ИНФОРМАТИКА И УПРАВЛЕНИЕ

УДК 681.3

К РЕШЕНИЮ ЗАДАЧИ МАСКИРОВАНИЯ СТИЛИЗОВАННЫХ ДВОИЧНЫХ ИЗОБРАЖЕНИЙ

© 2001 г. В.А.Райхлин, докт. физ.-мат. наук, **И.С.Вершинин**, магистрант, **Е.Е.Глебов**, инженер

КГТУ им. А.Н.Туполева, Казань

Маскирование стилизованных двоичных изображений при их хранении или передаче рассматривается как эффективное средство защиты от несанкционированного распознавания. Анализируются варианты сжатого представления изображений в терминах "объекты – координаты" и их представления без сжатия. Для первого варианта предлагается алгоритм маскирования и обсуждается его эффективность. Показывается, что задача маскирования для другого варианта практически неразрешима. Устанавливается целесообразность введения дополнительной байтовой сетки кадра.

1. Связь с распознаванием

Стилизация подразумевает получение (генерацию) плоских двоичных изображений машинным способом. Это могут быть карты разведывательного характера, карты полезных ископаемых, морские карты глубин и др., на которых объекты представлены их условными обозначениями; чертежи конструкций из типовых деталей, электрические принципиальные схемы цифровых устройств и т.д. По условию объекты рассматриваемых изображений не пересекаются.

Плоское двоичное изображение использует битовую сетку кадра. Состояние бита с координатами (i, j) – 1 либо 0. Каждый объект занимает прямоугольную область размерами $k^t \times l^t$ бит, t – номер типа объекта. Его идентификация происходит, например, по правой нижней границе [1]. Применение дополнительной байтовой сетки (обычно длина байта не превышает 8 бит), такой, что границы любого объекта изображения проходят по этой сетке, позволяет упростить решение задачи распознавания в терминах "объекты – координаты" [2].

В общем случае задача распознавания стилизованных двоичных изображений формулируется следующим образом [1]. Для данного троичного эталона (троичной матрицы)

$$X^t = \left| x^t_{pq} \right|; \; x^t_{pq} \in \{0, 1, –\}, p = 1 \ldots k^t,$$
$$q = 1 \ldots l^t; t \in \{\overline{1,\gamma}\}$$

(γ – число типов объектов) найти координаты всех покрываемых им объектов двоичного изображения (булевой матрицы)

$$A = \left| a_{ij} \right|; a_{ij} \in \{0, 1\}, i = 1 \ldots K, j = 1 \ldots L; K \geq k^t, L \geq l^t.$$

Запись x^t_{pq} = (–) означает безразличное (замаскированное) значение соответствующего элемента эталона. Множество замаскированных элементов отображается единичными элементами матрицы масок:

$$M^t = \left| m^t_{pq} \right|; \; m^t_{pq} = \begin{cases} 0, x^t_{pq} \in \{0,1\}; \\ 1, x^t_{pq} \in \{–\}. \end{cases}$$

Маскирование может, например, учитывать локально-детерминированные дефекты объектов, связанные с небольшими отклонениями размеров, расположения или угловой ориентации их отдельных элементов в сравнении с двоичным эталоном. Однако возможности такого маскирования весьма ограниченны. В дальнейшем рассматриваемое изображение в целом полагается идеальным (каждый объект
в точности повторяет свой двоичный эталон), а размеры всех объектов – одинаковыми. Задачей маскирования считается защита передаваемых или хранимых в памяти ЭВМ изображений от несанкционированного распознавания, что весьма актуально. Анализируются случаи передачи и хранения как сжатых (в терминах "объекты – координаты"), так и полных изображений. Целью анализа является выяснение разрешимости и наметка возможных путей решения задачи маскирования в обоих случаях.

2. Основной алгоритм маскирования

Естественным требованием к маскированию объектов является взаимная непокрываемость любой пары троичных эталонов множества $\{X^t\}$, $t \in \{\overline{1,\gamma}\}$, что диктуется требованием однозначности санкционированного распознавания. Достаточное условие такой непокрываемости – различие хотя бы в одном значащем элементе x^t_{pq} троичных матриц X^{t1} и X^{t2}, $t1 \neq t2$.

Элементы эталона X^t, не подлежащие маскированию, определены единичными компонентами инверсной матрицы масок $\overline{M}^t = \left| \overline{m}_{pq} \right|$ для этого

эталона. Решение задачи маскирования в данном случае существенно многозначно. Два возможных варианта решения на множестве десятичных цифр показаны на рис. 1. Точками обозначены сохраняемые значения битов (случай $k^t = 5$, $l^t = 3$).

