

Multimedia Security- 2nd Course-PHD2025

Lecturer: Prof. Bashar AIEsawi

Email: bmn774@uomustansiriyah.edu.iq

Official Website: ([Click Here](#))

Personal Website: ([Click Here](#))

Time: SUN: 12:00 PM-

WhatsApp Group: (Here)



Course Name: Multimedia Security

Target Audience: PhD Students

Course Description:

This course explores the principles and techniques of securing multimedia data, including images, audio, and video. It focuses on cryptographic methods, watermarking, steganography, and authentication protocols. Students will analyze real-world applications, security threats, and emerging trends.

Course Objectives:

1. Understand the fundamental concepts of multimedia security.
2. Analyze various security threats and their countermeasures in multimedia systems.
3. Explore and apply techniques like steganography, watermarking, and cryptography to secure multimedia content.
4. Investigate forensic techniques for multimedia integrity and authenticity.
5. Explore emerging technologies and trends in multimedia security.

Course Plan: Week-by-Week Breakdown

Week 1: Introduction to Multimedia Security

- Overview of multimedia (images, audio, video).
- Security threats and challenges.
- The role of cryptography in multimedia security.
- Reading: Chapter 1

Week 2: Basic Cryptographic Techniques

- Fundamentals of encryption and decryption.
- Symmetric vs. asymmetric cryptography in multimedia.
- Introduction to AES and RSA.
- **Exercise: Implementing AES for image encryption.**
- Reading: Chapter 2

Week 3: Image and Video Encryption Techniques

- Selective encryption techniques for images and videos.
- Compression standards and their impact on encryption.
- **Case Study: H.264 video encryption.**
- Reading: Chapter 3

Week 4: Principles of Steganography

- Steganography fundamentals and applications.
- Spatial vs. frequency domain techniques.
- **Exercise: LSB-based image steganography.**
- Reading: Chapter 4,5.

Week 5: Fundamentals of Digital Watermarking

- Basics and importance of watermarking.
- Types: visible, invisible, fragile, robust.
- **Exercise: Embedding and detecting watermarks in images.**
- Reading: Chapter 6

Week 6: Watermarking Techniques for Videos and Audio

- Temporal and spatial watermarking in videos.
- Watermarking techniques for audio signals.
- **Case Study: Copyright protection using watermarking.**
- Reading: Chapter 7

Week 7: Midterm Exam and Project Proposal Presentation

- Midterm exam covering weeks 1–7.
- Presentation of project proposals for multimedia security applications.

Week 8: Multimedia Authentication and Integrity

- Techniques for ensuring multimedia authenticity.
- Hash functions and digital signatures.
- **Exercise: Implementing HMAC for multimedia authentication.**
- Reading: Chapter 8

Week 9: Multimedia Forensics

- Fundamentals of forensic analysis for multimedia.
- Forgery detection and tampering analysis.
- **Case Study: Deepfake detection techniques.**
- Reading: Chapter 9

Week 10: Real-Time Multimedia Security Challenges

- Challenges in securing live multimedia streams.
- Secure RTP (SRTP) and its applications.
- **Case Study: Securing VoIP communications.**
- Reading: Chapter 10

Week 11: Emerging Technologies in Multimedia Security

- Blockchain applications for DRM.
- AI and machine learning for securing multimedia.
- **Exercise: Using machine learning for anomaly detection in multimedia.**
- Reading: Chapter 11

Week 12: Privacy and Legal Aspects of Multimedia Security

- Privacy concerns in multimedia sharing.
- Legal frameworks for digital rights management.
- **Case Study: GDPR and its implications for multimedia security.**
- Reading: Chapter 12

Week 13: Student Project Presentations

- Final project presentations by students.
- Peer feedback and discussion.
- Activity: Evaluate real-world applicability of each project.

Week 14: Final Exam and Course Wrap-Up

- Comprehensive final exam covering all topics.
- Discussion of future trends and research opportunities in multimedia security.

Assessment Components:

1. **Minimum 2 Exam: %**
2. **Final Exam: %**
3. **Seminars and Activity: 20%**



Required Textbook:

Multimedia Security: Watermarking, Steganography, and Forensics by Frank Y. Shih (CRC Press).

