Dct Based Image Watermarking

R. Shri raam[a], .k. Sathyam[b], a. Srivatsan[c], T. Devakumar[d]

[a,b ,c, d] Department of Electronics and Communication Engineering, National Engineering College, Tamil Nadu - 628503, India
[a]raamshri0405@gmail.com ,[b] sathyamji1999@gmail.com ,[c] vatsan18012000@gmail.com, [d]tdkece@nec.edu.in

Article History Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Use of social networking in the internet has an exponential growth in recent years, storage of data content is easy, the ease gave birth to issues like, piracy, authenticity and copyright protection while handling digital media. The art of hiding secret information inside an image is technically referred to as image watermarking or steganography. Steganography solemnly serves the purpose of delivering secret information, while image watermarking is used to verify integrity and authenticity of the image. Steganography focuses on the secret data embedded into the image and image watermarking focusses on the image. The watermarking schemes with the help of spread spectrum and quantisation, suffers scaling attacks and Host Signal Interference. The embedding parameter employed here is fixed and so it gets difficult for robustness and imperceptibility into account for all the images which are watermarked with this technique. This paper solves these problems referred before, Discrete Cosine Transform (DCT) based watermarking which assures the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) values. Discrete Cosine Transform (DCT) based watermark scheme reduces Host Signal Interference (HSI). Spatial domain watermarking suffers serious spatial distortion and loss. Quantisation type of embedding technique results in distortion during geometrical operations like compression, filtering. Introduction of threshold for error serves the purpose of analysis of watermarked image. Spread Spectrum Scheme with Adaptive Embedding Strategy (SSAES) promises low Host Signal Interference (HSI) but fails to yield required Peak Signal to Noise Ratio (PSNR). The proposed system overcomes the drawbacks of Host Signal Interference (HSI) and scaling attacks.

1. Introduction

Nowadays digital information and data are transmitted more often. Free-access to digital data communication unfortunately leads to virtually more opportunities to pirate copyrighted materials. Now more than ever, the idea of using digital watermarking to detect violations has stimulated interests among engineers, lawyers, artists, scientists, and publishers. Two major areas of watermarking are spatial domain watermarking and frequency domain watermarking. There are multiple transform techniques like DCT, DWT, DFT. We present robust digital watermark technologies. The basic is adopting function for choosing the best co-efficient which rules the conversion of real numbers to integers while the cosine transformation is in process. We develop a chaotic map, which performs better than the traditional ones by breaking spatial similarity, in order to increase the amount of significant co-efficient in the frequency domain transformed image without altering the pixel values. We are showing the advantages of the proposed technique in terms of better embedding capacity, lower secret message error rate. The algorithm works well under image-processing distortions, such as Gaussian noise, JPEG compression, and low-pass filter. Digital media is viable for production, transfer, duplication and modification, means the copyright violations taking place in an easy manner. It is very much important to identify the violations, to take actions. Digital watermark is such a technology, which embeds the secret data called a watermark inside digital media such as images, videos, audio and identify their authenticity and ownership by extracting the watermark data. This paper focuses on image watermarking. Image watermarking is practically effective if a watermark data can be embedded inside an image without tampering the quality of the image, watermark data can be extracted out correctly even when the image is distorted by geometric attacks.

1.1.1) Information Hiding

Encapsulation is the major technique used by the programmers for hiding the data. Information hiding using images is known as steganography. The information to be inserted into the signal is called watermark. Signal where the information to be inserted is called host signal.

1.1.2) Reversible Data Hiding

It is the method of embedding data into an image, after authenticating the image the watermark can be removed. This technique is majorly used for evidence collection. This technique is used by U.S Army for storing reconnaissance.

1.2) Cryptography

Cryptography is the technique of converting data into unreadable format. So that the data cannot be utilized by unauthorized user. There are multiple cryptographic algorithms employed for different purposes. Symmetric key algorithm and asymmetric key algorithm are majorly used cryptographic techniques. Encryption is a two-way

process where the data can be recovered, i.e. decrypted. There is one more cryptographic technique called hashing, hashing is more similar to encryption, but the data can't be recovered, once it is hashed, but can be used to verify the passwords. Most of the social media uses this technique for verifying passwords.

