a_{i,j})^{(v)}\}$ разрядов элемента $a_{i,j}$ фрагмента изображения на вектор $P = \{p_{i,j}^{(2)}; \dots; p_{i,j}^{(v)}\}$ весовых коэффициентов.

В связи с тем, что согласно (22) – (25), (27) и (28) весовой коэффициент $p_{i,j}^{(\gamma)}$ отдельного элемента $a_{i,j}$ фрагмента изображения определяется рекуррентно, выражение (29) приводится к виду:

$$\begin{aligned}
y_{i,j} = & \frac{(v+1)!}{(v+1-2\eta_{i,j})! \times (2\eta_{i,j})!} \times (b(a_{i,j}))^{(1)} \times \frac{v+1-2\eta_{i,j}}{v+1} + \overline{b(a_{i,j})}^{(1)} \times \frac{2\eta_{i,j}}{v+1} + \\
& + \overline{b(a_{i,j})}^{(2)} \times b(a_{i,j})^{(1)} \times \frac{v+1-2\eta_{i,j}}{v+1} \times \frac{2\eta_{i,j}}{v} + b(a_{i,j})^{(2)} \times \overline{b(a_{i,j})}^{(1)} \times \frac{2\eta_{i,j}}{v+1} \times \\
& \times \frac{(v-2\eta_{i,j}+1)(v-2\eta_{i,j})}{2\eta_{i,j} \times v} + b(a_{i,j})^{(2)} \times b(a_{i,j})^{(1)} \times \frac{v+1-2\eta_{i,j}}{v+1} \times \\
& \times \frac{2\eta_{i,j}(2\eta_{i,j}-1)}{(v+1-2\eta_{i,j}) \times v} + \overline{b(a_{i,j})}^{(2)} \times \overline{b(a_{i,j})}^{(1)} \times \frac{2\eta_{i,j}}{v+1} \times \frac{v-2\eta_{i,j}+2}{v} + \dots + \\
& + (b(a_{i,j})^{(\gamma-2)} \times b(a_{i,j})^{(\gamma-1)} \times \overline{b(a_{i,j})}^{(\gamma)} + b(a_{i,j})^{(\gamma-2)} \times \overline{b(a_{i,j})}^{(\gamma-1)} \times b(a_{i,j})^{(\gamma)}) \times \\
& \times p_{i,j}^{(\gamma-1)} \times \frac{\beta_{i,j}^{(\gamma-1)}+1}{v-\gamma+2} + (b(a_{i,j})^{(\gamma-2)} \times b(a_{i,j})^{(\gamma-1)} \times b(a_{i,j})^{(\gamma)} + b(a_{i,j})^{(\gamma-2)} \times \\
& \times \overline{b(a_{i,j})}^{(\gamma-1)} \times \overline{b(a_{i,j})}^{(\gamma)}) \times p_{i,j}^{(\gamma-1)} \times \frac{(\beta_{i,j}^{(\gamma-1)}+1)}{(v-\gamma+2-\beta_{i,j}^{(\gamma-1)})} \times \frac{\beta_{i,j}^{(\gamma)}}{(v-\gamma+2)} + \\
& + (b(a_{i,j})^{(\gamma-2)} \times b(a_{i,j})^{(\gamma-1)} \times \overline{b(a_{i,j})}^{(\gamma)} + b(a_{i,j})^{(\gamma-2)} \times \overline{b(a_{i,j})}^{(\gamma-1)} \times b(a_{i,j})^{(\gamma)}) \times \\
& \times p_{i,j}^{(\gamma-1)} \times b(a_{i,j})^{(\gamma-1)} \times \frac{(v-\gamma-\beta_{i,j}^{(\gamma-1)}+3)(v-\gamma+2-\beta_{i,j}^{(\gamma-1)})}{\beta_{i,j}^{(\gamma-1)}(v-\gamma+2)} + (b(a_{i,j})^{(\gamma-2)} \times \\
& \times b(a_{i,j})^{(\gamma)} + \overline{b(a_{i,j})}^{(\gamma-2)} \times \overline{b(a_{i,j})}^{(\gamma-1)} \times \overline{b(a_{i,j})}^{(\gamma)}) \times p_{i,j}^{(\gamma-1)} \times \frac{v-\gamma-\beta_{i,j}^{(\gamma-1)}+3}{v-\gamma+2} + \\
& + (b(a_{i,j})^{(v-2)} \times b(a_{i,j})^{(v-1)} \times \overline{b(a_{i,j})}^{(v)} + b(a_{i,j})^{(v-2)} \times \overline{b(a_{i,j})}^{(v-1)} \times b(a_{i,j})^{(v)}) \times \\
& \times \dots \times p_{i,j}^{(v-1)} \times \frac{\beta_{i,j}^{(v-1)}+1}{2} + (b(a_{i,j})^{(v-2)} \times b(a_{i,j})^{(v-1)} \times b(a_{i,j})^{(v)} + b(a_{i,j})^{(v-2)} \times \\
& \times \overline{b(a_{i,j})}^{(v-1)} \times \overline{b(a_{i,j})}^{(v)}) \times p_{i,j}^{(v-1)} \times \frac{(\beta_{i,j}^{(\gamma-1)}+1)\beta_{i,j}^{(v-1)}}{2(2-\beta_{i,j}^{(\gamma-1)})} + (b(a_{i,j})^{(v-2)} \times b(a_{i,j})^{(v-1)} \times \\
& \times b(a_{i,j})^{(v)} + b(a_{i,j})^{(v-2)} \times \overline{b(a_{i,j})}^{(v-1)} \times b(a_{i,j})^{(v)}) \times p_{i,j}^{(v-1)} \times \\
& \times \frac{(3-\beta_{i,j}^{(\gamma-1)})(2-\beta_{i,j}^{(v-1)})}{2\beta_{i,j}^{(\gamma-1)}} + (b(a_{i,j})^{(v-2)} \times b(a_{i,j})^{(v-1)} \times b(a_{i,j})^{(v)} + \\
& + \overline{b(a_{i,j})}^{(v-2)} \times \overline{b(a_{i,j})}^{(v-1)} \times \overline{b(a_{i,j})}^{(v)}) \times p_{i,j}^{(v-1)} \times \frac{3-\beta_{i,j}^{(v-1)}}{2}), \quad (31)
\end{aligned}$$

