РОССИЙСКАЯ АКАДЕМИЯ НАУК
СИБИРСКОЕ ОТДЕЛЕНИЕ
АВТОМЕТРИЯ
2003, том 39, № 3

УДК 519.688

С. В. Пискунов, Д. П. Шашков
(Новосибирск)

КОМПЬЮТЕРНАЯ КЛЕТОЧНАЯ МОДЕЛЬ СХЕМЫ ВИЗУАЛЬНОЙ КРИПТОГРАФИИ

Предложена клеточно-автоматная реализация визуальной пороговой схемы разделения секрета. Реализация выполнена в виде компьютерной модели в системе имитационного моделирования мелкозернистых вычислений WinALT и может служить основой для построения оптико-электронных специализированных устройств, выполняющих такие схемы разделения секрета.

Введение. Известна схема разделения секретной информации, называемая «пороговой схемой разделения секрета k из n» (ПСРС(k,n)) [1–3]. В этой схеме секретный ключ K делится на n частей (по числу участников схемы): а) любые k участников могут составить из своих частей ключ K; б) ни одна группа из $(k-1)$ участников не может составить весь ключ K или его часть. Секретной информацией для ПСРС может быть любая информация, например изображение, печатный или рукописный текст.

В работе [4] предложена визуальная ПСРС (ВПСРС), применение которой названо «визуальной криптографией». Наглядно проблема формулируется так: есть секретное черно-белое изображение, которое разделяется на части (разделения), и они раздаются n участникам схемы. Каждая часть – это некоторое шумоподобное изображение на прозрачной пленке – диапозитиве. Если $k(k \le n)$ участников положат свои пленки друг на друга в произвольной последовательности, то они смогут увидеть исходное изображение, в то время как меньшее число участников нет.

Возможны два основных применения таких схем – это визуальная идентификация [5] и передача изображения с сокрытием факта передачи, например, для ВПСРС (2, 2) вместо одного из шумоподобных разделений используется некоторое осмысленное изображение [4].

ВПСРС(k,n) [4] состоит из двух совокупностей матриц C_0 и C_1 размера $m \times n$. Чтобы разделить белый пиксел, случайным образом выбирается одна из матриц в C_0, а чтобы разделить черный пиксел, случайным образом выбирается одна из матриц в C_1. Матрицы задают разделение на группы подпикселов (по группе на каждое разделение) так, чтобы при объединении по ИЛИ групп черного пиксела получалась группа только с черными подпикселами, а при объединении групп белого пиксела получалась группа, содержащая как белые, так и черные подпикселы («нечерная» группа). Выбранная матрица определяет цвет m подпикселов в каждом из n диапозитивов.

ВПСРС имеет следующие параметры: m – число пикселов в разделении (отражает потерю в разрешающей способности при переходе от оригинального изображения к некоторому разделению, предпочтительно задавать m как можно меньше); r – размер совокупностей C_0 и C_1 ($\log_2 r$ отражает число случайных битов, необходимых для генерации разделений).

В работе [4] построены схемы разделений черных и белых подпикселов для $k = 2, 3, 4$ и $n = 2, 3, 4$ и обобщены на произвольное n. ВПСРС (3, 3) является обозримым и практичным примером визуальной схемы криптографии. В ВПСРС (3, 3) $m = 4$ и совокупность матриц C_0 образуют все матрицы, полученные перестановкой столбцов матрицы $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$, совокупность матриц C_1 образуют все матрицы, полученные перестановкой столбцов матрицы $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$. Шесть разделений, образованных строками этих матриц в виде массивов подпикселов, показаны на рис. 1. Каждая матрица из C_0 или C_1 содержит одно горизонтальное, одно вертикальное и одно диагональное разделение. Каждое разделение содержит случайный выбор двух черных подпикселов, а любая пара разделений из одной матрицы содержит случайный выбор из одного общего черного подпиксела и двух разных черных подпикселов. Следовательно, анализ одного или двух разделений делает невозможным различение матрицы из C_0 и C_1. Однако стопка из трех диапозитивов из C_0 черная только на 3/4, в то время как стопка из трех диапозитивов из C_1 полностью черная.

