

Visión Computacional aplicado en la Seguridad y Comunicaciones

Medina, Jahir., Pastor, Christian., Salinas, Jhosep y Sifuentes, Víctor.
{jahirmedina, cmpastors, jhsalinas, vsifuentes}@unitru.edu.pe
Universidad Nacional de Trujillo

Resumen—La visión computacional como técnica de detección o análisis de patrones, en la actualidad, es una norma. Desde la vigilancia mediante cámaras de circuito cerrado hasta la eliminación de ruidos en señales de audio.

La visión computacional ha avanzando hasta un punto donde es capaz de analizar contextos, pudiendo identificar si se comete un delito o si existe una persona con actitud sospechosa.

Es por esto que en el presente artículo, se hará un recuento de las aplicaciones modernas de la visión computacional. Mas concretamente su aplicación en el capo de la seguridad, vigilancia y telecomunicaciones.

Índice de Términos—Visión Computacional, Seguridad, Seguridad Informática, Vigilancia, Telecomunicaciones, Procesamiento de Señales, DeepFake.

I. INTRODUCCIÓN

Escribir Luego

II. LA VIGILANCIA AUTOMATIZADA

A. Década de los 90's

Desde que se empezó a usar de forma comercial tecnologías de procesamiento de imágenes para detectar movimiento en grabaciones tomadas por Cámaras de Circuito Cerrado (CCTV, por sus siglas en ingles) en los años 80's, se veía el potencial pero también su mal rendimiento, especialmente por la alta tasa de falsos negativos en la detección de intrusos (Sage and Young, 1998).

Sin embargo, una solución que se considero y trabajo por mucho tiempo fue la de recopilar mas información para así poder garantizar la disminución de falsos negativos (Esto Basado en una cuestión estadística, mas información, mejor predicción).

Sin embargo, arrojar hardware a un problema de software es una solución, que a la larga aumenta los costos de cualquier sistema. Ante esta problemática, se comenzó a plantear modelos estocásticos para no solo detectar variaciones en la escena filmada, sino para intentar también, trazar una ruta y aproximar este comportamiento a uno próximo de un humano (Sage and Young, 1998).

Gracias a las mejoras en las técnicas de análisis y la mejor calidad en vídeo, en los últimos años de los 90's, se empezaron a plantear sistemas de detección en escenarios dinámicos, siendo un caso particular, las carreteras (Manendez et al., 1999). La motivación, tal como menciona el paper *Vigilancia de Autopistas mediante visión computacional stereo* (Manendez et al., 1999, Abstract) se origina por el aumento

de la demanda de automatización, la ubicuidad de cámaras y la mayor necesidad de automatización y abaratamiento de costos.

En todo este escenario de crecimiento tecnológico, no solo de hardware, sino también de software y sus respectivos algoritmos, es que comienza a surgir la idea de extender estas aplicaciones a campos mas delicados: Detección de crímenes y Verificación Biométrica.

B. Década de los 2000's

III. EL AUGE DE LAS REDES NEURONALES

A. Las Redes Neuronales, excelentes Clasificadores

B. Las Redes Convencionales, excelentes Extractores de Características

IV. FIRMA BIOMETRICA Y PROCESAMIENTO AVANZADO DE SEÑALES

A. DeepFake y mas formas de suplantación de identidad

Con el avance de la capacidad de hardware, se volvió mas fácil implementar arquitecturas extremas. Estas arquitecturas capaces de procesar *batches* de mas 10gb empezaron a ser prometedoras en el ambito de la creacion de informacion artificial, analisis de patrones mas complejos y deteccion de caracterizticas jamas pensadas.

B. Espionaje de Vanguardia

V. CONCLUSIONES

VI. APÉNDICE

REFERENCIAS

- Manendez, J., Salgado, L., Rendon, E., and Garcia, N. (1999). Motorway surveillance through stereo computer vision. In *Proceedings IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology (Cat. No.99CH36303)*. IEEE.
- Sage, K. and Young, S. (1998). Computer vision for security applications. In *Proceedings IEEE 32nd Annual 1998 International Carnahan Conference on Security Technology (Cat. No.98CH36209)*. IEEE.