где $b(a_{i,j})^{(v)}$ – значение v -го (младшего) разряда элемента $a_{i,j}$;

$b(a_{i,j})^{(v-1)}$ – значение $(v-1)$ -го (предпоследнего) разряда элемента $a_{i,j}$.

После формирования структурного представления двоичных данных образуется биномиальное структурное число $Y(G(g_i, g_j, A_\varphi))$. Для этого числа (i, j) -е координаты определяют местоположение элемента в локальном фрагменте изображения.

На **третьем** этапе для сокращения длины кода, полученных структурных представлений $y_{i,j}$ двоичной последовательности отдельных элементов $a_{i,j}$ фрагмента изображения, предлагается уменьшить значения оснований на основании значения двоичного признака G_φ . Для чего величина $s'_{i,j}$ рассчитывается по одной из следующих формул:

$$s'_{i,j} = \min(G^{(\text{row})}(i); G^{(\text{col})}(j)), i = \overline{1; m}, j = \overline{1; n}, G_\varphi = 0, \quad (32)$$

$$s'_{i,j} = W_{i,j}, i = \overline{1; m}, j = \overline{1; n}, G_\varphi = 1. \quad (33)$$

С учетом выражений (32) и (33) величина $s'_{i,j}$ для фрагмента изображения вычисляется по следующей формуле:

$$s'_{i,j} = \min(G^{(\text{row})}(i); G^{(\text{col})}(j)) \times \overline{G_\varphi} + \frac{(v+1)!}{(2\eta_{i,j})!(v+1-2\eta_{i,j})!} \times G_\varphi. \quad (34)$$

После чего на **четвертом** этапе для построения ИС ККП изображения на основе плавающей схемы необходимо выполнить линеаризацию биномиального структурного числа $Y(G(g_i, g_j, A_\varphi))$.

