CHAPTER  39

AN EFFICIENT HYBRID CHAOTIC IMAGE ENCRYPTION SCHEME

ASIM, M. AND JEOTI, V.
Department of Electrical & Electronic Engineering, Universiti Teknologi PETRONAS, Malaysia

Abstract: In recent years chaotic cryptography has attracted significant attraction for multimedia security. However, most of these chaotic ciphers still suffer from excessive computation for a given level of security [1–3]. In view of these, a novel scheme is proposed in this paper to encrypt digital images that has far smaller computational load. The proposed scheme is based on multiple-piecewise linear chaotic maps (m-PLCMs) and S-box, where the R, G and B channels of digital images are first segmented into low correlated frames of the appropriate length. Identical chaotic key stream is used for the various frames of the R, G and B channels of the segmented image. The reuse of the chaotic stream reduces the computational complexity by a higher factor and the combination of S-box makes it infeasible to extract the chaotic stream due to its low differential and linear probabilities. The analysis of the proposed scheme proves that it efficiently fulfills the tradeoff between security and encryption speed.

1.  INTRODUCTION

In today’s digital world, secure transmission of images and videos have become an important issue for the applications such as Pay TV, video conferencing and medical imaging systems etc. Many cryptographic algorithms have been proposed and are widely used today such as DES, IDEA, Triple-DES, AES, and RSA etc.

Properties of the chaotic systems such as sensitivity to initial conditions and control parameters, ergodicity, mixing and exactness can be usefully used for in cryptography and also for generating pseudo-random codes. Due to these attention grabbing properties of the chaotic systems, a number of cryptographic algorithms have been proposed recently for the secure transmission of digital images and videos [1–3] [7], but many of them have been reported to be insecure against the known-plaintext and chosen plaintext attacks [8].

Along with the existing security problems of the chaotic ciphers, their speed has also come under great scrutiny due to their low throughput compared to that of AES,
DES etc. However like other researchers [12], we believe that both conventional and chaotic cryptography can benefit from each other.

In this paper, a Hybrid Chaotic Image Encryption Scheme (HyChIES) is proposed. HyChIES is based on m-PLCMs and S-box. HyChIES achieves a good performance both from speed and security analysis point of view.

This article is organized as follows. In section 2, detailed description of HyChIES is presented. Section 3 presents detailed security analysis of HyChIES. In section 4, we talk about the efficiency of HyChIES and compare its computational load with the recently proposed chaotic ciphers for digital images. This article is closed with conclusion.

2. HYBRID CHAOTIC IMAGE ENCRYPTION SCHEME—HYCHIES

Hybrid Chaotic Image Encryption Scheme (HyChIES) is a complete image encryption scheme which operates on pixel values of the image. In HyChIES, digital image is first divided into less correlated frames of the appropriate length. After dividing image into less correlated frames, same chaotic stream is used for masking the corresponding pixel values in all frames. In order to make chaotic key stream extraction infeasible, an S-box is introduced. Input and output of S-box are masked with the output of chaotic stream. In what follows, we describe each and every step of the proposed HyChIES in some detail.

2.1. Scrambling

The ideal way to scramble the 2-D R, B and G channels of an image is to transform each pixel value to a different position in an unpredictable dynamic fashion by a 2-D or 3-D chaotic cat map like [7]. However, it entails high computational load as calculation of new coordinate values require large number of multiplications and additions. Hence to reduce the computational load, R, G and B channels are divided into multiple non-overlapping blocks of the size $4 \times 4$, $8 \times 8$ or $16 \times 16$ and scrambled.

In HyChIES, R, G and B channels are divided into multiple non-overlapping pixel blocks of dimension $16 \times 16$. If the size of the R, G and B channels is not a factor of 16, it is padded with extra zeros. When the image is decrypted, these pad pixels are chopped off.

After dividing into $16 \times 16$ non-overlapping pixel blocks, these blocks are permuted or scrambled by an efficient random pattern. The pattern for transforming the $16 \times 16$ pixel blocks to the new position is generated from generalized 2-D cat map. The pattern should be invertible in order to reproduce the original map correctly. The classical and generalized cat maps are given by (1).