MAKERERE UNIVERSITY

SCHOOL OF COMPUTING AND INFORMATICS TECHNOLOGY

GROUP 210 EVE

April 20, 2017

RESEARCH METHODOLOGY
CONCEPT PAPER

ON

COMPUTER VISION FOR PHYSICAL SECURITY

GROUP MEMBERS

NAME	REGISTRATION NUMBER	STUDENT NUMBER
MUHWEZI JERALD	14/U/25199	214024819
NDAGANO ROBERT	13/U/22514/EVE	STUDENT NO
NAMULI GRACE	14/U/12296/EVE	STUDENT NO
EKWARO DOMINIC	15/U/260	STUDENT NO

1 Introduction

Computer vision is an interdisciplinary field that deals with how computers can be made for gaining high-level understanding from digital images or videos. From the perspective of science and engineering, it pursues to automate tasks that the human visual system can fix.[Brown, 2010] And in the Sub-domains of computer vision in relation to security include; scene reconstruction, event detection, video tracking, object recognition, object pose estimation, motion estimation, and image restoration among others.

Physical security is often a second thought when it comes to information security and since physical security has technical and administrative elements, it is oftenly overlooked because most organizations focus on technology-oriented security countermeasures [Harris, 2013] to prevent hacking attacks. The computer vision system will be designed for the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise or company.

1.1 Background to the problem

Computer vision as a discipline that has made a significant impact on a number of diverse application domains eg [Grimson, 1994] and it has been around since the 1960s.

Beginning from the seventies through the nineties, computer vision started proving its practical value in a wide range of diverse application domains including medical diagnostics,manufacturing, environmental monitoring, space exploration, and military systems such as automatic target recognition, precision weapons, reconnaissance[Trivedi, 2010] and currently its at an extraordinary point in its development.

Physical security over the past decades has become increasingly more difficult for organizations. Technology and computer environments now allow more compromises to occur due to increased vulnerabilities. USB hard drives, laptops, tablets and smartphones allow for information to be lost or stolen because of portability and mobile access. In the early days of computers, they were large mainframe computers only used by a few people and were secured in locked rooms [Harris, 2013]. Today, desks are filled with desktop computers and mobile laptops that have access to company data from across the enterprise. Protecting data, networks and systems has become difficult to implement with mobile users being able to take their computers out of the facilities. Fraud, vandalism, sabotage, accidents, and theft are increasing costs for organizations since the environments are becoming more complex and dynamic [Harris, 2013].

1.2 Problem Statement

With the essence and urge of Protecting data, networks and systems for which has become difficult to implement due to technological advancement that has seen mobile users able to take their

computers out of the facilities, fraud, vandalism, sabotage, accidents, and theft are increasing costs for organizations since the environments are becoming more complex and dynamic with the current tech trend characterized with limited memory that cannot even remember a quickly flashed image,thus prompting new innovations in terms of computer vision systems for enhancing physical security.

1.3 purpose

To develop method that enable a machine to understand, analyze, process and acquire digital images, videos and extraction of high-dimensional data from the real world in order to produce numerical or symbolic information that is used for the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution.

1.3.1 Objectives

1. To collect data on the current existing systems
2. To analyze the data collected and generate requirements
3. To design and implement the proposed system
4. To test and validate the system.

2 Methodology

- To achieve the first objective. We shall carry-out literature review related systems where computer vision is being applied. we shall also carry-out interviews, to gather vital information to aid designing of the proposed system
- Secondly, we intend to use excel software to analyze the collected data. Models such as Data Flow Diagrams (DFD) will be used to document and visual the true and real requirements for the system being developed.
- Thirdly, we shall use ERD and UML diagrams to design the system. We intend to use machine learning and python for implementing the system.
- Lastly, we shall test the system in order to correct errors or remove defects that will have arose through compiling and running on the development platforms.

References

[Brown, 2010] Brown, B. (2010). Computers for cyber crimes. *University of California*.

[Grimson, 1994] Grimson, W.E.L., . J. M. (Mar. 1994). Computer vision applications. *Communications of the ACM*, pages 45+.Academic OneFile, Accessed 11 Apr. 2017.

[Harris, 2013] Harris, S. (2013). Physical and environmental security. *In CISSP Exam Guide*, pages 6th ed., pp.427–502 USA McGraw–Hill.

[Trivedi, 2010] Trivedi, M. (2010). Computer vision for homeland security. *University of California*.