Структурное число $Y(G(g_i, g_j, A_\varphi))$ в исходном виде представляет собой двумерную матрицу биномиального представления исходного фрагмента изображения $A = \{a_{i,j}\}$, $i = \overline{1; m}$, $j = \overline{1; n}$, которая преобразовывается в одномерный вектор

$$Y(G(g_i, g_j, A_\varphi)) = \{y_{i,j}\} = \{y_\tau\}_{\tau=\overline{1; mn}} = \{y_{m(j-1)+i}\}, i = \overline{1; m}, j = \overline{1; n}. \quad (35)$$

Для удобства проведения расчетов и для определения взаимнооднозначного соответствия элементов фрагмента изображения с основаниями предлагается расширить систему оснований до мощности исходного фрагмента изображения в одномерном векторном виде. Для этого воспользуемся формулой

$$S'^{(m \times n)} = \{s'_\tau\} = \{s'_{m(j-1)+i}\}, \tau = \overline{1; mn}. \quad (36)$$

Для контроля переполнения кодового слова при формировании кода ИС ККП N введем дополнительную величину T_Q , равную накопленному

произведению оснований для Q элементов, принимающих участие в формировании кода ИС ККП, которая определяется по формуле

$$T_Q = \prod_{\xi=1}^Q s'_\xi. \quad (37)$$

Переполнения кодового слова не произойдет, если выполняется неравенство

$$T_Q \leq 2^M - 1. \quad (38)$$

Учитывая выражение (34) величина T_Q для фрагмента изображения определяется следующей формулой:

$$T_Q = \prod_{\xi=1}^Q \min \left(G^{(\text{row})} \left(\xi - m \left\lfloor \frac{\xi-1}{m} \right\rfloor \right); G^{(\text{col})} \left(\left\lfloor \frac{\xi-1}{m} \right\rfloor + 1 \right) \right) \times \overline{G_\varphi} + \frac{(v+1)!}{(2\eta_{i,j})!(v+1-2\eta_{i,j})!} \times G_\varphi \quad (39)$$

Максимальное количество элементов $Q_{\text{пр}}$, принимающих участие в формировании кода ИС ККП, определяется как значение аргумента, при котором величина T_Q достигает максимума при условии выполнения неравенства (38) и рассчитывается по формуле

$$Q_{\text{пр}} = \arg \max_Q (T_Q) = \arg \max_Q \left(\prod_{\xi=1}^Q s'_\xi \right), \quad (40)$$

которая при использовании выражения (39) примет вид:

$$Q_{\text{пр}} = \arg \max_Q \left(\prod_{\xi=1}^Q \min \left(G^{(\text{row})} \left(\xi - m \left\lfloor \frac{\xi-1}{m} \right\rfloor \right); G^{(\text{col})} \left(\left\lfloor \frac{\xi-1}{m} \right\rfloor + 1 \right) \right) \times \overline{G_\varphi} + \frac{(v+1)!}{(2\eta_{i,j})!(v+1-2\eta_{i,j})!} \times G_\varphi \right) \quad (41)$$

где $G^{(\text{row})} \left(\xi - m \left\lfloor \frac{\xi-1}{m} \right\rfloor \right)$, $G^{(\text{col})} \left(\left\lfloor \frac{\xi-1}{m} \right\rfloor + 1 \right)$ – максимальное значение элемента $a_{i,j}$ в строке и столбце фрагмента изображения, соответственно.

Пятый этап состоит во втором каскаде формирования ИС ККП изображений (представления данных в системе обобщенного позиционного кодирования) в базисе по верхним границам на основе плавающей схемы задается выражением:

$$N = \sum_{\tau=1}^Q y_\tau V_\tau. \quad (42)$$

В данном выражении весовой коэффициент v_τ определяется формулой:

$$V_{\tau} = \begin{cases} \prod_{\xi=\tau+1}^Q s'_{\tau}, & \rightarrow \tau < Q; \\ 1, & \rightarrow \tau = Q. \end{cases} \quad (43)$$

