тронной почты, социальных сетей, приложений IP-телефонии, чатов, форумов, SMS- и MMS-сообщений и т. п. Возможность восстановления переписки позволяет выявить возможных соучастников и организаторов проводимых акций, установить лиц, осуществляющих руководство и финансирование радикальных организаций.

Кроме того, извлеченные из мобильных устройств геолокационные сведения, совмещенные с данными операторов электросвязи, позволяют определить места проживания и подготовки членов радикальных организации, расположение возможных схронов оружия и боеприпасов.

Все вышеизложенное свидетельствует о возможности повышении качества работы правоохранительных органов по пресечению деятельности радикальных политизированных формирований за счет внедрения современных информационных технологий и технических средств.

УДК 621.391.01

А.С. Поляков, Д.В. Белый

ПРОСТОЙ СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ОШИБОК ПРИ ПЕРЕДАЧЕ ПО ЛИНИЯМ СВЯЗИ

Несмотря на серьезные достижения в области создания надежных каналов связи, проблема зашиты информации от ошибок при ее передаче остается достаточно актуальной. В настоящее время для решения этой задачи используются различные методы кодирования/декодирования информации, которые достаточно сложны, трудоемки при реализации и не всегда соответствуют требованиям по производительности (быстродействию). Наиболее простой способ обнаружения и исправления ошибок основан на операции вычисления четности единичных символов в строках и столбцах бинарной матрицы, представляющей собой передаваемую информацию. При кодировании двухмерных кодов этот способ позволяет определять адреса ошибок, но при условии, что и в столбцах, и в строках бинарной матрицы имеются только одиночные ошибки.

Предлагаемый ниже способ устранения ошибок основан на использовании результатов проверок четности по четырем координатам бинарной матрицы: строкам, столбцам, главным диагоналям и вспомогательным диагоналям.

Под главными диагоналями понимается как основная главная диагональ матрицы, так и все параллельные ей диагонали, рассматриваемые как непрерывные цепочки элементов матрицы, начинающиеся в первой строке и проходящие в направлении «сверху – вниз – направо» через все строки матрицы до достижения крайнего правого элемента

предыдущей строки с переходом на левый элемент следующей строки. Нумерация элементов новой строки начинается с номера, который был последним в предыдущей строке. На рисунке 1 элементы основной главной диагонали обозначены цифрой 1, а номера остальных главных диагоналей – цифрами, расположенными в верхних левых углах элементов матрицы.

Под вспомогательными диагоналями подразумеваются основная вспомогательная диагональ матрицы и все параллельные ей диагонали, проходящие в направлении «сверху – вниз – налево», начиная с первой строки матрицы и заканчивая последней строкой. С крайнего левого элемента строки происходит переход на крайний правый элемент следующей строки. Номера вспомогательных диагоналей на рисунке выделены курсивом и размещены в нижних правых углах элементов матрицы. Номера диагоналей на рисунке соответствуют номерам столбцов в первой строке матрицы: *b* – номера главных диагоналей в прямом направлении, *b̲* – номера вспомогательных диагоналей, *d* – номера главных диагоналей (расположены в верхних левых углах элементов матрицы), *d̲* – номера вспомогательных диагоналей (расположены в правых нижних углах элементов матрицы), *a* – номера строк матрицы.

		d						n	d		
b		1	2	3	4	5	6	7	8	9	10
b̲		9	8	7	6	5	4	3	2	1	Ln
a	1	1 9	2 8	3 7	4 6	5 5	6 4	7 3	8 2	9 1	
	2	9 8	1 7	2 6	3 ▼ 5	4 4	5 3	6 2	7 1	8 9	■
	3	8 7	9 6	1 5	2 4	3 3	4 2	5 1	6 9	7 1	
	4	7 ▼ 6	8 5	9 4	1 3	2 2	3 1	4 9	5 8	6 7	■
	5	6 5	7 4	8 ▼ 3	9 2	1 1	2 9	3 8	4 ▼ 7	5 6	
m	6	5 4	6 3	7 2	8 1	9 9	1 8	2 7	3 6	4 5	
MD	7	4 ■ 3	5 2	6 1	7 ■ 9	8■ 8	9 7	1 6	2 5	3■ 4	
AD̲	8	2	1	9	8	■7	■6	■ 5	4	■ 3	
Cln	9	■		■	■				■		

Размещение номеров диагоналей и проверочных символов четности

Результаты подсчета четности отображаются в дополнительно вводимых в матрицу столбце *Ln* и строках *MD*, *AD, Cln*, представляющих значения четности по строкам, главным диагоналям, вспомогательным диагоналям и столбцам матрицы соответственно.

