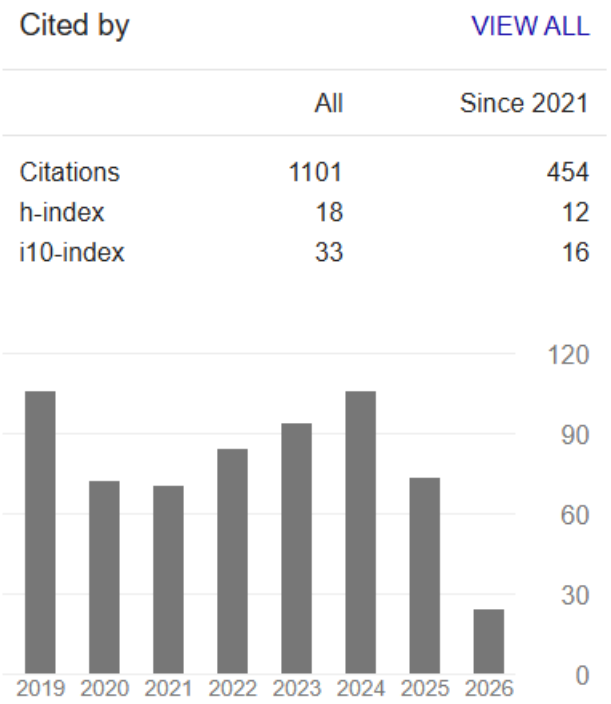
MAY 2026: Top 10 Cited Articles in Cryptography and Information Security (IJCIS)

International Journal on Cryptography and Information Security (IJCIS)

ISSN : 1839-8626

https://airccse.org/journal/ijcis/index.html



ECG Based Human Authentication using Wavelets and Random Forests

Noureddine Belgacem1 , Amine Nait-Ali2 , Régis Fournier2 and Fethi Bereksi-Reguig1

[1]Biomedical Engineering Laboratory, Abou Bekr Belkaid University, Tlemcen, Algeria

[2] Images Signals and Intelligent Systems Laboratory, UPEC University, France

ABSTRACT

The electrocardiogram (ECG) is an emerging novel biometric for human identification. It can be combined in a multi-modal biometric identification system or used alone for authentication of subjects. His primary application can be in health care systems where the ECG is used for health measurements. It does furthermore, better than any other biometrics measures, deliver the proof of subject's being alive as extra information which other biometrics cannot deliver as easily. The main purpose of this study is to present a novel personal authentication approach for human authentication based on their ECG signals. We present a methodology for identity verification that quantifies the minimum number of heartbeats required to authenticate an enrolled individual. The cardiac signals were used to identify a total of 80 individuals obtained from four ECG databases from the Physionet database (MIT-BIH, ST-T, NSR, PTB) and an ECG database collected from 20 student volunteers from Paris Est University. Feature extraction was performed by using Discrete Wavelet Transform (DWT). Wavelets have proved particularly effective for extracting discriminative features in ECG signal classification. The Random Forest was then presented for the ECG signals authentication. Preliminary experimental results indicate that the system is accurate and can achieve a low false negative rate, low false positive rate and a 100% subject recognition rate for healthy subjects with the reduced set of features.

KEYWORDS

ECG; human authentication; wavelet decomposition; random forests.

Source URL: https://airccse.org/journal/ijcis/current2012.html

Volume URL: https://wireilla.com/papers/ijcis/V2N2/2212ijcis01.pdf

Image Encryption Using Fibonacci-Lucas Transformation

Minati Mishra1 , Priyadarsini Mishra2 , M.C. Adhikary3 and Sunit Kumar4

[1] P.G. Department of Information & Communication Technology, F.M. University, Balasore, Odisha, India

[2]District Rural Development Agency, Balasore, Odisha, India

[3]Department of Applied Physics and Ballistics, Fakir Mohan University, Balasore, Odisha, India

[4] Jamshedpur Co-operative College, Kolhan University, Jharkhand, India

Abstract:

Secret communication techniques are of great demand since last 3000 years due to the need of information security and confidentiality at various levels of communication such as while communicating confidential personal data , patients' medical data, countries' defence and intelligence information, data related to examinations etc. With advancements in image processing research, Image encryption and Steganographic techniques have gained popularity over other forms of hidden communication techniques during the last few decades and a number of image encryption models are suggested by various researchers from time to time. In this paper, we are suggesting a new image encryption model based on Fibonacci and Lucas series.

