AN IMPROVED RDWT-BASED IMAGE STEGANOGRAPHY SCHEME USING QR DECOMPOSITION AND HUMAN VISUAL SYSTEM

NG KE HUEY

Master of Science

UNIVERSITI MALAYSIA PAHANG

SUPERVISOR'S DECLARATION

We hereby declare that we have checked this thesis and, in our opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Master of Science.

_____

(Supervisor's Signature)

Full Name : DR. LIEW SIAU CHUIN

Position : SENIOR LECTURER

Date : 01 OCTOBER 2021

_____

(Co-supervisor's Signature)

Full Name : DR. FERDA ERNAWAN

Position : SENIOR LECTURER

Date : 01 OCTOBER 2021

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

(Student's Signature)

Full Name : NG KE HUEY

ID Number : MCC16003

Date : 01 OCTOBER 2021

AN IMPROVED RDWT-BASED IMAGE STEGANOGRAPHY SCHEME USING QR DECOMPOSITION AND HUMAN VISUAL SYSTEM

NG KE HUEY

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Master of Science

Faculty of Computing
UNIVERSITI MALAYSIA PAHANG

OCTOBER 2021

ACKNOWLEDGEMENTS

First of all, I would like to express my sincere thanks to my project supervisor, Dr. Eric Liew Siau Chuin and co-supervisor, Dr. Ferda Ernawan for their insightful comments, outstanding advice, and exceptional guidance. I would also like to express my heartiest appreciation for their patience in spending precious time to guide me in my project and provide a lot of valuable and practical suggestions during this period.

Also, I would like to express my appreciation to my evaluators, Dr. Taha and Dr. Suryanti for sharing their valuable idea and knowledge with me in order to assist myself to succeed the project.

I would like to express my high appreciation to all lecturers and fellow friends that have guided me throughout the completion of this project. Moreover, I am very grateful to my family for their love and endless support.

ABSTRAK

Kebelakangan ini, terdapat peningkatan trend penggunaan maklumat secara intensif melalui internet. Perlindungan data telah menjadi masalah yang cukup penting kerana kemajuan teknologi maklumat dan komunikasi yang cepat dan peningkatan besar penggunaan internet melalui pengiriman dan penerimaan data. Steganografi menjadi semakin penting kerana banyak yang bergabung dengan revolusi ruang siber yang menggunakan teknologi pertukaran maklumat. Walaupun pertukaran maklumat melalui teks tidak lagi selamat, menyembunyikan mesej rahsia dalam gambar telah mendapat banyak populariti kerana mempunyai ruang persembunyian yang lebih besar dan oleh itu, lebih sukar untuk melihat kehadiran maklumat tersembunyi. Oleh itu, ketidaklihatan memainkan peranan penting dalam kes ini. Apabila mesej peribadi atau rahsia mudah dilihat dalam sistem steganografi yang lemah dan tidak dapat dilihat, ia mengalahkan tujuan asalnya dan diminta untuk diserang oleh pengganggu. Kajian ini memperkenalkan peningkatan steganografi gambar berdasarkan RDWT dengan penguraian QR dan sistem visual manusia. Berbanding dengan domain spatial, transform domain lebih disukai kerana memberikan kekuatan yang lebih baik ketika datang ke serangan seperti serangan geometri dan pemampatan. RDWT membolehkan penyisipan gambar rahsia bersaiz sama ke dalam gambar sampul berbanding dengan DWT yang hanya menawarkan separuh kapasiti penyematan RDWT. Ia juga menyelesaikan masalah shift variance yang disebabkan oleh DWT untuk mengelakkan ketidaktepatan semasa proses pengekstrakan. Penguraian QR telah dimasukkan ke dalam skema yang dicadangkan kerana ia membantu menghilangkan masalah positif palsu yang biasanya berlaku pada skema yang melibatkan Singomponen Nilai (SVD). Kajian ini juga mencadangkan untuk menyembunyikan maklumat rahsia berdasarkan nilai entropi menggunakan sistem visual manusia. Sistem ini mempertimbangkan kedua-dua nilai entropi blok gambar penutup dan blok gambar rahsia sebelum proses penyisipan bermula. Blok gambar rahsia dengan nilai entropi terendah akan dimasukkan ke dalam blok gambar sampul dengan nilai entropi terendah. Proses penyisipan berlanjutan sehingga semua blok gambar rahsia telah dimasukkan ke dalam gambar sampul sesuai dengan nilai entropi yang sesuai, dari nilai terendah hingga nilai tertinggi. Sebabnya adalah bahawa HVS kurang sensitif terhadap kawasan dengan nilai entropi rendah. Pendekatan ini meningkatkan ketidaklihatan skema dengan memasukkan maklumat di blok gambar sampul dengan nilai entropi yang lebih rendah kerana nampaknya kurang sensitif bagi HVS untuk memperhatikan perbezaan antara gambar stego dan gambar sampul. Dengan menerapkan sistem visual manusia, skema yang dicadangkan berjaya mencapai nilai PSNR rata-rata yang tinggi iaitu 62.5628 dengan menanamkan gambar rahsia dengan ukuran antara 32x32 hingga 512x512 menggunakan ukuran blok gambar antara 4x4 hingga 32x32. Walau bagaimanapun, skema yang dicadangkan mempunyai kekuatan yang tinggi terhadap serangan. Sebagai kesimpulan, skema yang dicadangkan telah menunjukkan hasil yang lebih baik berbanding dengan karya sebelumnya dari segi ketidaklihatan dan kualiti gambar.

