



INFORMATICS INSTITUTE OF TECHNOLOGY

In collaboration with

UNIVERSITY OF WESTMINSTER, UK

Digital Document Forgery Detection System

By

U. Hasanga Sanduni
(2014522)

Supervised by

Mr. Pumudu Fernando

Submitted in partial fulfillment of the requirement for the
BENG (Hons) Software Engineering degree

April 2019

© The copyright for this project and all its associated products resides with Informatics Institute of
Technology

Abstract

Digital forgeries of documents occur in most confidential document systems. One of them is the electronic procurement system, which involves fraud at every step of the process. Most procurement systems in Sri Lanka do the process manually even though there are ways to submit the tender response document online. Main reason not to use online systems is that bidding organizations don't trust electronic systems.

The proposed system provides a secure and trustful solution for current electronic procurement systems. The solution will report and notify the authorized individuals if any fraud activity has been occurred in the tender response document submitted. This helps to get any litigation before the winning bid is selected. Because of the inability to find fraud in current electronic systems, the winning bid goes to the wrong bidder. The problem is that the other people who are involved in the process don't know if any fraud activity happens to the documents, so nobody ever gets to know about the scenarios like this.

The proposed solution uses steganography along with fuzzy hashing to detect forgeries that occur in the system in real time. It will detect where the forgery occurs in the document and point out the forged content to the user. More importantly, the solution works with most types of content in documents: Texts, images, tables and forgeries of searchable graphs can be identified from the solution.

Using selected test approaches, functional and structural (non-functional) software was performed. The evaluated results demonstrate system accuracy at a satisfied level. A critical evaluation process was performed based on different evaluation criteria involving different evaluator groups. The results of the evaluation process identify the strengths, weaknesses and enhancements of the project.

Key Words:

Steganography, Fuzzy Hash, Data Hiding, Document Forgery