



Technology Transfer Opportunity

FORTRESS: FORensic Tool for Resilient Steganographic Signatures

OPPORTUNITY:

Steganography is the ancient art of hiding information. Digital technology gives new ways to hide information in multimedia content such that it remains perceptually unchanged. An example is digital watermarking which balances the need to achieve statistical transparency while maximizing the amount of transmitted information.

FORTRESS is deployed to detect hidden information amongst otherwise innocuous Internet traffic. This hidden information may comprise of illegal or offensive images such as pornography, terrorist messages or unauthorized data such as industrial espionage.

Description of Technology:

FORTRESS is an open platform for detecting hidden communication on the Internet. FORTRESS behaves as a simple proxy server, configurable via a web interface. New detection methods can be added as plug-ins making the administration of FORTRESS efficient and scalable.

The main features of the FORTRESS system are:

- User Friendly: easy to configure (using a HTTP configuration service) and easy to use (as an Internet proxy).
- High Scalability: new steganalysis algorithms can be added to the system as plug-ins (flexible API available)
- High Efficiency: in-memory cache and database cache eliminate redundant computation. Distributed architecture fully utilizes available computation resource.
- High Practicability: FORTRESS is an effective proxy to detect hidden communication, which can be deployed in many different organisational situations.

The FORTRESS system runs on a Linux platform, but can be used and configured from any other OS platforms such as Windows, OSX, UNIX etc.

FORTRESS can accommodate thousands of users but may also be installed on single-user PC. FORTRESS provides a reliable, low latency method for withholding unauthorised content from Internet users while being easy to use like an anti-virus filter.

Value Proposition:

For Corporate Information Officer and IT administrators who want to prevent information leakage or unwanted importation of illegal data, FORTRESS provides an easy to implement, real-time and expandable analysis solution that is specifically geared to find hidden information in network data.

Market:

Corporate Information Officers who need to protect valuable information from leaking out. Corporate HR functions that need to protect employees from illegal data.

Development Team:

Dr. Guenole Silvestre and Dr. Neil Hurley School of Computer Science & Informatics.

Status:

FORTRESS has gone through a Proof of Concept phase of development is currently available for user trials and commercialisation.

Opportunity Sought:

Licensing or development partner opportunity available.

Contact:



Technology Transfer Opportunity

FORTRESS: FORensic Tool for Resilient Steganographic Signatures

Peter Conlon,
Project Manager, Technology Transfer,
NovaUCD,
Belfield Innovation Park,
UCD, Dublin 4,
Ireland.

t: +353 1 716 3728
e: peter.conlon@ucd.ie
w: www.ucd.ie/nova