Detecção de Roubo de Computadores em Laboratório Usando Visão Computacional

Itamar Junior de Azevedo
Universidade Positivo
itamar.jda@gmail.com

Gabriel Andrade Cordeiro
Universidade Positivo
gabriel.cordeiro@aluno.positivo.edu.br

Giovani Grockotzki
Universidade Positivo
giovani.grockotzki@aluno.positivo.edu.br

Matheus Henrique da Silva Santos
Universidade Positivo
matheus.santos@aluno.positivo.edu.br

João Mantovani
Universidade Positivo
joaovbmantovani@gmail.com

Ricardo Vinicius Poncio
Universidade Positivo
ricardo.poncio@aluno.positivo.edu.br

Caroline Mazetto Mendes
Universidade Positivo
caroline.mendes@up.edu.br

ABSTRACT

Computer theft in computer labs causes academic damage to courses that require this resource and ends up directly harming students. In this context, this paper describes a methodology applied to detect computer removal through video analysis in real-time. For each frame, image processing and computer vision techniques were used, subtracting background information, binarization, segmentation of the region of interest and definition of contours. The case study was developed at a Brazilian university. For theft detection, it was considered a black computer tower case carried by people leaving the laboratory. Monitoring is carried out by a camera positioned in front of the lab exit door. The software developed alerts a suspicious activity that may indicate a possible computer theft.

KEYWORDS

Detecção de Roubo, Laboratório de Computação, Visão Computacional, Processamento de Imagens

1 INTRODUÇÃO

Um problema recorrente em laboratórios de computação é o roubo de equipamentos, tais como monitores, computadores e acessórios. Essa prática causa prejuízos financeiros às instituições de ensino, além de dificultar as atividades acadêmicas. As universidades, sejam públicas ou privadas, são as mais vulneráveis devido ao tamanho dos campus e a grande circulação de pessoas.

Os métodos tradicionais de vigilância visual em geral não são suficientes para inibir os furtos de equipamentos. O monitoramento visual realizado por humanos, de diversos ambientes ao mesmo tempo, pode ser impraticável ou ineficiente [1]. Nesse contexto, o monitoramento automático por meio da análise de vídeos pode ser uma ferramenta útil para diminuir a incidência de roubos.

Considerando o ambiente tecnológico em que os departamentos de computação estão inseridos, torna-se possível incorporar câmeras e implementar sistemas de monitoramento automático. Contudo, fatores como iluminação, posicionamento da câmera, e posição dos objetos, por exemplo, precisam ser considerados. Tais fatores podem dificultar o processo de análise das imagens nos sistema baseados em visão computacional.

Abordagens baseadas em visão computacional têm sido propostos para esse fim. Miguel e Martínez [2] apresentaram uma abordagem para detecção automática de objetos roubados. Primeiro, regiões em primeiro plano são detectadas e rastreadas. Essas regiões são então classificadas em humanos, objetos estáticos e dinâmicos. Assim, objetos não humanos são analisados por detectores específicos a fim de determinar ação de roubo.

Patil e Talele [3] desenvolveram um sistema para detecção de comportamentos suspeitos em ambientes internos. Atividades suspeitas como abandono e roubo de objetos são detectados. A detecção é realizada usando subtração de fundo e rastreamento de objetos com técnica blob. A abordagem proposta garantiu desempenho em tempo real, eliminando o uso de métodos baseados em aprendizado de máquina.

Rahangdale e Kokate [1] propuseram um sistema para a detecção de eventos suspeitos em imagens de sistemas de segurança. O objeto roubado foi definido como uma bagagem recolhida por uma pessoa que não é a proprietária do objeto. Para realizar a detecção, objetos de interesse são obtidos por meio da subtração de fundo e são rastreados usando a técnica blob.

Nesse contexto, este trabalho apresenta uma metodologia para detecção de roubos de computadores em laboratório usando visão computacional. O estudo foi realizado em uma instituição de ensino superior, localizada no Brasil. Uma câmera foi posicionada em frente à porta de saída do laboratório. Devido às características dos computadores da instituição, foram considerados gabinetes da cor preta carregados por pessoas. Assim, um *software* que está em fase de desenvolvimento analisa as imagens capturadas, emitindo alertas para as situações suspeitas.

2 SOLUÇÃO PROPOSTA

O *software* em desenvolvimento tem como objetivo realizar a detecção de eventos que possam configurar um possível roubo. O algoritmo de detecção é composto pelas seguintes etapas: subtração de fundo; binarização, segmentação da região de interesse e definição de contornos.

Para realizar a subtração de fundo foi utilizado um método de subtração baseado no algoritmo de classificação supervisionada

KNN (K Nearest Neighbors) [4]. O processo resulta em uma imagem binária contendo objetos em primeiro plano. Para remover pequenos componentes, são aplicadas as operações morfológicas erosão e dilatação. Um limiar mínimo de pixels de primeiro plano foi definido empiricamente (600 pixels), a fim de selecionar as imagens para detecção.

