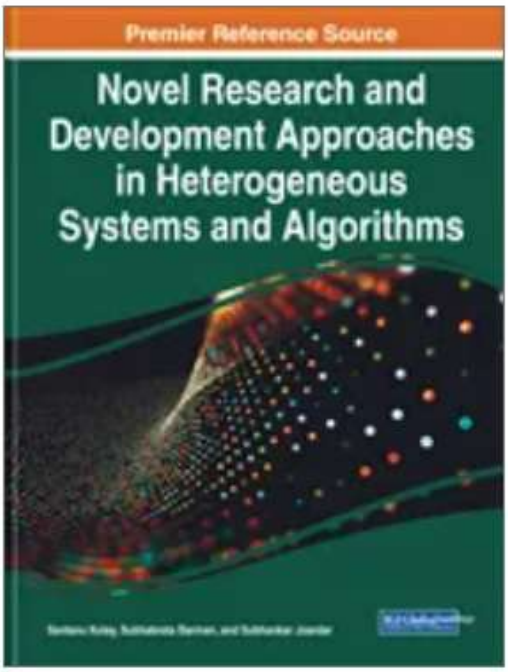


Secure Cryptography Using Chaotic Algorithm

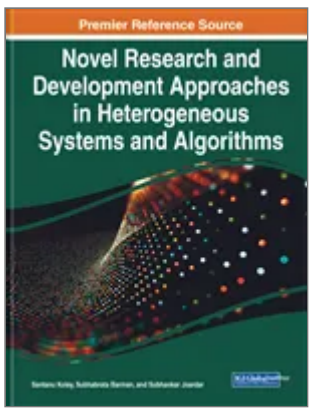
Uday Kumar Banerjee (Dr. B.C. Roy Engineering College, Durgapur, India), Anup Kumar Das (Dr. B.C. Roy Engineering College, Durgapur, India), Rajdeep Ray (Dr. B.C. Roy Engineering College, Durgapur, India), and Chandan Koner (Dr. B.C. Roy Engineering College, Durgapur, India)

Source Title: Novel Research and Development Approaches in Heterogeneous Systems and Algorithms

 | Pages: 26

DOI: 10.4018/978-1-6684-7524-9.ch011

Table of Contents



Secure Cryptography Using Chaotic Algorithm

Uday Kumar Banerjee, Anup Kumar Das, Rajdeep Ray, Chandan Koner

Source Title: Novel Research and Development Approaches in Heterogeneous Systems and Algorithms (/book/novel-research-development-approaches-heterogeneous/308298)

Pages: 26
DOI: 10.4018/978-1-6684-7524-9.ch011

Abstract

A chaotic cryptographic method and bit shuffle methodology for image encryption and decoding have both been suggested. In order to evaluate the encryption's effectiveness and determine whether it met the desired standard, a number of performance analysis tools were also used. These included the number of pixel change rate (NPCR), the unified average changing intensity (UACI), the entropy analysis, which is a component of an encryption scheme that shows how random the image is, and the correlation coefficient. These results reveal the safety of the suggested cryptographic technique.

Chapter Preview

Top

Introduction

Secure Cryptography: An Overview

Security is not only a word; it is a very important aspect in today’s world especially for communication and data or information transmission. As the increase of online transmission not for only simple information but for economic data, the protection of this information becomes very crucial. To do so security techniques like cryptography becomes more and more important as well before. Information security has emerged as the most fascinating and interesting technological sector in the modern world in the information age as a result of widespread computerization and their interaction via networks. Confidentiality, authentication, integrity, non-repudiation, access control, and availability are the guiding principles of every security mechanism. A crucial component of secure communications is cryptography, which was designed with the intention of providing secret communication since it shields information transmission from the impact of adversaries. The concept of security and its characteristics have come to the forefront due to the overabundance of digital content and the ossification of internet technology. For instance, telemedicine provides interactive healthcare in far-off places while transmitting patient health information and imaging data over an insecure connection. Second, the satellite image provides time-specific data that is useful for a variety of purposes, including environmental protection, meteorology, defence and remote sensing. The government, private detectives and criminal organizations may now closely monitor people and public behavior online thanks to the development of surveillance technology. The security of picture data during transmission and storage is a key factor in determining the quality of the service in the aforementioned applications. The word, cryptography came from ancient Greek which contains two words: “kryptos” means “hidden” or “vault” and “graphy” means “writing” or “study”. Cryptography is the study of secure communication between the sender and the receiver and it allow viewing the message to intended recipient without intervention of the adversary element.

The history of cryptography is really old. At the time of ancient Egyptian civilization around 2000 B.C. the hieroglyphic language makes complex by using cryptography picture and only the elite community knew the meaning then. At the time of Julius Caesar at 100 B.C. to 44 B.C. the modern-day cipher concept was found. Julius Caesar did not want that the message should read by the messenger or anyone so he changes the original letter by its next third letter and make a coded form of message which can only be understood by those who knew the decoding process. The modern day’s techniques come along lot of paths and it becomes a strong mechanism to protect information. Nowadays the different mathematical concepts with the help of different rule base calculation are used which are called cryptographic algorithm. By applying these algorithms different text, image, audio, video or other type of files can be encoded such a way that the original meaning of this file is hidden in a masking and cannot be understood easily.

The conversion of plain text to a cipher text is called encryption process. The reverse process to convert the cipher text to original message is called decryption process. The persons who deal with cryptography are called cryptographers. The algorithms are used mainly for cryptographic key generation, to protect the email documents, digital signing, verification to protect data authenticity and privacy, secure web browsing through internet and confidential communications such as debit and credit card transactions.

