СИСТЕМА ТЕХНИЧЕСКОГО ЗРЕНИЯ МОБИЛЬНОГО КОМПЛЕКСА ОБНАРУЖЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Конопелько Я.Д.
Качинский М.В. - доцент кафедры ЭВС, к.т.н.

В последнее время в развитие беспилотных летательных аппаратов произошел значительный прогресс. Подобная техника находит применение в различных условиях и для решения разных задач. В результате чего расширился и спектр противоправных действий, осуществляемых с их применением. В связи с этим появилась необходимость создания систем противодействия беспилотным летательным аппаратам, способных обнаружить, распознать и нейтрализовать их. Возникла потребность в защите определенных объектов и территорий от проникновения беспилотных летательных аппаратов. По этой причине в последнее время большое внимание уделяется противодействию беспилотным системам.

Система технического зрения мобильного комплекса обнаружения беспилотных летательных аппаратов –это система, входящая в состав комплекса обнаружения и борьбы с беспилотными летательными аппаратами. В состав современных комплексов входят радиолокационные станции с разными характеристиками, вероятность обнаружения воздушной цели зависит от эффективной площади рассеивания. В случае с малогабаритными летательными аппаратами ЭПР уменьшается, что значительно увеличивает сложность обнаружения. Применение технического зрения в системах такого класса совместно с радиолокационными системами позволяет увеличить вероятность обнаружения цели.

Основной функцией рассматриваемой в докладе системы является обнаружение беспилотных летательных аппаратов в видимом диапазоне волн на основании данных от оптико-электронного модуля. В основе системы лежит нейронная сеть, при помощи которой происходит обнаружение летательных аппаратов в зоне наблюдения. После обнаружения цель сопровождается и классифицируется.

Использование системы технического зрения в комплексах обнаружения беспилотных летательных аппаратов позволит повысить вероятность обнаружения, точность определения класса и типа летательного аппарата при этом снизив его стоимость.

Список использованных источников:
1. OpenCV [Электронный ресурс]. – Электронные данные - Режим доступа:https://opencv.org
2. Xilinx [Электронный ресурс]. – Электронные данные – Режим доступа:https://www.xilinx.com
3. Zedboard [Электронный ресурс]. – Электронные данные – Режим доступа:http://www.zedboard.org
4. Demuth H., Beale M. Neural Network Toolbox. For Use with MATLAB. The MathWorks Inc. 1992-2000.

IP – ЯДРО АЛГОРИТМА SHA – 1

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Корбут А.А.
Станкевич А.В. – к.т.н., доцент

Необходимость обеспечения конфиденциальности и сохранения целостности данных в рамках систематизации повседневной жизни бесспорна и очевидна. В настоящее время – это одна из самых актуальных задач, решения которой совершенствуются с каждым днем. Secure Hash Algorithm 1 — алгоритм криптографического хеширования, являющийся классическим.

Множество алгоритмов разработаны и разрабатываются по сей день. Алгоритм MD4 послужил прототипом SHA – 1.

Организация SHA – 1 состоит из нескольких этапов[1]:

1. Инициализация переменных. Определение операций и констант.
2. Приведение исходного сообщения к необходимому для обработки виду.
3. Обработка главным циклом.

Инициализация.

Используются пять переменных размера 32 бит.

A = a = 0x67452301
B = b = 0xEFCDAB89
C = c = 0x98BADCFE
D = d = 0x10325476
E = e = 0xC3D2E1F0

Номер итерации t определяет действующую функцию и константу.

Табл. 1 – Функции и константы алгоритма SHA – 1

$Ft\ (m,l,k)\ =\ (m \wedge l) \vee (\overline{m} \wedge k)$	$K_t\ =\ 0x5A827999$	$0 \le t \le 19$
$Ft\ (m,l,k)\ =\ m \oplus l \oplus k$	$K_t\ =\ 0x6ED9EBA1$	$20 \le t \le 39$
$Ft(m,l,k)\ =\ (m \wedge l) \vee (m \wedge k) \vee (l \wedge k)$	$K_t\ =\ 0x8F1BBCDC$	$4 \le t \le 59$
$Ft\ (m,l,k)\ =\ m \oplus l \oplus k$	$K_t\ =\ 0xCA62C1D6$	$60 \le t \le 79$

Подготовка сообщения.

Сообщение делится на блоки. Каждый блок не превышает 448 бит, кратен 512. К каждому блоку добавляется 1 и множество нулей для дополнения длины до 448 бит. Добавление осуществляется всегда, даже если сообщение уже имеет нужную длину. В последние 64 бита записывается длина сообщения в битах.

Главный цикл.

Основой алгоритма является модуль, состоящий из 80 циклических обработок, обозначенный как HSHA. Все 80 циклических обработок имеют одинаковую структуру.

