Accepted Manuscript

Improved chaos-based video steganography using DNA alphabets

Nirmalya Kar, Kaushik Mandal, Baby Bhattacharya

PII: S2405-9595(17)30356-9
DOI: https://doi.org/10.1016/j.icte.2018.01.003
Reference: ICTE 126

To appear in: *ICT Express*

Received date : 1 December 2017
Accepted date : 7 January 2018

Please cite this article as: N. Kar, K. Mandal, B. Bhattacharya, Improved chaos-based video steganography using DNA alphabets, *ICT Express* (2018), https://doi.org/10.1016/j.icte.2018.01.003

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

ICT Express
Information & Communications Technology

Improved Chaos-Based Video Steganography using DNA Alphabets

Nirmalya Kar[1]*, Kaushik Mandal[1], Baby Bhattacharya[2]

[1] CSE Department, NIT Agartala, Jirania, India (e-mail: nirmalya@ieee.org)
[2] Mathematics Department, NIT Agartala, Jirania, India (e-mail: babybhatt75@gmail.com)
* Corresponding author

ABSTRACT
DNA based steganography plays a vital role in the field of privacy and secure communication. Here, we propose a DNA properties-based mechanism to send data hidden inside a video file. Initially, the video file is converted into image frames. Random frames are then selected and data is hidden in these at random locations by using the Least Significant Bit substitution method. We analyze the proposed architecture in terms of peak signal-to-noise ratio as well as mean squared error measured between the original and steganographic files averaged over all video frames. The results show minimal degradation of the steganographic video file.

Index Terms: Chaotic Map, DNA, Linear Congruential Generator, Video Steganography, Least Significant Bit.

I. INTRODUCTION

Relaying data in a secure manner between two or more communication points has captured the imagination of mankind for ages. Steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message [1]. Any steganography method must satisfy two properties such as perceptual transparency and high data rate. DNA steganography analyzes and utilizes DNA molecular techniques to conceal information [2]. It is a new territory that emerged after the discovery of the computational prowess of DNA [3]. Moreover, the randomness of DNA strands makes them more suitable to encrypt data and hide sensitive information [4]. The chaotic map is a collection of a noisy sequence. So, utilizing the chaotic map, we identify random pixel locations in an image [5, 6]. Most video-based steganography algorithms are developed based on the relationships between frames. Eltahir et al. [7] presented a video steganography based on the Least Significant Bit (LSB) where they increased the secret message size which would be embedded into video frames. A 3-3-2 approach has been used for embedding data into images which means they take the Least Significant Bit of all RGB color components (3-bits of Red, 3-bits of Green, and 2-bits of Blue). As compared to this technique, a method proposed by Ramalingam et al. [8] using a modified LSB algorithm provides better efficiency. Cao, Zhang, Xianfeng and Yu [9] proposed a novel video steganography scheme based on motion vectors as carriers to embed the secret message through compression processing using H.264 video compression processing. The algorithm also uses the principle of linear block codes to reduce motion vectors' modification rates. A video steganography method proposed by Bin, Li-Yi and Wei-Dong [10] was based on motion vectors by using matrix encoding. Kelash, Wahab and El-sayed [11] proposed a steganography algorithm to embed data into video clips directly, where each pixel in each video frame is divided into two parts, where the number of bits which will be embedded in the right part are counted in the left part of the pixel based on a color histogram.

In our work, we use an .avi video file as the input video. This video will be considered as the cover medium. We will collect all frames from the video file and store these in a folder. After extraction, all frames will be converted into a set of .png frames. Fig. 1 shows the entire procedure of our proposed approach.

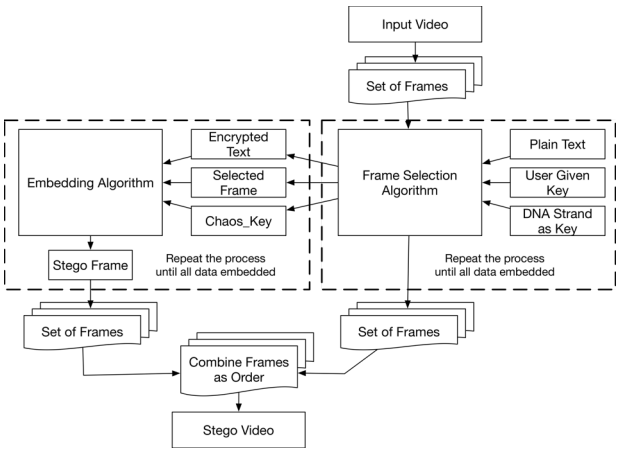

Figure 1. Overview of Proposed Architecture

II. BACKGROUND DESCRIPTION

The methodologies mentioned here are required to establish our proposed approach. This paper does not make use of biological properties; instead, it uses DNA sequences properties to achieve its goal.

A. DNA Alphabets

Download English Version:

https://daneshyari.com/en/article/6925861

Download Persian Version:

https://daneshyari.com/article/6925861

Daneshyari.com