جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة ديالى / كلية العلوم
قسم علوم الحاسوب

حماية الخصوصية للوجه استناداً على طرق التشفير العميق والخفيف الوزن في مقاطع فيديو المراقبة

رسالة

مقدمة الى قسم علوم الحاسوب / كلية العلوم/ جامعة ديالى / وهي جزء من متطلبات نيل درجة الماجستير في علوم الحاسوب

من قبل

مها مطر عطيوس

بإشراف

ا. د. طه محمد حسن

١٤٤٥ هـ العراق - ديالى ٢٠٢٣ م

Chapter One
General Introduction

Chapter one
General Introduction

1.1 Introduction

Privacy face protection employs advanced object detectors and lightweight encryption to safeguard identities in surveillance videos. With expanding surveillance systems, personal privacy concerns are critical. This innovative solution identifies and anonymizes faces through advanced object detection algorithms. Lightweight encryption secures sensitive data during anonymization, preventing unauthorized access and breaches. Striking a balance between public safety and individual privacy, this approach is a promising step towards responsible and ethical surveillance practices.

Privacy face protection in surveillance videos using multiple object detectors faces numerous challenges. Accuracy issues, such as false positives or missed detections, can compromise data integrity and undermine the system effectiveness . The computational burden of running multiple detectors may hamper real-time performance, hindering quick and efficient video analysis. Additionally, variations in face appearances present challenges, as different lighting conditions, facial expressions, and angles can decrease the accuracy of face detection and anonymization.

1.2 Related Work

- Shifa, et al 2023[5]: To reduce the number of lives lost and the amount of money wasted in smart cities due to traffic accidents, automated detecting systems are being installed in surveillance cameras. Despite the obvious advantages of monitoring technologies, protecting individuals' privacy is still essential. s. Therefore, EU-GDPR, or the General Data Protection Regulation of the European Union. Has been implemented to protect the confidentiality of personal information. To comply with EU-GDPR, gathering and storing the minimum amount of necessary information.is best in a surveillance system that values individual liberty,.
- Varghese ,et al in 2021[6]:

This paper introduces a method called PriSE (Surveillance with little invasion of privacy as an edge service) to protect privacy while conducting surveillance. It utilizes a combination of scanners for objects in the foreground, a video encryption system which operates on local cameras and remote cloud/fog processing. The objective is privacy detection-related attributes such as windows, personalities, and offenders. To ensure anonymity throughout the process, the Reversible Chaotic Masking (ReCAM) approach is employed. Additionally, resource utilization is optimized using a reduced foreground-object detector that eliminates frames without foreground objects. A reliable system has been created to detect objects near windows, ensuring privacy by preventing people from looking inside, An MTCNN, or multi-task cascaded convolutional neural network, is employed To identify individuals without disclosing their identities.

- AL-Rubaie and Chang.in 2020[7]: Surveillance with the protection of personal data at the network's periphery (PriSE). is proposed by the authors after reviewing of several approaches based on deep learning (DL), image processing, and image scrambling techniques ,the authors propose this method . In the PriSE, a simple foreground object detector is followed by an efficient and lightweight

Reversible Chaotic Masking (ReCAM) technique used by the edge cameras. The scrambling system ensures complete confidentiality from beginning to end, making it impenetrable to any form of eavesdropping. The streamlined motion detector reduces resource usage (Time, energy, and space for processing and storing space) by skipping over frames without motion. To prevent eavesdropping through windows, the scrambling technique is used in tandem with face detection and emotion recognition using a multi-task convolutional neural network a robust window-detector hosted on a fog/cloud server Numerous experiments and an in-depth study of the results demonstrate that PriSE can effectively edge cameras that can identify foreground objects and jumble images, as well as window and facial objects that may be detected and denatured on a cloud server. Thereby guaranteeing the confidentiality and anonymity of communications from the beginning to the end. It is carried out Immediately before to the images are sent to the numerous displays.