ABSTRACT

Recent years have seen a rising trend in the use of intensive transmission of information via the internet. Data protection has become a fairly important issue due to the fast progress of information and communication technology and the huge increase in internet usage by sending and receiving data. Steganography becomes more and more important as many joined the cyberspace revolution that utilizes the information exchanging technology. While exchanging information via text is no longer secure, hiding a secret message in images has gained much popularity as it has larger hiding space and therefore, more difficult to notice the presence of hidden information. Hence, imperceptibility plays an important role in this case. Once the private or secret message is easily noticeable in a weak steganography system with poor imperceptibility, it defeats the original purpose and prompts to be attacked by intruders. This study introduces a hybrid RDWT-based image steganography system with QR decomposition and the human visual system. Compared to the spatial domain, transform domain is preferable because it provides better robustness when it comes to attacks such as geometric attacks and compression. RDWT allows embedding of the same-sized secret image into the cover image as compared to DWT that only offers half the embedding capacity of RDWT. It also solves the shift variance problem caused by DWT to avoid inaccuracy during the extraction process. QR decomposition has been incorporated into the proposed scheme because it helps to eliminate the false positive issue which usually occurs in schemes involving Singular Value Decomposition (SVD). This study also proposes to hide secret information based on the entropy values using the human visual system. The system considers both entropy values of cover image blocks and secret images blocks before embedding process begins. Secret image block with the lowest entropy value will be embedded into the cover image block with the lowest entropy value. The embedding process continues until all secret image blocks have been embedded into a cover image according to their corresponding entropy values, from the lowest to the highest value. The reason is that HVS is less sensitive to areas with low entropy value. This approach enhances the imperceptibility of the scheme by embedding information in cover image blocks with lower entropy values as they appeared to be less sensitive for HVS to notice the difference between stego image and cover image. By applying the human visual system, the proposed scheme managed to achieve high average PSNR value of 62.5628 dB by embedding secret image of sizes ranging from 32x32 to 512x512 using image block size ranging from 4x4 to 32x32. However, the proposed scheme has low robustness against attacks. As a conclusion, the proposed scheme has shown better result compared to previous work in terms of imperceptibility and image quality.

TABLE OF CONTENT

REFERENCES

A.Cheddad et al. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing 90*, 727–752.

Abdesselam and Imad Fakhri. (2018). A Review of Steganographic Methods and Techniques. *International Journal on Perceptive and Cognitive Computing (IJPCC), 4*(1).

Abod, Z. A. (2018). A Hybrid Approach to Steganography System Based on Quantum Encryption and Chaos Algorithm. *Journal of Babylon University, 26*(2), 280-294.

