Chapter 15
An Intelligent 8-Queen Placement Approach of Chess Game for Hiding 56-Bit Key of DES Algorithm Over Digital Color Images

Bala Krishnan Raghupathy
https://orcid.org/0000-0002-4752-6400
SASTRA University (Deemed), India

Rajesh Kumar N.
https://orcid.org/0000-0001-5394-218X
SASTRA University (Deemed), India

Priya Govindarajan
SASTRA University (Deemed), India

Manikandan G.
SASTRA University (Deemed), India

Senthilraj Swaminathan
University of Technology and Applied Sciences, Oman

ABSTRACT

Secured data transmission between the communication channels would be a challenging. Attainment of secured key transmission of cryptographic algorithms between communication channel partners is one of the most difficult tasks in data communication. Various cryptography and steganographic principles have been presented for this purpose. This chapter presents a new steganographic approach in which the 56-bit key of data encryption standard (DES) algorithm is safely conveyed between communicators by embedding it in a color digital image. The popular chess game-based 8 Queens placement scheme is used to identify pixel positions for the key embedding process. From observational consequences, it is accomplished that the nominated scheme would lead to achieving assured content contagion over the network.

DOI: 10.4018/978-1-7998-8892-5.ch015

INTRODUCTION

The rapid expansion of network communication and extension methods in the current period has increased the necessity for security in data repositioning and transmission of secret data, which is embedded in digital images and transferred over the network medium. Bulk data capabilities and efficient correlations among surrounding pixels are what distinguish digital images. Traditional encryption procedures based on the private and public key principles, such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and the international data encryption algorithm (IDEA), are not suitable for digital image encryption, especially for high-speed and real-time applications. Table 1 shows the comparative structure of various covert communication principles for the attainment of secret content sharing over the network or communication medium. Cryptography ensures secure communication by requiring a key to access the data. The term "steganography" refers to the logic of concealing a secret code in images that are not legible or understood. Both cryptography and steganography are employed to ensure data privacy. The fundamental difference between them, however, is that with cryptography, anyone can see that both sides are having a private conversation. The advantage of hidden writing over cryptography is that the designated hidden content does not appeal to itself as a topic of investigation. To put it another way, information hiding refers to the use of a document's secret content as a screen. All the traditional Electronic based transmissions may enable secret writing code within the transportation layer, such as text documents, videos, photos, protocol, or computer programmes, executable program files, in the digitized form of stego principles. To ensure the overall security of the confidential content, equally compacting requirements are introduced, because the steganographic arrangement is expensive and has a higher capability known as "payload." In general, a system is considered worthy of "content concealment" when it meets Friedrich's triangle requirements, namely, robustness, large capacity, and imperceptibility.

Table 1. Evolution of various Secret Content Sharing Principles

Communication Principle for Sharing the Secret Content	Obfuscation	Virtue	Unchangeable
Digital Signature Scheme (DSS)	No	Yes	No
Cryptography	Yes	No	Yes
Steganography	Yes / No	Yes / No	Yes

For the steganographic principles, all of the contents of a digitized file, with a high degree of redundancy, are known for their presence; redundant breaks refer to those sections adequate to change without any hypothesis to witness the change. This requirement is particularly well met by audio and image files. Transform and spatial domain steganography are two different types of steganography. In the spatial theme, the secret code is directly hidden via pixel manipulations, with Least Significant Bit (LSB) replacement being the most capable and popular way. However, in the transform domain, transformation techniques such as discrete wavelet transform (DWT) or discrete cosine transform (DCT) are used, and the coefficients are then tapped for the purpose of secret content concealment process. For algorithm compartmentalization, promoted steganography techniques have been divided into two categories. The