Declaration

I hereby declare that the work presented in this thesis entitled *Novel and Robust Methodologies on Image Security* submitted to the Indian Institute of Technology Jodhpur in partial fulfillment of the requirements for the award of the degree of *Doctor of Philosophy*, is a bonafide record of the research work carried out under the supervision of *Dr. Gaurav Bhatnagar*. The contents of this thesis in full or in parts, have not been submitted to, and will not be submitted by me to, any other Institute or University in India or abroad for the award of any degree or diploma.

Satendra Pal Singh
PG201383504

Certificate

This is to certify that the thesis titled *Novel and Robust Methodologies on Image Security*, submitted by *Satendra Pal Singh (PG201383504)* to the Indian Institute of Technology Jodhpur for the award of the degree of *Doctor of Philosophy*, is a bonafide record of the research work done by him under my supervision. To the best of my knowledge, the contents of this report, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Dr. Gaurav Bhatnagar
Ph.D.Thesis Supervisor

Acknowledgments

First and foremost, I am thankful to God for the blessings he has bestowed upon me and for giving me strength and courage to complete this work. I am thankful to my parents who taught me many great things in simple ways that helped me for surviving during weak moments of my life.

I thank my Ph.D. Thesis Supervisor, *Dr. Gaurav Bhatnagar*, for introducing me to the area of technical writing and its nuances. In the process, i have learnt many technical and non-technical aspects of professional work. I am grateful to him for his help and patience as well as for constantly reminding me to be perfect even in the little things that i do each day. Also, i am indebted to the Members of the Doctoral Committee, *Dr. Puneet Sharma, Dr. A.K. Tiwari* and *Dr. Chiranjoy Chattopadhyay*, for their enthusiastic and continued guidance during the research work. My sincere thanks also goes to Indian Institute of Technology Jodhpur for providing necessary infrastructure and resources to accomplish my thesis work.

I would like to give thanks to my friend *Tushar Shinde*. I am greatful to him for his support during my Ph.D.. My stay at the Institute was a wonderful experience because of my seniors and friends, *Vishal Sharma, Rohit Kumar, Prashant Kumar, Ishan Varun, Ram nivas, Kumar Rahul and Alankar Agrawal* for all the liveliness they infused into the non-academic part of the days at IIT Jodhpur.

I acknowledge and thank my family, for the patience and love with which they ushered on me, and for bearing with me even when I was spending less time with them. They always guided me while I was facing moral break downs. I pay respects to my *family members* for all their *love, sacrifices and blessings*.

Satendra Pal Singh
Ph.D. Student

List of Figures

Figure	*Title*	*page*
1.1	A general framework of image hashing system.	3
1.2	A framework of image authentication using perceptual hash function.	7
1.3	A framework of content identification using perceptual hash function.	8
1.4	A General framework for image encryption and decryption.	9
1.5	A typical framework of secret key cryptosystem.	9
1.6	A typical framework public key cryptosystem.	10
1.7	a,e) Original images; b,f) Encrypted Images using raster; c,g) Encrypted Images using Zig-zag scan; d,h) Encrypted Images using hilbert scan.	11
1.8	Histograms of the original images and their encrypted versions.	12
1.9	A general framework for watermarking system.	14
1.10	Trade-off between the different characteristics of watermarking system.	15
1.11	Classification of watermarking techniques.	18
1.12	Experimental Images: a,e) Original images; b,d) Watermark images; e,g) Invisible watermarked images; d,h) Visible watermarked images.	19
2.1	Lifting wavelet decomposition and reconstruction	28
2.2	First-level lifting wavelet decomposition of an image and corresponding different sub-band.	29
2.3	Working process of arnold transformation	33
2.4	An illustration of the log-polar mapping as defined in Eqn. 2.26.	34
3.1	Experimental Images: (a) Cameraman, (b) Lena, (c) Barbara, (d) Goldhill, (e) Boat.	40
3.2	Distribution of normalized hamming distances: (a) Rotation, (b) Scaling, (c) Gaussian noise addition and (d) JPEG compression	41
3.3	Performance of various hashing schemes: (a) Rotation, (b) Scaling, (c) Gaussian noise addition, (d) JPEG compression.	42
3.4	(a) Original image, (b,c,d) Maliciously modified images.	43
3.5	Distance between hash using wrong keys	43
4.1	Robustness and comparative analysis of the proposed hashing technique under different distortions: (a) Additive Gaussian noise, (b) Salt & pepper noise, (c) Image blurring, (d) Average Filtering, (e) Median Filtering (f) Rotation, (g) Scaling, (h) Shearing, (i) Contrast Adjustment, (j) Brightness, (k) JPEG Compression, (l) SPIHT Compression.	51
4.2	Distribution of normalized hamming distance for visually identical image pairs.	52
4.3	Distribution of normalized hamming distance for perceptually different image pairs.	53
4.4	The normalized hamming distance between true hash sequence and randomly generated binary sequence	54
4.5	Original image and corresponding maliciously modified version	55
4.6	Comparison of ROC curve of different existing techniques	57
5.1	Experimental Images:(a-e) Fingerprint images, (f-j) Original medical image, (k-o) Encrypted medical images, (p-t) Decrypted medical images.	66
5.2	Edge images detected by the Canny edge detector with different thresholds: (a) Original image. (b) t = [0, 0.1]. (c) t = [0.1, 0.2], (d) t = [0.2, 0.3].	69