AH Mohsin et al. (2019). New Method of Image Steganography Based on Particle Swarm Optimization Algorithm in Spatial Domain for High Embedding Capacity. *IEEE Access*, 168994-169010.

Ahn, C.-J. (2008). Ahn CJ . Parallel detection algorithm using multiple QR decompositions with permuted channel matrix for SDM/OFDM. *IEEE Transactions on Vehicular Technology*, 2578-2582.

Al-Dmour H. and Al-Ani A. (2016). A steganography embedding method based on edge identification and XOR coding. *Expert Systems with Applications*, 293-306.

Amine K. (2020). Steganographic Techniques Classification According to Image Forma. *International Annals of Science*, 143-149.

Aqeel I. and Suleman M.B. (2019). A Survey on Digital Image Steganography Approaches. *Intelligent Technologies and Applications*, 769-778.

Bradley, A.P. (2003). Shift-invariance in the discrete wavelet transform. *Proc. VIIth Digital Image Computing: Techniques and Applications*, (pp. 29-38).

C. Qin et al. (2018). Separable reversible data hiding in encrypted images via adaptive emb e dding strategy with block selection. *Signal Processing 153*, 109-122.

Chatterjee A. and Pati S.K. (2020). Data Hiding with Digital Authentication in Spatial Domain Image Steganography. *Computational Intelligence in Pattern Recognition*, 897-907.

Cheddad A. et al. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 727-752.

Chu et al. (2004). A DCT-based image steganographic method resisting statistical attacks. *In Acoustics, speech, and signal processing* (pp. 953-956). IEEE.

Clair, B. (2001, October 8). Steganography: How to Send a Secret Message. *International Journal of Information Technology Modeling and Computing (IJITMC), 2*(1), 55-62.

D.K. Sarmah and A.J. Kulkarni. (2019). Improved Cohort Intelligence—A high capacity, swift and secure approach on JPEG image steganography. *Journal of Information Security and Applications*, 90-106.

Debalina et al. (2018). A Novel Approach of Image Steganography with Encoding and Location Selection. *Proceedings of International Ethical Hacking Conference*, (pp. 115-124).

Erna Zuni Astuti et al. (2019). Flipping the Message Bits to Increase Imperceptibility in the Least Significant Bit Image Steganography. *Journal of Physics: Conference Series*, 1-8.

Ferda Ernawan and Kabir. (2018). A block-based RDWT-SVD image watermarkingmethod using human visual system characteristics. *The Visual Computer*, 19-37.

Fowler. (2004). The Redundant Discrete Wavelet Transform and Additive Noise. *IEEE Signal Processing Letters 12 (9)*, 629-632.

Golub and Van Loan. (1989). *Matrix Computations.* Baltimore: Johns Hopkins University Press.

Gupta Garg. (2014, December). Detecting LSB Steganography in Images. *International Conference on Applied System Innovation (ICASI)*, (pp. 995-997).

HA Santoso et al. (2018). An improved message capacity and security using divide and modulus function in spatial domain steganography. *International Conference on Information and Communications Technology (ICOIACT)* (pp. 186-190). Yogyakarta, Indonesia: IEEE.

Habibi et al. (2013). Using SFLA and LSB for text message steganography in 24-bit RGB color images. *Int. J. Eng*, 68–75.

Hashim M. and Rahim, M. (2017). Image steganography based on odd/even pixels distribution scheme and two parameters random function. *J. Theor. Appl. Inf. Technol.*, 5977–5986.

Hien T.D. et al. (2006). RDWT domain watermarking based on independent component analysis extraction. *Advance Software Computing*, 401-414.

Hien T.D. et al. (2006). Robust multi-logo watermarking by RDWT and ICA. *Signal Processing*, 2981-2993.

Hossain et al. (2009). Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation. *Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009).* Dhaka, Bangladesh.

Hsu L.Y. and Hu H.T. (2017). Robust blind image watermarking using crisscross inter-block prediction in the DCT domain. *J. Vis. Commun. Image R.*, 33-47.

I.J. Kadhim et al. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, 299-326.

I.J. Kadhim et al. (2020). High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. *Cognitive Systems Research 60*, 20-32.