1.3) Watermark Properties

A) Robustness

A watermark is considered fragile if the data embedded inside the image, modifies or remain undetectable when the image is edited or modified. A watermark is robust only when the data embedded inside the image remains unchanged even after the modification of image. The modification of image is usually due to attacks like lowpass filter attack, JPEG compression etc. It also includes geometrical attacks like rotation, cropping etc.

B) Capacity

Capacity is the amount of data that can be embedded inside an image. Larger the capacity larger the data can be embedded into the image.

C) Imperceptibility

The quality of the embedded data being undetected. The embedded data should not be visible for bare human eyes. It is the most important part of the image watermarking and steganography, The image should look like a normal image and it should be a carrier of the secret data. Visible watermarks doesn't have this quality.

1.4) Watermarking Attacks

The information embedded into an image is called watermarked image. The watermarked image is transmitted or stored. Usually the watermarked image is transmitted. If a person tries to modify it, it is called attack. The modification can be malicious or not, but the modification is a form of attack.

A) Removal Attack

In this attack, the unauthorized user tries to remove the watermark. The attacker will remove the watermark and so, that person can claim the image or evidence and also its authenticity.

B) Interference Attack

In this type of attack the noise gets added to the watermarked image or watermarked media. Usually quantization and compression are the major reasons this type of attack.

C) Geometric Attack

These types of attacks occur due to the geometric operations like rotation, cropping etc.

D) Low Pass Filtering Attack

This type of attacks happens when the watermarked image is passed through the low pass filters. This type of attack causes blurring effect in the image, because it filters out the high frequency components.

1.5) Additive White Gaussian Noise

This type of noise gets added to the image in the transmission medium while being transmitted. This kind of noise is a random one, since the Additive White Gaussian Noise (AWGN) is caused due to many reasons including heat generated in the wired transmission medium and also due to the magnetic components of other device and antennas in the wireless medium. Usually the heat generated in the guided medium is due to the electron flow.

1.6) DCT

Discrete cosine transform is a frequency domain transform used in image watermarking for transforming the image from spatial domain to frequency domain. The image will be split into 8x8 non overlapping blocks, every block will be subjected to DCT. After that the blocks all will be in frequency domain.

1.7) Jpeg Compression

JPEG compression is usually a lossy one. Due to this one high frequency components gets lost. This type of attack usually causes blurring of images. Higher compressions may lead to some errors in the watermark.

1.8) Encryption

Encryption is the art of converting the data into unreadable format. There are multiple algorithms employed in watermarking techniques.

1.8.1) Synchronous Stream Cipher

Synchronous Stream Cipher is a symmetric key cipher, the plaintext digits are combined with a cipher digit stream. The cipher consists of plaintext, in which each plaintext stream is encrypted one at a time with the corresponding digit of keystream, to give a digit of stream of ciphertext.

1.8.2) AES Encryption

Advanced Encryption Standard (AES) works by taking the plain text and converting into ciphertext made of random characters. Symmetric key algorithm, which involves the use of only one secret key to cipher and decipher i.e. encrypting and decrypting.

1.8.3) Asymetric Encryption

This type of encryption is also known as public key algorithm. This technique uses a pair of keys called public key and private key. Public keys are known to everyone and private keys will be known only to the owner. Mostly public keys are used for encrypting purposes and private keys are used for decrypting. Anyone can use the public key to encrypt the data, typically a private key will be generated, the private key will be given only to the intended user for decrypting. In case of the asymmetric or public key algorithm the robustness is possible. Sender can attach the private key with the data to be sent as a digital signature. Public key algorithms are the most fundamental and important feature of modern cryptographic techniques. Confidentiality, authentication is retained in the process.