Цель работы состоит в анализе возможности реализации ВПСРС с небольшими k, m, n как на обычной ЭВМ, использующей систему имитационного моделирования WinALT, обладающую развитыми средствами графического представления перерабатываемой информации, так и в однородном вычислительном устройстве, состоящем из нескольких слоев с оптическими межслойными связями.

Легко видеть, что для некоторой заданной ВПСРС (k, n) алгоритм шифрации изображения обладает следующими свойствами:

– *регулярность* (производятся одинаковые действия для каждого исходного пиксела);

– *независимость* (каждый исходный пиксел шифруется независимо от других);

– *простота* (производится случайный выбор матриц из совокупностей, заданных самой схемой разделения секрета).

Горизонтальные разделения | Вертикальные разделения | Диагональные разделения

Рис. 1. Разделения для ВПСРС (3, 3)

В перечисленных свойствах прослеживаются принципы клеточных вычислений (простота, локальность и массовость вычислений), что и делает привлекательной реализацию ВПСРС на клеточном автомате.

Клеточная реализация ВПСРС (k, n). Пусть задана ВПСРС с известными k, m, n и r. Требуется получить клеточный автомат (КА), реализующий шифрацию по данной ВПСРС. Автомат задается алфавитом состояния клеток A, шаблоном рабочей окрестности N, множеством правил перехода R. Клетки, входящие в окрестность N, участвуют в совместном изменении своих состояний согласно правилам из R. Такой автомат предложен в [6]. В соответствии с поставленной целью его описание используется для построения компьютерной модели ВПСРС (3, 3) и оценки на ее основе возможности оптической реализации клеточных автоматов, реализующих ВПСРС.

Приведем описание КА. Он реализует функцию f, ставящую в соответствие исходному пикселу p и случайному числу r' матрицу c, входящую в одну из совокупностей C_0 или C_1:

$$f: (p, r') \rightarrow c,$$

где $p \in \{0,1\}$, $r' \in \{0,1,\ldots,r-1\}$ и ($c \in C_0$ и $c \notin C_1$ или $c \in C_1$ и $c \notin C_0$).

Правила переходов состояний предлагаемого КА выглядят следующим образом:

$$p, r', *, *, \ldots, * \rightarrow *, *, c_1, c_2, \ldots, c_n, \qquad (1)$$

где $c_1, c_2, \ldots, c_n$ – матрицы размера $m \times 1$ нового состояния КА в слоях участников ВПСРС (проекция матрицы c на соответствующий слой); «*» - «безразличный» символ.

Клеточный автомат имеет многослойную структуру со слоями по оси Z (рис. 2). Семантика слоев указана на рисунке. Поскольку каждый пиксел ВПСРС шифруется независимо от других, то шаблон рабочей окрестности N разбивает клеточное пространство на независимые домены вычислений. Таким образом, новое состояние клеток рабочей окрестности не зависит от состояния клеток любой другой рабочей окрестности. Это означает, что КА бу-

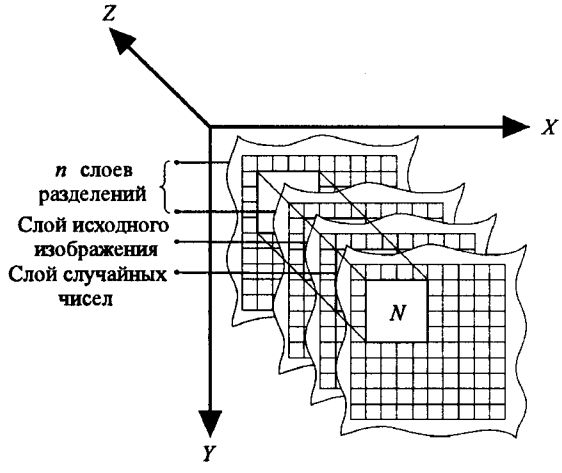

Рис. 2. Многослойный клеточный автомат

дет работать только один такт, в течение которого произойдет независимая шифрация каждого пиксела исходного изображения. Клеточный автомат имеет следующие характеристики:

1) размер алфавита состояний $|A|=2$ (битовое представление информации);

2) количество слоев равно $n+2$;

3) размер всей рабочей окрестности $|N|=(n+2)\times\max(2,\ m,\ \log_2 r)$ клеток;

4) число правил $|R|=2\times r$.