J. Qin et al. (2020). Coverless Image Steganography: A Survey. *IEEE Access*, 171372 - 171394.

Jaeyoung Kim et al. (2017). A Statistical Approach for Improving the Embedding Capacity of Block Matching based Image Steganography. *Journal of Broadcast Engineering*, 643-651.

Joseph P. and Vishnukumar S. (2015). A study on steganographic techniques. *In Global conference on communication technologies*, 206-210.

K. Biswas and S. Chand. (2019). An RGB image steganography algorithm with dual layer security. *Comunication and Computing Systems*, 25-31.

Kalra M. and Singh P. (2014). EMD techniques of image steganography : a comparative study. *Int. J. Technol. Explor*, 385-390.

Kini N.G. et al. (2019). A Secured Steganography Algorithm for Hiding an Image in an Image. *Integrated Intelligent Computing, Communication and Security*, 539-546.

Kumar Gaurav and Umesh Ghanekar. (2018). Image steganography based on Canny edge detection, dilation operator and hybrid coding. *Journal of Information Security and Applications 41*, 41-51.

Lai, C.C. (2011). An improved SVD-based watermarking scheme using human visual. *Optical Commununication*, 938-944.

M.S. Subhedar and V.H. Mankar. (2016). Image steganography using redundant discrete wavelet transform and QR factorization. *Computers and Electrical Engineering*, 406-422.

M.Y. Valandar et al. (2017). A new transform domain steganography based on modified logistic chaotic map for color images. *Journal of Information Security and Applications 34*, 142–151.

Makbol et al. (2016). Block-based discrete wavelet transform singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Process*, 34-52.

Manoj Kumar and Gursewak Singh. (2017). Block based Image Steganography using Entropy with LSB and 2-bit Identical Approach. *International Journal of Computer Applications (0975 – 8887)*.

Mehdi et al. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication,* 46-66.

Milad et al. (2017). A new transform domain steganography based on modified logistic. *Journal of Information Security and Applications,* 142-151.

Minati Mishra et al. (2012). Digital Image Data Hiding Techniques- A Comparative Study. *ANVESA,* 105-115.

Miri A. and Faez K. (2018). An image steganography method based on integer wavelet transform. *Multimedia Tools and Applications*, 13133–13144.

Muhammad K. et al. (2018). Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems,* 951-960.

Muzafer et al. (2019). A novel approach to steganography based on the properties of Catalan. *Future Generation Computer Systems,* 186-197.

Ogihara T. et al. (1996). Data embedding into pictorial images with less distortion using discrete cosine transform. *Proceedings - International conference on pattern recognition,* (pp. 675-679).

Patricia Lafferty and Farid Ahmed. (2004). Texture-based steganalysis: results for color images. *Proc. SPIE 5561, Mathematics of Data/Image Coding, Compression, and Encryption VII, with Applications.* Colorado.

Prerna Gupta and Girish Parmar. (2017). Image Watermarking using IWT-SVD and its Comparative Analysis with DWT-SVD. *International Conference on Computer, Communications and Electronics (Comptelix)* (pp. 527-531). IEEE.

Provos N. and Honeyman P. (2003). Hide and seek: An introduction to steganography. *IEEE Security & Privacy*, 32-44.

Q. Su et al. (2012). Embedding color watermarks in color images based on Schur decomposition. *Optics Communications 285*, 1792-1802.

R. Wazirali and Z. Chaczko. (2015). Hyper edge detection with clustering for data hiding. *Journal of Information Hiding and Multimedia Signal Processing (JIHMSP)*, 1-9.

Ramakrishnan, S. (2019). *Introductory Chapter: Digital Image and Video Watermarking and Steganography.* India: IntechOpen.

Ranjani. (2017). Data hiding using pseudo magic squares for embedding high payload in digital image. *Multimedia Tools Appl*, 3715–3729.

Rassem et al. (2016). Performance evaluation of RDWT-SVD and DWT-SVD watermarking schemes. *International Conference on Advanced Science, Engineering and Technology (ICASET).*

Rehman et al. (2014). Virtual machine security challenges: case studies. *International Journal of Machine Learning and Cybernetics*, 729-742.

