2026 Innovations in Machine, Engineering, and Digital Conference (IMED) | 979-8-3315-6997-6/26/$31.00 ©2026 IEEE | DOI: 10.1109/IMED68921.2026.11484830

Enhancing CyberSecurity Through Coverless Steganography with Diffusion Based Image Synthesis

Shaurya Chattopadhyay, Ayantik Ray, Ayan Ghosh, Pabak Indu
Institute of Engineering and Management
University of Engineering and Management
Kolkata, West Bengal, India
pabakindu@yahoo.co.in

***Abstract*—As digitization takes over the world, the proportional increase of cyber threats endanger the confidentiality and integrity of digital communications. The safekeeping of sensitive information hence become essential. Sophisticated cyber-attacks like data interception exploit vulnerabilities of systems using traditional data protection methods. Therefore the rising need for innovative solutions to ensure secure communication. Steganography is a technique of hiding information within seemingly harmless carriers like images, texts, audios or videos. It provides security by hiding secret data so it cannot be detected. By hiding messages in digital media, steganography provides a hidden channel for transmitted data to remain secure and therefore provides value in protecting against cyber attacks that will intercept or modify information intended for a third party. However, traditional steganography embeds secret data into existing cover media format reducing detection of the secret data, while still leaving detectable characteristics in the cover media that sophisticated steganalysis can uncover and thwart the efficacy of steganography endeavors. To address this, coverless steganography has emerged as an alternative approach, generating carriers that inherently encode secret data without altering pre-existing media, thus significantly reducing detectability. This study proposes a novel coverless steganography algorithm using Stable Diffusion to create high-quality carrier images to conceal secret information within their latent space representations. Exploiting Stable Diffusion's ability to produce natural-looking images, the method enhances security and hiding capacity while minimizing the risk of detection by even the most advanced steganalysis tools. In our proposed method we split the generated image into 3x3 pixel matrices where each block goes through a IWT channel. Thus possessing minimal changes in the for hiding the information. This paper provides better security for private communication while also adding to the cybersecurity landscape with a completely secure, efficient, and undetectable data protection method.**

***Index Terms*—Steganography, stable diffusion, cover image, stego-image, generative adversarial networks (GANs), multi-modal steganography.**

I. INTRODUCTION

Steganography hides confidential data in multimedia files like images or videos for secret communication without suspicion [1]. Unlike cryptography, it conceals data's existence within cover files. Traditional methods using existing files create detectable distortions [2], [7]. Coverless steganography uses AI models like Stable Diffusion or GANs to generate cover images with embedded data, evading steganalysis [2], [6]. This review covers advancements, suggests improvements, and highlights its cybersecurity role. In 2024, cyber threats like ransomware and breaches, fueled by AI and IoT, target data [10]. Zero-trust and private clouds bolster defenses, but robust data protection is vital [10].

A. MAJOR HISTORICAL CYBER ATTACKS

1) Marriott Data Breach [10]: 2018 breach exposed 500M guests' data (names, addresses, passports), affecting 339M records. 2020 breach hit 5.2M guests. More attacks followed.
2) Yahoo Attack [10]: 2014 state-sponsored hack compromised 500M accounts, stealing names/emails via phishing. Delayed disclosure raised risks. Cost Yahoo $117.5M.
3) Adobe Attack [10]: 2013 hack stole 38M accounts' data (emails, some credit cards, passwords) and source code via phishing. Adobe downplayed scope.
4) MOVEit [10]: 2023 MOVEit vulnerability enabled the Cl0p gang to steal data from approximately 2000 firms, exposing the personal information of around 60M people. Cybersecurity revenue increased from $3.5M (2014) to $3.8M (2023), while cybercrimes rose from 1.2M to 1.5M (Fig. 1, 2).

- June 2024 [11]: Japan's space agency faced cyberattacks on non-critical networks, with no rocket or satellite data compromised.
- June 2024: Ransomware hit Indonesia's data center, disrupting immigration and deleting non-backed-up data, leading to a national audit and an official's resignation.
- June 2024 [11]: Belarusian hackers targeted Ukraine's Ministry of Defense and a military base using phishing emails and malicious Excel files.
- June 2024 [11]: Germany's opposition party faced a cyberattack before European elections, following Russian attacks on another party, causing IT service suspension.
- June 2024 [11]: Chinese hackers stole 20,000 documents from Palau after a U.S.–Palau security deal, marking Palau's first major cyberattack.