**FINAL YEAR PROJECT SYNOPSIS**

**Project Proposed Title : - Optimized Video Steganography using Cuckoo Search Algorithm**

**Project Area** **: - Information Security**

**Project Guide** **: - Dr. G R Manjula**

**Project associates** **: -** **Batch – B2**

|  |  |
| --- | --- |
| **Name** | **USN** |
|  |  |
| Abhay K P | 4JN16CS001 |
|  |  |
| Rashmi B S | 4JN16CS077 |
|  |  |
| Suchetan J | 4JN16CS102 |
|  |  |
| K SuhasBharadwaj | 4JN16CS103 |
|  |  |

**PROBLEM DESCRIPTION: -**

Information hiding is an active area of research where secret information is embedded in innocent-looking carriers such as images and videos for hiding its existence while maintaining their visual quality.

Steganography is a Greek origin word meaning protected writing. It is a special branch of information hiding and is considered as an art of science for invisible communication, aiming an imperceptible hiding of a secret message inside a cover image whose existence is known to the sender and receiver only.

Steganography can be used for a wide range of applications such as safe circulation of secret data in military and intelligence agencies, improving mobile banking security, online voting security, and covert communication between two communicating bodies. Cryptography which is the process of encrypting sensitive information into scrambled messages has been used as a solution to information security for ages.

A secure image steganographic framework combining the strengths of Steganography and cryptography while maintaining a better balance between image quality, payload, and security, making this framework more suitable for real-time and top-secret level security applications.

There are two important factors have a type of contradiction that every successful steganography system should take into consideration, which are embedding efficiency and embedding payload. The former means good quality of stego data and fewer amounts of host (carrier) data are going to be changed. While the latter means the capacity of secret information to be hidden inside host data is large. The approach in this project is a kind of video steganography in spatial domain. This approach is based on trying to get a large data-hiding capacity with minimal distortion in the host video stream.

The aim of this project is to get a large data-hiding capacity with minimal distortion in the host video stream. This is achieved through an optimized search technique known as Cuckoo Search.

**PROBLEM SOLUTION: -**

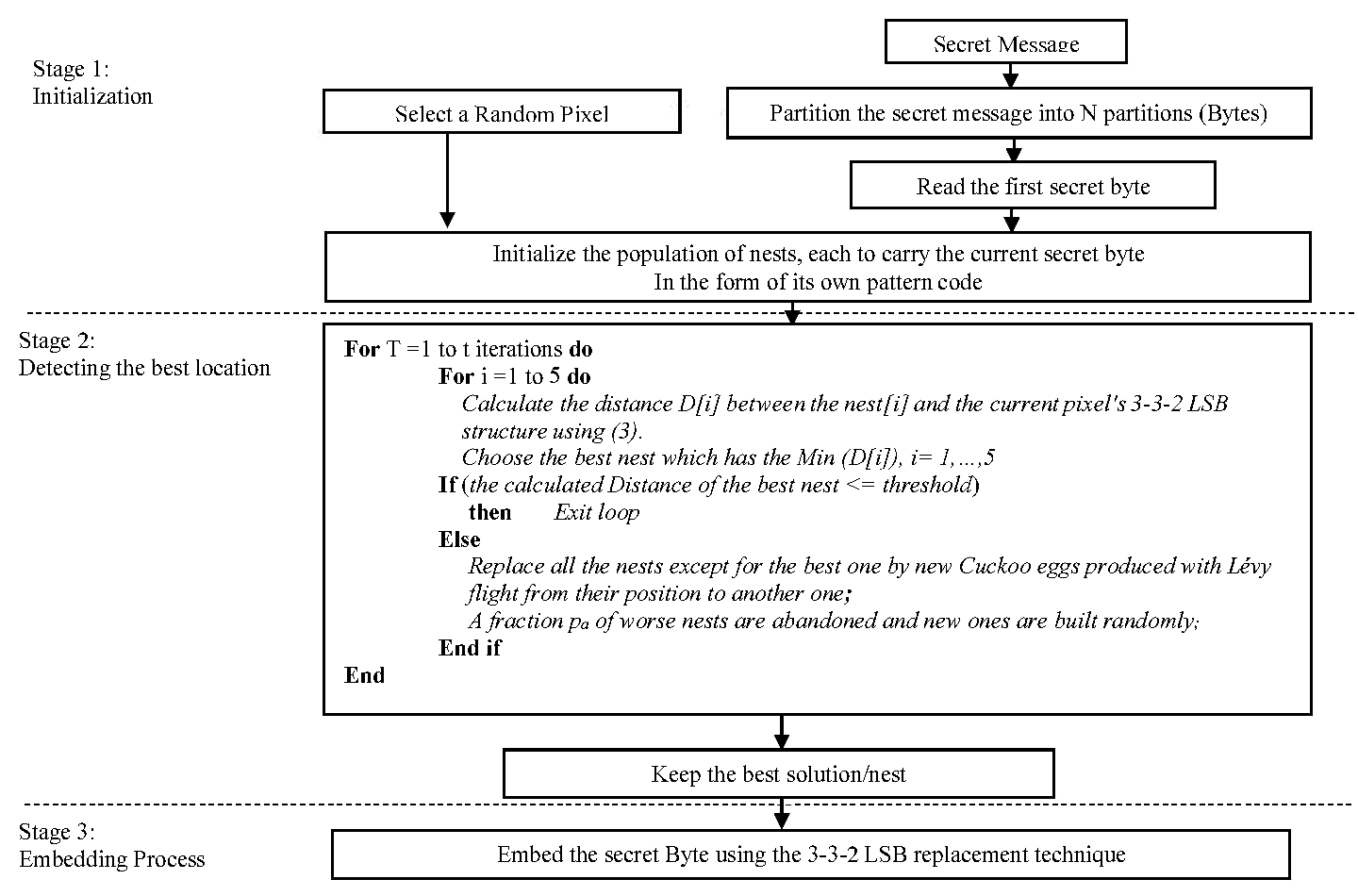
Cuckoo Search is one of the most recent intelligent algorithms that are used to find the best pixels locations in cover frames, where the secret message can be concealed. The founded carrier pixels are concealed in its RGB components using the 2-3-3 LSB replacement technique. The entered secret bytes are restructured according to different five pre-indexed patterns before embedding. In addition, these secret bytes are not embedded in the same order. So, it is difficult for attacker to retrieve the secret information from stego-video.

