



Application of CSK Encryption Algorithm in Video Synergic Command Systems

Lele Qin, School of Economics and Management, Hebei University of Science and Technology, Shijiazhuang, China

 <https://orcid.org/0000-0003-3222-6453>

Guojuan Zhang, Department of Industrial Basic Education, Hebei College of Industry and Technology, Shijiazhuang, China

Li You, Department of Economics and Trade, Hebei College of Industry and Technology, Shijiazhuang, China

 <https://orcid.org/0000-0002-7186-0142>

ABSTRACT

Video command and dispatch systems have become essential communication safeguard measures in circumstances of emergency rescue, epidemic prevention, and control command as data security has become especially important. After meeting the requirements of voice and video dispatch, this paper proposes an end-to-end encryption method of multimedia information that introduces a multiple protection mechanism including selective encryption and selective integrity protection. The method has a network access authentication and service encryption workflow, which implants startup authentication and key distribution into the information control signaling procedure. This method constitutes a key pool with the three-dimensional Lorenz system, the four-dimensional cellular neural network (CNN) system, and the four-dimensional Chen system where the key source system and initial conditions are decided by the plaintext video frame itself. Then, this method optimizes the chaotic sequences to further enhance system security.

KEYWORDS

Chaos Algorithm, Encryption and Decryption, Key Distribution, Synergic Commands, Video Conferencing, Video Encryption, Video Security, Video Synergic Command System, Video Systems

1. INTRODUCTION

As a kind of real-time communication system relying on image and voice communication, video systems enable geographically dispersed users to gather in one virtual conferencing space as the various information exchange modes through image and voice enable real and visualized exchange of cooperating members, and facilitate participant understanding of conference content (Yang et al., 2014). At present, video systems have been gradually developing in the directions of multi-network cooperation, high definition quality, development and intelligence. Video synergic command and dispatch systems can be deployed in public networks or private networks, and are broadly applied in cities' emergency responses, environmental protection, safety supervision, digital city management, public security, electric power and other industries. Particularly for public security and emergency management departments, video command and dispatch systems have become essential communication safeguard measures for large-scale security activities and emergency rescue. Especially in the prevention and control of COVID-19 outbreak in the beginning of 2020, video synergic command

DOI: 10.4018/JOEUC.20220301.oa1

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

systems played a crucial role in areas of teleconference, rescue command, video monitoring command, telemedicine and enterprise work resumption. In the application of video systems, video content may concern state secrets, military intelligence, business secrets and private information. Any leakage of such sensitive information will lead to huge safety risks. Therefore, this paper extracts cryptographic demands from typical video conferencing systems and designs a video conferencing encryption scheme using research in combination with commercial cryptographic algorithm, and by taking full advantage of chaos algorithm. This is done to guarantee the information data security, ensure the sustainable development and secure application of video conferencing. This paper proposes an end-to-end encryption scheme for multimedia information in video synergic command systems which studies, combines and designs technologies such as user authentication, end-to-end information encryption protocol, and chaotic encryption algorithm. This implements the video synergic command system and meets various personalized user demands for multimedia information encryption.

1.1. Research Status

Video encryption technology appeared contemporarily with the rise of the Internet, both in the 1970s, and has undergone changes from analog signal to digital signal. At the beginning of the 1990s, with the establishment of video coding standards, new video encryption algorithms were continuously proposed, but only concerning the encryption of videos without considering the relation between coding and encryption. There were two encryption methods. In the first method, original videos were processed through traditional cryptographic encryption methods before coding, i.e. substituting and disturbing the pixels of videos. The other method was also called the complete encryption algorithm, which encrypted the code stream after coding and adopted a typical encryption algorithm for its high encryption efficiency. This was deemed as having low research value because of the abnormal decoding due to the change of video format after encryption. Then these two methods, were followed by entropy coding based encryption algorithm, which fused the encryption process into the entropy coding process resulting in preferable encryption results, and high encryption and decryption efficiency (Spanos et al., 1995; Shi et al., 2006). From the beginning of the 21st century, various video encryption algorithms began to attract the attention of researchers gradually and more and more technical proposals followed. Cao brought up the video encryption algorithm using discrete cosine transform coefficient, but it had unsatisfactory encryption results because it encrypted only one type of data (Cao et al., 2005). In 1963, Antonio presented a chaotic system and applied the system in video encryption (Antonio et al., 2015). He proposed a model using the three-dimensional Lorenz Chaos to avoid the complexity in solving high-dimensional chaos (He et al., 2013). However, it was inadequate for real-time transmission when combined with coding. Tian put forward a RC4 hyperchaotic video encryption algorithm that generated four pseudorandom sequences through four-dimensional hyper chaotic mapping to work respectively as the seed keys of RC4 algorithm (Tian et al., 2015). The purpose is to realize the joint encryption of Direct Coefficient (DC), Motion Vector Difference (MVD) symbol and non-zero Alternate Coefficient (AC) symbol. This algorithm featured big key space, strong key sensitivity and high security. The above literature all sought to achieve a sound balance between the efficiency and security of video encryption. Liu et al. came up with a puzzle algorithm that first separated the code stream into blocks, scrambled the blocks and then encrypted them respectively by key streams produced through AES-CTR (Liu et al., 2015). This algorithm was applicable in multimedia P2P video conferencing systems. Traditional encryption methods are primarily mathematical methods requiring costly equipment, and don't fit the document coding structure and mass data characteristic of video information. Chaotic encryption methods are mainly physical methods utilizing the chaotic features of chaotic systems and requiring low-cost equipment. Chen discovered the Chen System in 1999 and applied the four-dimensional hyper chaotic mathematical model (Guan et al., 2015). Chua and Yang were first to establish the Cellular Neural Network (CNN), in 1988, and utilized the four-dimensional CNN hyper chaotic system (Qi et al., 2013; Duan et al., 2014). An ideal chaotic random sequence should have certain characteristics

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/application-of-csk-encryption-algorithm-in-video-synergic-command-systems/281267

Related Content

Teaching End-User Applications with Computer-Based Training: Theory and an Empirical Investigation

Brent Bowman, Fritze Grupe and Mark G. Simkin (1995). *Journal of End User Computing* (pp. 12-18).

www.irma-international.org/article/teaching-end-user-applications-computer/55717

The Value of TAM Antecedents in Global IS Development and Research

Chad S. Anderson, Said Al-Gahtani and Geoffrey Hubona (2013). *Innovative Strategies and Approaches for End-User Computing Advancements* (pp. 19-39).

www.irma-international.org/chapter/value-tam-antecedents-global-development/69610

Developing an Instrument for E-Public Services' Acceptance Using Confirmatory Factor Analysis: Middle East Context

Ahmed Alzahrani, Bernd Carsten Stahl and Mary Prior (2012). *Journal of Organizational and End User Computing* (pp. 18-44).

www.irma-international.org/article/developing-instrument-public-services-acceptance/68022

Advanced Middleware Architectural Aspects for Personalised Leading-Edge Services

Nancy Alonistioti (2009). *Intelligent User Interfaces: Adaptation and Personalization Systems and Technologies* (pp. 94-117).

www.irma-international.org/chapter/advanced-middleware-architectural-aspects-personalised/24472

The Impact of Decision Support Training on Computer Use: The Effect of Prior Training, Age, and Gender

F. Nelson Ford, William N. Ledbetter and Tom L. Roberts (1996). *Journal of End User Computing* (pp. 15-23).

www.irma-international.org/article/impact-decision-support-training-computer/55731