где Q – плавающее количество элементов одномерного структурного числа, принимающих участие в формировании кода в двухмерном базисе с учетом особенностей структурного кода двоичной последовательности на основе плавающей схемы с учетом проверки на переполнение кодового слова. Это плавающее количество ограничено следующим значением:

$$Q \leq mn. \quad (44)$$

Формулу (43) вычисления весовых коэффициентов V_{τ} на основе выражений (34) и (7) преобразуется к следующему выражению:

$$V_{\tau} = \begin{cases} \prod_{\xi=\tau+1}^Q \min(G^{(row)}(\xi - m[\frac{\xi-1}{m}]); G^{(col)}([\frac{\xi-1}{m}] + 1)G_{\varphi} + \frac{(v+1)!}{(2\eta_{i,j})!(v+1-2\eta_{i,j})!}) \times G_{\varphi}, & \tau < Q; \\ 1, & \tau = Q. \end{cases} \quad (45)$$

Для значения двоичного признака $G_{\varphi} = 1$ представляется возможным развертывание формулы (42) вычисления кода N в следующее выражение:

$$\begin{aligned} N = & \sum_{\xi=1}^{Q_{пр}} \left(\frac{(v+1)!}{(v+1-2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})! \times (2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})!} \times \right. \\ & \times (b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(1)} \times \frac{v+1-2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}}{v+1} + b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(1)} \times \\ & \times \frac{2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}}{v+1} + b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(2)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(1)} \times \\ & \times \frac{v+1-2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}}{v+1} \times \frac{2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}}{v} + b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(2)} \times \\ & \left. \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(1)} \times \frac{2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}}{v+1} \times \right) \end{aligned}$$

$$\begin{aligned}
& \times \frac{(\nu - 2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1} + 1)(\nu - 2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})}{2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1} \times \nu} + b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(2)} \times \\
& \quad \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(1)} \times \frac{\nu + 1 - 2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}}{\nu + 1} \times \\
& \quad \times \frac{2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1} (2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1} - 1)}{(\nu + 1 - 2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}) \times \nu} + b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(2)} \times \\
& \quad \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(1)} \times \frac{2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}}{\nu + 1} \times \frac{\nu - 2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1} + 2}{\nu} + \\
& \quad + \dots + (b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-2)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-1)} \times \\
& \quad \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma)} + b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-2)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-1)} \times \\
& \quad \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma)} \times p_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)} \times \frac{\beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)} + 1}{\nu - \gamma + 2} + \\
& \quad + (b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-2)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-1)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma)} + \\
& \quad + b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-2)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-1)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma)} \times \\
& \quad \times p_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)} \times \frac{(\beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)} + 1) \beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma)}}{(\nu - \gamma + 2 - \beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)}) (\nu - \gamma + 2)} + \\
& \quad + (b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-2)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-1)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma)} + \\
& \quad + b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-2)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-1)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma)} \times \\
& \quad \times p_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)} \times \frac{(\nu - \gamma - \beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)} + 3)(\nu - \gamma + 2 - \beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)})}{\beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)} (\nu - \gamma + 2)} +
\end{aligned}$$

$$\begin{aligned}
& + (b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-2)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-1)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma)} + \\
& + \overline{b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-2)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma-1)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(\gamma)}} \times \\
& \times p_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)} \times \frac{v-\gamma-\beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)}+3}{v-\gamma+2} + \dots + \overline{(b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-2)})} \times \\
& \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-1)} \times \overline{b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v)}} + b_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(v-2)} \times \\
& \times \overline{b_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(v-1)}} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v)} \times p_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(v-1)} \times \\
& \times \frac{\beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(v-1)}+1}{2} + \overline{(b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-2)})} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-1)} \times \\
& \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v)} + \overline{b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-2)} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-1)}} \times \\
& \times \overline{b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v)}} \times p_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(v-1)} \times \\
& \times \frac{(\beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)}+1)\beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(v-1)}}{2(2-\beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)})} + \overline{(b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-2)})} \times \\
& \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-1)} \times \overline{b_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(v)}} + \overline{b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-2)}} \times \\
& \times \overline{b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-1)}} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v)} \times p_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(v-1)} \times \\
& \times \frac{(3-\beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)})(2-\beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(v-1)})}{2\beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(\gamma-1)}} + \overline{(b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-2)})} \times \\
& \times \overline{b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-1)}} \times \overline{b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v)}} \times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-1)} \times
\end{aligned}$$

$$\times b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v)} + \overline{b(a_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})^{(v-2)}} \times p_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(v-1)} \times \\ \times \frac{3 - \beta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1}^{(v-1)}}{2} \times V_{\xi} \quad . \quad (46)$$

