J. Vis. Commun. Image R. 96 (2023) 103911

Contents lists available at ScienceDirect

Journal of Visual Communication and Image Representation

journal homepage: www.elsevier.com/locate/jvci

Full Length Article

A unique database synthesis technique for coverless data hiding☆

Anandaprova Majumder [a,*], Sumana Kundu [a], Suvamoy Changder [b]

[a] Department of CSE, Dr. B. C. Roy Engineering College, Durgapur, India
[b] Department of CSE, National Institute of Technology, Durgapur, India

ARTICLE INFO

Keywords:
Security and privacy protection
Coverless data hiding
Privacy attacks
Object synthesis
Database synthesis
Steganography

ABSTRACT

Coverless data hiding is a powerful technique for data security, but synthesizing text or images, often leads to semantically incorrect results. Prior state-of-the-art works have typically used media files as covers or as references for cover synthesis. This scope of improvement has inspired us to propose a novel data hiding technique by synthesizing self-sufficient, independent object without using any cover, even as metadata for data hiding. The approach focuses on synthesis of a database, by generating a dataset for the domain values of the attributes of it. Application of comparison-based sorting technique to the dataset, reveals the hidden message. The skill of the technique lies in unlimited hiding capacity, while preserving the semantic integrity of the database. Multiple security measures are taken into account along with thorough analysis of time complexity, to evaluate the efficacy of our method, that surpasses recently proposed approaches, providing solution for highly resistant covert communication.

1. Introduction

1.1. Current digital forgeries and application of steganography

Digital content used in various applications like authentication, chat platforms, and online banking is vulnerable to malicious attacks and unauthorized access when shared in plain text format. The need for secure communication and protection of sensitive information has led to a high demand for multimedia security and covert communication [1]. Coverless steganography, an effective technique for hiding information, has gained attention in the cybersecurity and data communication industries [2]. Steganography, with its origins in ancient times, conceals data within cover files to protect against attacks, and its modern formulation stems from the prisoner's problem. It involves cover media, secret messages, data hiding and extraction functions, and optional encryption keys. Steganography aims to invisibly transmit confidential information so that only the intended recipient can detect it. Over the years, numerous data hiding algorithms have been developed for steganography using various multimedia covers.

1.2. Different steganography approaches

The modern digital method for data hiding by steganography can be categorized under three major heads. The categorization is done depending on the process of data hiding by modifying the cover, by selection of the cover or by synthesis of the cover [4] as follows:

1.2.1. By modifying the cover

The cover modification model has lured more recognition in the domain of data hiding because of its high embedding capacity and easier implementation ability. The secret confidential message is concealed by moderating the original cover file according to the applied data hiding [4,5] algorithm. The changed cover file is shared over the communication channel with the receiver, and it regenerates the secret message following the data extraction method. These techniques provide a good amount of privacy protection based on human sensitivity and perception level. However, eavesdroppers may apply different orders of statistical attacks to identify the changes, which can easily invalidate the ongoing covert communication.

1.2.2. By selection of the cover

A number of cover image(s) are selected from the naturally available dataset of images for data hiding by cover selection, and their index is covertly shared [6]. These kinds of data hiding methods contribute no changes to the cover files and hence can be named to be a no-modification-based method. The confidential blocks of the image are

☆ This paper has been recommended for acceptance by Zicheng Liu.

* Corresponding author.
E-mail addresses: anandaprova.majumder@bcrec.ac.in (A. Majumder), sumana.kundu@yahoo.co.in (S. Kundu), suvamoy@cse.nitdgp.ac.in (S. Changder).

https://doi.org/10.1016/j.jvcir.2023.103911
Received 26 April 2023; Received in revised form 18 July 2023; Accepted 5 August 2023
Available online 7 August 2023