1.9) Applications

Watermarking is used for wide range of applications such as,

- Copyright protection
- Source tracking
- Authentication of video
- Tamper and fraud detection
- Medical applications

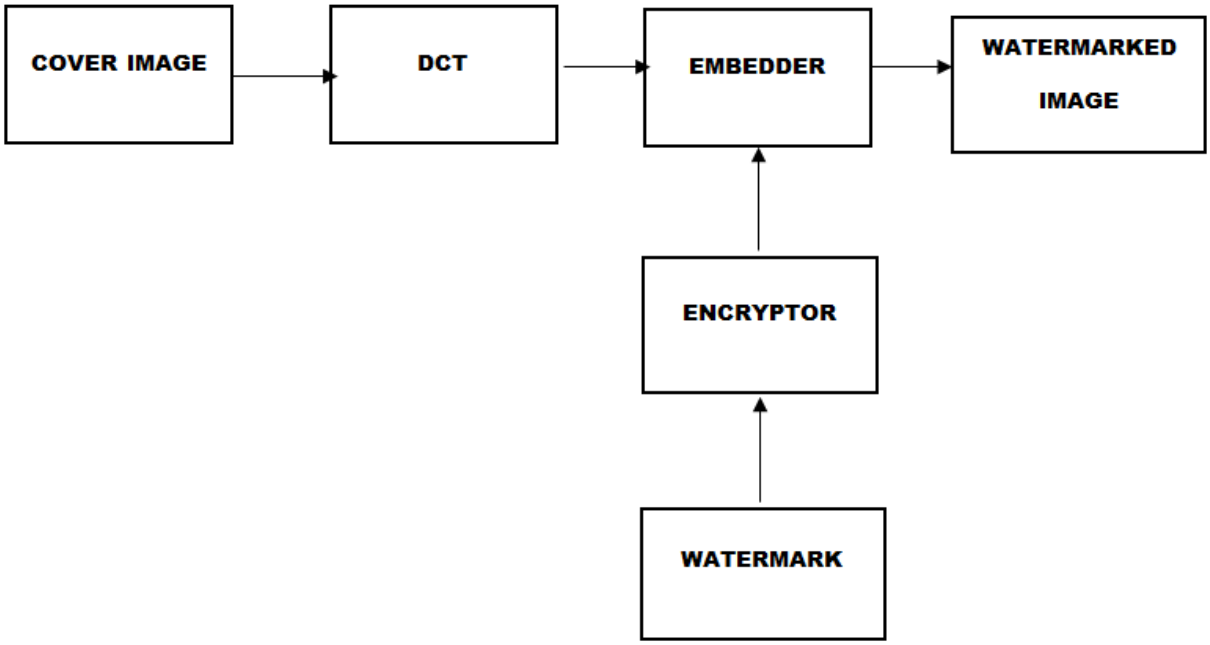
1.9.1) Copyright Protection

Content protection and copy prevention are plays an important part in information management and information security. Reproduction of media like films, music, songs, videos, photographs are easier nowadays due to the ease modes of transmission. Peer to peer communication modes like torrents has made piracy easier. Unauthorized distribution and copying of media costed nearly $2.4 billion in United States alone in 1990s. Watermarking can be used for copyright protection purposes.

1.9.2) Medical Applications

Medical reports are very much important. If the scan and X-ray reports gets mixed with other patients, it will be very dangerous. By using watermark techniques we can embed the patient’s ID or name in the report.

2. Proposed Methodology



2.1) Embedding Watermark

1)Discrete Cosine Transform (DCT) based watermarking is implemented in this work, Discrete Cosine Transform (DCT) is a frequency domain watermarking technique, where the watermark can survive noise. DCT is generally used for signal processing purposes. Frequency domain watermarking proves to be more robust than spatial domain watermarking.

2)The cover image is divided into non over-lapping 8x8 blocks.

3)Discrete Cosine Transform (DCT) is applied to each block by selecting the highest coefficient using HVS block selection criteria.

4)The secret data to be watermarked is encrypted with public key.

5)Discrete Cosine Transform applied blocks can be separated into low frequency, middle frequency and high frequency bands. The encrypted data is embedded into the middle frequency band. Because high frequency components gets rejected while passed through the low pass filters, low pass filters are used in image processing for rejecting high frequency noise, along with the high frequency noise, the high frequency components of the image also gets deleted, that's why the secret data is embedded into middle frequency band.

6)Embedding parameter is kept constant, since the secret data is embedded into middle frequency band.

7)To improve efficiency and robustness and to reduce scaling attacks, the Differential Quantization scheme is used, so that difference between two DCT co- efficient remains stable.

