1.	Name of Course/Module/Subject	Digital Watermarking
2.	Course/Subject Code	TWM 3431
3.	Status of Subject	Elective for B.IT Security Technology
4.	MQF Level/Stage	Bachelor – MQF Level 6
5.	Version	Date of previous version: June 2012 Date of current version: June 2014
6.	Pre-Requisite	TMA1211 Discrete Mathematics and Probability, AND TAC3121 Applied Cryptography
7.	Name(s) of academic/teaching staff	Low Cheng Yaw Tee Connie Pang Ying Han Ooi Shih Yin
8.	Semester and Year offered	Trimester 1, Year 3

9. Objective of the course/module/subject in the programme :

The objective of this subject is to apply digital watermarking as an authentication tool for distribution of content over the Internet. This is especially due to the proliferation of high-capacity, digital recording devices which have fuelled increased concerns over copyright protection of content.

10. Justification for including the subject in the program :

Digital watermarking is a sub-discipline of Applied Cryptography (or best known as Information Hiding). Watermarks are a valuable mechanism for protecting audio, video, and data and they are also becoming an important tool in facilitating e-commerce. Any company that is serious about safely protecting and distributing their content and products will need to know about digital watermarks.

11.

Subject Learning Outcomes :		Domain	Level
LO1	Distinguish digital watermarking from other related fields.	Cognitive	Level 4
LO2	Explain different types of watermarking applications and watermarking frameworks.	Cognitive	Level 2
LO3	Describe digital watermarking systems in terms of imperceptibility, robustness, and watermark.	Cognitive	Level 6
LO4	Design digital watermarking systems according to application domains.	Cognitive	Level 5

12. Mapping of Learning Outcomes to Programme Outcomes :

Learning Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9
LO1	X						X	X	
LO2	X						X	X	

	LO3	X						X	X	
	LO4	X						X	X	
	Percentage	33.3	0.0	0.0	0.0	0.0	0.0	33.3	33.3	0.0

13. Assessment Methods and Types :

Method and Type	Description/Details	Percentage
Mid Test	Written test	20%
Assignment	Research papers and report	15%
Quizzes	Written quizzes	5%
Final Examination	Written examination	60%

14. Mapping of Assessment Components to Learning Outcomes:

Assessment Components	%	LO1	LO2	LO3	LO4
Mid Test	20	23.5	20	20	
Assignment	15		15	15	100
Quizzes	5	5.9	5	5	
Final Examination	60	70.6	60	60	
Total	100	100	100	100	100

15. Details of Subject:

Topics	Mode of Delivery	
	Lecture	Tutorial
Introduction Information Hiding, Stenography, and Watermarking. History of Watermarking. Importance of Digital Watermarking.	2	1
Applications and Properties Embedding Effectiveness. Fidelity. Data Payload. Blind or Informed Detection. False Positive Rate. Robustness. Security. Cipher and Watermark Keys. Modification and Multiple Watermarks. Cost. Evaluating Watermarking Systems.	3	1
Models of Watermarking Watermarking as Communication with Side Information at the Transmitter. Watermarking as Multiplexed Communications. Geometric Models of Watermarking. Distribution and Regions in Media Space. Marking Spaces. Correlation-Based Watermarking Systems. Linear Correlation. Normalized Correlation. Correlation Coefficient.	4	2
Basic Message Coding Direct Message Coding. Multi-Symbol Message Coding. The Problem with Simple Multi- Symbol Messages. Error Correction Coding. The Idea of Error-Correction Codes. Trellis Codes and Viterbi Decoding. Detecting Multi-Symbol Watermarks.	4	2

	Watermarking with Side Information Optimization with Respect to a Detection Statistic. Optimization with Respect to an Estimate of Robustness. Informed Encoding. Writing on Dirty Paper. A Dirty-Paper Code for a Simple Channel	3	2
	Robust Watermarking Approaches. Redundant Embedding. Spread Spectrum Coding. Embedding in Perceptually Significant Coefficients. Embedding in Coefficients of Known Robustness. Inverting Distortions in the Detector. Pre-inverting Distortions in the Embedder. Robustness to Valumetric Distortions.	4	2
	Watermark Security Security Requirements. Restricting Watermark Operations. Public and Private Watermarking Applications. Categories of Attack. Assumptions About the Adversary. Watermark Security and Cryptography. Cryptographic Tools. The Analogy Between Watermarking and Cryptography. Preventing Unauthorized Detection. Preventing Unauthorized Embedding. Preventing Unauthorized Removal.	2	1
	Content Authentication Exact Authentication. Fragile Watermarks. Embedded Signatures. Erasable Watermarks. Selective Authentication. Legitimate and Illegitimate Distortions. Semi-Fragile Watermarks. Embedded, Semi-Fragile Signatures. Tell-Tale Watermarks.	2	1
	Total	**24**	**12**

16.	Total Student Learning Time (SLT)	Face to Face	Total Guided and Independent Learning
	Lecture	24	24
	Tutorials	12	12
	Laboratory/Practical	0	0
	Presentation	2	6
	Assignment	0	10
	Mid Term Test	2	6
	Final Exam	2	15
	Quizzes	5 times	5
	Sub Total	42	78
	Total SLT	**120**	
17.	Credit Value	**120/40 = 3**	
18.	Reading Materials :		
	Textbook:	Reference Materials:	
	1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, The Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.	1. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann. 2. Bruce Schneier, (1996). Applied	

		Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley & Sons. 3. Warren G. Kruse II, Jay G. Heiser, (2001). Computer Forensics: Incident Response Essentials, Pearson.