Передаваемая информация разбивается на строки длиной n бит каждая. Из m последовательно следующих строк формируется бинарная матрица размером $(m \times n)$ бит, $m \le n$, в которой выполняются операции подсчета четности по строкам, столбцам и диагоналям. Получается бинарная матрица размером $(m + 3) \times (n + 1)$ бит. После передачи информации в полученной матрице производится проверка четности по всем упомянутым выше направлениям и по результатам проверок формируются списки номеров: ошибочных строк – *SX,* ошибочных столбцов – *SY,* ошибочных главных диагоналей – *SD* и ошибочных вспомогательных диагоналей – *SD*. Предположим, что в матрице (рисунок) после ее передачи по каналу связи появились ошибки (отмечены символом ▼), соответственно, после подсчета четности были выявлены ошибочные координаты (отмечены символом ■) и сформированы списки ошибочных координат: *SX* = 2, 4; *SY* = 1, 3, 4, 8; *SD* = 3, 4, 7, 8; *SD* = 3, 5, 6, 7.

Предлагаемый способ поиска ошибок предусматривает формирование множества строк $S = \{S_1, S_2, S_3, S_4\}$, где S_1 и S_2 – номера ошибочных строк и столбцов из списков *SX* и *SY*, а S_3 и S_4 – номера ошибочных диагоналей из *SD* и *SD*, соответствующие элементам матрицы, адреса которых указаны в S_1 и S_2. Множество S представляет собой множество возможных вариантов размещения ошибок. Формирование S производится на основе двух списков, например *SX* и *SY*, из элементов которых составляются все возможные пары, которые записываются в столбцы S_1 и S_2. Значения остальных столбцов в строках множества S вычисляются с помощью уравнений: $d\,(a,b) = (n - a + b + 1)\,MDn$, $b\,(a,d) = (a + d - n - 1)\,MDn$, $a\,(b,d) = (b + n - d + 1)\,MDn$, $\underline{b} = n - b + 1$, $\underline{d}\,(a,\underline{b}) = (2n - a - b + 2)\,MDn$.

Производится анализ множества S с целью исключения строк, представляющих адреса несуществующих (ложных) ошибок. Принцип выявления ложных ошибок достаточно прост: из S удаляются строки, в которых значение хотя бы одного столбца отсутствует в соответствующем списке (*SX*, *SY*, *SD*, *SD*).

Рассмотрим применение способа на примере представленной выше матрицы, в строках которой имеются ошибки: двойная – (5, 3), (5, 8) и две одиночные – (2, 4) и (4, 1). Процесс формирования множества S и анализа его элементов показан в нижеприведенной таблице. На основании списков *SX* и *SY*, формируется множество S_I, т. е. составляются

пары из элементов этих списков: 2 и 1, 2 и 3, 2 и 4, …, 4 и 8 (выделены курсивом) и записываются в столбцы S_1 и S_2 соответственно. С помощью приведенных выше формул вычисляются номера главных и вспомогательных диагоналей и записываются в столбцы S_3 и S_4. Из S_I удаляются строки, в которых значения столбцов S_3 и S_4 отсутствуют в списках *SD* и *SD* (отмечены --). Остались две строки (отмечены +), которые представляют собой адреса ошибок (2, 4) и (4, 1). Из списков *SX*, *SY*, *SD*, *SD* удаляются элементы, присутствующие в оставшихся строках.

Поскольку в *SX* нет элементов, множество S_{II} составляется на основе списков *SY* и *SD*. Из S_{II} удаляются строки, в которых столбцы S_3 и S_4 содержат номера диагоналей, отсутствующие в списках *SD* и *SD* (отмечены символами --). Оставшиеся две строки представляют собой адреса двойной ошибки (5, 3) и (5, 8). После удаления из списков ошибочных координат номеров, представленных в этих строках, списки *SX*, *SY*, *SD* и *SD* оказались пустыми. Это свидетельство того, что все ошибки обнаружены.

Таблица

Списки ошибочных координат				Множество строк S_I					Множество строк S_{II}				
SX	*SY*	*SD*	*SD*	S_1	S_2	S_3	S_4	Ошибки в строках	S_1	S_2	S_3	S_4	Ошибки в строках
До анализа множества S				*2*	*1*	9	8	--	9	*3*	*4*	8	--
2	1	3	3	*2*	*3*	2	6	--	5	*3*	*8*	3	+
4	3	4	5	*2*	*4*	3	5	+	5	*8*	*4*	7	+
–	4	7	6	*2*	*8*	7	1	--	1	*8*	*8*	2	--
–	8	8	7	*4*	*1*	7	6	+					
После анализа множества S_1				*4*	*3*	9	4	--					
–	3	4	3	*4*	*4*	1	3	--					
–	8	8	7	*4*	*8*	5	8	--					
После анализа множества S_2													
–	–	–	–										
–	–	–	–										

Эффективность способа повышается с увеличением соотношения «число столбцов/число строк» (n/m) бинарной матрицы, представляющей собой содержание передаваемой по каналу связи информации.