The modern cryptography has four objectives, confidentiality, integrity, non-repudiation and authenticity. Confidentiality means only the intended recipient will understand the meaning of the information, no one else. The integrity means any alteration or eavesdropping cannot be possible without knowing the sender and receiver. In non-repudiation features the receiver or sender can’t deny the involvement for information creation or transmission in future. When sender and the receiver of the transmitted information can confirm each and every ones identity as well as the origin and destination of the information, the deciphering can be done.

The four different subcategories of cryptography are Modern cryptography, Chaos based cryptography, DNA based cryptography and quantum cryptography. There are mainly two types of cryptographic techniques used, single key or symmetric key encryption and public key or asymmetric key encryption. In single key encryption system, the same key is used to encrypt the data as well as decrypt it. This is also called private key encryption. The Advanced Encryption System (AES), Data Encryption System (DES) are different types of symmetric key encryption. There are two keys used in public key encryption, one key is used to encrypt the data and another key is used to decrypt it. RSA (Rivest–Shamir–Adleman), Elliptic Curve Digital Signature Algorithm (ECDSA), Digital Signature Algorithm (DSA), Diffie-Hellman key exchange are some algorithms of public key infrastructure. Due to their exceptional speed and low complexity, symmetric encryption methods are typically used to encrypt private data. In contrast, asymmetric encryption imposes a heavy computational cost, tends to be much slower, and is frequently employed for digital signature and key distribution. Traditional cryptography, on the other hand, is not suited for quick encryption of a huge volume of data (for instance, colour photos and video) in real time. Traditional picture encryption schemes are more difficult to accomplish when realised by software due to the significant correlation between image pixels. As a result, there is still more effort to be done in the creation of novel encryption techniques.

Complete Chapter List

Search this Book: Full text search terms

Reset

Table of Contents

View Full PDF (/pdf.aspx?tid=320116&ptid=308298&ctid=15&t=Table of Contents&isxn=9781668475249)

Chapter 7

A Novel Steganography Approach Using S-CycleGAN With an Improvement of Loss Function (/chapter/a-novel-steganography-approach-using-s-cyclegan-with-an-improvement-of-loss-function/320127) (pages 123-142)

Minakshi Sarkar, Indrajit Banerjee, Tarun Kumar Ghosh, Anirban Samanta, Anirban Sarkar

Preview Chapter (/viewtitlesample.aspx?id=320127&ptid=308298&t=A Novel Steganography Approach Using S-CycleGAN With an Improvement of Loss Function&isxn=9781668475249) **$37.50** Add to Cart

Chapter 8

AI-Based DBMS Controlled Speech Recognition Model for Some Common Computing Commands (/chapter/ai-based-dbms-controlled-speech-recognition-model-for-some-common-computing-commands/320128) (pages 143-154)

Mrinmoy Sen, Sunanda Jana, Swarnajit Bhattacharya, Gitika Maity

Preview Chapter (/viewtitlesample.aspx?id=320128&ptid=308298&t=AI-Based DBMS Controlled Speech Recognition Model for Some Common Computing Commands&isxn=9781668475249) **$37.50** Add to Cart

Chapter 9

MEDA-Based Biochips: Proposed New Structural Testing Techniques for Fault Detection (/chapter/meda-based-biochips/320129) (pages 155-172)

Priyatosh Jana, Pranab Roy, Sarit Chakraborty, Tanmoy Biswas, Soumen Ghosh

Preview Chapter (/viewtitlesample.aspx?id=320129&ptid=308298&t=MEDA-Based Biochips: Proposed New Structural Testing Techniques for Fault Detection&isxn=9781668475249) **$37.50** Add to Cart

Chapter 10

A Radical Image Steganography Method Predicated on Intensity and Edge Detection (/chapter/a-radical-image-steganography-method-predicated-on-intensity-and-edge-detection/320130) (pages 173-190)

Abhijit Sarkar, Sabyasachi Samanta

Preview Chapter (/viewtitlesample.aspx?id=320130&ptid=308298&t=A Radical Image Steganography Method Predicated on Intensity and Edge Detection&isxn=9781668475249) **$37.50** Add to Cart

Chapter 11

Secure Cryptography Using Chaotic Algorithm (/chapter/secure-cryptography-using-chaotic-algorithm/320131) (pages 191-216)

Uday Kumar Banerjee, Anup Kumar Das, Rajdeep Ray, Chandan Koner

Preview Chapter (/viewtitlesample.aspx?id=320131&ptid=308298&t=Secure Cryptography Using Chaotic Algorithm&isxn=9781668475249) **$37.50** Add to Cart

Chapter 12

An Image Steganography Approach Using Arnold Transformation (/chapter/an-image-steganography-approach-using-arnold-transformation/320132) (pages 217-235)

Solanki Pattanayak, Sabyasachi Samanta, Dipankar Dey, Abhijit Sarkar, Souvik Bhattacharyya

Preview Chapter (/viewtitlesample.aspx?id=320132&ptid=308298&t=An Image Steganography Approach Using Arnold Transformation&isxn=9781668475249) **$37.50** Add to Cart

Chapter 13

Machine Learning-Based Algorithms Towards Crop Recommendation Systems (/chapter/machine-learning-based-algorithms-towards-crop-recommendation-systems/320133) (pages 236-257)

Soumya Roy, Yuvika Vatsa, Moumita Sahoo, Somak Karan

Preview Chapter (/viewtitlesample.aspx?id=320133&ptid=308298&t=Machine Learning-Based Algorithms Towards Crop Recommendation Systems&isxn=9781668475249) **$37.50** Add to Cart