Chapter 4
Integrated Multimodal Redaction Architecture With Reversible Cryptographic Obfuscation

Anshik Kumar Tiwari
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India

Brindha Subburaj
http://orcid.org/0000-0003-2173-5228
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India

ABSTRACT

This work proposes a combined multimodal redaction framework that mitigates the fundamental drawbacks of traditional document anonymization methods. In healthcare, like many other domains such as legal, finance, and government sectors, traditional redaction relies heavily on manual processes that cause permanent data loss through irretrievable deletion of sensitive content. Once information is redacted using these conventional approaches, there is no way to recover it when access is required again, or it loses its utility in encrypted form. A patient's clinical report may contain personal information such as name, age, blood group, gender and even payment details. To address this, we propose an intelligent framework capable of handling diverse inputs: text in different formats, fonts, images with varying resolutions and aspect ratios; and mixed document types. The framework

DOI: 10.4018/979-8-3373-7426-0.ch004

encrypts sensitive data using keys provided by one or more authorities. It is designed to manage the complexity of real-world medical documentation, while maintaining strong security guarantees and reversibility.

1. INTRODUCTION

Between 2007 and 2015, WakeMed Health and Hospitals, a major healthcare system in North Carolina, filed thousands of documents in bankruptcy court to recover unpaid medical bills. The organization operated under the belief that its actions were in line with established procedures. What they didn't realize, or perhaps didn't care enough to verify, was that their "redacted" documents left Social Security numbers, full dates of birth, and detailed medical information completely exposed in filings that were publicly accessible to anyone with an internet connection through the federal court's PACER electronic records system. The staff member responsible for these filings had annual HIPAA training for 33 years but had never had a single review on how to properly perform their task of document "redaction" when filing for bankruptcy, was unsupervised, had no system in place to audit her work, and was incredibly ignorant on how crucial it was to follow these protocols - an egregious error that ultimately has already set them back an astonishing $70,000 for punitive damages, another almost $60,000 for attorneys' fees, mandatory breach notification letters to 6,861 patients with an offer of credit monitoring, as well as five years of compliance reports with the court on their effort to properly mitigate their breach. The Houston Chronicle documented another large health system's embarrassment when it published personal, pointable-to-the-patient identifying characteristics with a press release, turning what easily could have remained anonymous reporting on a public health concern into an impermissible disclosure of protected health information so "sensitive that it would reasonably be condensed with time, place, and context to direct particular attention to diagnosis, treatment, internal pessoa," making this breach much more than simple public reporting but an impermissible breach of protected health privacy guidelines.

The same pattern appears across healthcare institutions: many traditional methods of protecting patient privacy no longer work. Records are manually redacted in ways that still leave the underlying text readable, security measures lag evolving threats, and permanent deletion sometimes removes information that clinicians, researchers, or legal teams may later need. As a result, organizations face a difficult trade-off. On one hand, overly aggressive redaction can render records unusable when they're needed for legitimate purposes. On the other, weak safeguards risk exposing sensitive data—leading to breaches, regulatory penalties, and lasting harm to patient trust. The same pattern keeps coming up across healthcare institutions, and