Отметим, поскольку правила перехода являются параллельными подстановками, которые применяются одновременно и повсеместно во всех доменах пространства данных КА, то функционирование КА описывается алгоритмом параллельных подстановок (АПП) [7].

Компьютерная модель ВПСРС (3, 3). Реализация КА, описывающего ВПСРС (3, 3), выполнена в виде модели в системе WinALT [8]. Эта система позволяет в простой и наглядной форме представлять клеточные автоматы: и клеточное пространство данных, и совокупность правил перехода (1) автомата, записанную в виде АПП.

Опишем модель. Клеточное пространство данных модели имеет такое же расположение и семантику слоев, как на рис. 2, с одним лишь отличием: оно содержит не пять слоев, как должно быть в соответствии с характеристиками ВПСРС, а шесть. Наличие шестого, самого удаленного от зрителя, слоя объясняется тем, что в модели совмещены и алгоритм шифрации, и алгоритм дешифрации, и этот слой служит для демонстрации результата работы алгоритма дешифрации. Далее на рисунках покажем стопку слоев в виде развертки на плоскости. Ближайший к зрителю слой имеет нулевой номер и при показе на развертке расположен в самой левой позиции. Такие же соглашения принимаются при графическом изображении левых и правых частей команд подстановок, заданных слоями окрестности N. Окрестность N имеет в плоскости размер 2×2 клетки.

Множества C_0 и C_1 для ВПСРС (3, 3) содержат по 24 матрицы, т. е. $r=24$. Средства системы WinALT позволяют в любой клетке хранить любое число общепринятого типа, однако для более простого визуального представления состояний клеток всех слоев в данной модели было принято битовое представление чисел. Как следствие, на битовое представление случайного числа r' не хватило четырех клеток в нулевом слое рабочей окрестности N, поэтому пятый (старший) бит был перенесен в первый слой рабочей окрестности N в ее левую верхнюю клетку. Поскольку информация продублирована во всех клетках окрестности N этого слоя (для согласования размеров исходного изображения и разбиений), стало возможным использовать такую клетку как служебную и хранить в ней бит случайного числа r'. Правда, в этом случае исходное изображение получается несколько зашумленным.

ВПСРС (3, 3) в модели описывается с помощью программы, содержащей два модуля: модуль шифрации и модуль дешифрации. Модуль шифрации состоит из нескольких процедур. Процедура инициализации обнуляет состояния клеток всех слоев (делает их черными), кроме слоя с исходным изображением. Процедура генерации случайных чисел заполняет случайными битами клетки нулевого и некоторые клетки первого слоев. Это вспомогательные процедуры и детально рассматриваться не будут. Главной является процедура шифрации, которая реализует КА, выполняющий построение разделений.