Keywords:

Digital Image, Fibonacci series, Lucas series, Image scrambling, Fibonacci-Lucas map

Source URL: https://airccse.org/journal/ijcis/current2012.html

Volume URL: https://wireilla.com/papers/ijcis/V2N3/2312ijcis12.pdf

Combining Blockchain and IoT for Decentralized Healthcare Data Management

Sajad Meisami1 , Sadaf Meisami2 , Melina Yousefi3 and Mohammad Reza Aref4

1Department of Computer Science, Illinois Institute of Technology, Chicago, USA

2Department of Management, Kharazmi University, Tehran, Iran

3Department of Industrial Engineering, Isfahan University of Technology, Isfahan, Iran
4Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran

ABSTRACT

The emergence of the Internet of Things (IoT) has resulted in a significant increase in research on e-health. As the amount of patient data grows, it has become increasingly challenging to protect patients' privacy. Patient data is commonly stored in the cloud, making it difficult for users to control and protect their information. Moreover, the recent rise in security and surveillance breaches in the healthcare industry has highlighted the need for a better approach to data storage and protection. Traditional models that rely on third-party control over patients' healthcare data are no longer reliable, as they have proven vulnerable to security breaches. To address these issues, blockchain technology has emerged as a promising solution. Blockchain-based protocols have the potential to provide a secure and efficient system for e-health applications that does not require trust in third-party intermediaries. The proposed protocol outlined in this paper uses a blockchain-based approach to manage patient data securely and efficiently. Unlike Bitcoin, which is primarily used for financial transactions, the protocol described here is designed specifically for e-health applications. It employs a consensus mechanism that is more suitable for resource constrained IoT devices, thereby reducing network costs and increasing efficiency. The proposed protocol also provides a privacy-preserving access control mechanism that enables patients to have more control over their healthcare data. By leveraging blockchain technology, the protocol ensures that only authorized individuals can access the patient's data, which helps prevent data breaches and other security issues. Finally, the security and privacy of the proposed protocol are analysed to ensure that it meets the necessary standards for data protection. The protocol's effectiveness and efficiency are tested under different scenarios to ensure that it can perform reliably and consistently. Finally, the protocol proposed in this paper shows that how blockchain can be used to provide a secure and efficient system that empowers patients to take control of their healthcare data.

KEYWORDS

Internet of Things (IoT), Blockchain Technology, Healthcare data management, IoT e-health, privacy, access control, Security

Source URL: https://airccse.org/journal/ijcis/current2023.html

Volume URL: https://wireilla.com/papers/ijcis/V13N1/13123ijcis02.pdf

Video Surveillance in the Cloud?

DJ Neal1 and Syed (Shawon) Rahman, Ph.D.2

1 Information Assurance and Security, Capella University, Minneapolis, MN, USA

2Assistant Professor, University of Hawaii-Hilo, HI USA and Adjunct Faculty, Capella University, Minneapolis, MN, USA

ABSTRACT

A high-resolution video surveillance management system incurs huge amounts of storage and network bandwidth. The current infrastructure required to support a high-resolution video surveillance management system (VMS) is expensive and time consuming to plan, implement and maintain. With the recent advances in cloud technologies, opportunity for the utilization of virtualization and the opportunity for distributed computing techniques of cloud storage have been pursued on the basis to find out if the various cloud computing services that are available can support the current requirements to a highresolution video surveillance management system. The research concludes, after investigating and comparing various Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) cloud computing provides what is possible to architect a VMS using cloud technologies; however, it is more expensive and it will require additional reviews for legal implications, as well as emerging threats and countermeasures associated with using cloud technologies for a video surveillance management system..