The main idea of Cuckoo Search algorithm is to conceal a secret message into a carrier video. This approach depends on selecting suitable RGB pixel values from the cover frames which are chosen by using CS optimization algorithm for concealing the secret message. At the beginning, a carrier video is converted to frames and audio. Though both audio and frames can be used to embed secret data. A set of frames have been used as the carrier in our suggested approach. The selected carrier frame(s) is given as input to the suggested approach. As shown in the below figure, the suggested approach is comprised of three successive stages:

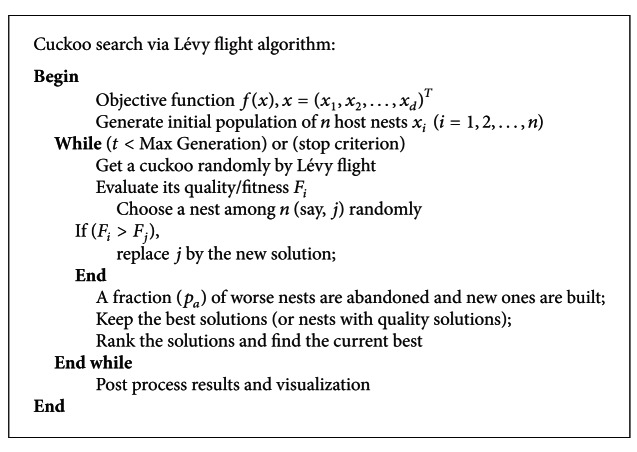
1. Initialization stage.

2. Stage of detecting the best location for embedding and embedding stage.

3. Embedding Stage

*Fig.Stages in our approach for video steganography*

Pseudo Code for Cuckoo Search algorithm:



**APPLICATIONS: -**

Steganography is applicable to, but not limited to, the following areas.

**1)** Confidential communication and secret data storing.

1. Protection of data alteration.
2. Access control system for digital content distribution.
3. Media Database systems.
4. **Medical area:** - If a doctor wants to send some confidential data about the patient, that canbe hidden it in a particular cover medium (For ex, X-ray) and send it to the person who needs it.

**6) Military Areas**: - Customized steganography software can be for embedding encrypted textmessages inside image files for certain communications with "illegal agents" (agents under non-diplomatic cover) stationed abroad..

**7) Network area: -** Covert channels in TCP/IP involve masking identification information inthe Internet when absolute secrecy is needed for an entire communication process and not just one document as mentioned next.

1. **Use in Modern Printers** : -Some modern computer printers use steganography,

IncludingHP and Xerox brand color laser printers. These printers add tiny yellow dots to each page. The barely-visible dots contain encoded printer serial numbers and date and time stamps.