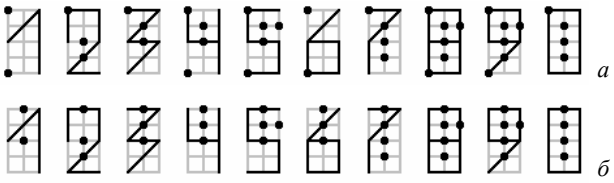


Рис. 1

Алгоритм случайного поиска сохраняемых элементов двоичных эталонов заданного множества в случае битовой сетки кадра будем называть основным алгоритмом маскирования. Формулируемый далее алгоритм построен таким образом, что каждой случайно упорядоченной перестановке двоичных эталонов, рассматриваемых на определенном этапе, отвечает свое множество вариантов решения задачи маскирования. Выбор того или иного варианта выполняется случайным образом. Поэтому вероятность несанкционированного (без знания маски) распознавания объектов изображения должна быть достаточно низкой.

Обозначим через D_l множество рассматриваемых на каждом этапе работы алгоритма двоичных эталонов. По условию множество D_0 включает полный перечень типов эталонов для всех объектов изображения.

Алгоритм

1. $l := 0$.

2. Занумеровать случайную перестановку эталонов множества D_l в натуральном порядке $Э_1$, $Э_2$, …, $Э_\gamma$, образовав тем самым список $C_l = (Э_j)$, $j = 1, 2, \ldots \gamma$. Дополнить этот список пустым элементом $Э_{\gamma+1}$. Ни один элемент списка C_l изначально не отмечен.

3. $i := 1$.

4. $j := i$, $k := 1$. Считать $Э_i$ первым элементом множества D_{l+1}.

5. Пока не встретится неотмеченный элемент списка $C_l j := j + 1$. Если $Э_j$ не пуст, идти к п. 6. Иначе – к п. 16.

6. $Э_i \oplus Э_j$ (побитно) $\rightarrow A_1$ (булева матрица).

7. Пока не встретится неотмеченный элемент списка $C_l j := j + 1$. Если $Э_j$ не пуст, идти к п. 8. Иначе – к п. 13.

8. $Э_i \oplus Э_j$ (побитно) $\rightarrow A_2$ (булева матрица).

9. $A_3 := A_1$.

10. A_1 & A_2 (побитно) $\rightarrow A_1$. Если $A_1 \neq |0|$, идти к п. 7. Иначе – к п. 11.

11. $k := k + 1$. Считать $Э_j$ k – элементом множества D_{l+1}.

12. $A_1 := A_3$. Переход к п. 7.

13. Случайным образом выбрать один из единичных элементов матрицы A_1. Его координаты (p, q) определяют новый единичный элемент $\overline{m}_{pq}$ инверсной матрицы масок $\overline{M}$ для всех неотмеченных эталонов списка C_l.

14. Отметить элементы списка C_l, включенные во множество D_{l+1}.

15. $l := l + 1$; $D_l := D_{l+1}$, $\gamma := k$. Переход к п. 2.

16. Формирование инверсной маски для последнего неотмеченного элемента списка C_l считать законченным. Отметить этот элемент, аннулировав тем самым список C_l и множество D_{l+1} (сделав их пустыми).

17. $l := l - 1$. Если $l \geq 0$, идти к п. 18. Иначе – к п. 19.

18. Пока не встретится неотмеченный элемент списка C_l

$i := i + 1$. Переход к п. 4.

19. КОНЕЦ.

Работу алгоритма иллюстрирует рис. 2. Переупорядочение элементов при переходе на вышестоящий уровень на рисунке не показано. Точками выделены элементы списков C_l. Кружками – отметки этих элементов. Факт аннулирования списка обозначен петлей обратной связи для его последнего неотмеченного элемента. Цифры на стрелках проставлены в порядке наступления совокупных событий подъема – спуска между уровнями. Замечаем, например, что списки C_1 и C_2 аннулировались по четыре раза, а списки C_0 и C_3 – по одному.