Здесь количество $Q_{\text{пр}}$ кодируемых во втором каскаде элементов определяется выражением:

$$Q_{\text{пр}} = \arg \max_Q \left(\prod_{\xi=1}^Q \frac{(v+1)!}{(2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})! (v+1-2\eta_{\xi-m[\frac{\xi-1}{m}], [\frac{\xi-1}{m}]+1})!} \right).$$

Выводы

1. Для понижения динамического диапазона значений исходных элементов фрагмента изображения и сокращения разрядов на их представление в ККП предлагается организовать двухкаскадную обработку на основе обобщенного позиционного кодирования с учетом двоичного признакового пространства, которая заключается в:

- биномиальном кодировании двоичного представления элементов фрагмента изображения;
- формировании ККП изображений с учетом полученных структурных особенностей кодированного фрагмента изображения на основе плавающей схемы обобщенного позиционного кодирования в базисе по верхним границам двоичного структурного пространства по количеству серий единиц.

Данный подход приведет к увеличению количества кодируемых элементов, принимающих участие в формировании кодов ИС ККП изображений на основе плавающей схемы обобщенного позиционного кодирования. Это обеспечивает криптостойкость за счет увеличения неопределенности при формировании ККП и повышения оперативности за счет уменьшения ИС ККП.

2. Кодирование двоичного представления элементов фрагмента изображения для повышения оперативности выполнения преобразования предлагается организовать на основе блока байтовой замены с входом по значению элемента исходного изображения и выходом со значениями его кода и количества серий единиц. Блок замены предлагается формировать на этапе инициализации выполнения преобразования (или заранее) на основе матрицы размерностью 2×256 элементов, подсчитанной для всех 256 возможных вариантов значений элементов исходного фрагмента изображения в диапазоне $[0; 255]$. Входом в таком блоке замены будет номер столбца, равный значению элемента исходного изображения, а для нулевого значению входом будет 266-ой столбец (или номер столбца,

равный значению элемента исходного изображения, увеличенный на один). Выходом будет с одной из строк данного столбца – количество серий единиц исходного элемента изображения, а со второй строки – значение его кода. Количество серий единиц для 8-битных исходных данных может принимать значение 0 для нулевого значения исходного элемента видеоданных и от 1 до 4 для остальных элементов. При этом количество серий единиц, равное 1, наблюдается у 36 исходных элементов, равное 2 – у 126 элементов, равное 3 – у 84 элементов, равное 4 – у 9 элементов. При разных значениях входных элементов на выходе:

- один из 9 кодов структурного представления будет соответствовать 4-м входным значениям исходных данных (при кодировании нулевого входного значения в одной группе с исходными значениями с количеством серий единиц, равным 4, значение одного из 10 кодов структурного представления будет одинаковым для 4-х входных элементов);

- один из 27 кодов структурного представления будет соответствовать 3-м входным значениям исходных данных;

- один из 47 кодов структурного представления будет соответствовать 2-м входным значениям исходных данных;

- только 42 кода структурного представления будут соответствовать одному входному значению исходных данных.

Биномиальное кодирование двоичного представления элементов фрагмента изображения приводит к изменению структуры видеоданных на синтаксическом уровне, связанном с уменьшением количества разрядов для хранения значений структурного представления двоичных данных для отдельного элемента. Однако на семантическом уровне представления изображения наблюдается незначительная корреляция между исходным элементом и его структурным представлением. При условии наличия априорной информации про количество разрядов, выделяемых для хранения каждого структурного представления отдельного элемента, появляется возможность построения изображения с ошибками и потерей мелких объектов.