S. Kumar et al. (2019). Information hiding with adaptive steganography based on novel fuzzy edge identification. *Defence Technology 15* , 162-169.

S. S. Kumar and S. V. Sylish. (2017). Image steganography in high entropy regions using a key & modified LSB for improved security. *International Conference on Computing Methodologies and Communication* (pp. 1104-1108). IEEE.

S.I. Nipanikar et al. (2018). A sparse representation based image steganography using Particle Swarm Optimization and wavelet transform. *Alexandria Engineering Journal*, 2343-2356.

S.I. Nipanikar et al. (2018). A sparse representation based image steganography using Particle Swarm Optimization and wavelet transform. *Alexandria Engineering Journal 57*, 2343–2356.

Sahu et al. (2018). Improved exploiting modification direction-based steganography using dynamic weightage array. *Electron. Lett.*, 498-500.

Serdean et al. (2002). Protecting intellectual rights: Digital watermaking in the wavelet domain. *Trends and Recent Achievements in Information Technology* (pp. 8-16). IEEE.

Shannon, C.E. (1948). A Mathematical Theory of Communication. *Bell Syst. Tech. J. 27*, 379–423, 623–656.

Shaoli Jia et al. (2017). A Novel Color Image Watermarking Scheme Based on DWT and QR Decomposition. *Journal of Applied Science and Engineering*, 193-200.

Shet et al. (2019). Novel high-speed reconfigurable FPGA architectures for EMD-based image steganography. *Multimedia Tools Appl*, 1-30.

Shuming Jiao et al. (2019). Review on optical image hiding and watermarking techniques. *Optics & Laser Technology*, 370-380.

Siddharth S. and Siddiqui T.J. (2014). Transform domain techniques for image steganography. *Information Security in Diverse Computing Environments*, 245-259.

Sunil et al. (2017). An Improved Image Steganography based on 2-DWT-FFT-SVD on YCBCR Color Space. *International Conference on Trends in Electronics and Informatics* (pp. 567-572). IEEE.

Swati Bhargava and Manish Mukhija. (2019). Hide Image and Text Using LSB, DWT and RSA Based on Image Steganography. *ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING*, 1940-1946.

Tejeshwar, G. (2014). Colour image steganography using LZW compression and fisher-yates shuffle algorithm . *Int. J. Innovative Res. Develop*, 54-61.

Thiyagarajan, P., Aghila, G., & Prasanna, V. V. (2012). *Stego-Image Generator (SIG) – Building Steganography Image Database.* Puducherry 605 014: CDBR-SSE Lab Department of Computer Science, Pondicherry University.

Verma, J. K. (2013). A hybrid approach for image security by combining encryption and steganography. *Second International Conference on Image Information Processing* (pp. 607-611). IEEE.

Vijay Kumar, Dinesh Kumar. (2019). Performance evaluation of modified color image steganography using discrete wavelet transform. *Journal of Intelligent Systems*, 749-758.

Wang et al. (2010). An improved section-wise exploiting modification direction method. *Signal Process*, 2954–2964.

Wang H and Wang S. (2004). Study on esterification and acylation modification of carbon nanotubes functionalized with carboxylic group. *Carbon Techniques*, 10-12.

X.Y. Liu et al. (2015). Quality assessment of speckle patterns for digital image correlation by Shannon entropy. *Optik 126*, 4206–4211.

Yahya, A. (2019). Introduction to Steganography. In A. Yahya, *Steganography Techniques for Digital Images* (pp. 1-7). Springer, Cham.

Zeyad Safaa Y. and Ghada Thanoon Y. (2019). Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data. *Journal of Intelligent Systems*.

Zeyad Safaa Younus and Mohammed Khaire Hussain. (2019). Image steganography using exploiting modification direction for compressed encrypted data. *Journal of King Saud University – Computer and Information Sciences*.

A.Cheddad et al. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing 90*, 727–752.

Abdesselam and Imad Fakhri. (2018). A Review of Steganographic Methods and Techniques. *International Journal on Perceptive and Cognitive Computing (IJPCC)*.