KEYWORDS

Video Surveillance, Cloud-Computing, IP-Camera, SPI Model, Cloud storage, virtualization

Source URL: https://airccse.org/journal/ijcis/current2012.html

Volume URL: https://wireilla.com/papers/ijcis/V2N3/2312ijcis01.pdf

Chaos Based Mixed Keystream Generation for Voice Data Encryption

Musheer Ahmad1 , Bashir Alam1 and Omar Farooq2

[1]Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India

[2]Department of Electronics Engineering, ZH College of Engineering and Technology, AMU, Aligarh, India

ABSTRACT

In this paper, a high dimensional chaotic systems based mixed keystream generator is proposed to secure the voice data. As the voice-based communication becomes extensively vital in the application areas of military, voice over IP, voice-conferencing, phone banking, news telecasting etc. It greatly demands to preserve sensitive voice signals from the unauthorized listening and illegal usage over shared/open networks. To address the need, the designed keystream generator is employed to work as a symmetric encryption technique to protect voice bitstreams over insecure transmission channel. The generator utilizes the features of high dimensional chaos like Lorenz and Chen systems to generate highly unpredictable and random-like sequences. The encryption keystream is dynamically extracted from the pre-processed chaotic mixed sequences, which are then applied to encrypt the voice bitstream for integrity protection of voice data. The experimental analyses like auto-correlation, signal distribution, parameter-residual deviation, key space and key-sensitivity demonstrate the effectiveness of the proposed technique.

KEYWORDS

High dimensional chaotic systems, security, mixed keystream, voice encryption

Source URL: https://airccse.org/journal/ijcis/current2012.html

Volume URL: https://wireilla.com/papers/ijcis/V2N1/2112ijcis04.pdf

Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption

S G Srikantaswamy1 and Dr. H D Phaneendra2

1Research scholar, National Institute of Engineering, Mysore

2 Professor and Research Guide, National Institute of Engineering, Mysore

ABSTRACT

Secured Communication involves Encryption process at the sending end and Decryption process at the receiving end of the communication system. Many Ciphers have been developed to provide data security . The efficiency of the Ciphers that are being used depends mainly on their throughput and memory requirement. Using of large key spaces with huge number of rounds with multiple complex operations may provide security but at the same time affects speed of operation. Hence in this paper we have proposed a method to improve Caesar cipher with random number generation technique for key generation operations. The Caesar cipher has been expanded so as to include alphabets, numbers and symbols. The original Caesar cipher was restricted only for alphabets. The key used for Caesar Substitution has been derived using a key Matrix Trace value restricted to Modulo 94. The Matrix elements are generated using recursive random number generation equation, the output of which solely depends on the value of seed selected . In this paper, we made an effort to incorporate modern cipher properties to classical cipher. The second stage of encryption has been performed using columnar transposition with arbitrary random order column selection. Thus the proposed Scheme is a hybrid version of classical and modern cipher properties. The proposed method provides appreciable Security with high throughput and occupies minimum memory space. The Method is resistant against brute-force attack with 93! Combinations of keys, for Caesar encryption.

KEYWORDS

Encryption, Decryption, Substitution, Cipher, Random Number, Recursive, Primitive root, Plaintext, Ciphertext

Source URL: https://airccse.org/journal/ijcis/current2012.html

Volume URL: https://wireilla.com/papers/ijcis/V2N4/2412ijcis05.pdf

Information Hiding in CSS: A Secure Scheme Text-Steganography Using Public Key Cryptosystem

Herman Kabetta1 , B. Yudi Dwiandiyanta2 , Suyoto3

Department of Informatics Engineering, Atma Jaya Yogyakarta University, Yogyakarta, Indonesia

ABSTRACT

In many recent years, the programming world has been introduced about a new programming language for designing websites, it is CSS that can be be used together with HTML to develop a web interface. And now, these two programming languages as if inseparably from each other. As a client-side scripting, CSS is visible by all users as the original script, but it can not be granted changed. Website is a tool of information disseminator throughout the world, this is certainly can be used to a secret communication by using CSS as a message hider. This paper proposed a new scheme using web tools like CSS for hiding informations. This is a secret communication mechanism using text steganography techniques that is embedded messages on CSS files and is further encrypted using RSA as a public key cryptographic algorithm.