- CAVALLRO,et al 2020[8]: We offer a new approach to protecting minor privacy by processing videos at the networks edge in real time (MiPRE). Identifying children and taking necessary precautions to protect their privacy has been perfected to the point that it is now practical and accurate. To improve MiPRE's accuracy, we adapt and reuse cutting-edge deep learning models. Face detection and extraction from input frames are performed through a pipeline. The minors' faces are then disguised using a simple algorithm. Classification is performed using over 20,000 publicly available labelled sample points.
- Gubbi, et al 2020[9]: Multi-Level Video Security (MuLViS) is a surveillance system proposed in this research that uses multiple layers of encryption to keep private footage secure. To begin, a Smart Surveillance Security Ontology (SSSO) is included into the MuLViS to automatically choose a degree of privacy suitable for the running device based on its hardware requirements and

network speed. Overall, the system allows for reasonably quick indexing and retrieval of surveillance footage ,and device-specific security. Second, many layers of encryption safeguard the videos' contents throughout capture, streaming, and storage. Statistical examination of experimental video data, including the Encryption Space Ratio (ESR), and eye inspection, have confirmed the accuracy of the security level allocations. The solution is GDPR-compliant, thus it may be used to safeguard surveillance footage while still protecting people's right to privacy in the face of legitimate data access. INDEX TERMS General Data Protection Regulation; ontology; partial encryption; privacy .

1.4 Problem Statement

We are in a time of globalization filled with a time of changes media and changes that I have come to need more protection than I can provide to users.is there any type of protection which is video protection.

1.5 Research Objectives

The aims of the proposed privacy face protection model utilizing Lightweight CNN classification and Modified GIFT block lightweight cryptography algorithm (Face Protect Model-LCNN-MGIFT) are addressed as following points :

Create an accurate binary gender classifier, "Lightweight CNN," through fine-tuning and the EfficientNet-B7 Deep Transfer Learning Algorithm. This approach will effectively differentiate between male and female individuals, even within complex multi-object settings.

2.The "Modified GIFT (MFIGT)" lightweight cryptography algorithm ,Was proposed incorporating 128-bit secret key generation and dynamic round constants. Both methods utilize the 3D-Chua attractor chaotic map. MFIGT aims to enhance security and resilience against unauthorized access by strengthening the algorithm's confusion and diffusion elements.

1.6 Outline of the Thesis

Chapter Two (Theoretical Background)

This chapter provides a background and overview of, surveillance Video (VS), theoretical background and techniques used in this thesis.

Chapter Three (Proposed System Design)

The chapter comprehensively illustrates the dataset, algorithms, techniques, and flowcharts used to explain the design and implementation of this proposed model.

Chapter Four (Experimental Test Results)

This chapter presents the experimental tests and outcomes of the privacy-focused facial protection model, coined as (Face Protect Model-LCNN-MGIFT), which capitalizes on Lightweight CNN classification and Modified GIFT block lightweight cryptography algorithms

Chapter Five (Conclusions and Suggestions for Future Work)

This chapter presents the conclusions of this work. Furthermore, it provides suggestions for future work.

الخلاصـــة

نظـرًا للاسـتخدام الواسـع النطـاق لكـاميرات المراقبـة، تعـد حمايـة الخصوصـية فـي لقطات المراقبة أمرًا بالغ الأهمية. أحد أهم التحديات الاجتماعية والسياسية التي يمكن مواجهتها هو حمايـة خصوصـية الفـرد، والتـي يـتم تحديـدها مـن خـلال مجموعـة متزايـدة مـن التكنولوجيـا والخـدمات التمكينيـة والـدعم. تزايـدت المخـاوف المتعلقـة بالحفـاظ علـى خصوصـية الأشـخاص بشكل ملحوظ نتيجة للتطورات الأخيرة في مراقبـة الفيديو. تركـز الأسـاليب المقدمـة حاليًـا بشـكل قوي على تحديد موقع المنطقة الحساسة والحفاظ علـى سلوك الهدف. تعد عمليـة تطـوير نمـوذج التصنيف العميق للجنس (Deep-GCM) وعمليـة اكتشـاف وتشـفير منـاطق الوجـه (DE-FR) مرحلتين رئيسيتين في هيكل نموذج حماية الوجه المقترح-LCNN-MGIFT. بلغت الدقة التـي حصـل عليهـا النظـام المقتـرح ٩٧% لطريقـة LCNN، و٩٦% لنمـوذج الـتعلم العميـق، و٩٦% لخوارزمية CNN-fine Tuning-EfficientNet-B7 خفيفة الوزن واظهرت التجارب علـى مجموعه البيانات فعالية النموذج المقترح من حيث الدقة الامنية وكفـاءة البحـث مقارنـه بالاعمـال حيث حقق PSNR-8.17899 و MSE-10004.37 dB بين الصورة الاصلية والمشفرة.