



ISSN:1306-3111
e-Journal of New World Sciences Academy
2007, Volume: 2, Number: 3
Article Number: A0029

NATURAL AND APPLIED SCIENCES
COMPUTER ENGINEERING

Received: March 2007
Accepted: July 2007
© 2007 www.newwsa.com

Deniz Taşkın
Nurşen Suçsuz
Cem Taşkın

University of Trakya
deniztaskin@trakya.edu.tr
Edirne-Türkiye

SIKIŞTIRILMIŞ VIDEO GÜVENLİĞİ

ÖZET

Günümüz şifreleme algoritmaları geleneksel metin verisini şifrelemeye ve çözmeye yöneliktir. Video akımının şifrelenmesinde sıkça rastlanan yaklaşım, sayısal videonun bir bit akımına dönüştürülerek geleneksel veri gibi şifrelenmesidir. Kendine has bir yapısı olan video akımının şifrelenmesi, şifreyi çözmek isteyen saldırganın açık noktalar bırakmaktadır. Bu çalışmada, video verisinin artan güvenlik ihtiyaçlarına karşın, geleneksel yöntemlerle akım şifrelendiğinde ortaya çıkan zayıf noktalar gösterilecek ve alternatif bir yöntem açıklanacaktır. Önerilen yöntem, düşük sistem kaynak ihtiyacı ve karmaşıklık seviyesine karşılık sıkıştırılmış video akımına özel şifreleme, yüksek güvenlik, taşınabilirlik ve hız sağlamaktadır.

Anahtar Kelimeler: Video Güvenliği, Video Kodlama, MPEG

COMPRESSED VIDEO SECURITY

ABSTRACT

Conventional cryptography algorithms deal with the encryption and decryption of text data. Common method for crypting video stream is encoding digital video into bit stream and encrypting in the same way as generic data. Crypting video data that have a unique structure gives weak points to the attacker. In this study, despite of increasing security requirements of video data, weak points that appear when stream is crypted by traditional methods are demonstrated and an alternative method is explained. Given method provides special cryptography for compressed video stream, high security, mobility and speed for lower system requirements and complexity.

Keywords: Video Security, Video Coding, MPEG