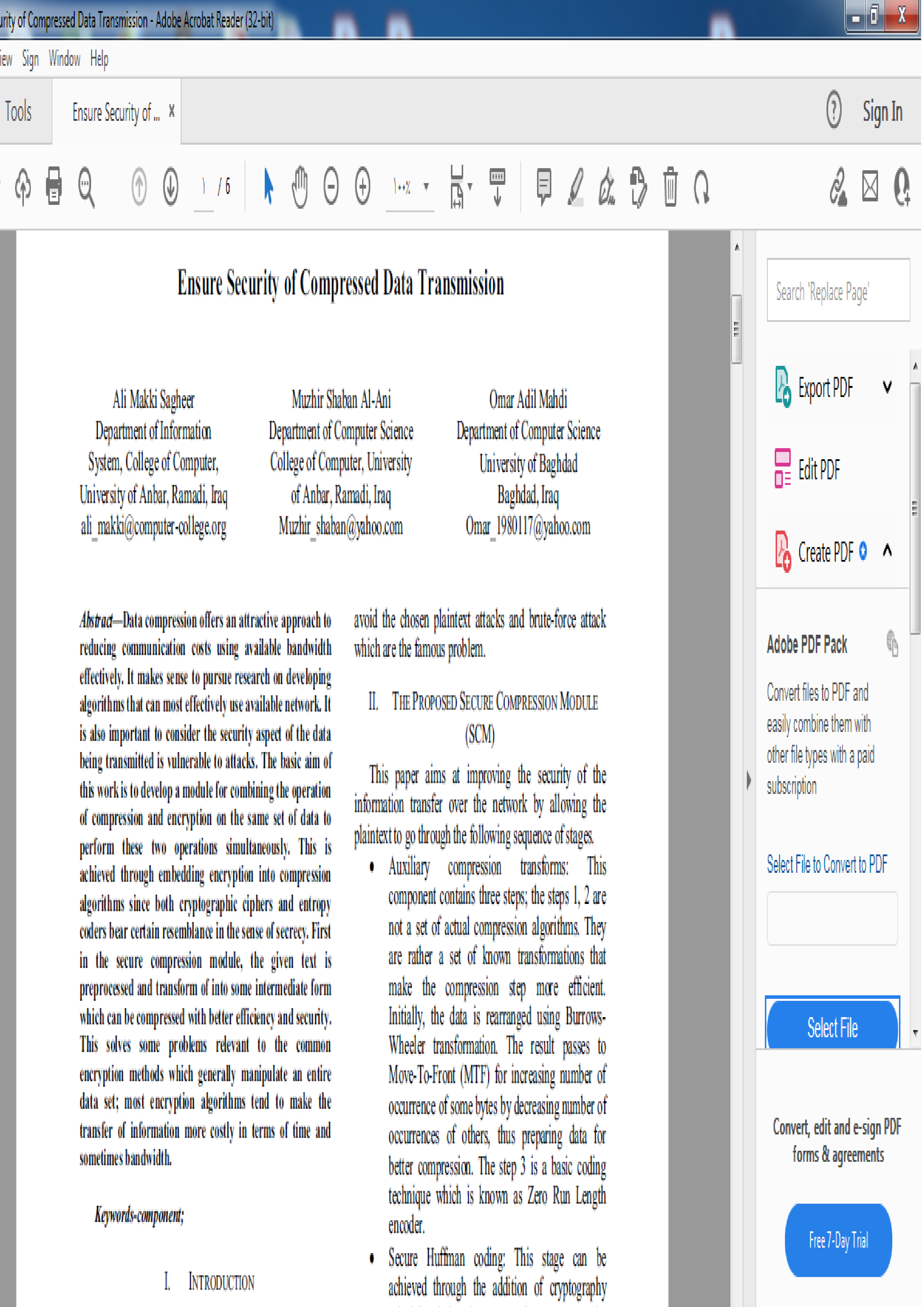
urity of Compressed Data Transmission - Adobe Acrobat Reader (32-bit)
iew
Sign
Window
Help
Tools
Ensure Security of ...
Sign In
1 / 6
Search 'Replace Page'
Export PDF
Edit PDF
Create PDF
Adobe PDF Pack
Convert files to PDF and easily combine them with other file types with a paid subscription
Select File to Convert to PDF
Select File
Convert, edit and e-sign PDF forms & agreements
Free 7-Day Trial

Ensure Security of Compressed Data Transmission

Ali Makki Sagheer
Department of Information System, College of Computer, University of Anbar, Ramadi, Iraq
ali_makki@computer-college.org

Muzhir Shaban Al-Ani
Department of Computer Science College of Computer, University of Anbar, Ramadi, Iraq
Muzhir_shaban@yahoo.com

Omar Adil Mahdi
Department of Computer Science
University of Baghdad
Baghdad, Iraq
Omar_1980117@yahoo.com

Abstract—Data compression offers an attractive approach to reducing communication costs using available bandwidth effectively. It makes sense to pursue research on developing algorithms that can most effectively use available network. It is also important to consider the security aspect of the data being transmitted is vulnerable to attacks. The basic aim of this work is to develop a module for combining the operation of compression and encryption on the same set of data to perform these two operations simultaneously. This is achieved through embedding encryption into compression algorithms since both cryptographic ciphers and entropy coders bear certain resemblance in the sense of secrecy. First in the secure compression module, the given text is preprocessed and transform of into some intermediate form which can be compressed with better efficiency and security. This solves some problems relevant to the common encryption methods which generally manipulate an entire data set; most encryption algorithms tend to make the transfer of information more costly in terms of time and sometimes bandwidth.

Keywords-component;

I. Introduction

avoid the chosen plaintext attacks and brute-force attack which are the famous problem.

II. The Proposed Secure Compression Module (SCM)

This paper aims at improving the security of the information transfer over the network by allowing the plaintext to go through the following sequence of stages.

- Auxiliary compression transforms: This component contains three steps; the steps 1, 2 are not a set of actual compression algorithms. They are rather a set of known transformations that make the compression step more efficient. Initially, the data is rearranged using Burrows-Wheeler transformation. The result passes to Move-To-Front (MTF) for increasing number of occurrence of some bytes by decreasing number of occurrences of others, thus preparing data for better compression. The step 3 is a basic coding technique which is known as Zero Run Length encoder.
- Secure Huffman coding: This stage can be achieved through the addition of cryptography