International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

SECURE DATA WIPING

Mr. M. Mohanasundharam, Sakthivel . A, Sanjay. A, Sanjeevi Krishnaa. A, Siva Balaji.T

*(CSE, Hindusthan College of Eng & Tech, and Coimbatore

Email: mohanasundharam.cse@hicet.ac.in)

**(CSE, Hindusthan College of Eng & Tech, and Coimbatore

Email:720723104130@hicet.ac.in)

***(CSE, Hindusthan College of Eng & Tech, and Coimbatore

Email:720723104132@hicet.ac.in)

****(CSE, Hindusthan College of Eng & Tech, and Coimbatore

Email:720723104134@hicet.ac.in)

*****(CSE, Hindusthan College of Eng & Tech, and Coimbatore Email:720723104145@hicet.ac.in)

ABSTRACT:

This project presents a secure file wiping system that permanently destroys data beyond forensic recovery. The application implements the Department of Defense 5220.22-M standard through three-pass overwriting using random data, binary zeros, and binary ones. A SHA-256 hash is calculated before wiping to provide cryptographic verification and proof of file existence. The system also wipes freed disk space to prevent slack space recovery and maintains comprehensive JSON audit logs with timestamps and file metadata. Built with Python and PyQt5, the software features an intuitive graphical interface for selecting files or folders, previewing contents, and monitoring real-time progress. The final product is packaged as a standalone executable using PyInstaller, requiring no Python installation on the target Windows system. Extensive testing with forensic recovery tools confirms that wiped data cannot be recovered, making this solution suitable for both personal privacy and organizational compliance requirements.

KEYWORDS: DoD 5220.22-M, SHA-256 Hashing, Three-Pass Overwrite, Cryptographic Verification, Forensic Recovery Prevention, JSON Audit Logging, PyQt5 GUI.

INTRODUCTION :

Every day, millions of people delete files from their computers thinking those files are gone forever. Students delete old assignments, professionals remove sensitive documents, and individuals clear out personal photos before selling their old laptops. But here is the uncomfortable truth that most people do not realize. When you press the delete key or move a file to the recycle bin, the operating system does not actually erase anything. It simply removes the reference to that file, kind of like tearing out a page from a book's index while leaving the actual page still sitting inside the book. The data remains on your hard drive, completely intact, until something else comes along and happens to write over that exact spot.

This creates a massive security risk that most people are completely unaware of. Anyone with basic recovery software, many of which are free and available online, can scan a hard drive and bring back files that were deleted months or even years ago. I have seen it happen myself. A friend sold an old laptop after deleting all his files, and the next owner ran a simple recovery tool and found tax documents, bank statements, and personal photos. This is not some Hollywood hacking scenario. It is a real vulnerability that affects every computer user.

The problem becomes even more serious when you consider organizations that handle sensitive data. Hospitals storing patient records, banks holding financial information, law firms managing client documents, and government agencies handling classified materials all have legal and ethical obligations to protect data.

RELATED WORK :

Over the years, researchers have proposed various methods for secure data destruction. The Department of Defense developed a standard called DoD 5220.22-M that requires three passes of overwriting with specific patterns. Some experts recommend even more passes, up to thirty five, while others argue that for modern drives, a single pass is sufficient. There is also the challenge of solid state drives which work completely differently from traditional hard drives and can retain data even after multiple overwrites due to something called wear leveling.Beyond just destroying the data, there is another important requirement. How do you prove that data was properly destroyed? If a regulator asks for proof that sensitive information was deleted, you cannot just say "trust me, I deleted it." You need evidence. You need cryptographic verification, audit logs, timestamps, and documentation that stands up to scrutiny.This project addresses all of these challenges. I have built a secure file wiping system that implements the DoD 5220.22-M three-pass overwrite standard, works on both traditional hard drives and solid state drives as much as possible, and provides comprehensive audit trails with SHA-256 hash verification. The system calculates a unique digital fingerprint of every file before wiping it, so there is cryptographic proof that the file existed. Detailed logs capture timestamps, file names, sizes, hash values, and pass completion status. Everything is saved in JSON format that can be exported for compliance reviews.But I did not want to build just another command line tool that only technical experts can use. I built a graphical interface using PyQt5 that anyone can understand. Users select files or folders with a simple browse dialog, preview what they are about to delete, and watch a progress bar as the system works. There are confirmation dialogs to prevent accidental clicks, and clear status messages that explain what is happening at every step.

The final product is packaged as a standalone executable file using PyInstaller. No Python installation is required, no dependencies to install, no complicated setup. Just download and run. Testing with forensic recovery tools like Recuva and PhotoRec confirmed that after using this system, not a single byte of original data could be recovered. The system blocks attempts to delete protected system folders, handles permission errors gracefully, and keeps memory usage low even when processing huge files.

PROPOSED ALGORITHM:

The proposed system implements DoD 5220.22-M three-pass overwrite with SHA-256 hashing and JSON audit logging for permanent data destruction. Built with PyQt5 and packaged as a standalone executable, it provides an intuitive GUI, parallel processing, and forensic-resistant wiping on Windows systems.Algorithm Steps .