Suggested Textbook:

Title: "Multimedia Security: Watermarking, Steganography, and Forensics"

Authors: Frank Y. Shih

Publisher: CRC Press

Edition: Latest available

Advanced Research Reports Topics in Multimedia Security

1. **Foundations of Multimedia Security and Cyber Threats:**
 - Overview of multimedia vulnerabilities in cyberspace
 - Security challenges in digital content protection
 - Role of cryptographic mechanisms in securing multimedia
2. **Steganography and Covert Communication in Cybersecurity:**
 - Principles and methodologies of steganography
 - Adversarial steganalysis and detection techniques
 - Applications in secure communication and cyber warfare
3. **Digital Watermarking for Cybersecurity and Intellectual Property Protection:**
 - Robust watermarking techniques against cyber-attacks
 - Watermarking in blockchain-based digital rights management (DRM)
 - Case studies on forensic watermarking in cybersecurity investigations
4. **Encryption Techniques for Secure Multimedia Transmission in Cyber Networks:**
 - Comparative analysis of AES, RSA, and post-quantum encryption for multimedia
 - Challenges in real-time encryption for streaming services
 - Secure video conferencing and VoIP encryption methods
5. **Multimedia Forensics and Deepfake Detection in Cybersecurity:**
 - AI-powered forensics for digital content authentication
 - Deepfake generation and countermeasure techniques
 - Cyber forensic tools for image, video, and audio integrity verification
6. **Emerging Trends: AI and Blockchain in Multimedia Cybersecurity:**
 - Machine learning for real-time anomaly detection in multimedia systems
 - Blockchain-based content protection and decentralized DRM
 - Legal and ethical considerations in AI-driven multimedia security

Helping Tools:

Research Report Template (Scopus & Clarivate Standard)

Title Page

- Title: (Concise and informative)
- Author(s): (Full name, affiliation, and email)
- Abstract: (150–250 words summarizing objectives, methods, results, and conclusion)
- Keywords: (4–6 keywords relevant to the study)

1. Introduction

- 1.1 Background and Motivation (Explain the significance of the research topic and its relevance.)
- 1.2 Problem Statement (Define the core research problem.)
- 1.3 Research Objectives (List the main aims of the study.)
- 1.4 Research Questions/Hypotheses (Include key research questions or hypotheses.)
- 1.5 Scope and Limitations (Define what is covered and what is excluded.)
- 1.6 Structure of the Report (Outline the organization of the paper.)

2. Literature Review

- 2.1 Overview of Existing Research (Summarize key studies related to the topic.)
- 2.2 Theoretical Framework (Explain any models or theories used.)
- 2.3 Gap Analysis (Identify gaps in past research and justify the study.)
- 2.4 Comparison Table (Optional) (Create a table summarizing previous work.)

3. Methodology

- 3.1 Research Design (Describe whether the study is qualitative, quantitative, experimental, etc.)
- 3.2 Data Collection Methods (Explain how data was gathered, e.g., surveys, experiments, case studies.)
- 3.3 Data Analysis Techniques (Describe statistical or analytical methods used.)
- 3.4 Ethical Considerations (Discuss ethical concerns such as data privacy and consent.)
- 3.5 Tools & Technologies Used (List software, programming languages, or instruments applied.)

4. Results and Discussion

- 4.1 Results Presentation (Display findings using tables, graphs, or figures.)
- 4.2 Interpretation of Results (Explain what the results indicate.)
- 4.3 Comparison with Previous Research (Compare findings with past studies.)
- 4.4 Theoretical and Practical Implications (Discuss the study's impact on research and industry.)
- 4.5 Limitations (Acknowledge constraints and potential biases.)

5. Conclusion and Future Work

- 5.1 Summary of Findings (Highlight key contributions.)
- 5.2 Practical Applications (Describe real-world implications.)
- 5.3 Future Research Directions (Suggest areas for further investigation.)

6. References: (Follow IEEE, APA, or Harvard referencing format.)

8. Appendices (If Needed)

- Additional tables, raw data, or extended explanations that do not fit in the main text.

U can use this template for final version please with the following Info.:

https://mjs.uomustansiriyah.edu.iq/index.php/MJS/libraryFiles/downloadPublic/64/Template_MJS_24.docx

First Name: Student NAME.

Corresponding Author Name: Bashar M. Nema

Email: bmn774@uomustansiriyah.edu.iq

Finally, Please Register your Information Using the following QR-Code:

