IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 2, August 2025

Impact Factor: 7.67

A Empirical Study on Steganography in Tamilnadu

U. Varun Kumar[1] and Ms. Umamaheswari U[2]
BA. LLB (Hons)[1]
Assistant Professor[2]
Saveetha School of Law, Saveetha institute of Medical and Technical sciences (SIMATS), Chennai
uvarunkumar46@gmail.com and umamaheshwariu.ssl@saveetha.com

Abstract: *Steganography is the practice of concealing information within another message or physical object to avoid detection. Steganography can be used to hide virtually any type of digital content, including text, image, video, or audio content. That hidden data is then extracted at its destination. Content concealed through steganography is sometimes encrypted before being hidden within another file format. If it isn't encrypted, then it may be processed in some way to make it harder to detect. As a form of covert communication, steganography is sometimes compared to cryptography. However, the two are not the same since steganography does not involve scrambling data upon sending or using a key to decode it upon receipt. The term 'steganography' comes from the Greek words 'steganos' (which means hidden or covered) and 'graphein' (which means writing). Steganography has been practiced in various forms for thousands of years to keep communications private. For example, in ancient Greece, people would carve messages on wood and then use wax to conceal them. Romans used various forms of invisible inks, which could be deciphered when heat or light were applied. Steganography is relevant to cybersecurity because ransomware gangs and other threat actors often hide information when attacking a target. For example, they might hide data, conceal a malicious tool, or send instructions for command-and-control servers. They could place all this information within innocuous-seeming image, video, sound, or text files*

Keywords: hidden files, transparency, decoded, steganography

DOI: 10.48175/IJARSCT-28708