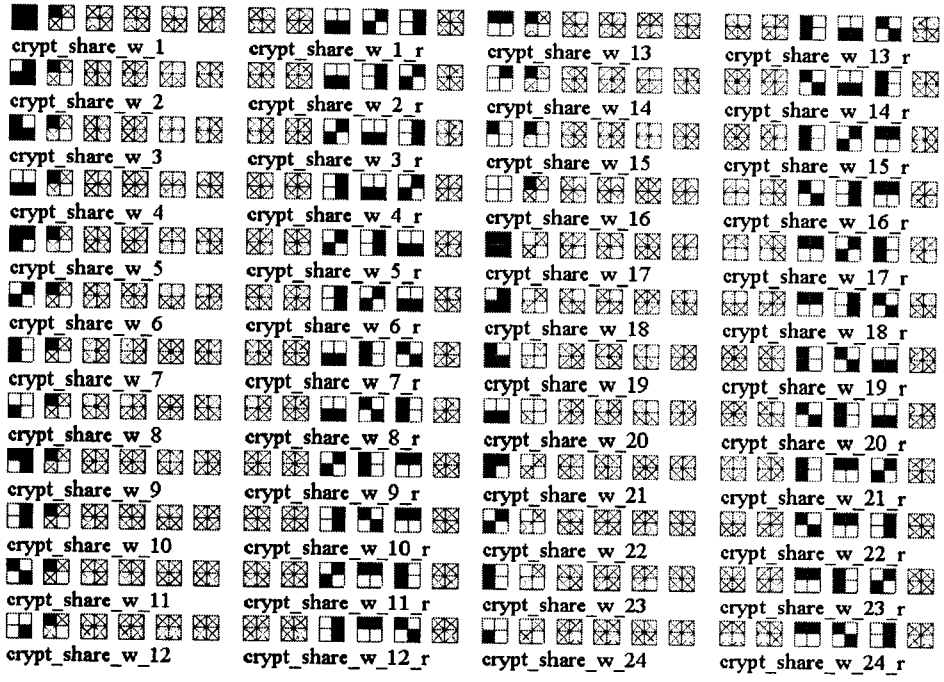

Рис. 3. Развертки левых и правых частей команд подстановок клеточного автомата для белого пиксела

Процедура довольно естественно делится на две части. Первая часть содержит команды подстановок, выполняющие разделение белого пиксела исходного изображения, вторая – черного пиксела исходного изображения. На рис. 3 показаны развертки левых и правых частей 24 команд подстановок, выполняющих разделение белого пиксела. Белый пиксел расположен в правой нижней клетке первого слоя окрестности N. Клетка, перечеркнутая косым крестом, означает клетку в «безразличном» состоянии. У каждой развертки есть имя; две развертки с именами crypt_share_w _i и crypt_share_w_i_r, где $i = 1, \ldots, 24$, образуют команду подстановки. Символически это можно изобразить, соединив их стрелкой. В модели роль стрелки выполняет связка операторов at – do [7, 8], параметрами в которых служат соответственно имена crypt_share_w_i и crypt_share_w_i_r. Совершенно аналогично, но только с использованием матриц совокупности C_1 строятся 24 команды подстановок, выполняющие разделение черного пиксела. Объединение команд для белого и черного пикселов будем называть АПП шифрации. Разбиение клеточного пространства на домены вычислений, к которым привязывается выполнение подстановок АПП шифрации, реализуется с помощью оператора step [7, 8] с параметрами, задающими шаг, равный 2, вдоль осей X и Y клеточного пространства модели.

Модуль дешифрации содержит процедуру дешифрации, выполняющую наложение друг на друга трех разбиений. Результат наложения фиксируется в шестом слое. Развертки левых и правых частей команд подстановок, задающих КА дешифрации, показаны на рис. 4. Чтобы получить команды, достаточно соединить стрелками пары разверток, расположенных в одной строке. Команды выполняются для всех пикселов, имеющих одинаковые координа-

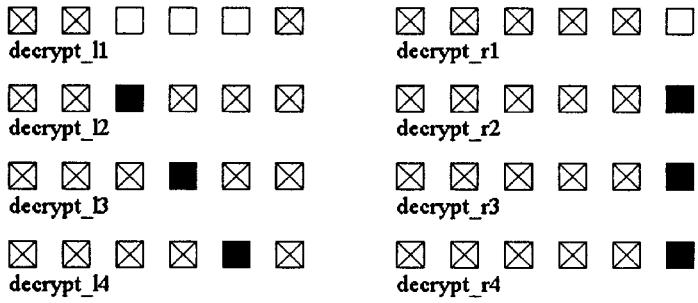

Рис. 4. Развертки левых и правых частей команд подстановок клеточного автомата дешифрации

ты вдоль осей X, Y, всех слоев клеточного пространства модели. Выполнение команд означает, что пиксел в слое с номером 5 клеточного пространства становится белым, если и только если все три пиксела в разделениях белые. На рис. 5 показан результат работы программы по шифрации и дешифрации исходного образа, содержащего букву Е.

