генерировать новые правила по новым поступающим данным в целях обнаружения большего количества актуальных векторов атак.

Литература

1. Anderson, James P., "Computer Security Threat Monitoring and Surveillance" Washing, PA, James P. Anderson Co., 1980.

2. Википедия. Система обнаружения вторжений [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Система_обнаружения_вторжений (дата обращения: 06.05.2019).

3. Википедия. Snort [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Snort (дата обращения: 06.04.2019).

4. OWASP Top 10 - 2017. The Ten Most Critical Web Application Security Risks [Электронный ресурс]. Режим доступа: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf (дата обращения: 06.04.2019).

5. OWASP Top 10 - 2013. The Ten Most Critical Web Application Security Risks [Электронный ресурс]. Режим доступа: https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf (дата обращения: 07.04.2019).

6. OWASP Топ-10 2017: обзор изменений [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/blog/company/a1qa/343176.php (дата обращения: 06.04.2019).

7. Hussein Alnabulsi, Md Rafiqul Islam, Quazi Mamun. Detecting SQL injection attacks using SNORT IDS. URL: https://www.researchgate.net/publication/278677876_Detecting_SQL_injection_attacks_using_SNORT_IDS (дата обращения: 06.04.2019).

8. HTTP DATASET CSIC 2010 [Электронный ресурс]. Режим доступа: http://www.isi.csic.es/dataset/ (дата обращения: 12.05.2019).

9. GitHub. SecLists, the security tester's companion [Электронный ресурс]. Режим доступа: https://github.com/danielmiessler/SecLists (дата обращения: 12.05.2019).

Д.А. Зенцов

РАЗРАБОТКА АЛГОРИТМА ПРОВЕРКИ ПОДЛИННОСТИ ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЕЙ ПУТЕМ ОБНАРУЖЕНИЯ В НИХ ПРЕДНАМЕРЕННЫХ ИЗМЕНЕНИЙ

(Самарский университет)

Сходство между соседними кадрами используется видеокодерами путем прогнозирования конкретного кадра в зависимости от его соседей и кодирования ошибок прогнозирования. Закодированное видео состоит из последовательности I-кадров (начало видеопоследовательности, содержит изображение

целиком), P-кадров (содержат макроблоки со ссылками на предыдущий кадр), B-кадров (могут содержать макроблоки со ссылками как на предыдущие, так и на последующие кадры).

Каждая подпоследовательность кадров может рассматриваться как локальное временное окно. I-кадр – базовый, P- и B- кадры – разностные сдвиги соответствующего базового кадра. Однако разнообразная структура подпоследовательностей кадров в современных видеопотоках делает исследование видео, основанное на анализе подпоследовательностей кадров, невозможным. В качестве альтернативы предлагается алгоритм, использующий разностные сдвиги кадров.

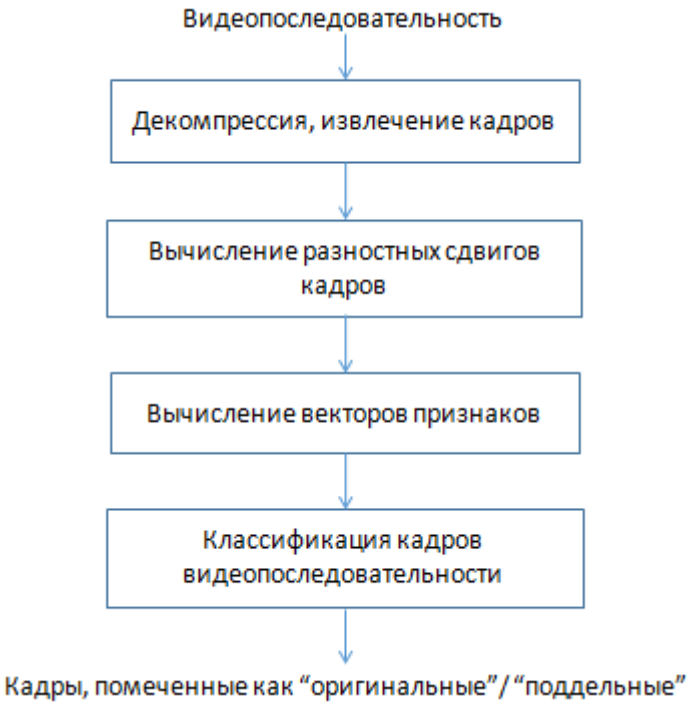

Рисунок 1 - Алгоритм обнаружения удаленных объектов на видеопоследовательности

Обозначим последовательность распакованных видеокадров длины N как:

