Cryptanalysis of Chaos Based Secure Satellite Imagery Cryptosystem

Musheer Ahmad

Department of Computer Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi 110025, India

Abstract. Recently Usama et al. proposed a chaos-based satellite image cryptosystem, which employed multiple one-dimensional chaotic maps in novel manner to enhance the robustness, security and efficiency of sensitive satellite imagery. It is very efficient in terms of encryption time. The authors of the cryptosystem under study claimed that it has high level of security and can be applied to transmit confidential multimedia images over Internet/shared network. Unfortunately, the security analysis of the cryptosystem reveals that it has serious security flaws. Consequently, it is susceptible to a number of attacks. In this paper, the cryptanalysis of original cryptosystem is presented and it is shown that the attacker can recovers the plain-image from given cipher-image under three types of classical cryptographic attacks without knowing the secret key. The simulation results of cryptanalysis demonstrate that the cryptosystem highly lacks security and cannot be utilized for the protection of confidential/sensitive multimedia images such as the satellite imagery.

Keywords: Satellite image cryptosystem, chaotic maps, security, cryptanalysis, cryptographic attacks.

1 Introduction

Nowadays, modern multimedia and telecommunications technologies make possible to share, exchange and transmit large amount of multimedia data more frequently. This brings challenges to build faster and stronger security solutions for confidential and sensitive multimedia data to be transmitted over the public wired or wireless networks. Inadequate security can leads to unauthorized access, usage or disruption of data. Traditional cryptographic algorithms such as DES, triple-DES, AES, are considered inefficient in providing ample security to multimedia data that has bulk data capacity and high redundancy [1]. The features of chaotic systems like high sensitivity to initial conditions/parameters, non-periodicity, high randomness, mixing property etc have been highly exploited for the design of efficient security methods that suit for multimedia data. An enormous numbers of chaos-based multimedia image and video encryption proposals have been suggested [2-19] since the arrival of first such proposal given by R. Mathews in 1989 [2]. For a thorough discussion of chaos-based image and video encryption techniques, readers are referred to some review and study [20-21]. The work of assessing the security of the proposed
multimedia encryption techniques is equally significant; it has been performed with the intent to arrive at more robust, reliable and efficient security solutions. As a consequence, the security analyses of proposed chaos-based multimedia encryption techniques have also been performed. It has been found that some of them suffer from various security weaknesses and are incompetent to withstand even the classical and other types of cryptographic attacks, as exposed by many cryptanalysts in the literature [22-27].

Recently, Usama et al. [16] proposed a new chaos-based satellite imagery cryptosystem. The cryptosystem is a block cipher which employed multiple one-dimensional chaotic maps e.g. Logistic map, Henon map, Tent map, Cubic map, Sine map and Chebyshev map for enhancing the key space, robustness and security of satellite imagery in novel manner. The experimental and security analyses illustrate that the cryptosystem has high robustness and security. The cryptosystem is very fast as it incurs a very low encryption time. Moreover, the distinctive feature of the algorithm is that it uses a variable length secret key and generates a number encryption keys out of it. In spite of this, the security analysis of the proposed satellite image cryptosystem exposes its serious security flaws from cryptographic viewpoint. Consequently, it is susceptible to the classical cryptographic attacks. In this paper, the satellite image cryptosystem described in [16] is successfully cryptanalyzed. It is shown that we can recover the original plain-image from given cipher-image using three types of attacks (chosen-plaintext, chosen-ciphertext and known-plaintext attacks) without knowing the secret key. Moreover, it is also shown that the cryptosystem is not at all sensitive to a small change in the plain-image, which is a very desirable feature of a good cryptosystem. The outline of the rest of paper is as follows: Section 2 briefly describes the satellite image cryptosystem under study. The cryptanalysis results with simulations are illustrated in Section 3 and finally the conclusions are drawn in the Section 4.

2 Brief Description of Cryptosystem under Study

This section concerns with the review and description of the cryptosystem recently proposed in [16]. The cryptosystem is a block cipher in which the efficiencies of six one-dimensional chaotic maps are exploited to improve the security of the cryptosystem by enhancing its confusion and diffusion properties. The 1D chaotic maps namely Chebyshev Map, Logistic Map, Cubic Map, Sine Map, Henon Map and Tent Map are employed in the system, the governing equations of chaotic maps are:

- **Chebyshev Map**: \( x_{n+1} = \cos(\lambda\cos^{-1}(x_n)) \)
- **Logistic Map**: \( x_{n+1} = \lambda x_n(1-x_n) \)
- **Cubic Map**: \( x_{n+1} = \lambda x_n(1-x_n^2) \)
- **Sine Map**: \( x_{n+1} = \lambda \sin(\pi x_n) \)
- **Henon Map**: \( x_n = 1 + \lambda(x_{n-2} - x_{n-3}) + \alpha x_{n-2} x_{n-2} \)
- **Tent Map**: \( x_{n+1} = x_n/\mu \) if \( x_n \leq \mu \) else \( (1-x_n)/(1-\mu) \)

The Usama et al. cryptosystem takes an integer value \( n \) and a variable length secret key \( S \) of \( \rho \) (=128/256/512) bits as input. It evaluates the initial conditions of all the 1D chaotic maps using the secret key \( S \). Reader may consult the Table 2 in [16] for the