Extracting Watermark

1)Watermarked image is subjected to inverse Discrete Cosine Transform.

2)Encrypted watermark is extracted from the image.

3)Data is decrypted using private key.

3. Results And Discussion

3.1 Images before and after watermarking

This section evaluates performance of our work on Discrete Cosine Transform (DCT) based watermarking scheme. Experimental test data sets, evaluation, setup and environment are described in section A.

A) TDSS adaptive watermarking algorithm is a state of art technique uses watermarking framework which is similar as our work, which has a fair comparison to ours. The overall performance is evaluated by comparing our work with TDSS scheme. The embedding domain, embedding location are different on both techniques, it is difficult for evaluating both methods based on same conditions.

The test set included 80 rectangular and 20 square images of different sizes, which are randomly picked from test set which were commonly used for evaluation.

Identical watermark binary sequence of 128 bits are embedded into these images.

The concept of imperceptibility is checked by comparing the Peak Signal to noise (PSNR) values.

The Bit Error Rate (BER) is used for evaluating the robustness.

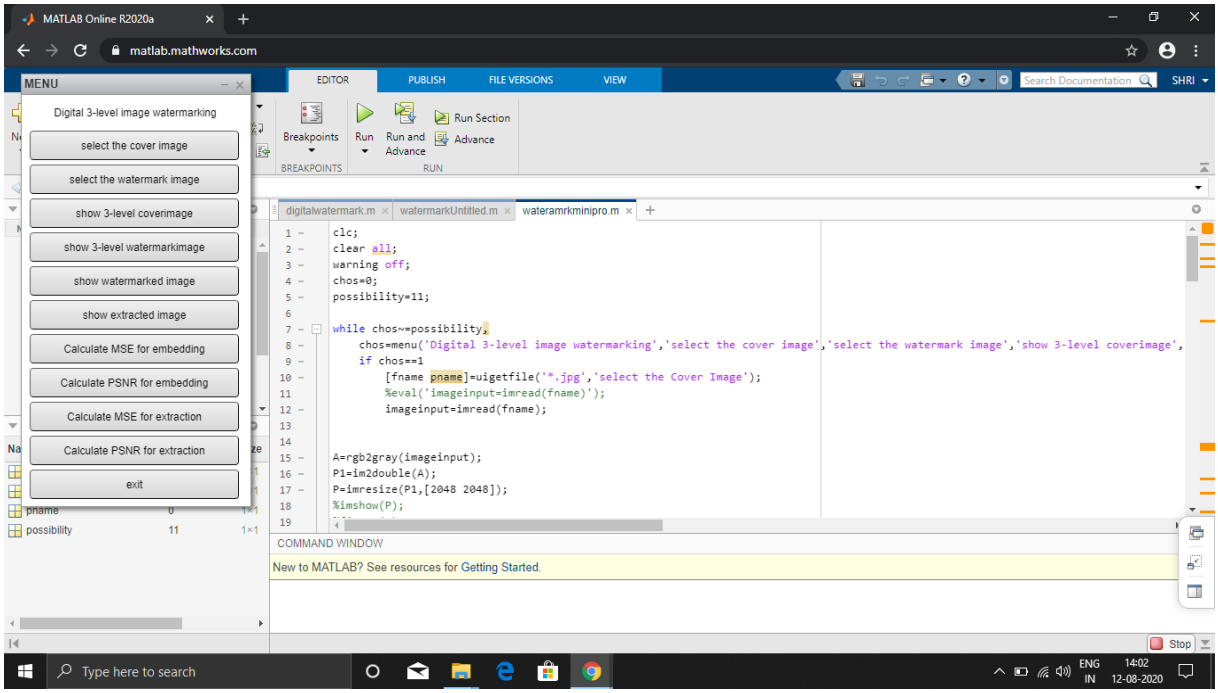
B)This methodology achieved high PSNR and low BER. The values were calculated by averaging the values for 100 test cases.

All experiments were performed in MATLAB online.

C)The PSNR values ranged from 57.4758 to 65.5593 , The average PSNR value was around 64.

D)The test for assessing the JPEG compression effects are executed by starting the attack from 1% loss to 45% loss, the test resulted in blurring of the images but did not affected the watermark data.