Abod, Z. A. (2018). A Hybrid Approach to Steganography System Based on Quantum Encryption and Chaos Algorithm. *Journal of Babylon University, 26*(2), 280-294.

AH Mohsin et al. (2019). New Method of Image Steganography Based on Particle Swarm Optimization Algorithm in Spatial Domain for High Embedding Capacity. *IEEE Access*, 168994-169010.

Ahn, C.-J. (2008). Ahn CJ . Parallel detection algorithm using multiple QR decompositions with permuted channel matrix for SDM/OFDM. *IEEE Transactions on Vehicular Technology*, 2578-2582.

Al-Dmour H. and Al-Ani A. (2016). A steganography embedding method based on edge identification and XOR coding. *Expert Systems with Applications*, 293-306.

Amine K. (2020). Steganographic Techniques Classification According to Image Forma. *International Annals of Science*, 143-149.

Aqeel I. and Suleman M.B. (2019). A Survey on Digital Image Steganography Approaches. *Intelligent Technologies and Applications*, 769-778.

Bradley, A.P. (2003). Shift-invariance in the discrete wavelet transform. *Proc. VIIth Digital Image Computing: Techniques and Applications*, (pp. 29-38).

C. Qin et al. (2018). Separable reversible data hiding in encrypted images via adaptive emb e dding strategy with block selection. *Signal Processing 153*, 109-122.

Chatterjee A. and Pati S.K. (2020). Data Hiding with Digital Authentication in Spatial Domain Image Steganography. *Computational Intelligence in Pattern Recognition*, 897-907.

Cheddad A. et al. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 727-752.

Chu et al. (2004). A DCT-based image steganographic method resisting statistical attacks. *In Acoustics, speech, and signal processing* (pp. 953-956). IEEE.

Clair, B. (8 October, 2001). *Steganography: How to Send a Secret Message.* Retrieved from http://www.strangehorizons.com/2001/20011008/steganography.shtml

D.K. Sarmah and A.J. Kulkarni. (2019). Improved Cohort Intelligence—A high capacity, swift and secure approach on JPEG image steganography. *Journal of Information Security and Applications*, 90-106.

Debalina et al. (2018). A Novel Approach of Image Steganography with Encoding and Location Selection. *Proceedings of International Ethical Hacking Conference*, (pp. 115-124).

Erna Zuni Astuti et al. (2019). Flipping the Message Bits to Increase Imperceptibility in the Least Significant Bit Image Steganography. *Journal of Physics: Conference Series*, 1-8.

Ferda Ernawan and Kabir. (2018). A block-based RDWT-SVD image watermarkingmethod using human visual system characteristics. *The Visual Computer*, 19-37.

Fowler. (2004). The Redundant Discrete Wavelet Transform and Additive Noise. *IEEE Signal Processing Letters 12 (9)*, 629-632.

Golub and Van Loan. (1989). *Matrix Computations.* Baltimore: Johns Hopkins University Press.

Gupta Garg. (December, 2014). *Detecting LSB Steganography in Images.* Retrieved from rahuldotgarg.appspot.com/data/steg.pdf

HA Santoso et al. (2018). An improved message capacity and security using divide and modulus function in spatial domain steganography. *International Conference on Information and Communications Technology (ICOIACT)* (pp. 186-190). Yogyakarta, Indonesia: IEEE.

Habibi et al. (2013). Using SFLA and LSB for text message steganography in 24-bit RGB color images. *Int. J. Eng*, 68–75.

Hashim M. and Rahim, M. (2017). Image steganography based on odd/even pixels distribution scheme and two parameters random function. *J. Theor. Appl. Inf. Technol.*, 5977–5986.

Hien T.D. et al. (2006). RDWT domain watermarking based on independent component analysis extraction. *Advance Software Computing*, 401-414.

Hien T.D. et al. (2006). Robust multi-logo watermarking by RDWT and ICA. *Signal Processing*, 2981-2993.

Hossain et al. (2009). Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation. *Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009).* Dhaka, Bangladesh.

Hsu L.Y. and Hu H.T. (2017). Robust blind image watermarking using crisscross inter-block prediction in the DCT domain. *J. Vis. Commun. Image R.*, 33-47.

