OUTCOMES:

Upon completion of the course, the student will be able to

- Have a clear impression of the breadth and practical scope of digital image processing and have arrived at a level of understanding that is the foundation for most of the work currently underway in this field.
- Critically analyze the role of video in modern technologies.
- Implement basic image and video processing algorithms.
- Design and develop various applications that incorporates different techniques of Image and Video processing.
- Apply and explore new techniques in the areas of image and video Processing.

REFERENCES:

1. Rafael C.Gonzalez and Richard E.Woods, “Digital Image Processing”, Third Edition, Pearson Education, New Delhi, 2008,.
2. S.Sridhar, “Digital Image Processing”, Oxford University Press, New Delhi, 2011.
3. Al Bovik (Alan C Bovik, “The Essential Guide to Video Processing”, Academic Press, Second Edition, 2009.
4. A. Murat Tekalp, “Digital Video Processing”, Prentice Hall, 1995.
5. Oges Marques, “Practical Image and Video Processing Using MATLAB”, Wiley-IEEE Press, 2011.

CO	PO						PSO		
	1	2	3	4	5	6	1	2	3
1.	√		√	√			√	√	
2.	√		√	√			√	√	
3.	√		√	√			√	√	
4.	√		√	√		√	√	√	√
5.	√		√	√		√	√	√	√

CP5085 PRINCIPLES OF CRYPTOGRAPHY L T P C
3 0 2 4

OBJECTIVES:

- To understand the mathematical foundations of security principles.
- To appreciate the different aspects of encryption techniques.
- To understand various attacks present over encryption and authentications techniques.
- To understand the role played by authentication in security.
- To appreciate the current trends of security practices.

UNIT I CLASSICAL ENCRYPTION AND BLOCKCIPHERS 9+6

Classical Encryption – Substitution Cipher – One-time-pad Encryption – Block Ciphers – DES – Key Recovery Attacks on Block Ciphers – Iterated-DES and DESX – AES – Limitations of Key-recovery based Security.

UNIT II PSEUDO RANDOM FUNCTIONS AND SYMMETRIC ENCRYPTION 9+6

Random Functions – Permutations – Pseudo Functions – Pseudo-random Permutations – Modelling Blockciphers – Security Against Key Recovery – The Birthday Attack – Symmetric Encryption Schemes – Chosen Plaintext Attacks – Semantic Security – Security of CTR and CBC – Chosen Ciphertext Attack.

UNIT III HASH FUNCTIONS AND MESSAGE AUTHENTICATION 9+6

Hash Function SHA1 – Collision resistant Hash Functions – Collision Finding Attacks – Onewayness of Collision resistant Hash Functions – MD Transform – Syntax for message Authentication – PRF as a MAC Paradigm – CBC MAC – Universal-hashing Approach – Authenticated Encryption.

UNIT IV NUMBER THEORY AND ASYMMETRIC ENCRYPTION 9+6

Computational Number Theory – Number Theoretic Primitives – Diffie Hellman Problem – Asymmetric Encryption Schemes – Hybrid Encryption – ElGamal Scheme and its Variants – Homomorphic Encryption – Digital Signatures

UNIT V SECURITY PRACTICES AND ADVANCED TOPICS 9+6

Electronic Mail Security – IP Security – Digital Cash – Schnorr's Identification Protocol and Signature – Blind Signature – Distributed Ledger and Bitcoin –– Secret Sharing – Shamir Threshold Scheme – Security in Routing – Mixnet

TOTAL : 45 +30 = 75 PERIODS

OUTCOMES:

Upon completion of the course, the student will be able to

- Demonstrate the various classical encryption techniques and the adversary capabilities.
- Apply computational secrecy and semantic security to find out the probability of how strong are the security schemes.
- Illustrate the various MAC and HASH functions and apply the Birthday attack over Hash.
- Apply number theory in public key encryption techniques.
- Analyze the application of cryptography for secure E-Commerce and other secret transactions.

REFERENCES:

1. MihirBellare and Phillip Rogaway, "Introduction to Modern Cryptography", 2005.
2. Jonathan Katz and Yehuda Lindell, "Introduction to Modern Cryptography ",Chapman and Hall/CRC Press Second Edition,2015.
3. Hans Delfts and Helmut Knebl, "Introduction to Cryptography – Principles and Applications", Springer, Third Edition by,2015.

CO	PO						PSO		
	1	2	3	4	5	6	1	2	3
1.	√		√				√	√	
2.	√		√	√			√	√	
3.	√		√				√	√	
4.	√		√				√	√	
5.	√		√	√			√	√	√