Chapter 4
DNA Sequence Based Cryptographic Solution for Secure Image Transmission

Grasha Jacob
Rani Anna Government College, India

Murugan Annamalai
Dr. Ambedkar Government Arts College, India

ABSTRACT

With the advent of electronic transactions, images transmitted across the internet must be protected and prevented from unauthorized access. Various encryption schemes have been developed to make information intelligible only to the intended user. This chapter proposes an encryption scheme based on DNA sequences enabling secure transmission of images.

INTRODUCTION

Internet has become ubiquitous, faster, and easily manageable by anyone on the earth. Social Networking enables people of all ages and strata to interact with each other in any part of the world through sites like Facebook, Twitter, Linked-In, YouTube, Blogs, Wikis and so on. In today's information epoch, individuals, businesses, corporations, and countries are interconnected and Information on demand is practically inevitable anytime, anywhere. The essence of global economy is influenced by the internet being available, and it is tough to imagine a day without email or social networking. The idea of being connected anytime, anywhere and having instant information and data sharing certainly comes out with a substantial risk. Security has become more and more of an issue in recent years. Data in transit can be regarded as secure if and only if both the sender and the receiver are capable of protecting the data and the communication between the two hosts is identified, authenticated, authorized and private, meaning that no third party can eavesdrop on the communication between them. Hackers constantly find ways of stealing sensitive data using various techniques. It is estimated that the number of devices connected

DOI: 10.4018/978-1-7998-1763-5.ch004

to Internet will reach to more than 50 billion around the year 2020.Corporate Espionage has become a reality in this age of the Internet and the global economy. E-commerce transactions are currently plagued with cyber-attacks and are a serious deterrent to the growth of e-commerce globally. In 2008, 4.8 million credit cards were compromised in USA. Revenue losses to the tune of $ 3.3 billion were reported in 2009 from US alone due to cyber-attacks. Successful penetration of Web sites has become the trend of the day. Unfortunately, security issues are more complex no matter how much technology is used.

Data Security and Cryptography go hand in hand as cryptography is an accepted and effective way of protecting data. Though cryptography is used commonly in transit, it is now increasingly being used for protecting data at rest as well. Encryption consists of changing the data located in files into unreadable bits of characters unless a key to decode the file is provided. The security of the sensitive information transmitted through an insecure public communication channel poses a great threat by an unintended recipient. Cryptographic techniques help in ensuring the security of such sensitive information. Cryptography enables the sender to securely store or transmit sensitive information across insecure networks so that it can be understood only by the intended recipient. A cryptographic system applies encryption on the information and produces an encrypted output which will be meaningless to an unintended user who has no knowledge of the key. Knowledge of the key is essential for decryption.

Defense organizations often use encryption systems to ensure that secret messages will be unreadable if they are intercepted by unintended recipients. Encryption methods can include simple substitution codes, like switching each letter for a corresponding number, or more complex systems that require complicated algorithms for decryption. As long as the coding is kept secret, encryption can be a good method for securing information. On computers systems, there are a number of ways to encrypt images in order to make them more secure.

An encryption scheme is unconditionally secure if the ciphertext generated does not contain enough information to determine uniquely the corresponding plaintext no matter how much ciphertext is available or how much computational power the attacker has. With the exception of the one-time pad, no cipher is unconditionally secure.

The security of a conditionally secure algorithm depends on the difficulty in reversing the underlying cryptographic problem such as how easy it is to factor large primes. All ciphers other than the one-time pad fall into this category.

An encryption scheme is said to be computationally secure ifthe cost of breaking the cipher exceeds the value of the encrypted information the time required to break the cipher exceeds the useful lifetime of the information Shannon introduced two fundamental properties for any cipher to be perfectly secure - diffusion and confusion. The idea of diffusion is to hide the relationship between the cipher text and plain text. Diffusion implies that each bit in the cipher text is dependent on all bits in the plain text i.e., if a single bit in the plain text is changed several or all bits in the cipher text will be changed. The idea of confusion is to hide the relation between the cipher text and the key. This will infuriate the adversary who tries to use the cipher text to find the key. The diffusion effect can be introduced on cipher text by permutation. The confusion effect can be introduced on cipher text by substitution box or S-box.

In secure cryptographic schemes, the legitimate user should be able to decipher the messages and the task of decrypting the cipher text should be infeasible for an adversary. But today, the breaking task can be easily performed by a non-deterministic polynomial-time machine.

The Data Encryption Standard (DES) is an algorithm with approximately 72 quadrillion possible keys. The security of the DES is based on the difficulty of picking out the right key after the 16-round nonlinear function operations. Boneh et al. describe in detail a library of operations which were useful