Техническая реализация клеточных алгоритмов визуальной криптографии. В предыдущем разделе фактически предложен компьютерный вариант и шифрации, и дешифрации визуальных данных с использованием ВПСРС. Использование системы WinALT позволило представить эти операции в наглядной форме. Моделирование подтвердило, что построение всех разделений выполняется за один такт и независимо одно от другого. Но нужно помнить, что выполнялась имитация работы КА на последовательной машине, поэтому реальная временная оценка сложности такого варианта равна по порядку d^2, где d – размер клеточного пространства вдоль осей X и Y. Конечно, так как операции шифрации и дешифрации легко распараллеливаются, то, используя параллельную версию системы WinALT, реализованную на кластере, можно практически в s раз улучшить временную сложность, где s – число машин в кластере. Но в любом случае остается зависимость временной сложности от размеров клеточного пространства, в то время как в КА ее нет. Поэтому представляется интересным оценить возможность непосредственной реализации КА в аппаратуре.

Было отмечено, что построение всех разделений выполняется за один такт и независимо одно от другого. Поэтому может быть выполнена очевидная декомпозиция АПП шифрации: каждая команда подстановки разделяет-

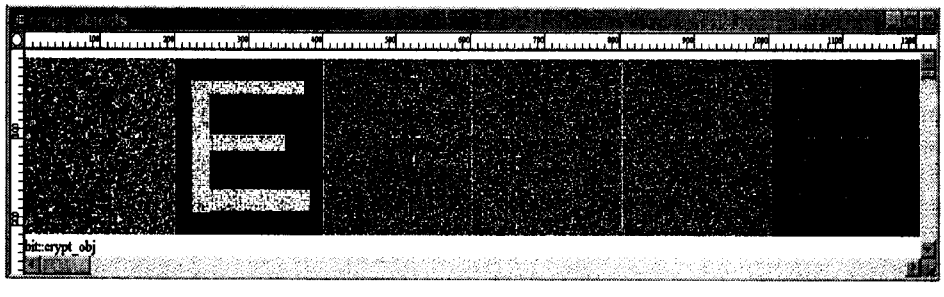

Рис. 5. Окно модели с результатами работы модулей программ

ся на три команды так, что первые два шаблона в левых частях являются общими у всех команд, третий шаблон составлен из клеток в безразличном состоянии, в то время как правая часть исходной команды разделяется так, что в первую команду в третью позицию развертки попадает шаблон, определяющий первое разделение, во вторую – шаблон, определяющий второе разделение, в третью – шаблон, определяющий третье разделение. Шаблоны в первой и второй позициях разверток правых частей всех трех команд составлены из клеток в безразличном состоянии. Команды, выполняющие i-е ($i=1,2,3$) разделение, объединяются в АПП i шифрации.

Выполнив декомпозицию АПП шифрации, КА можно реализовать в виде устройства со следующей архитектурой. В плоскости размещены три матрицы, у которых в каждой клетке расположен фотоприемник. Средствами оптики (линзы, призмы и т. п.) на каждую из них проектируется и запоминается в ячейках памяти, связанных с фотоприемниками, вначале кодируемый образ, а затем матрица случайных битов. Далее в каждой матрице с номером i ($i=1,2,3$), в каждой ее окрестности N, выполняется вычисление новых состояний клеток в соответствии с подстановками из АПП i шифрации, на основе которого строится простейшее АЛУ, обеспечивающее изменение состояний клеток окрестности N. Состояния клеток хранятся в ячейках памяти, которые управляют либо активными, либо пассивными излучателями, что обеспечивает оптическое считывание разделений. Другими словами, декомпозиция обеспечивает независимое построение разделений (каждого в своей матрице), но для одного и того же кодируемого образа и одной и той же таблицы случайных битов.

