**CHRISLAND UNIVERSITY**

**DESIGN AND IMPLEMENTATION OF A FACIAL RECOGNITION SECURITY DATABASE SYSTEM**

**(EMEDIONG UBOM)**

**ABSTRACT**

 Security technology is evolving in this modern day and security personnel are always updating their database with users in order to track potential threats and protect data against possible threats such as accidental, loss destruction or misuse. The following pose a threat to database integrity and access, the implementation of the security system database stores student’s details. The aim of this project is to develop an image based facial recognition security database system. To test the system, the system allows the user to log in by using username and password given default as “admin”. The system allows the user to input image to be matched, and the system allows the image to be compared. Hence, this project developed a facial recognition database system using the Viola Jones algorithms and Haar-like features in training the model used for facial recognition images. The development of an easy secure security database system was reported in this study. The system has a web-based framework and it works on any web browser. The design of the system was done using the flowcharts and the UML diagrams while the implementation of the system was done using python programming, HTML and Heroku. The system was evaluated and scored high as user friendly security database system. The system had a 97% efficiency rate. In conclusion, the main purpose of the system is to improve security in the university making administrators and users who are granted access to the database to keep track records of students whose information have been uploaded to the database. Facial recognition technology accuracy depends on the quality of the image uploaded. Facial recognition technology should consider the following; the technology should treat everyone fairly, use database and web application firewalls to protect security database, regularly backup database, keep applications up to date, use strong user authentication, and lastly facial recognition technology should enhance database security to integrate the risks of data compromise. Companies should document capabilities and limitation in the technology for future analysis and solutions.