I.J. Kadhim et al. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, 299-326.

I.J. Kadhim et al. (2020). High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. *Cognitive Systems Research 60*, 20-32.

J. Qin et al. (2020). Coverless Image Steganography: A Survey. *IEEE Access*, 171372 - 171394.

Jaeyoung Kim et al. (2017). A Statistical Approach for Improving the Embedding Capacity of Block Matching based Image Steganography. *Journal of Broadcast Engineering*, 643-651.

Joseph P. and Vishnukumar S. (2015). A study on steganographic techniques. *In Global conference on communication technologies*, 206-210.

K. Biswas and S. Chand. (2019). An RGB image steganography algorithm with dual layer security. *Comunication and Computing Systems*, 25-31.

Kalra M. and Singh P. (2014). EMD techniques of image steganography : a comparative study. *Int. J. Technol. Explor*, 385-390.

Kini N.G. et al. (2019). A Secured Steganography Algorithm for Hiding an Image in an Image. *Integrated Intelligent Computing, Communication and Security*, 539-546.

Kumar Gaurav and Umesh Ghanekar. (2018). Image steganography based on Canny edge detection, dilation operator and hybrid coding. *Journal of Information Security and Applications 41*, 41-51.

Lai, C.C. (2011). An improved SVD-based watermarking scheme using human visual. *Optical Commununication*, 938-944.

M.S. Subhedar and V.H. Mankar. (2016). Image steganography using redundant discrete wavelet transform and QR factorization. *Computers and Electrical Engineering*, 406-422.

M.Y. Valandar et al. (2017). A new transform domain steganography based on modified logistic chaotic map for color images. *Journal of Information Security and Applications 34*, 142–151.

Makbol et al. (2016). Block-based discrete wavelet transform singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Process*, 34-52.

Manoj Kumar and Gursewak Singh. (2017). Block based Image Steganography using Entropy with LSB and 2-bit Identical Approach. *International Journal of Computer Applications (0975 – 8887)*.

Mehdi et al. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, 46-66.

Milad et al. (2017). A new transform domain steganography based on modified logistic. *Journal of Information Security and Applications*, 142-151.

Minati Mishra et al. (2012). Digital Image Data Hiding Techniques- A Comparative Study. *ANVESA*, 105-115.

Miri A. and Faez K. (2018). An image steganography method based on integer wavelet transform. *Multimedia Tools and Applications*, 13133–13144.

Muhammad K. et al. (2018). Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems*, 951-960.

Muzafer et al. (2019). A novel approach to steganography based on the properties of Catalan. *Future Generation Computer Systems*, 186-197.

Ogihara T. et al. (1996). Data embedding into pictorial images with less distortion using discrete cosine transform. *Proceedings - International conference on pattern recognition*, (pp. 675-679).

Patricia Lafferty and Farid Ahmed. (2004). Texture-based steganalysis: results for color images. *Proc. SPIE 5561, Mathematics of Data/Image Coding, Compression, and Encryption VII, with Applications.* Colorado.

Prerna Gupta and Girish Parmar. (2017). Image Watermarking using IWT-SVD and its Comparative Analysis with DWT-SVD. *International Conference on Computer, Communications and Electronics (Comptelix)* (pp. 527-531). IEEE.

Provos N. and Honeyman P. (2003). Hide and seek: An introduction to steganography. *IEEE Security & Privacy*, 32-44.

Q. Su et al. (2012). Embedding color watermarks in color images based on Schur decomposition. *Optics Communications 285*, 1792-1802.

R. Wazirali and Z. Chaczko. (2015). Hyper edge detection with clustering for data hiding. *Journal of Information Hiding and Multimedia Signal Processing (JIHMSP)*, 1-9.

Ramakrishnan, S. (2019). *Introductory Chapter: Digital Image and Video Watermarking and Steganography*. India: IntechOpen.

Ranjani. (2017). Data hiding using pseudo magic squares for embedding high payload in digital image. *Multimedia Tools Appl*, 3715–3729.