KEYWORDS

Text Steganography, Cryptography, Cascading Style Sheet (CSS), RSA Algorithm, public key algorithm

Source URL: https://airccse.org/journal/ijcis/currentissue.html

Volume URL: https://www.wireilla.com/papers/ijcis/V1N1/1111ijcis02.pdf

Implementation and Analysis of Homomorphic Encryption Schemes

Nitin Jain1 , Saibal K. Pal2 & Dhananjay K. Upadhyay2

1USIT, Guru Gobind Singh Indraprastha University, Delhi – 110 075 INDIA,

2 Scientific Analysis Group, DRDO, Metcalfe House Complex, Delhi – 110 054 INDIA

ABSTRACT

An encryption scheme is "homomorphic" if it is possible to perform implicit operation on the plaintext by processing the ciphertext only. The scheme is said to be "fully homomorphic'' when we can perform (a sequence of operations) both addition and multiplication, whereas, it is "somewhat homomorphic'' if it supports a limited number of operations. We describe how Gentry's transformation can be applied on bootstrappable Somewhat Homomorphic Encryption (SHE) scheme to make it a fully homomorphic scheme (FHE) by squashing the decryption circuit i.e. evaluating with a low-degree polynomial. The security of the above scheme is based on the hardness of Approximate Integer Common Divisor Problem (ACDP) which was introduced in 2001 by Howgrave–Graham. Among the two versions of ACDP, the general version (GACDP) is apparently more secure than its partial version (PACDP).

We have implemented and analyzed Gentry's scheme and have suggested some improvements to make it more secure by selecting the Keys parameter in the permissible range

KEYWORDS

Homomorphic encryption, SHE, FHE, Bootstrapping, Approximate GCD, Learning with error.

Source URL: https://airccse.org/journal/ijcis/current2012.html

Volume URL: https://wireilla.com/papers/ijcis/V2N2/2212ijcis03.pdf

Secure Data Transmission Using Steganography and Encryption Technique

Shamim Ahmed Laskar1 and Kattamanchi Hemachandran2

Department of Computer Science Assam University, Silchar, India

ABSTRACT

With the spread of digital data around the world through the internet, the security of the data has raised a concern to the people. Many methods are coming up to protect the data from going into the hands of the unauthorized person. Steganography and cryptography are two different techniques for data security. The main purpose in cryptography is to make message concept unintelligible, while steganography aims to hide secret message. Digital images are excellent carriers of hidden information. We propose a method of combining steganography and cryptography for secret data communication. In this paper, we propose a high-performance JPEG steganography along with a substitution encryption methodology. The approach uses the discrete cosine transform (DCT) technique which used in the frequency domain for hiding encrypted data within image. Experimental results show that the visual and the statistical values of the image with encrypted data before the insertion are similar to the values after the insertion thus reduces the chance of the confidential message being detected and enables secret communication. The effectiveness of the proposed method has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR)

KEYWORDS

Steganography, Cryptography, plaintext, encryption, decryption, ciphertext, substitution cipher, discrete cosine transform, JPEG, quantization, Mean square error and Peak Signal to Noise Ratio.

Source URL: https://airccse.org/journal/ijcis/current2012.html

Volume URL: https://wireilla.com/papers/ijcis/V2N3/2312ijcis14.pdf

Cryptanalyzing of Message Digest Algorithms MD4 and MD5

Md. Alam Hossain, Md. Kamrul Islam, Subrata Kumar Das and Md. Asif Nashiry

Department of Computer Science & Engineering, Jessore Science & Technology University, Jessore, Bangladesh.

ABSTRACT

Hash functions are tools used in integrity of messages, digital signatures and digital time stamping. Message digest algorithms started with public key cryptography for authentication. Digest algorithms compute some hash functions, which are message digest values based on a simple set of primitive operations of 32-bit words. Among the digest algorithms MD4 and MD5 are most popular. Both these algorithms perform a set of bitwise logical operations. They generate 128-bit digest values from a given message. Time complexity of MD5 is more than MD4 and hence somewhat slower to execute. The message digest algorithms MD4, MD5 have been discussed in detail. A new method has been introduced for obtaining collisions for reduced number of rounds of MD4 and MD5 algorithms. The time complexity, performance and attacks of MD4 and MD5 algorithm have been computed using this method. The strength has been computed on change in message; the new method can prove its strength.

KEYWORDS

Data integrity, Authentication, Non-repudiation, Time complexity

Source URL: https://airccse.org/journal/ijcis/current2012.html

Volume URL: https://wireilla.com/papers/ijcis/V2N1/2112ijcis01.pdf