A Cryptographic, Discrete Cosine Transform and Frequency Domain Watermarking Approach for Securing Digital Images

Quist-Aphetsi Kester [1,2,3], Laurent Nana[1], Anca Christine Pascu[1], Sophie Gire[1],Jojo M. Eghan[3], Nii Narku Quaynor[3]

[1] Lab-STICC (UMR CNRS 6285), European University of Brittany, University of Brest, France
Kester.quist-aphetsi@univ-bret.fr / kquist@ieee.org
[2] Faculty of Informatics, Ghana Technology University College
[3]Department of Computer Science and Information Technology, University of Cape Coast

Abstract - *The growth in multimedia messaging, social networks, live streaming and in other applications have increased overtime. The rise in the engagement of Unmanned Ariel vehicles for agricultural, surveillance and deliver services has become a debate in its security and engagement in today's cyber physical space. Authentication and security between control units and these devices are of paramount importance. And also a fast and energy efficient algorithms are highly needed to ensure uncompromised situation of compunctions with these devices. Due to fictitious activities over communication channels by unauthorized users, security and authentication of such transmissions are needed to provide privacy, authentication and confidentiality. In this paper, we proposed a cryptographic encryption technique and a discrete cosine transform for encryption and compression of the transmitted image. We further engaged a frequency domain watermarking approach for the authentication of the digital images. These approaches were engaged to provide several security layers for transmitted image and at the, results showed to be very effective. The implementation in this work was simulated in MATLAB.*

Keywords: cryptography, discrete cosine transforms, UAVs, compression, watermarking

1 Introduction

The cyberspace today is challenged with security of transmitted and stored data. The future of computing looks forward to a full potential of sensor networks distributed across the geographical space and yielding a continuous massive data from which knowledge can be deduced from in shaping the way we perceive and adapt to our environment. This will help build and make the physical and the cyberspace be one with each other and resulting into an integrated and interdependent cyber-physical world. One can see these applications gradually evolving from the emergence of new directions in science with restless researchers aiming to get results for complex problems in today's world. Applications ranging from ubiquitous computing, internet of things, bionics etc. Brain to machine interfacing and brain to brain via device interfacing are gradually progressing in becoming a reality.

With all these advancements poses threats to mankind's security of control. Hence security approaches to securing devices in today's cyberspace has become key issue in deployment of remote control or Unmanned Ariel Vehicles. These devices first emerge with human autonomy over them and they were gradually given partial independence of autonomous behavior in time. The only interface between these devices and man is the visuals they obtain from afar. These visuals consist of transmitted valuable information such as coordinates, speed, payloads, signal strength etc. Hence a compromise situation or interception of transmitted visuals data can put the vehicle under threat and can expose it to being compromised by a third unauthorized party. And hence the safety and security of the commutations from these devices are key concern.

For most of the devices that depend on wireless networks and independent power sources, maximizing cryptographic approaches for them means putting more computational power load on them as well as demanding for more power source and memory for their processes. Hence an effective and efficient and easily implementable but a good layer of security approach is required in providing safety and security for these devices. I n contributing to the security developments and demands in these area, we proposed a cryptographic encryption technique to ensure confidentiality and a discrete cosine transform for the compression of the transmitted image. We further engaged a frequency domain watermarking approach for the authentication of the digital images. The paper has the following structure; section II Related works, section III is Methodology, section IV Results and analysis, and section V concluded the paper.