Rassem et al. (2016). Performance evaluation of RDWT-SVD and DWT-SVD watermarking schemes. *International Conference on Advanced Science, Engineering and Technology (ICASET).*

Rehman et al. (2014). Virtual machine security challenges: case studies. *International Journal of Machine Learning and Cybernetics*, 729-742.

S. Kumar et al. (2019). Information hiding with adaptive steganography based on novel fuzzy edge identification. *Defence Technology 15* , 162-169.

S. S. Kumar and S. V. Sylish. (2017). Image steganography in high entropy regions using a key & modified LSB for improved security. *International Conference on Computing Methodologies and Communication* (pp. 1104-1108). IEEE.

S.I. Nipanikar et al. (2018). A sparse representation based image steganography using Particle Swarm Optimization and wavelet transform. *Alexandria Engineering Journal*, 2343-2356.

S.I. Nipanikar et al. (2018). A sparse representation based image steganography using Particle Swarm Optimization and wavelet transform. *Alexandria Engineering Journal 57*, 2343–2356.

Sahu et al. (2018). Improved exploiting modification direction-based steganography using dynamic weightage array. *Electron. Lett.*, 498-500.

Serdean et al. (2002). Protecting intellectual rights: Digital watermaking in the wavelet domain. *Trends and Recent Achievements in Information Technology* (pp. 8-16). IEEE.

Shannon, C.E. (1948). A Mathematical Theory of Communication. *Bell Syst. Tech. J. 27*, 379–423, 623–656.

Shaoli Jia et al. (2017). A Novel Color Image Watermarking Scheme Based on DWT and QR Decomposition. *Journal of Applied Science and Engineering*, 193-200.

Shet et al. (2019). Novel high-speed reconfigurable FPGA architectures for EMD-based image steganography. *Multimedia Tools Appl*, 1-30.

Shuming Jiao et al. (2019). Review on optical image hiding and watermarking techniques. *Optics & Laser Technology*, 370-380.

Siddharth S. and Siddiqui T.J. (2014). Transform domain techniques for image steganography. *Information Security in Diverse Computing Environments*, 245-259.

Sunil et al. (2017). An Improved Image Steganography based on 2-DWT-FFT-SVD on YCBCR Color Space. *International Conference on Trends in Electronics and Informatics* (pp. 567-572). IEEE.

Swati Bhargava and Manish Mukhija. (2019). Hide Image and Text Using LSB, DWT and RSA Based on Image Steganography. *ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING*, 1940-1946.

Tejeshwar, G. (2014). Colour image steganography using LZW compression and fisher-yates shuffle algorithm . *Int. J. Innovative Res. Develop*, 54-61.

Thiyagarajan, P., Aghila, G., & Prasanna, V. V. (2012). *Stego-Image Generator (SIG) – Building Steganography Image Database.* Puducherry 605 014: CDBR-SSE Lab Department of Computer Science, Pondicherry University.

Verma, J. K. (2013). A hybrid approach for image security by combining encryption and steganography. *Second International Conference on Image Information Processing* (pp. 607-611). IEEE.

Vijay Kumar, Dinesh Kumar. (2019). Performance evaluation of modified color image steganography using discrete wavelet transform. *Journal of Intelligent Systems*, 749-758.

Wang et al. (2010). An improved section-wise exploiting modification direction method. *Signal Process*, 2954–2964.

Wang H and Wang S. (2004). Study on esterification and acylation modification of carbon nanotubes functionalized with carboxylic group. *Carbon Techniques*, 10-12.

X.Y. Liu et al. (2015). Quality assessment of speckle patterns for digital image correlation by Shannon entropy. *Optik 126*, 4206–4211.

Yahya, A. (2019). Introduction to Steganography. In A. Yahya, *Steganography Techniques for Digital Images* (pp. 1-7). Springer, Cham.

Zeyad Safaa Y. and Ghada Thanoon Y. (2019). Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data. *Journal of Intelligent Systems*.

Zeyad Safaa Younus and Mohammed Khaire Hussain. (2019). Image steganography using exploiting modification direction for compressed encrypted data. *Journal of King Saud University – Computer and Information Sciences*.