doi:10.1093/comjnl/bxs062

Capsule Reviews

FAIROUZ KAMAREDDINE

The Capsule Reviews are intended to provide a short succinct review of each paper in the issue in order to bring it to a wider readership. The Capsule Reviews were compiled by Fairouz Kamareddine. Professor Kamareddine is an Associate Editor of *The Computer Journal* and is based in the Department of Mathematical and Computer Sciences at Heriot-Watt University, Edinburgh, UK.

Steganography: A Class of Secure and Robust Algorithms. JACQUES M. BAHI, JEAN-FRANCOIS COUCHOT AND CHRISTOPHE GUYEUX

Chaos-based approaches to non-blind binary information hiding are frequently proposed to improve the quality of schemes in information hiding. These approaches are almost based on two fundamental chaotic maps: the Chebychev and logistic maps. The authors argue that functions should be iterated on finite domains and that there are other functions that provide secure algorithms. The paper starts by recalling Boolean discrete dynamical systems and formalize the information-hiding algorithms based on these Boolean iterations. Then, the state-of-the-art in information-hiding security is presented along with the probabilistic stego-security approach used to evaluate the security of data hiding against Watermarked-Only Attack. The authors recall the results related to stego-security for the negation mode and give a new class of stego-secure schemes. Then, the authors move from the probabilistic to the topological behaviour of security, define chaos-security and show that functions whose graph is strongly connected are sufficient to provide new instances of dhCI dissimulation that are chaos-secure. Next, the authors give applications of these functions to frequential domains and focus on the analysis of image quality and robustness.

Image and Video Encryption based on Dual Space-Filling Curves. GAURAV BHATNAGAR, Q.M. JONATHAN WU AND BALASUBRAMANIAN RAMAN

In this paper, a new encryption scheme is proposed based on dual space-filling curves (SFCs), a non-linear chaotic map and fractional wavelet transform (FrWT). The proposed scheme has three different modes of operation and every operation produces different outputs. After an introduction to the preliminaries needed such as the theory of the non-linear chaotic map and the FrWT on which the encryption schemes are based, the dual SFCs are described in detail. Then, motivating factors in the design of the authors' approach to encryption are given and both the encryption and decryption algorithms are presented. The authors move to the pre-processing (which essentially adds redundancy in the image and enhances the security), and inverse pre-processing (which removes the added redundancy from the image). The robustness and validity of the proposed scheme are demonstrated by using the MATLAB platform. Different standard images are used as the experimental images in the experiments. Security analysis has been performed on the proposed image encryption algorithms. Comparison with other work is also given.

Transparency-Orientated Encoding Strategies for Voice-over-IP Steganography. HUI TIAN, HONG JIANG, KE ZHOU AND DAN FENG

Steganography is a technology of information hiding. Voice over IP (VoIP) is a new steganographic cover that provides better security for secret messages by virtue of its instantaneity and which can be considered a multi-dimensional carrier where both the packet protocol headers and the payload data can be used to hide data. The authors remark that the encoding problem for VoIP-based steganography is important and propose encoding strategies based on digital logical transformations for steganography over VoIP, which can reduce the embedding distortion and enhance the embedding transparency while maintaining the maximum embedding rate. The authors argue that the transparency of a given steganographic method can be improved by proper encoding and focus on transparency-orientated strategies (ToSs). First, the authors define steganography over VoIP and introduce measuring criteria for ToS, including similarity, distortion and efficiency. Then, the authors introduce previous approaches for steganography based on the storage media and analyse their theoretical steganographic performance. These approaches include the random interval method, random position method, the TSENG algorithm and the ME strategy. Then, the motivation and principle of the proposal in the paper is explained and the authors introduce strategies where: (1) encoding is based on logical operations, (2) encoding is based on shifting operations and (3) encoding is hybrid. These strategies are then implemented and evaluated.