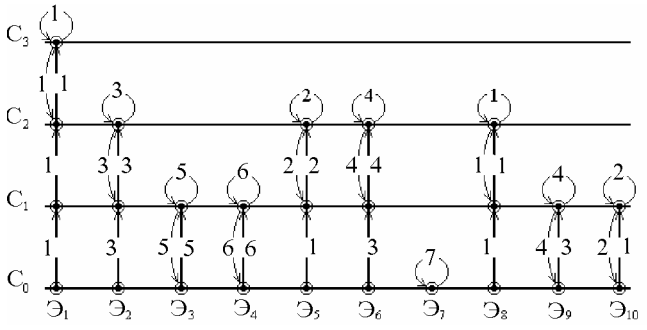


Рис. 2

Переход на вышестоящий уровень всегда означает разделение списка более низкого уровня на две противопоставляемые части. Такая дихотомизация осуществляется вновь вводимым единичным элементом $\overline{m}_{pq} = 1$ инверсной матрицы масок, ибо элемент x_{pq} троичных эталонов для одной части оказывается единичным, а для другой – нулевым. Из этого вытекает корректность алгоритма в том смысле, что он действительно решает поставленную задачу.

На рис. 3 представлены полученные программным путем по этому алгоритму некоторые варианты маскирования для трех различных исходных перестановок десятичных цифр. Здесь по-прежнему $k^t = 5$,

$l^t = 3$. Под каждой цифрой приводится соответствующая инверсная матрица маски.

Предложенный алгоритм дает решение задачи маскирования при хранении или передаче сжатого представления изображений в терминах "объекты – координаты". Тем самым установлена принципиальная разрешимость задачи для данного случая. При этом объекты описываются троичными матрицами, замаскированные элементы которых заполняются случайным образом с использованием процедуры рандомизации. Для распознавания объекта надо знать его точный (двоичный) эталон и соответствующую ему маску. Эта маска является закрытым ключом, передаваемым по спецканалу.

0	1	9	6	7	8	2	5	4	3	
100	100	100	100	100	100	000	000	100	100	
000	000	001	000	000	000	000	000	000	001	
010	000	000	000	001	010	000	000	001	000	*а*
100	000	010	100	010	100	110	110	010	010	
010	010	010	010	010	010	010	010	010	010	
3	2	6	9	8	0	7	4	1	5	
000	000	010	000	000	000	000	000	000	010	
100	000	001	100	001	001	000	001	001	001	
001	000	000	001	010	010	001	010	010	000	*б*
000	010	010	000	010	010	000	010	010	010	
001	001	001	001	011	101	001	011	101	001	
6	0	9	7	2	5	4	1	8	3	
100	110	100	100	100	110	110	100	110	100	
000	001	010	010	010	001	000	000	001	010	
010	010	010	010	010	000	000	010	010	010	*в*
000	001	001	001	001	001	001	000	001	001	
000	000	000	000	000	000	000	000	000	000	

Рис. 3

3. Эффективность алгоритма

За критерий эффективности сформулированного алгоритма маскирования принимается вероятность P получения "противником" точной копии всех масок, использованных для хранения или передачи данного изображения, при однократном запуске открытой программы генерации масок. Эффективность тем выше, чем меньше эта вероятность. Подсчитаем значение P для примера маскирования рис. 3, *а* согласно зафиксированным этапам работы программы, приняв за основу следующие положения.

Число различных перестановок n элементов равно $n!$ [3]. Поэтому вероятность получения использованной при маскировании перестановки n_i элементов i-го уровня (рис. 2) в случае равномерного распределения есть $1/(n_i!)$. Вероятность того или иного выбора единичного элемента булевой матрицы A_{1i} i-го уровня, содержащей k_i единиц, в том же случае равна $1/k_i$. Согласно теореме умножения вероятностей [4], учитывая наблюдаемую динамику перемещения по уровням рис. 2, для рассматриваемого примера получаем

$$P = \frac{1}{10!}\cdot\frac{1}{1}\cdot\frac{1}{5!}\cdot\frac{1}{1}\cdot\frac{1}{4}\cdot\frac{1}{5}\cdot\frac{1}{1}\cdot\frac{1}{1}\cdot\frac{1}{3}\cdot\frac{1}{10} = 3{,}8\cdot 10^{-12}.$$

Таким же способом были подсчитаны вероятности генерации точной копии всех масок для 10^3 случайных перестановок эталонов множества $\{\overline{0{,}9}\}$. Усредненная величина вероятности составила $7{,}9\cdot 10^{-11}$. Это говорит о теоретически высокой эффективности предлагаемого алгоритма маскирования.