Considerando a cor dos gabinetes dos computadores, as imagens selecionadas são binarizadas. Essa etapa realiza o descarte dos pixels que possuem cor mais clara que a cor do gabinete. Assim, são mantidos apenas os objetos que na imagem original possuem valor de pixel inferior a um limiar RGB (50,50,50), também definido empiricamente. Depois, é realizada uma inversão das cores para auxiliar a próxima etapa.

A etapa de segmentação da região de interesse tem como objetivo segmentar objetos que possuam características similares a um gabinete de computador. Para isso, os contornos são simplificados usando o algoritmo de aproximação poligonal de Douglas-Peucker [5]. Por fim, o algoritmo de Sklansky [6] é aplicado a fim de obter contornos convexos.

Além do formato retangular, para ser considerado um gabinete a região de interesse segmentada deve possuir entre 5000 e 25000 pixels de área, limiares estes definidos empiricamente. Por fim, é calculado o histograma da região de interesse. Caso mais de 30% dos pixels da região possuam valores menores que 20, a região é considerada um computador. Com isso aumenta-se a acurácia do *software* e reduz o falso positivo.

O *software* foi desenvolvido usando a Linguagem Python e a biblioteca OpenCV. A câmera foi posicionada frente à porta, no lado de fora do laboratório. Assim, as imagens mostram a entrada e saída de pessoas do ambiente.

Para realização dos testes iniciais, usou-se um computador com a seguinte configuração: Positivo Unique S1990 com Intel Celeron 1007U 1.50GHz, 2GB de Memória RAM e SSD de 120GB. Para a obtenção das imagens foi utilizada a câmera do *smartphone* da Xiaomi, o Redmi Note 7, com resolução para vídeo 1080p e *frame rate* de 30 a 120fps.

3 CONSIDERAÇÕES FINAIS

Para realização dos testes iniciais, foi gravado um vídeo com a simulação de possíveis eventos. Foram simulados ao todo 10 eventos, sendo 5 suspeitos e 5 não suspeitos. A porta do laboratório permaneceu fechada por padrão, sendo aberta apenas para a saída de pessoas. Nos eventos suspeitos, uma pessoa saiu do laboratório carregando um computador junto ao corpo. As pessoas usaram roupas de diferentes cores, incluindo roupas pretas e escuras.

A Fig. 1 mostra um dos eventos para o qual o algoritmo detectou uma atividade suspeita. Todos os eventos suspeitos foram detectados, não tendo ocorrido falso positivo. O algoritmo detectou o gabinete mesmo em um dos eventos no qual a pessoa carregando o computador estava com roupa preta, similar a cor do gabinete. Atualmente, a detecção de roubo de computador ocorre a cada *frame* assim que um evento de saída é iniciado. Para melhorar o desempenho do algoritmo, será adicionada uma etapa de rastreamento do objeto detectado. Também, serão simulados diferentes eventos realizados por pessoas para a avaliação da solução proposta, incluindo eventos de entrada no laboratório.

Figura 1: Pessoa saindo do laboratório carregando um gabinete na cor preta. O computador detectado está destacado em verde.

Os resultados iniciais mostraram que é possível realizar a detecção de roubo de computadores de um laboratório usando técnicas de processamento de imagens e visão computacional. Técnicas de aprendizado de máquina também podem ser usadas para auxiliar o reconhecimento de objetos similares a um gabinete de computador. Contudo, destaca-se que o foco do projeto é desenvolver uma solução eficiente para detecção em tempo real. Assim, espera-se a solução final possa minimizar a prática de roubos de computadores em laboratórios.

REFERÊNCIAS

[1] Komal Rahangdale and Mahadev Kokate. Event detection using background subtraction for surveillance systems. *International Research Journal of Engineering and Technology*, 3(01):1300–1304, 2016.

[2] Juan Carlos San Miguel and José M Martínez. Robust unattended and stolen object detection by fusing simple algorithms. In *2008 IEEE Fifth International Conference on Advanced Video and Signal Based Surveillance*, pages 18–25. IEEE, 2008.

[3] Sandesh Patil and Kiran Talele. Suspicious movement detection and tracking based on color histogram. In *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*, pages 1–6. IEEE, 2015.

[4] Zoran Zivkovic and Ferdinand Van Der Heijden. Efficient adaptive density estimation per image pixel for the task of background subtraction. *Pattern recognition letters*, 27(7):773–780, 2006.

[5] David H Douglas and Thomas K Peucker. Algorithms for the reduction of the number of points required to represent a digitized line or its caricature. *Cartographica: the international journal for geographic information and geovisualization*, 10(2):112–122, 1973.

[6] Jack Sklansky. Finding the convex hull of a simple polygon. *Pattern Recognition Letters*, 1(2):79–83, 1982.