Subject Description Form

Subject Code	COMP4134
Subject Title	Biometrics and Security
Credit Value	3
Level	4
Pre-requisite	Nil.
Objectives	• To understand the fundamental issues and technologies for network security, in particular the basic technologies for cryptography and various applications • To introduce biometric computing knowledge and methods • To learn some basic biometrics systems with real case studies
Intended Learning Outcomes	Upon completion of the subject, students will be able to: *Professional/academic knowledge and skills* (a) understand fundamental issues and challenges for network security (b) get familiar with the basic techniques for cryptography including conventional encryption, public-key cryptograph, message authentication, hash functions and digital signature (c) understand the key issues and importance of biometric systems for security concerns; (d) recognize physical and behavior biometric characteristics; (e) apply biometric technology for different security applications. *Attributes for all-roundedness* (f) communicate effectively with project presentation and technical reports; (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 Satndard). 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; basic PCA/LDA approaches of automated biometrics identification and verification. 7. Typical physical biometrics Basic physical characteristics of biometrics; some basic introduction of physical biometrics systems (such as fingerprint, palm-print, finger, hand, face, iris, and face etc.). 8. Typical behavial biometrics Basic behavial characteristics of biometrics; some basic introduction of behavial biometrics systems (such as voice, signature, and gesture recognition, etc.). 9. Multi-biometrics and applications Security application: Internet/Intranet; e-commerce; banking services; immigration and naturalization service; computer systems; physical access; telephone systems; time, attendance and monitoring. Case Study: Network 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.

Assessment Methods in Alignment with Intended Learning Outcomes

Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed (Please tick as appropriate)						
		a	b	c	d	e	f	g
1. Assignments	60%	✓	✓	✓	✓	✓	✓	✓
2. Lab exercises								
3. Project		✓		✓	✓	✓	✓	✓
4. Mid-term								
5. Examination	40%	✓	✓				✓	✓
Total	100 %							

Student Study Effort Expected

Class contact:	
▪ Lecture	39 Hrs.
▪ Tutorial	0 Hrs.
Other student study effort:	
▪ Homework	25 Hrs.
▪ Project	41 Hrs.
Total student study effort	105 Hrs.

Reading List and References

Reference Books:

1. Stallings, W. *Cryptography and Network Security: Principles and Practice*, Third Edition, Prentice Hall, 2003.
2. Zhang, D., *Automated Biometrics: Technologies & Systems*, Kluwer Publisher, 2000.
3. Zhang, D., (Ed.), *Biometric Solutions for Authentication in an e-World*, Kluwer Publisher, 2002.
4. Jain, et al. (Eds.), *Biometrics: Personal Identification in Networked Society*, Kluwer Publisher, 1999.
5. Sid-Ahmed, M.A., *Image Processing, Theory, Algorithms, & Architectures*, McGraw-Hill, 1995.
6. Abrams, M.D., Jajodia, S., and Podell, H.J., *Information Security: An Integrated Collection of Essays*, IEEE Computer Society Press, 1994.
7. Derek Atkins, et al., *Internet Security Professional Reference*, Second Edition. New Riders Publishing, 1997.
8. Russell, D., *Computer Security Basics*, O'Reilly & Associates, 1991.
9. Zhang, D. and Jain, A.K. (Eds.), *Proc. First International Conference on Biometric Authentication (ICBA)*, 800pp, Springer Verlag, LNCS 3072, 2004
10. Zhang, D. and Jain, A.K. (Eds.), *Advances in Biometrics*, International Conference - ICB2006, Springer Verlag, LNCS 3832, 2006.
11. IEEE Transaction on Pattern Analysis and Machine Intelligence.
12. IEEE Transaction on Image Processing.