E)The encryption technique i.e. asymmetric key algorithm provides better security since public key is used to encrypt the secret data and a private key is given to the intended user to decrypt it.



3.2 The proposed algorithm in GUI format

4 Conclusion

This work provides novel watermarking scheme which outperforms most of the existing methods by providing being robust, imperceptible, high PSNR values and low error rates. The proposed DCT based watermarking scheme algorithm is implemented with Graphical User Interface (GUI), so that it can be of ease for everyone. Our watermark scheme is robust because it is immune to low pass filtering attack as the watermark data or secret data is embedded into medium frequency band. The proposed algorithm is tested by using images of multiple resolutions. The error correction code shows that the bit error rate for the low pass filtering attack is 0. JPEG lossy compression doesn't bother our mode of watermarking, because JPEG lossy compression mostly leads to the loss of the high frequency components, while the embedded watermark will be in the middle frequency areas

References

1. M. J. Hwang, J. S. Lee, M. S. Lee, and H. G. Kang, "SVD-Based Adaptive QIM Watermarking on Stereo Audio Signals," IEEE Trans. Multimedia, vol. 20, no. 1, pp. 45-54, 2017.
2. Deanship of Scientific Research, Taibah University, Al-Madinah Al-Munawwarah(2018) in" An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations"IEEE Access ,vol 6,2016.
3. M. Asikuzzaman and M. R. Pickering, "An Overview of Digital Video Watermarking," IEEE Trans. Circuits Syst. Video Technol., vol. 28, no. 9, pp. 2131-2153, Sept. 2018.
4. M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "Robust DT CWT-Based DIBR 3D Video Watermarking Using Chrominance Embedding," IEEE Trans. Multimedia, vol. 18, no. 9, pp. 1733-1748, 2016.
5. M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "Imperceptible and robust blind video watermarking using chrominance embedding: A set of approaches in the DT CWT domain," IEEE Trans. Inf. Forensics Security, vol. 9, no. 9, pp. 1502–1517, Sept. 2014.
6. H. Sadreazami, M. O. Ahmad, and M. N. S. Swamy, "Multiplicative Watermark Decoder in Contourlet Domain Using the Normal Inverse Gaussian Distribution," IEEE Trans. Multimedia, vol. 18, no. 2, pp. 196-207, 2016.
    A. Valizadeh and Z. J. Wang, "An Improved Multiplicative Spread Spectrum Embedding Scheme for Data Hiding," IEEE Trans. Inf. Forensics Security, vol. 7, no. 4, pp. 1127-1143, 2012.
7. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.
8. Valizadeh and Z. J. Wang, "Correlation-and-Bit-Aware Spread Spectrum Embedding for Data Hiding," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 267-282, 2011.
9. P. Bhinder, K. Singh, and N. Jindal, "Image-adaptive watermarking using maximum likelihood decoder for medical images," Multimedia Tools and Applications, Multimed Tools Appl, pp. 1-26, 2018.
10. H. Guan, Z. Zeng, J. Liu, and S. Zhang, "A novel robust digital image watermarking algorithm based on two-level DCT," in Proc. IEEE Int. Conf. ISEEE, pp. 1804-1809, 2014.
11. X. Zhu, J. Ding, H. Dong, K. Hu, and X. Zhang, "Normalized Correlation-Based Quantization Modulation for Robust Watermarking," IEEE Trans. Multimedia, vol. 16, no. 7, pp. 1888-1904, 2014.
12. B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," Int. Symposium Inf. Theory, vol. 47, no. 4, pp. 1423-1443, 2000.
13. X. Gao, C. Deng, X. Li, and D. Tao, "Local Feature Based Geometric-Resistant Image Information Hiding," Cognitive Computation, vol. 2, no. 2, pp. 68-77, 2010.
14. Nasir, F. Khelifi, J. Jiang, and S. Ipson, "Robust image watermarking via geometrically invariant feature points and image normalisation," Image Processing Iet, vol. 6, no. 4, pp. 354-363, 2012.
15. S. A. Parah, J. A. Sheikh, N. A, Loan, and G. M. Bhat, "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing," Digital Signal Processing, vol. 53, pp. 11-24, 2016
16. Ibrahim, R. and Kuan, T. S., Steganography Imaging (SIS): Hiding Secret Message inside an Image. Proceedings of the World Congress on Engineering and Computer Science, 2010, San Francisco, USA.
17. Er-Hsien Fu, Literature Survey on Digital Image Watermarking, EE381K Multidimensional Signal Processing, 1998.
18. L. Robert, T. Shanmugapriya, A Study on Digital Watermarking Techniques, International Journal of Recent Trends in Engineering, 2009.
19. G. Rosline Nesa Kumari, B. Vijaya Kumar, L. Sumalatha, and Dr V. V. Krishna, Secure and Robust Digital Watermarking on Grey Level Images, International Journal of Advanced Science and Technology, 2009.