В условиях практики найденные значения определяют нижние границы оценок вероятности, ибо эти значения получены для строго равномерного закона распределения. Используемые в ПЭВМ стандартные программы в точности не реализуют такой закон. Кроме того, в условиях рандомизации объектов не исключена возможность распознавания даже при несовпадении масок. Поэтому более объективную оценку эффективности может дать статистический анализ экспериментальных данных.

Эксперимент проводился следующим образом.

1. Однократный запуск программы генерации масок.

2. Доопределение замаскированных элементов объектов с использованием стандартной функции рандомизации языка программирования C++.

3. Повторный запуск программы генерации масок.

4. Идентификация рандомизированных объектов с использованием вновь полученных масок.

5. Повторение пп. 3, 4 заданное число раз с набором статистики.

Для целей эксперимента была разработана специальная программная система. Одна из ее программ случайным образом генерирует маски для заданного множества объектов и проводит их рандомизацию. Другая программа, имитируя действия "противника", использует точные эталоны и рандомизированные объекты. Она генерирует свой набор масок, с помощью которого проводит идентификацию этих объектов, реализуя известный алгоритм распознавания по фрагментам [1].

В процессе идентификации каждого объекта с ним сопоставляется γ пар "эталон – маска", сгенерированных для данного опыта. При этом всякий раз фиксируется факт однозначной идентификации (не обязательно правильной). И так – по всему множеству рандомизированных объектов. По завершении цикла начинается следующий опыт. Эксперимент проводился на ЭВМ класса PENTIUM-2 над множеством

десятичных цифр ($\gamma = 10$), представленных двоичными эталонами 10×20.

Была проведена серия из 10^5 опытов с целью определения числа циклов, в которых правильно распознаются только группы из одного объекта, только группы из двух объектов и т.д. Циклы следовали непрерывно один за другим в течение суток. При этом велись промежуточные подсчеты после 10^3 и 10^4 опытов. Набранная статистика представлена в табл. 1. Полученные данные говорят об устойчивом отсутствии распознавания в одном опыте семи и более объектов. Экспериментально найденное значение $P<10^{-6}$ представляет верхнюю границу искомой оценки.

Таблица 1

Статистика идентификации групп объектов

Число рандомизированных объектов в группе	Число циклов правильного распознавания только данной группы		
	10^3 опытов	10^4 опытов	10^5 опытов
'1 obj'	428	4090	40757
'2 obj'	235	2444	24696
'3 obj'	79	778	7776
'4 obj'	19	161	1567
'5 obj'	0	19	212
'6 obj'	2	7	48
'7 – 10 obj'	0	0	0

Заметим, что увеличение объема серии до $1/P$ опытов не может в данном случае привести к распознаванию, ибо все найденные в эксперименте идентификации групп из 10 объектов могут претендовать на истинность. Поэтому не приходится ожидать, что в некотором опыте будет выявлено правильное решение. Оценка криптостойкости предложенного метода рандомизации является самостоятельным вопросом.

4. Маскирование изображения в целом

В случае сжатого представления изображений в терминах "объекты – координаты" сами координаты общедоступны. Неизвестен лишь тип объекта, расположенного по тем или иным координатам. Иногда целесообразно маскировать и сами координаты. При этом изображение следует передавать или хранить как таковое (без сжатия).

Теорема 1. При хранении или передаче изображения в целом (без сжатия) задача маскирования для битовой сетки кадра в общем случае неразрешима.

Для доказательства этой теоремы достаточно установить неразрешимость задачи маскирования хотя бы для одного частного случая. Будем считать изображение "неплотным", т.е. между объектами имеются промежутки (пробелы) как по горизонтали, так и по вертикали. Эти пробелы следует рассматривать как дополнительные объекты, которые также подлежат маскированию.

Пусть основные объекты (не пробелы) представляют собой десятичные цифры, располагаемые по строкам. В качестве базовой возьмем перестановку

3, 6, 9, 2, 5, 8, 1, 4, 7, 0.

Один из вариантов маскирования объектов для этого случая показан на рис. 4 (размеры объектов 5×3).

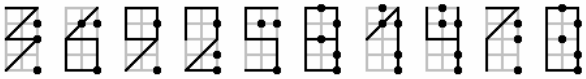


Рис. 4

Попытаемся определить допустимый вертикальный фон (вектор-столбец) промежутков в горизонтальном ряду объектов, действие которого не может вызвать ложной санкционированной идентификации. На рис. 5 показаны "занятые" объектами комбинации нулей (кружок) и единиц (точка) по этим вертикалям. Путем перебора вариантов убеждаемся в отсутствии допустимых фоновых комбинаций.

