Subject Description Form

Subject Code	COMP4134
Subject Title	Biometrics and Security
Credit Value	3
Level	4
Pre-requisite	AMA1104 Introductory Probability or HKDSE Maths Extended Module or equivalent subjects COMP3422 Creative Digital Media Design or equivalent subjects.
Co-requisite/ Exclusion	Nil
Objectives	The objectives of this subject are to: 1. understand the fundamental technologies for e-security, in particular the basic technologies for digital watermarking and cryptography for various applications; 2. introduce biometric computing knowledge and methods; and 3. learn some basic biometrics systems with real case studies
Intended Subject Learning Outcomes	**Upon completion of the subject, students will be able to:** *Category A: Professional/academic knowledge and skills* (a) understand fundamental issues and challenges for e-security; (b) get familiar with the basic techniques for cryptography including conventional encryption, public-key cryptography, message authentication, hash functions and digital signature; (c) comprehend and appreciate digital watermarking applications for data security; (d) recognise physical and behaviour biometric characteristics for human identification; (e) have a good understanding on biometrics technologies for different security applications; *Category B: Attributes for all-roundedness* (f) communicate effectively with project presentation and technical reports; and (g) learn independently for problem solving and solution seeking for various applications.
Subject Synopsis/ Indicative Syllabus	**Topic** **1. Introduction to Information Security** Why is information security important? What is information security concerned? How to achieve information security – basic concepts, techniques and applications. **2. Conventional Encryption Technology** Classic and modern techniques for encryption, stream ciphers and block ciphers, DES (Data Encryption Standard).

	3. Public-key Cryptography and Message Authentication public-key cipher, classes of public-key algorithms, message authentication **4. Digital Watermarking for Information Security** watermarking concept, watermarking definition, problems with watermarking,watermark attacks, classification of watermarking, applications of watermarking (copyright protection, authentication and integrity checking, hidden annotation, secure and invisible communication **5. Introduction to Biometrics and Authentication** Why biometrics? What about biometrics? How to design biometric systems? Biometrics definitions and notations; biometric applications; information security; security technologies and systems; authentication. **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; biometrics system performance using error rates and plots. **7. Typical Physical Biometrics** Basic physical characteristics of biometrics; introduction tobiometrics systems using physiological features (such as fingerprint, palmprint, finger knuckle, iris, face, etc.). **8. Typical Behavioral Biometrics** Basic behavioural characteristics of biometrics; some basic introduction of behavioural biometrics systems (such as voice, signature, and gait recognition, etc.). **9. Multi-Biometrics and Applications** Security application: Internet/Intranet; e-commerce; banking services; immigration and naturalisation service; computer systems; physical access; telephone systems; time, attendance and monitoring. Case Study: Electronic security and biometric applications.
Teaching/Learning Methodology	The course material will be delivered as a combination of lectures, tutorials and small group project. Students will get familiar with basic concepts and technologies of network security, biometric systems and applications.

<table>
<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="7">Intended Subject Learning Outcomes to be Assessed</th></tr>
<tr><td>a</td><td>b</td><td>c</td><td>d</td><td>e</td><td>f</td><td>g</td></tr>
<tr><td>1. Continuous Assessment</td><td>60%</td><td colspan="7"></td></tr>
<tr><td>• Assignments</td><td></td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>• Lab exercises</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>• Project</td><td></td><td>✓</td><td></td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>• Mid-term</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>2. Examination</td><td>40%</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="7"></td></tr>
</table>
</td>
</tr>
<tr>
<td><b>Student Study Effort Expected</b></td>
<td>
<table>
<tr><td><b>Class contact (time-tabled):</b></td><td></td></tr>
<tr><td>• Lecture</td><td>39 Hrs.</td></tr>
<tr><td><b>Other student study effort:</b></td><td></td></tr>
<tr><td>• Homework</td><td>25 Hrs.</td></tr>
<tr><td>• Project</td><td>41 Hrs.</td></tr>
<tr><td><b>Total student study effort:</b></td><td><b>105 Hrs</b>.</td></tr>
</table>
</td>
</tr>
<tr>
<td><b>Reading List and References</b></td>
<td>
<b>Reference Books:</b>
1. R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, <i>Guide to Biometrics</i>, Springer 2004
2. A. K. Jain, A. Kumar, Biometrics on Next Recognition, An Overview, <i>Second Generation Biometrics</i>, Springer, 2010.Frank Y. Shih, Digital Watermarking and Steganography: Fundamentals and Techniques, 2^{nd} Edition, Taylor & Francis, 2017. A. Kumar, <i>Contactless 3D Fingerprint Identification</i>, Springer, 2018.IEEE Transaction on Pattern Analysis and Machine Intelligence.
3. IEEE Transaction Biometrics Behavior and Identity Science
</td>
</tr>
</table>