20. Baisa L. Gunjal, R.R. Manthalkar, An overview of transform domain robust digital image watermarking algorithms, Journal of Emerging Trends in Computing and Information Sciences, 2010.
21. Darshana Mistry, Comparison of Digital Watermarking methods, 21st Computer Science Seminar SA1-T1-7, IJCSE, 2010.
22. R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, A digital watermark, in Proc. IEEE Int. Conf. Image Processing (ICIP), 1994.
23. W. Hong and M. Hang, Robust Digital Watermarking Scheme for Copy Right Protection, IEEE Trans. Signal Process, vo.l2, pp. 1- 8, 2006.
24. X. Xia, C. Boncelet, and G. Arce, A Multiresolution Watermark for Digital Images, Proc. IEEE Int. Conf. on Image Processing, Oct.1997.
25. Akhil Pratap Shing, Agya Mishra, Wavelet Based Watermarking on Digital Image, Indian Journal of computer Science and Engineering, 2011.
26. Bhatnagar, G. and Raman, B., A new robust reference watermarking scheme based on DWTSVD, Elsevier B.V. All rights reserved, 2008.
27. Barni M, Bartolini F, Piva, An Improved Wavelet Based Watermarking Through Pixelwise Masking, IEEE transactions on image processing, 2001.
28. D. Kundur and D. Hatzinakos, Digital Watermarking using Multiresolution Wavelet Decomposition, Proceedings, IEEE International Conference Acoustic, Speech, Signal Processing, 1998.
29. Nilanjan Dey, Anamitra Bardhan Roy, Sayantan Dey, A novel approach of color image hiding using RGB color planes and DWT, International Journal of Computer Applications, 2011.
30. Blossom Kaur, Amandeep Kaur, Jasdeep Singh, Steganographic Approach for hiding Image in DCT Domain, International Journal of Advances in Engineering & Technology, July 2011.
31. V . santhi, P,Arulmozhivarman, " Hadamard transform based adaptive visible/invisible watermarking scheme for digital images", journal of information security and applications 1 8 (2 0 1 3), Elsevier,(http://dx.doi.org/10.1016/j.istr.2013.01.001), pp: 1 6 7 -1 7 9.
32. Ling-Yuan Hsu , Hwai-Tsu Hu, "Blind image watermarking via exploitation of inter-block prediction and visibility threshold in DCT domain", Elsevier, J. Vis. Commun. Image R. 32 (2015) 130–143.
33. Jagdish Prasad Maheshwari, Mahendra Kumar, Garima Mathur, R P Yadav, Rajesh Kumar Kakerda, "Robust Digital Image Watermarking using DCT based Pyramid Transform via image compression", IEEE ICCSP 2015, pp: 1059-1063.
34. Madhuri Rajawat, D S Tomar, "A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT", 2015 Fifth International Conference on Communication Systems and Network Technologies, 2015 IEEE, pp:638-342.
35. Anurag Mishra, Charu Agarwal, Arpita Sharma, Punam Bedi, "Optimized gray-scale image watermarking using DWT–SVD and FireflyAlgorithm", Elsevier, Expert Systems with Applications 41 (2014) 7858–7867 .
36. Pan-PanZheng , JunFeng , ZhanLi , Ming-quanZhou , "A novel SVD and LS-SVM combination algorithm for blind watermarking",2014Elsevier, Neurocomputing142(2014), pp: 520–528.
37. Shao-li Jia, "A novel blind color images watermarking based on SVD", Optik 125 (2014) , pp: 2868–2874.
38. = Nasrin M.Makbol, Bee EeKhoo, " A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition", 2014 Published by Elsevier Inc., http://dx.doi.org/10.1016/j.dsp.2014.06.0121051-2004
39. = Muath AlShaikh, Lamri Laouamer, Laurent Nana, Anca Pascu, "A Novel CT Scan Images Watermarking Scheme in DWT Transform Coefficients", IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.1, January 2016, pp:62-71.
40. = Prasanth Viadya, Chandra Mouli, " Adap[tive Digital watermarking for copyright protection of digital images in wavelet domain", Elsevier, Procedia Computer Science 58 (2015), pp: 233 – 240.
41. Nasrin M. Makbol, Bee Ee Khoo, "Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition", International Journal of Electronics andCommunications (AEÜ), www.elsevier.com/locate/aeue, 2013, pp:102-112.
42. Pratibha Sharma, Shanti Swami, "Digital Image Watermarking Using 3 level Discrete Wavelet Transform" presented at Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013), pp: 129-133.
43. Alghoniemy M. and Tewfik A. H., 2000. Geometric distortion correction in image watermarking. Proc. SPIE Security and Watermarking of Multimedia Contents II ,3971:82- 89.
44. Alghoniemy M. and Tewfik A.H., 2000. Geometric distortion correction through image normalization. Proc. IEEE Int. Conf. Multimedia and Expo. 3:1291–1294.
45. Alghoniemy M. and Tewfik A.H., 2006. Progressive quantized projection approach to data hiding. IEEE Transactions on Image Processing, 15(2):459-472.