$$V \triangleq \{F^{(1)}, F^{(2)}, \dots, F^{(N)}\}, N \in Z, \quad (1)$$

где $F^{(k)} = (F_{i,j}^{(k)}) \in \{0, \dots, 255\}^{n_1 \times n_2}, N \in Z$ представляет k-й декомпрессированный кадр, являющийся 8-битным полутоновым изображением 8×8. Оператор согласования внутри временного окна с центром в $F^{(k)}$ и размерностью $L = 2 \times L_h + 1$ (L_h - число соседей левее/правее опорного кадра, входящих в окно):

$$C^{(k)} = \left(C_{i,j}^{(k)}\right) = \mathfrak{C}[(F_{i,j}^{(k-L_h)}), \dots, (F_{i,j}^{(k)}), \dots, (F_{i,j}^{(k+L_h)})] \quad (2)$$

где $C^{(k)}$ – результат согласования $F^{(k)}$ и $\mathfrak{C}$. Оператор согласования $\mathfrak{C}$ – агрегирующая функция, которая группирует пиксели каждого кадра с соответствующими координатами во временное окно для получения $C_{i,j}^{(k)}$. Разностный сдвиг кадра $F^{(k)}$представляется в виде

$$R^{(k)} = \left|F^{(k)} - C^{(k)}\right| = (R_{i,j}^{(k)}) = \left|F_{i,j}^{(k)} - C_{i,j}^{(k)}\right|, \quad (3)$$

В работе были использованы два оператора согласования:

$$\mathfrak{C}_{MIN} \triangleq \min_{l \in [-L_h, L_h]}\{F_{i,j}^{(k+l)}\}, \quad (4a)$$

$$\mathfrak{C}_{MEDIAN} \triangleq \tilde{F}_{i,j}^{((L+1)/2)}, \quad (4b)$$

где $\left\{\tilde{F}_{i,j}^{(l)}\right\}$ - отсортированная последовательность $F_{i,j}^{(k+l)}$.

Результирующая матрица $R^{(k)}$ – 8-битное полутоновое изображение. Ускорение движения в сцене приводит к увеличению разницы между $F^{(k)}$ и $C^{(k)}$, что, в свою очередь, приводит к росту элементов матрицы $R^{(k)}$. Поэтому $C^{(k)}$ описывает перемещение объекта внутри временного окна согласования, а $R^{(k)}$ отражает меру движения в окне. $R^{(k)}$ не основывается на гибкой структуре последовательности разных видов кадров и поэтому подходит для предлагаемого метода.

Используя разностные сдвиги в качестве посредников, мы можем заимствовать некоторые мощные статистические функции из стегоанализа изображений для моделирования изменения свойств фрагментов видео, представляющего собой объектно-ориентированную подделку.

В работе исследовалось использование трех векторов признаков кадра *w:*

- $\bar{X}_1(w) = (x_0, \dots, x_{547})^T$, рассчитываемый по алгоритму CC-PEV (Cartesian-calibrated Pevny feature) при помощи Global histogram, Local histograms, Dual histograms, Variation, Blockiness features, Cooccurrence, Markov features.
- $\bar{X}_2(w) = (x_0, \dots, x_{686})^T$, рассчитываемый по алгоритму SPAM (Subtractive Pixel Adjacency Model feature) при помощи моделирования вероятности переходов между соседними элементами разностных сдвигов по восьми направлениям с помощью цепей Маркова второго порядка
- $\bar{X}_3(w) = (x_0, \dots, x_{486})^T$, рассчитываемый по алгоритму MP-486 (Markov Process feature) при помощи марковского процесса, использующего как внутриблочные, так и межблочные корреляции между коэффициентами JPEG.

Классификация кадров видеопоследовательности осуществлялась при помощи следующих классификаторов:

- Ансамбля из 500 линейных классификаторов (при обучении используется линейный дискриминант Фишера).
- Квадратичный SVM
- Дерево принятия решений

Исследование проводилось на двух датасетах:

- REWIND (20 видеопоследовательностей: 10 оригинальных и соответствующие им 10 поддельных; разрешение всех видео – 320 × 240, кадровая частота – 30 кадров в секунду).