1. DoD 5220.22-M Three-Pass Overwrite – Implements sequential overwriting with random data, binary zeros, and binary ones to permanently destroy data beyond forensic recovery

2. SHA-256 Cryptographic Verification – Calculates and stores unique file hash before wiping, providing verifiable digital fingerprint as proof of file existence

3. Free Space Wiping – Cleans freed disk sectors with zeros after deletion to prevent slack space recovery attacks

4. Comprehensive JSON Audit Logging – Records timestamps, file paths, sizes, hash values, and pass completion status for complete accountability and compliance

5. Parallel Processing Engine – Uses Thread Pool Executor for concurrent file operations, achieving 60-70% faster wiping speeds than traditional tools

6. Intuitive PyQt5 Graphical Interface – Provides simple file/folder selection, preview functionality, real-time progress bars, and clear confirmation dialogs

7. Buffer Pooling Memory Optimization – Reuses fixed-size buffers and processes files in chunks to maintain constant memory usage below 50MB

8. Standalone Executable Packaging – Bundled as single .exe file using PyInstaller, requiring no Python installation on target Windows systems

9. Protected System File Validation – Blocks accidental deletion of critical operating system folders like Windows, Program Files, and system32

10. Error Handling and Graceful Recovery – Continues processing remaining files when individual files fail, with detailed error logging for troubleshooting

11. Forensic Tool Resistance – Tested against Recuva, PhotoRec, and TestDisk with zero data recovery after wiping completion

12. Cross-Version Windows Compatibility – Runs on Windows 7, 8, 10, and 11 without additional configuration or dependencies

PSEUDO CODE:

Begin

Initialize GUI

While app runs:

If file selected:

Store path

If wipe clicked:

Confirm

Calculate SHA-256 hash

For pass = 1 to 3:

If pass 1: Write random

If pass 2: Write zeros

If pass 3: Write ones

Delete file

Wipe free space

Save logs

Show success

If cancel clicked:

Stop process

End while

Stop

SIMULATION RESULTS :

The system was tested on 500 files totaling 50GB across different storage media including SSD, HDD, and USB drives. A 1GB file was completely wiped in 21 seconds using 4 parallel threads, achieving 65% faster performance compared to traditional sequential wiping tools which took 60 seconds for the same operation.

Forensic recovery software including Recuva, PhotoRec, and TestDisk were used to attempt data recovery after wiping. None of these tools were able to recover any original file content, confirming that the three-pass overwrite with random data, zeros, and ones permanently destroys all data traces.

Memory consumption remained constant at approximately 45MB throughout all operations regardless of file size, proving the effectiveness of buffer pooling and chunk-based processing. The system successfully handled folders containing up to 10,000 files without crashing or performance degradation.

All 500 test operations were logged with accurate timestamps, SHA-256 hash values, and pass completion status.

CONCLUSION AND FUTURE WORK :

The Secure File Wiping System successfully implements DoD 5220.22-M three-pass overwrite with SHA-256 verification and comprehensive logging, making data permanently unrecoverable even by forensic tools. The application provides an intuitive GUI, 65% faster performance through parallel processing, and standalone executable deployment, offering both individuals and organizations a reliable solution for verifiable data.

REFERENCES :

1. National Institute of Standards and Technology. "Guidelines for Media Sanitization." NIST Special Publication 800-88 Revision 2, September 2025.

2. Reardon, Joel. "Secure Data Deletion." Information Security and Cryptography Series, Springer, 2016.

3. Oh, Dong Bin, et al. "Forensic analysis and evaluation of file-wiping applications on Android OS." Journal of Forensic Sciences, vol. 71, no. 1, 2025.

4. Gilbert, Chris, and Mercy Gilbert. "Exploring Secure Hashing Algorithms for Data Integrity Verification." SSRN Electronic Journal, May 2025.

5. Bhat, Wasim Ahmad. "Achieving Efficient Purging in Transparent per-file Secure Wiping Extensions." In Emerging Research in Computing and Information Technology, IGI Global, 2015.

6. Wright, Craig, et al. "Overwriting Hard Drive Data: The Great Wiping Controversy." Information Systems Security, vol. 17, no. 4, 2008, pp. 227-237.

7. Jang, Eun-Jin, and Seung-Jung Shin. "A Proposal on Data Modification Detection System using SHA-256 in Digital Forensics." Korea Science, 2021.

8. Wei, Michael, et al. "Reliably Erasing Data from Flash-Based Solid State Drives." Proceedings of the 9th USENIX Conference on File and Storage Technologies (FAST), 2011, pp. 105-117.

9. Garfinkel, Simson L., and Abhi Shelat. "Remembrance of Data Passed: A Study of Disk Sanitization Practices." IEEE Security & Privacy, vol. 1, no. 1, 2003, pp. 17-27.

10. Conlan, K., Baggili, I., and Breitinger, F. "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy." Digital Investigation, vol. 18, 2016, pp. S66-S75.