Теорема доказана.

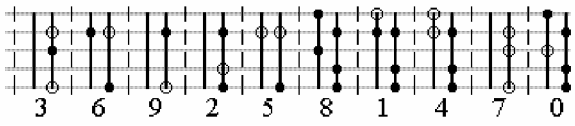


Рис. 5

При доказательстве теоремы 1 рассматривается некоторый частный случай. Остается показать, что такие случаи нередки. С этой целью был поставлен еще один программный эксперимент. Он проводился с использованием расширенной версии разработанной инструментальной системы (см. разд. 3). Это расширение позволяет выполнить анализ рандомизированных сцен (в терминах "объекты – координаты"), представленных без сжатия. В процессе анализа по предъявляемому троичному эталону выявляются все локализации соответствующего объекта в анализируемом кадре.

В кадре 300×300 случайным образом расставлялись объекты 10×20 по сетке с такими же размерами ячеек. Промежутки между объектами считались плотно упакованными объектом – помехой. В качестве него был принят пустой символ, включенный при генерации масок в единое множество эталонов. Сформированный таким образом кадр показан на рис. 6, *а*. Результат его рандомизации по сгенерированным маскам – на рис. 6, *б*.

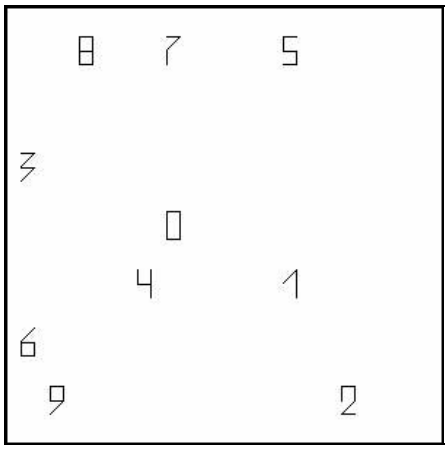
Каждый тип объекта представлен на исходном кадре однократно. Однако экспериментальные итоги распознавания рандомизированной сцены по сетке 300×300 с использованием тех же масок совсем иные (табл. 2). Полученные данные позволяют сделать вывод о практической неразрешимости задачи маскирования

для битовой сетки кадра. Это более "сильный" вывод, чем утверждение теоремы 1.

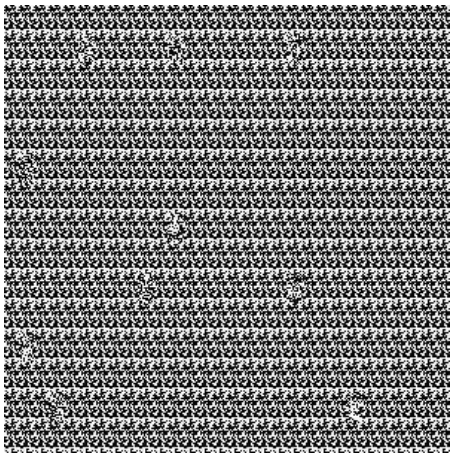
Таблица 2

Результаты анализа рандомизированной сцены по битовой сетке кадра

Имя (тип) маскируемого объекта	Количество объектов данного типа в исходном кадре	Число распознаваний объектов данного типа в рандомизированном кадре
0.obm	1	8605
1.obm	1	7864
2.obm	1	11363
3.obm	1	7599
4.obm	1	1674
5.obm	1	13083
6.obm	1	4114
7.obm	1	8252
8.obm	1	5741
9.obm	1	2055



а



б

Рис. 6

5. Применение байтовой сетки кадра

Решению задачи маскирования изображения в целом может помочь использование дополнительной байтовой сетки кадра, когда размеры всех компонентов изображения (объектов и пробелов) кратны байту. Распознавание в данном случае ведется байтами, границы которых на изображении строго фиксированы. Поэтому промежуточные ложные идентификации по битовой сетке между истинными объектами внутри байтов заведомо исключены. Но они возможны на границах байтов, если не вводить специальные "пустые" объекты для обозначения пробелов. Опасность особенно велика в случае малых объектов размерами (1×1) байт.

Крупные объекты размерами ($c^t \times d^t$) байт; c^t, $d^t > 1$, естественным образом разбиваются на элементарные фрагменты (1×1) байт. Это позволяет проводить распознавание в два этапа [2]. Сначала распознаются отдельные фрагменты. Затем они "сцепляются" в соответствии с эталоном объекта. По условию мощность η множества типов элементарных фрагментов для всех объектов изображения $2<\eta<Q$, где Q – число возможных двоичных представлений байта. Обозначив каждый тип фрагмента определенным символом, получим представление эталона объекта в виде матрицы принятых символов.