3. Для повышения криптостойкости кодирования предлагается в блоке замены произвести случайную перестановку кодов структурного представления элемента в пределах групп одной серии единиц. Данный подход позволит изменить структуру видеоданных на синтаксическом и семантическом уровне. Блок байтовой замены, построенный таким образом, может выступать в роли долгосрочного ключевого элемента (по аналогии с S-блоками алгоритма ГОСТ 28147-89), быть одинаковым в одной группе пользователей, храниться в секрете и использоваться на протяжении определенного времени (его передача между пользователями не требуется).

4. Отойдя от принципа прямого математического построения кодов структурного представления элемента можно пойти дальше по пути

совершенствования построения блока байтовой замены. Вместо деления на группы по количеству серий единиц предлагается значения исходных элементов перераспределить между группами или случайным образом разбить на четыре группы (нумерация которых может быть тоже случайной в диапазоне $[0; 3]$). Один из возможных вариантов, формирующий полные группы, предусматривает следующее распределение количества элементов по группам:

- по 32 элемента в двух группах, что потребует для их хранения по 5 бит для каждого кода структурного представления;
- 64 элемента в третьей группе с выделением 6 бит для хранения каждого кода структурного представления;
- 128 элементов в последней группе с выделением 7 бит для хранения каждого кода структурного представления.

Предложенный блок байтовой замены обеспечивает:

- перемешивание значений исходных элементов;
- рассеивание на битовом уровне за счет перераспределения элементов исходной битовой последовательности между номерами группы и кодом структурного представления элемента с неравномерно уменьшенным количеством разрядов для его хранения;
- изменение структуры изображения на синтаксическом и семантическом уровнях;
- уменьшение динамического диапазона для кодов структурного представления элемента в зависимости от номера группы, что при выполнении второго каскада гарантированно обеспечит формирование кода ИС ККП на переменном количестве элементов;
- при записи выходной кодограммы двоичного представления элементов фрагмента изображения в разнотипном динамическом диапазоне, определяемом номером группы и, соответственно, количеством разрядов для их хранения, обеспечивается неопределенность определения начала и конца битовой последовательности для каждого отдельного кода структурного представления. При этом значения номеров группы для каждого кода выступают в качестве ключевого элемента. Информационная составляющая ККП в таком случае может быть сформирована без выполнения второго каскада преобразования, что значительно повысит оперативность формирования кодограммы с обеспечением ее криптостойкости.

5. Служебная составляющая ККП изображений формируется на основе двоичного признакового пространства и представляет собой биномиальный код значений количества серий единиц для всех элементов фрагмента изображений. Это обеспечит повышение криптостойкости служебных данных за счет отсутствия прямой взаимосвязи, которая наблюдалась между значениями системы оснований и исходными значениями фрагмента изображения, что позволяло восстановить

изображение с локализованной ошибкой, базируясь только на значениях системы оснований (в варианте построения ККП изображения без криптологического преобразования служебной составляющей). А так как система служебных данных для всего изображения, являющаяся ключевым элементом для декодирования (кодирования) ИС ККП, организуется по двум подходам и несет в себе разный физический смысл, то это создает криптоаналитику больше неопределенности при дешифровке служебных данных ККП.