5.3 Amplitude spectra of Original Images (left column), Encrypted Images (middle column), Decrypted Images (right column). 71
5.4 Correlation distribution of horizontal pixels in: Original Images (left column), Encrypted Images (middle column), Decrypted Images (right column). 72
5.5 Experimental Images: (a-y) Decrypted medical images; (a,g,m,s,y) Decrypted images with true fingerprint images. 74
5.6 Objective metric with different fingerprint images and decrypted medical images- First column: Normalization coefficients; Second column: structural similarity; Third column: Peak signal to noise ratio; Fourth column: Universal image quality index. 75

6.1 Experimental Images: (a, e, i, m) Host images, (b, f, j, n) Watermark images, (c, g, k, o) Watermarked images, (d,h,l,p) Extracted watermarks. 80
6.2 Amplitude spectra of: (a,c) Host image, and (b,d) watermarked image. 82
6.3 Demonstration of attacked image: (a) Additive gaussian noise (mean=0, var=0.01), (b) Salt & pepper noise (noise density=0.01), (c) Speckle noise (var=0.01), (d) Sharpening (100%) ,(i) Histogram equalization, (j) Contrast adjustment (100%), (k) Gamma correction (gamma=5), (l) Resizing (512$\rightarrow$ 1536 $\rightarrow$ 512), (q) Cropping (50% area), (r) JPEG compression (10%), (s) High pass filter (7×7), (t) Average blur (7×7), (y) Swirl (35 %), (z) Wrapping (70 %), (a1) Row deletion (20), (a2) Image tempering, II, IV, VI, VII row shows the corresponding extracted watermark images. 83
6.4 Correlator response between: (a) Decimal sequence with true key and 100 wrong keys, (b) Decimal sequence with true key and 100 random binary sequences. 89
6.5 Magnitude of correlation coefficients against attacks with: (a) wrong seed s, (b) wrong primes $q11$ and $q21$, (c) wrong primes $q11$, $q12$ and $q22$, (d) wrong primes $q11$, $q12$, $q21$ and $q22$, (d) wrong seed and all wrong primes $q11$, $q12$, $q21$ and $q22$. (The nomenclature of x-axis are depicted in Table-5) 90
6.6 Experimental Images: (a) Original watermark, (b) Scrambled watermark, (c) Reconstructed watermark, (d) Extracted with wrong seed, (e) Extracted with wrong key $q11$, (f) Extracted with wrong key $q12$, (g) Extracted with wrong key $q21$. 91

7.1 Particle in bistable double well system crossing the barrier from weak state to strong state. 94
7.2 (a,b,c,d,e) Original images; (f,g,h,i,j) Original watermarks; (k,l,m,n,o) Watermarked images; (p,q,r,s,t) Extracted watermark images. 102
7.3 Imperceptibility of the proposed technique via histogram. 104
7.4 Watermarked images exposed to different distortions: (a) Gaussian noise addition (90%); (b) Salt & Pepper Noise addition (60%); (c) Speckle noise addition (60%); (d) Gaussian blurring (13×13); (e) Average filtering (13×13); (f) Median filtering (13×13); (g) JPEG compression (quality factor 90); (h) Sharpen (increased by 100%); (i) Histogram equalization; (j) Contrast adjustment (decreased by 100%); (k) Gamma correction (γ=5); (l) Cropping (50% area cropped); (m) Resizing ($256 \rightarrow 64 \rightarrow 256$); (n) Rotation ($50^{\circ}$); (o) Wrapping; (p) Swirl (80%). 105
7.5 Extracted watermark images after various distortions: (a) Gaussian noise addition (90%); (b) Salt & Pepper Noise addition (60%); (c) Speckle noise addition (60%); (d) Gaussian blurring (13×13); (e) Average filtering (13×13); (f) Median filtering (13×13); (g) JPEG compression (quality factor 90); (h) Sharpen (increased by 100%); (i) Histogram equalization; (j) Contrast adjustment (decreased by 100%); (k) Gamma correction (γ=5); (l) Cropping (50% area cropped); (m) Resizing ($256 \rightarrow 64 \rightarrow 256$); (n) Rotation ($50^{\circ}$); (o) Wrapping; (p) Swirl (80%). 108
7.6 Results for composite attacks (a) GNA+AF+HE; (b) extracted watermark; (c) MF+W+JPEG; (d) extracted watermark; (e) MF+HE+RS; (f) extracted watermark; (g) SW+AF+JPEG+GNA; (h) extracted watermark. 109
7.7 Illustration of the suitability of watermark images. 114