Пример такого описания в алфавите {A, B, C, D, E, F, G, H} показан на рис. 7. Сканирование этого эталона сверху вниз и вправо дает его описание в виде цепочки символов (слова) ACEGBAFDEDCAHDGB.

A	B	E	H
C	A	D	D
E	F	C	G
G	D	A	B

Рис. 7

Байтовая фоновая помеха даже в случае ее принадлежности фрагментарному алфавиту объектов не опасна, если никакое фоновое слово с возможным вхождением в него частей объектов не совпадает ни с одной из эталонных цепочек. Однако задача нахождения подходящих фоновых комбинаций в этом случае может оказаться трудноразрешимой, хотя ситуация в сравнении с показанной на рис. 5 и не столь критична ($\eta > 2$). Как и ранее, выход состоит в использовании расширенного алфавита символов для элементарных фрагментов с включением в него подмножества "пустых" символов.

Теорема 2. Задача маскирования "неплотных" изображений, хранимых или передаваемых без сжатия, при использовании дополнительной байтовой сетки кадра и мощности множества элементарных фрагментов по совокупности объектов $\eta < Q$ принципиально разрешима в расширенном алфавите символов.

Справедливость этой теоремы вытекает из следующего. При использовании байтовой сетки кадра на втором этапе распознавания происходит

сопоставление с образцом в виде незамаскированной цепочки символов длиной $l \geq 1$. После первого этапа никакая область ($c^t \times d^t$) байт (c^t, $d^t > 1$), которая включает промежутки между объектами, не должна давать цепочки, совпадающей хотя бы с одной из эталонных. Чтобы убедиться в принципиальной достижимости этого, достаточно рассмотреть тривиальный случай однородной фоновой помехи, когда все ее элементарные фрагменты представлены единственным символом вне принятого для объектов алфавита. По условию ($\eta < Q$) такой символ всегда может быть введен.

Теорема доказана.

Заключение

Рассмотренная задача маскирования приобретает серьезное практическое значение в связи с тем, что вопросам информационной безопасности уделяется сейчас особое внимание. Полученная оценка эффективности основного алгоритма маскирования достаточно высока. Однако вопросы криптостойкости предложенного метода, т.е. реальные возможности несанкционированного анализа рандомизированных сцен, представленных в сжатом виде, требуют специального изучения.

При использовании битовой сетки кадра задача маскирования изображения в целом, передаваемого или хранимого без сжатия, оказывается практически неразрешимой. Применение дополнительной байтовой сетки сводит эту задачу к двум принципиально разрешимым подзадачам: маскированию элементарных фрагментов каждого объекта и генерации подходящей фоновой помехи в расширенном алфавите фрагментов.

Тривиальный вариант генерации однородной фоновой помехи вне принятого для описания объектов алфавита может дать недостаточный маскирующий эффект по координатам идентификации.
В этом смысле более эффективна генерация неоднородного фона в расширенном алфавите.

СПИСОК ЛИТЕРАТУРЫ

1. *Райхлин В.А.* Об использовании аппарата двумерного ассоциативного поиска в процессе распознавания // Проблемно-ориентированные средства повышения эффективности вычислительных систем: Межвуз. сб. / Казан. авиац. ин-т. 1991. С. 38–54.
2. *Райхлин В.А.* Анализ производительности процессорных матриц при распознавании двоичных образов // Автометрия. 1996. №5. С. 97–103.
3. *Курош А.Г.* Курс высшей алгебры. М.: Физматгиз, 1963.
4. *Вентцель Е.С.* Теория вероятностей. М.: Физматгиз, 1962.

Поступила в редколлегию 15.12.00

ON SOLVING THE PROBLEM OF MASKING OF CONVENTIONALIZED DUAL IMAGES

V.A.Raikhlin, I.S.Vershinin, and E.E.Glebov

The masking of the conventionalized dual images in the course of their storage or transmission is considered as the effective means of protection from non-sanctional recognition. We analyze some variants of condensed representation of images in terms of "objects – coordinates" and their representations without condensation. For the first variant, we suggest the algorithm of masking and discuss its effectiveness. We show that the problem about masking for any other variant is practically unsolvable. Also shown is the expediency of introduction of the additional byte frame network.