Рисунок 1 – Пример оригинального кадра, на котором присутствует человек

Рисунок 2 – Пример оригинального кадра, на котором человек отсутствует

- GRIP (30 видеопоследовательностей: 15 оригинальных и соответствующие им 15 поддельных; разрешение у видео различается, кадровая частота – 30 кадров в секунду).

В работе изучалось применение различных параметров алгоритма ($L_h = \overline{3,5}$, $\mathfrak{C}_{MIN}$ и $\mathfrak{C}_{MEDIAN}$, шаг, с которым кадры в видеопоследовательности подвергались анализу).

Наилучшие результаты были получены при использовании ансамбля классификаторов и вектора признаков CC-PEV ($L_h = 4$, $\mathfrak{C}_{MEDIAN}$, шаг анализа кадров – 8).

Таблица 1- Результаты исследования

Accuracy	Precision	Recall	F-score
0.74	0.62	0.90	0.73

Литература

1. Chen S. Automatic detection of object-based forgery in advanced video/ S. Chen, S. Tan, B. Li// IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, Issue: 11, pp. 2138–2151, 2016.

2. Pevny T. Steganalysis by subtractive pixel adjacency matrix/ T. Pevny, P. Bas, J. Fridrich// IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 215–224, 2010.

3. Kodovsky J. Ensemble classifiers for steganalysis of digital media/ J. Kodovsky, J. Fridrich// IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 432–444, 2012.

4. Pevny T. Merging Markov and DCT features for multiclass JPEG steganalysis/ T. Pevny, J. Fridrich// in Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, pp. 301– 304, 2007.

5. Bestagini P. Local tampering detection in video sequences/ P. Bestagini, S. Milani, M. Tagliasacchi, S. Tubaro// IEEE 15th International Workshop on Multimedia Signal Processing (MMSP), Pula, Italy, 2013

6. Qadir G. Surrey University Library for Forensic Analysis (SULFA) of video content/ G. Qadir, S. Yahahya, A.T.S. Ho// IET Conference on Image Processing (IPR 2012), July 2012.

7. REWIND Forged Videos Data Set [Электронный ресурс]. – URL: https://sites.google.com/site/rewindpolimi/downloads/datasets/video-copy-move-forgeries-dataset (дата обращения: 14.05.2019).

8. GRIP Forged Videos Data Set [Электронный ресурс]. – URL: http://www.grip.unina.it/download/prog/ForgedVideosDataset/Copymove (дата обращения: 14.05.2019).

Ю.М. Злобин, В.П. Пряхин

ОЦЕНКА ЭФФЕКТИВНОСТИ МАСКИРОВАНИЯ ФУНКЦИОНАЛЬНО-ЛОГИЧЕСКОЙ СТРУКТУРЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ

(Самарский университет)

Провести оценку эффективности функционирования ранее разработанного средства масштабирования («маскирования») распределенной информационной системы (ИС) представляется возможным путем сравнения вероятностно-временных характеристик (ВВХ) полученной функционально-логической структуры с исходными характеристиками ИС [1]. Очевидно, что исходная ИС обладает рядом параметров, которые подвергнутся изменениям во время работы средства «маскирования» и, более того, появятся новые параметры, коренным образом влияющие на ВВХ ИС. С точки зрения дезинформации злоумышленника важно, чтобы разница между исходной и масштабируемой ИС была минимальна, то есть она должна стремиться к 0. Оценка этой разницы позволит говорить об эффективности «маскирования» ИС.

Предполагается, что сравнение ВВХ ИС возможно с помощью расстояния Кульбака-Лейблера. Для оценки информационного выигрыша (демонстрации его минимума) на $t \to \infty$ необходимо оперировать абсолютно непрерывными распределениями P и Q и иметь в распоряжении плотности этих распределений p(x) и q(x) соответственно. На данном этапе исследования получение плотности распределения случайных величин для маскированной структуры q(x) остается актуальной задачей. Другой вариант оценки расстояния Кульбака-Лейблера – аппроксимация для дискретных значений случайных величин.

Дискретные значения случайных величин для построения распределений P и Q могут быть получены путем синтеза марковских моделей функционирования ИС и их последующим решением.