List of Tables

Table	*Title*	*page*
1.1	Content preserving operations and Content changing operations .	4
1.2	Different objective metrics for perceptual image hashing.	7
3.1	NHD for the set of different image processing attacks.	41
3.2	Normalized hamming distance between image pairs.	43
4.1	Normalized Hamming distance of different standard test images.	48
4.2	Content-Preserving Operation with Different Parameter Details.	50
4.3	Collision Probabilities for Different Thresholds (λ)	53
4.4	Time complexity of different hashing algorithms.	56
4.5	Estimated performance of different hashing algorithms.	56
4.6	Comparative analysis between proposed and existing algorithms.	57
4.7	Content sensitivity analysis among different algorithm.	58
5.1	Mathematical definitions of objective metrics used in perceptual security analysis.	67
5.2	Perceptual Security Analysis for experimental images.	68
5.3	Key Sensitivity Analysis for All Medical Images.	68
5.4	Edges similarity between the original and encrypted image for different threshold value.	69
5.5	Correlation Coefficients of Two Adjacent Pixels for All Medical Images.	73
5.6	Edge based comparison of proposed scheme with existing schemes.	74
5.7	Comparison of proposed scheme with existing scheme in terms of NC and UIQI.	75
5.8	Comparison of proposed scheme with existing scheme in terms of SSIM and PSNR.	76
6.1	Bit error rate and correlation coefficients of extracted watermarks at different gain factor.	80
6.2	Imperceptibility of host images at different gain factor.	81
6.3	Estimated correlation coefficient and threshold values in watermark extraction.	84
6.4	Estimated bit error rate (BER) in watermark extraction.	85
6.5	Detailed Comparison of proposed technique with existing techniques.	86
6.6	Comparative Analysis of proposed technique with existing techniques.	87
6.7	The nomenclature and details of the attacks.	91
7.1	Imperceptibility of the proposed technique.	103
7.2	Correlation coefficient and the number of iterations for the convergence of DSR.	107
7.3	Nomenclature (and the involved parameters) used for the composite distortions.	109
7.4	Correlation coefficients of the extracted watermarks after the series of attacks on the watermarked image.	110
7.5	Confusion matrix for the false-positive test where both singular vectors are from non-existent watermark.	110
7.6	Confusion matrix for the false-positive test where only left singular vector is from non-existent watermark.	110
7.7	Confusion matrix for the false-positive test where only right singular vector is from non-existent watermark.	111
7.8	Computational time complexities of the proposed technique.	112

7.9 Detailed Comparison of proposed technique with existing techniques. 113
7.10 Suitability of watermark with respect to host image 115

List of Symbols

Symbol	Description
ρ	Correlation Cofficients
E_S	Edge Similarity
S	Secret Key
$\in$	belongs to
$\subset$	subset
$\oplus$	XoR Operation
$\bigtriangledown$	Gradient
$\wedge$	AND Operation
$erfc(\cdot)$	Error Function

List of Abbreviation

Abbreviation	Full form
PIH	Perceptual Image Hashing
PHF	Perceptual Hash Function
AES	Advanced Encryption Standard
IDES	International Data Encryption Standard
RSA	Rivest-Shamir-Adleman
IPR	Intellectual Property Right
HD	Hamming Distance
ED	Euclidean Distance
BER	Bit Error Rate
PSNR	Peak Signal to Noise Ratio
ECC	Error Correcting Code
CC	Correlation Coefficient
NCC	Normalized Correlation Coefficients
DCT	Discrete Cosine Transform
ZM	Zernike Moment
SIFT	Scale Invariant Feature Transform
DFT	Discrete Fourier Transform
NFM	Non-negative Matrix Factorization
SVD	Singular Value Decomposition
SV	Singular Values
LSB	Least Significant Bit
PN	Pseudo Noise
SSC	Spread Spectrum Communication
LFSR	Linear Feedback Sift Register
SR	Stochastic Resonance
DSR	Dynamic Stochastic Resonance
PWNLCM	Piece-wise Non-linear Chaotic Map
IDCT	Integer Discrete Cosine Transform
PR − APBST	Parameterized All Phase Biorthogonal Sine Transform
DWT	Discrete Wavelet Transform