Література

1. Соколан Т. С. Адміністративно-правове регулювання застосування відеоспостереження правоохоронними органами України / Тетяна Сергіївна Соколан // Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07. – Київ : Київський національний університет імені Тараса Шевченка. – 2016. – 210 с.
2. Resolution of PACE 1604 (2008) “Video surveillance of public areas” [Електронний ресурс]. – Режим доступу: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17633&lang=en>.
3. Володин А. А. Обработка видео в системах телевизионного наблюдения / А. А. Володин, В. Г. Митько, Е. Н. Спинко // Вопросы защиты информации. – 2002. – № 4 (59). – С. 34 - 47.
4. Visual cryptography / M. Naor and A. Shamir // In EUROCRYPT'94. – Springer-Verlag Berlin, 1995 [Електронний ресурс]. – Режим доступу: <http://www.fe.infn.it/u/filimanto/scienza/webkrypto/visualdecryption.pdf>.
5. Barannik V. Methodology of creation of cryptographic transformations on the basis of methods excluding redundancy / V. Barannik, S. Sidchenko, V. Larin // 10th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science, TCSET'2010; Lviv-Slavske; Ukraine; 23 February 2010 - 27 February 2010. – p. 312.
6. Barannik V. Methodology compression of videoinformation in the cryptographic systems / V. Barannik, S. Sidchenko, V. Larin // Science-based technologies. – 2011. – Vol. 11. No. 3-4, doi.org/10.18372/2310-5461.11.5260 (eng).
7. Баранник В. В. Синтез комбинированных криптокомпрессионных систем для обеспечения безопасности видеоинформации в инфокоммуникациях / В. В. Баранник, С. А. Сидченко, И. М. Тупица // Автоматизированные системы управления и приборы автоматики. – Х.: ХНУРЭ. – 2014. – Вып. 169. – С. 39 - 44.
8. Barannik V. The methodological base of cryptocompression presentation of videoinformation resources / V. V. Barannik, S. A. Sidchenko, V. V. Larin // 12th International Conference: The Experience of Designing and Application of CAD Systems in Microelectronics, CADSM 2013, Lviv; Ukraine; 19 February 2013 - 23 February 2013. – pp. 27 - 28.
9. Баранник В. В. Методология позиционирования полиадических кодовых конструкций на основе классифицирующих признаков в системе криптокомпрессионного представления / В. В. Баранник, С. А. Сидченко, И. М. Тупица, Н. А. Королева // Інформаційно-керуючі системи на залізничному транспорті. – 2015. – № 4. – С. 56 - 60., doi.org/10.18664/ikszt.v0i4.53977 (rus).
10. Баранник В. В. Метод дешифруемо-стойкого представления изображений / В. В. Баранник, С. А. Сидченко, В. В. Ларин // Сучасна спеціальна техніка. – 2011. – №1 (24). – С. 24 - 29.

11. Barannik V.V. The Decoded-proof Presentation of Images on the Basis of the Polyadycal Encoding Systems / V. V. Barannik, S. A. Sidchenko, V. V. Larin // XIth International Conference CADSM 2011, The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv-Polyana, Ukraine, Lviv Polytechnic National University, February 23 – 25, 2011. – P. 182.
12. Сидченко С. А. Способ представления изображений стойких к дешифрированию на основе плавающей схемы кодирования / С. А. Сидченко // Системи озброєння і військова техніка. – 2011. – Вип. 3 (27). – С. 68 – 70.
13. Barannik V. Methodology constructions of floating chart of decoded-proof presentation of images / V. Barannik, S. Sidchenko // 11th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science, TCSET'2012; Lviv - Slavske; Ukraine; 21 February 2012 - 24 February 2012. – p. 437.
14. Barannik V. The method of crypto-semantic presentation of images based on the floating scheme in the basis of the upper boundaries / V. Barannik, I. Tupitsya, S. Sidchenko, R. Tarnopolov // 2nd International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2015; Kharkiv; Ukraine; 13 October 2015 - 15 October 2015. – pp. 248 - 250, doi.org/10.1109/infocommst.2015.7357326 (eng).
15. Баранник В. В. Метод криптосемантического представления изображений на основе плавающей схемы в базисе по верхним границам / В. В. Баранник, С. А. Сидченко, И. М. Тупица // Радиоэлектроника и информатика. – 2015. – № 4. – С. 9 - 12.
16. Barannik V. The application for internal restructuring the data in the entropy coding process to enhance the information resource security / V. Barannik, I. Tupitsya, S. Shulgin, S. Sidchenko, V. Larin // 2016 IEEE East-West Design & Test Symposium (EWDTS), Yerevan, 2016. – pp. 1 - 4, doi.org/10.1109/ewdts.2016.7807749 (eng).
17. Наукоемкие технологии в инфокоммуникациях: обработка и защита информации: коллективная монография / под ред. В.В. Баранник, В.М. Безрук. – Х. : СМІТ, 2013. – 398 с.