Weighted Stego-Image Steganalysis of Messages Hidden into Each Bit Plane. CHUNFANG YANG, FENLIN LIU, SHIGUO LIAN, XIANGYANG LUO AND DAOSHUN WANG

Steganography is a technology of information hiding that plays an important role in multimedia information security. However, this hiding nature of steganography may be abused by criminals who can carry out their acts undetected. Steganalysis (which is the opposite technology of steganography) has attracted much attention and has been one of the key technologies of digital forensics to detect illegal activities. Furthermore, the so-called quantitative steganalysis estimates the length of secret messages or the modification ratio of the cover signal. Since some of the important steganographic methods are based on the replacement of bit planes, steganalysis techniques have been developed for these methods. This paper concentrates on hiding messages into multiple least significant bit (MLSB) planes and the ID-MLSB steganography (where 'ID' denotes that the message lengths may be embedded into different bit planes independently with different ratios). The authors try to estimate the embedding ratios of ID-MLSB steganography based on the weighted stego-image (WS) more stably and accurately than the existing methods. First, a WS steganalysis for least significant bit (LSB) plane steganography is introduced and followed by the ID-MLSB steganography. Then, a WS steganalysis is proposed for ID-MLSB steganography where WS can be regarded as an estimation of the cover image on the average. The quantitative steganalysis of ID-MLSB steganography is then formalized and then the estimation equation of the embedding ratio in each bit plane is derived from this formalization and from an estimated cover image. Following this, a WS steganalysis algorithm for ID-MLSB steganography is presented and experiments are used to show that the new steganalysis method performs more stably than a typical structural steganalysis method with the change of embedding ratios, and can outperform the structural steganalysis on estimation accuracy.

Exploring Behavioral Patterns Through Entropy in Multimedia Peer-to-Peer Traffic. JOAO V. GOMES, PEDRO R.M. INACIO, MANUELA PEREIRA, MARIO M. FREIRE AND PAULO P. MONTEIRO

Network paradigms, like peer-to-peer (P2P) computing, give users the power to act as content providers. This makes it difficult to determine its nature of traffic since the dual role (client and server) played by P2P hosts increases the traffic load in the edges. This paper aims to analyse the traffic of several popular multimedia applications and protocols from a host-level perspective to allow the understanding of the properties of the traffic generated by a single host. After an introduction to the traffic features needed to mathematically describe the traffic from computer networks, the authors describe the method used for evaluating the heterogeneity of the packet lengths. This method was used to analyse the entropy for all the captured datasets. It was shown that chaotic behavior is reflected in the entropy level and is distinct for P2P and non-P2P traffic. The authors present their results and entropy analysis for different classes of applications (at the host level, simultaneous applications) and give a scheme to distinguish between P2P and non-P2P traffic.

Co-SVC-MDC-Based Cooperative Video Streaming Over Vehicular Networks. CHAO-HSIEN LEE, CHUNG-MING HUANG, CHIA-CHING YANG AND TAI-HSIANG WANG

Next-generation vehicles can connect with each other using different kinds of wireless technologies. This paper proposes a communication scenario based on the cooperation among vehicles. The proposed mechanism is called Cooperative Video Streaming over Vehicular Networks (CVS-VNs) and is able to improve the video quality of the requester because some neighboring vehicles are willing to share their bandwidth. After an introduction to related work, a CVS-VN is introduced where a cooperative group is dynamically formed based on the speed and direction of neighboring vehicles and where the lifetime of the cooperative group can be estimated based on the buffer status of the requester. Group formation and buffer-aware estimation are introduced in detail and then, priority assignment to each video layer and helper are introduced. The proposed CVS-VN is simulated using the Network Simulator version 2 where different policies are studied.

The Set-to-Set Disjoint-Path Problem in Perfect Hierarchical Hypercubes. ANTOINE BOSSARD AND KEIICHI KANEKO

This paper focuses on $(2^m + m)$-dimensional hierarchical hypercubes (HHCs) called 'perfect HHCs'. The node-to-node disjoint-path routing problem and the node-to-set disjoint-path routing problem in perfect HHCs have already been solved in the literature. This paper concentrates on the set-to-set disjoint-path routing and gives an algorithm HHC-S2S in an HHC. After an introduction to the needed preliminaries, the proposed set-to-set disjoint-path routing algorithm is given, which works by reducing the set-to-set disjoint-path routing problem in an HHC to the fault-tolerant set-to-set disjoint-path routing problem in a hypercube. Then, the time complexity of HHC-S2S and an upper bound for the maximum path length are established.