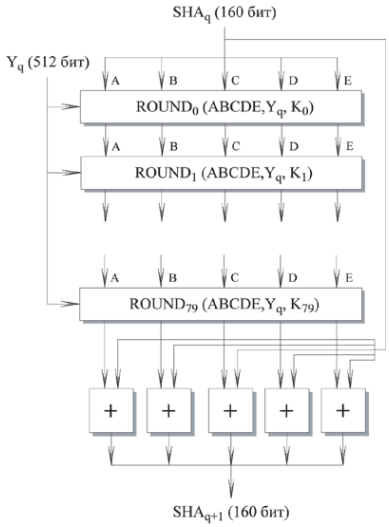

Рис.1 – Структура алгоритма

Состоит из 80 итераций от 0 до 79.

Логику одной итерации цикла можно представить в виде[1]:
A, B, C, D, E (CLS5 (A) + ft (B, C, D) + E + Wt + Kt), A, CLS30 (B), C, D,

где A, B, C, D, E - пять слов из буфера;
t - номер цикла, 0 t79;
ft - элементарная логическая функция;
CLSs - циклический левый сдвиг 32-битного аргумента на s битов;
Wt - 32-битное слово, полученное из текущего входного 512-битного блока;
Kt - дополнительная константа;
+ - сложение по модулю 2^{32}.

32-битные слова Wt получаются из очередного 512-битного блока сообщения следующим образом:

Рис.2 – Формирование слова

Первые 16 значений Wt берутся непосредственно из 16 слов текущего блока. Оставшиеся значения определяются следующим образом:

$$W_t\ =\ W_{t-16} \oplus W_{t-14} \oplus W_{t-8} \oplus W_{t-3}$$

В первых шестнадцати циклах вход состоит из 32 – битного слова данного блока. Для оставшихся 64 циклов вход состоит из сложения по модулю 2 нескольких слов.

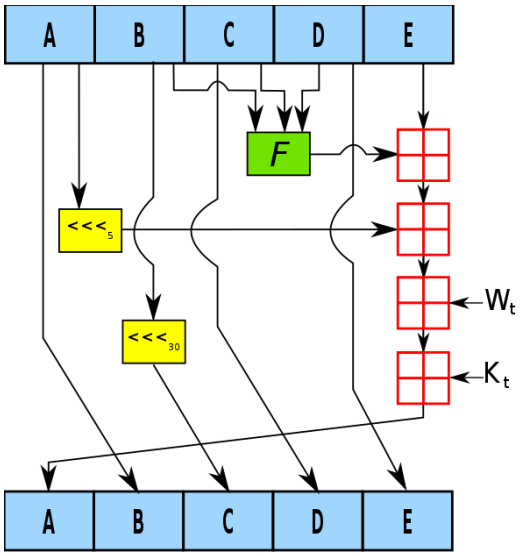

Рис. 3– Одна итерация цикла.

Длина дайджеста	160 бит
Размер блока обработки	512 бит
Число итераций	80
Число элементарных функций	3
Число дополнительных констант	4

Алгоритм прост в описании и реализации, однако достаточно устойчив к атакам грубой силы.

Список использованных источников:
1. D. Eastlake, P. Jones, RFC 3174 US Secure Hash Algorithm 1 (SHA1)// Cisco Systems – 2001.
2. Ярчук С. М. Конспект лекций по информационной безопасности/ С. Ярчук – Уральский Федеральный университет им. Б.Н. Ельцина «УПИ», 2011. - 75 с.

ОЦЕНКА РЕЧЕВОЙ МАСКИ ДЛЯ ИДЕНТИФИКАЦИИ ДИКТОРА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кручок Д.Н.

Петровский А.А. – д.т.н., профессор

В данной работе рассмотрены методы оценивания маски для речевого сигнала. Речевая маска позволяет использовать реконструированный сигнал для извлечения характеристического вектора и дальнейшей идентификации диктора в условиях акустических шумов.

Речевой сигнал, даже если он зашумлен, обладает значительной степенью избыточности, и информация о речевых характеристиках присутствует и в случае сильного зашумления. Методы, которые используют это наблюдение (англ. missingdataapproaches) используют речевые маски для маркировки сигнала для каждой точки время-частота по наличию речи или шума в ней [1]. В дальнейшем, маску используют для реконструирования сигнала, получения из него характеристического вектора для идентификации диктора. В случае, когда шум известен заранее, маску можно построить по критерию отношения сигнал-шум (англ. signaltonoise, SNR) для каждого временно-частотного компонента. Если такую маску использовать для идентификации, то распознавание диктора будет иметь высокую шумоустойчивость даже в присутствии сильных шумов и искажений [2]. На практике, отсутствие априорного знания о шуме толкает на осуществление оценки речевой маски.

Подходы оценивания речевой маски делятся на [1]:

1) Методы, основанные на оценке SNR;
2) Методы, основанные на слуховом восприятии;
3) Методы, основанные на классификации параметров оценивания.

При оценке SNR решение надежности того или иного временно-частотного компонента принимается