Subject Description Form

Subject Code	DSAI4201
Subject Title	Data Protection and Security
Credit Value	3
Level	4
Pre-requisite/ Co-requisite/ Exclusion	**Pre-requisite:** COMP1011/COMP1012/ENG2002
Objectives	The objectives of this subject are to: 1. understand the fundamental technologies for data security and forensics, in particular, the basic techniques for digital watermarking and cryptography; 2. introduce biometrics-based security technologies using unimodal and multimodal authentication; and 3. learn real-world usage and performance evaluation of biometrics systems in the domain of data protection and security.
Intended Learning Outcomes	Upon completion of the subject, students will be able to: *Professional/academic knowledge and skills* (a) Develop a critical understanding of challenges for data protection and planning for data security; (b) Get familiar with the real-world techniques for data protection, including hash functions and digital signature; (c) Comprehend and appreciate digital watermarking techniques for copyright protection, data ownership assertion, and digital content distribution; (d) Identify critical issues for real-world biometrics systems relating to their performance and applications for the high level of data protection; (e) Have an in-depth understanding of unimodal and multimodal biometrics systems for different security applications. *Attributes for all-roundedness* (f) Communicate effectively with project presentations and technical reports; (g) Learn independently for problem-solving and solution-seeking for various applications; and (h) Appreciate the broader perspectives of digital content protection and the societal impact of biometrics security.

Subject Synopsis/ Indicative Syllabus	Topic
	1. Introduction to Data Security Data Security Environment, Developing Data Security Plan, Dimensions of Data Security, E-Security Threats and Vulnerabilities, Web Bots, Bot Response Methods, Encryption Techniques.
	2. Secured Online Transactions Public Key Infrastructure, Certification Authority, Digital Signature, Hash Function and Authentication, Digital Envelope.
	3. Data Protection using Digital Watermarking Digital Watermarking Fundamentals, Desirable Properties of Watermarking Techniques, Robust and Fragile Watermarking, Spatial Domain Watermarking, Frequency Domain Watermarking, Watermark Extraction, Steganography and Data Hiding.
	4. Digital Copyright Protection and Data Privacy Copying Prevention and Control, Ownership Assertion, Online Digital Content Distribution and Security, Fingerprint Embedding for Multimedia Content and Attacks, Introduction to Data Protection Standards, and Privacy Laws such as GDPR and HIPPA.
	5. Introduction to Biometrics Security Introduction to Biometrics, Desirable Properties of Biometrics for Practical Systems, Strengths and Weaknesses of different biometric patterns, Behavioral Biometrics, Privacy Concerns and Social Challenges for Biometrics.
	6. Fundamental Techniques Biometrics data acquisition and biometrics database; the related image processing and pattern recognition technologies, including digital image and signal representation, pattern extraction, and classification.
	7. Performance Evaluation for Biometrics Systems Biometric Verification and Error Rates, Failure to Acquire, False Match Rate and False Non-Match Rate, Receiver Operating Characteristics, Equal Error Rate, Open Set and Closed Set Performance Evaluation, Cumulative Match Characteristics, and Rank-one Accuracy, False Positive Identification, and False Negative Identification Rates.
	8. Introduction to Unimodal and Multimodal Systems Introduction to popular unimodal biometrics systems using fingerprint, palmprint, iris, and face. Standards and deployment scenario for data security, Limitations of Unimodal Systems, Introduction to Multimodal Biometric Systems and Modes of Operations, Feature Level, Score Level, and Decision Level Fusion.

<table>
<tr><td><b>Teaching/ Learning Methodology</b></td><td>The course material will be delivered as a combination of lectures, tutorials, and small group projects. Students will get familiar with basic concepts and technologies of data security, biometric systems, and applications.</td></tr>
<tr><td><b>Assessment Methods in Alignment with Intended Learning Outcomes</b></td><td>
<table>
<tr><th rowspan="2">Specific assessment methods/tasks</th><th rowspan="2">% weighting</th><th colspan="8">Intended subject learning outcomes to be assessed</th></tr>
<tr><th>a</th><th>b</th><th>c</th><th>d</th><th>e</th><th>f</th><th>g</th><th>h</th></tr>
<tr><td><b>Continuous Assessment</b></td><td><b>55%</b></td><td colspan="8"></td></tr>
<tr><td>1. Assignments</td><td>10%</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>2. Lab exercises</td><td>10%</td><td></td><td></td><td>✓</td><td>✓</td><td></td><td></td><td></td><td>✓</td></tr>
<tr><td>3. Project</td><td>10%</td><td>✓</td><td></td><td></td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>4. Mid-term</td><td>25%</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td></td><td></td><td>✓</td><td>✓</td></tr>
<tr><td><b>Examination</b></td><td><b>45%</b></td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Total</td><td>100%</td><td colspan="8"></td></tr>
</table>
<p>Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:</p>
<p>The examination and assignments are designed to evaluate the students’ understanding of data security-related concepts and applications. The project, on the other hand, is designed to evaluate the students’ practical skills in solving biometric security-related real-world problems.</p>
</td></tr>
<tr><td><b>Student Study Effort Expected</b></td><td>
<table>
<tr><td colspan="2">Class contact:</td></tr>
<tr><td>▪ Lecture/Tutorial/Lab</td><td>39 Hrs.</td></tr>
<tr><td colspan="2">Other student study effort:</td></tr>
<tr><td>▪ Self-learning and class preparation</td><td>26 Hrs.</td></tr>
<tr><td>▪ Assignment, Project, Quiz, and Examination</td><td>52 Hrs.</td></tr>
<tr><td>Total student study effort</td><td>117 Hrs.</td></tr>
</table>
</td></tr>
</table>

Reading List and References	**Reference:** 1. Frank Y. Shih, Digital Watermarking and Steganography : Fundamentals and Techniques, 2nd Edition, Taylor & Francis, 2017. 2. R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, Guide to Biometrics, Springer, ISBN 978-1-4757-4036-3, 2013 3. N. F. Johnson, Z. Duric, S. Jajodia, Information Hiding: Steganography and Watermarking - Attacks and Countermeasures, Springer Science & Business Media, 2012. 4. A. K. Jain, A. Kumar, Biometrics on Next Recognition, An Overview, Second Generation Biometrics, Springer, 2010. 5. IEEE Transaction on Pattern Analysis and Machine Intelligence. 6. IEEE Transaction Biometrics Behavior and Identity ScienceHislop, D., *Knowledge Management in Organizations: A Critical Introduction*, Oxford University Press, 2009. 7. Zilli, A., Damiani, E., and Ceravolo, P., *Semantic Knowledge Management: An Ontology-Based Framework*, Information Science Reference, 2009. 8. Articles on knowledge, information, and decision support systems.