Устройство дешифрации представляет собою плоскую матрицу, в каждой клетке которой расположен пороговый фотоприемник. Средствами оптики на нее одновременно проектируются три матрицы разделений, состояния фотоприемников запоминаются в ячейках памяти, эти ячейки хранят дешифрованный образ. Если ячейки памяти соединены с излучателями, то дешифрованный образ можно увидеть визуально.

Как шифрация, так и дешифрация выполняются за один такт.

Предложенные устройства не ориентированы на микроэлектронное исполнение, но могут служить основой для построения устройств с $3D$-архитектурой, для которых возможна реализация в микроэлектронном исполнении с использованием оптики, например, в соответствии с принципами конструирования таких устройств, предложенными в [9].

Устройство дешифрации имеет $3D$-архитектуру и содержит три слоя с номерами 1, 2, 3. Первый слой предназначен для выполнения первого разделения, второй – второго и третий – третьего. Каждый слой – это матрица клеток. В клетке матрицы можно выделить электронную и оптическую компоненты. Оптическая компонента содержит излучатель и фотоприемник, ориентированные в противоположных направлениях. Электронная компонента содержит две ячейки памяти, основную и буферную, вместе они образуют внутреннюю память клетки. Ориентация фотоприемников и излучателей выбрана так, что фотоприемники первого слоя образуют оптический вход устройства, излучатели первого слоя оптически связаны с фотоприемниками второго слоя, излучатели второго слоя – с фотоприемниками третьего слоя, и, наконец, излучатели третьего слоя формируют оптический выход устройства. Изображение задается состояниями (включен – 1, выключен – 0) матриц фотоприемников и излучателей слоя, а также состояниями ячеек памяти клеток. Излучатель каждой клетки слоя управляется основной ячейкой памяти

клетки, которая имеет оптический вход с подключенным к нему фотоприемником. Кодируемый образ поступает на матрицу фотоприемников первого слоя. Матрица буферных ячеек памяти каждого слоя предназначена для промежуточного хранения разделений в электронном виде.

Для того чтобы разбить каждый i-й слой на домены вычислений, клетки с четными координатами по осям X и Y делаются активными, т. е. в каждую такую клетку включается дополнительное оборудование – АЛУ, реализующее АПП i. Это может быть, например, микропрограммный автомат [7], память которого хранит левые и правые части АПП i. Кроме того, каждая активная клетка слоя содержит регистр, разряды которого хранят случайное число. Все регистры слоя объединены двумерной системой шин, обеспечивающей ввод в слой матрицы случайных двоичных чисел (в предлагаемом устройстве – пятиразрядных чисел). Эта матрица может быть введена строка за строкой перед началом работы устройства шифрации во все три слоя из некоторого внешнего хранилища, которое может многократно превосходить по объему матрицу случайных чисел, используемую в устройстве, и может периодически пополняться новыми строками случайных чисел. Такая особенность хранилища позволяет регулярно заменять в устройстве матрицу случайных чисел новой матрицей и, более того, делать это динамически, «вталкивая» новые строки из хранилища в строки регистров слоев в промежутках между получениями очередных разбиений.

Примечание. В рассматриваемом примере реализации устройства, в отличие от его модели и первого варианта реализации, хранение таблицы случайных чисел полностью отделено от хранения шифруемого образа.

Опишем алгоритм функционирования устройства. Построение разделений и пересылка их на выход устройства выполняются в четыре фазы.

Первая фаза. Кодируемый образ проходит попеременно через фотоприемники и управляемые ими излучатели всех трех слоев и запоминается в основных ячейках памяти клеток каждого слоя. В каждом слое выполняется построение разделения, состояния подпикселов которого хранятся в виде нулей и единиц в буферных ячейках памяти клеток каждого слоя.

Вторая фаза. Состояния подпикселов, хранящиеся в третьем слое, переписываются из буферных ячеек памяти в основные и, следовательно, оказываются представленными состояниями излучателей этого слоя, и могут быть считаны вовне.

Третья фаза. Состояния подпикселов, хранящиеся во втором слое, переписываются из буферных ячеек памяти в основные и, пройдя путь излучатель – фотоприемник – излучатель, оказываются представленными состояниями излучателей третьего слоя, и могут быть считаны вовне.

Четвертая фаза. Состояния подпикселов, хранящиеся в первом слое, переписываются из буферных ячеек памяти в основные и, пройдя путь излучатель – фотоприемник – излучатель – фотоприемник – излучатель, оказываются представленными состояниями излучателей третьего слоя, и могут быть считаны вовне.

Быстродействие предлагаемого устройства может быть высоким, так как оно определяется временем вычисления разделения. Это время практически совпадает с временем ассоциативной выборки команды подстановки по случайному числу, хранящемуся в регистре активной клетки, из таблицы, содержащей в строках команды АПП i (в предлагаемом устройстве число команд равно 24), сложенным с временем записи результата вычислений в буферные

ячейки памяти клеток, входящих в окрестность N слоя. Отметим, что для всего устройства возможна оптическая синхронизация.

Опишем архитектуру устройства дешифрации. Устройство содержит четыре слоя. Первые три слоя одинаковы. Каждый слой содержит матрицу активных излучателей. В каждой клетке матрицы излучатель соединен с ячейкой памяти, управляемой фотоприемником. Входной образ поступает на матрицу фотоприемников, а считывается с матрицы излучателей. Разделения дешифрируемого образа одно за другим через слои с номерами 1, 2, 3 в конвейерном режиме проходят на слой с номером 4. Оптическое устройство этого слоя аналогично устройству предшествующих ему слоев с одним исключением: в каждой клетке матрицы фотоприемник подключен ко входу накопительной схемы ИЛИ, выходом которой является излучатель. Состояния излучателей последнего слоя составляют дешифрованный образ.

Заключение. Предложена методика реализации ВПСРС (k, n) в виде многослойного КА и приведен компьютерный пример выполнения ВПСРС (3, 3) с использованием системы имитационного моделирования WinALT. Этот пример демонстрирует возможность простой и наглядной реализации ВПСРС на обычной ЭВМ. Компьютерная модель ВПСРС (3, 3) была использована для построения оптико-электронных $3D$-устройств, выполняющих шифрацию и дешифрацию визуального образа. Легко видеть, что предложенный способ создания устройства может быть распространен на ВПСРС с другими параметрами k, n, m. Действительно, общая архитектура устройств сохраняется, меняются только окрестность N и число слоев.

СПИСОК ЛИТЕРАТУРЫ

1. **Shamir A.** How to share a secret // Comm. ACM. 1979. **22**, N 11. P. 612.
2. **Blakley G.** Safeguarding cryptographic keys // AFIPS Conf. Proc. Vashington: Arlington, 1979. Vol. 48. P. 313.
3. **Введение** в криптографию /Под ред. В. В. Ященко. М.: МЦНМО, 1998.
4. **Naor M., Shamir A.** Visual Cryptography // Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1995. Vol. 950. P. 1.
5. **Naor M., Pinkas B.** Visual Authentication // Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1997. Vol. 1294. P. 322.
6. **Шашков Д. П.** Клеточная реализация алгоритмов визуальной криптографии // Тр. конф. молодых ученых. Новосибирск: Изд-во ИВМиМГ СО РАН, 2002. С. 202.
7. **Achasova S., Bandman O., Markova V., Piskunov S.** Parallel Substitution Algorithm. Theory and Application. Singapore: World Sci., 1994.
8. **Beletkov D. T., Ostapkevich M. B., Piskunov S. V., Zhileev I. V.** WinALT, a software tool for fine-grain algorithms and structures synthesis and simulation // Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1999. Vol. 1662. P. 491.
9. **Egorov V. M., Kostsov E. G.** Integral optical digital computers // Appl. Opt. 1990. **29**, N 8. P. 1178.

Институт вычислительной математики и математической геофизики СО РАН, E-mail: piskunov@ssd.sscc.ru

Поступила в редакцию 2 апреля 2003 г.