46. Alvarez R.M. and Perez G.F. 2002. Analysis of pilot based synchronization algorithms for watermarking of still images. Signal Processing: Image Communication. 17(8): 611 – 633.
47. Andreas L., and Jana D., 2006. Profiles for Evaluation - the Usage of Audio WET. SPIE conference, at the Security, Steganography, and Watermarking of Multimedia Contents VIII, IS&T/SPIE Symposium on Electronic Imaging.
48. Barni M., 2005. Effectiveness of exhaustive search and template matching against watermark desynchronization. IEEE Signal Process. Lett. 12(2):158–161.
49. Bas P., Chassery J.M., and Macq B., 2002.Geometrically invariant watermarking using feature point. IEEE Transactions on Image Processing, 11(9):1014–1028.
50. Cayre F., Fontaine C. and Furon T., 2005. Watermarking security, part I: theory, In: Security, Steganography and Watermarking of Multimedia Contents VII, Proceedings of SPIE. 5681.
51. Cayre F., Fontaine C. and Furon T., 2005. Watermarking security, part II: practice, In: Security,Steganography and Watermarking of Multimedia Contents VII, Proceedings of SPIE. 5681.
52. Checkmark Benchmarking, http://watermarking.unige.ch/Checkmark/, 2006
53. Christian K., Jana D., Andreas L., 2006. Transparency benchmarking on audio watermarks and steganography, SPIE conference, at the Security, Steganography, and Watermarking of Multimedia Contents VIII, IS&T/SPIE Symposium on Electronic Imaging.
54. Coltuc D. and Bolon P., 1999. Robust watermarking by histogram specification. Proc. IEEE Int. Conf. Image Processing. 2:236–239.
55. Cox I.J. and Linnartz J.P.M.G.,1998. Some general methods for tampering with watermarks. IEEE J. Selected Areas Community., 16(4)587–593.
56. Cox I. J., Miller M. L., and Bloom J. A. 2001. Digital Watermarking. San Francisco, CA: Morgan Kaufman.
57. Cox I., Miller M., Bloom J., Fridrich J., and Kalker T., Digital Watermarking and Steganography, 2007. Multimedia Information and Systems. 142–143.
58. Cox I.J. and Miller M.L. 1997. A review of watermarking and the importance of perceptual modelling. Proc. SPIE Electronic Imaging '97, Storage
59. and Retrieval for Image and Video Databases.
60. Cox, I.J. 1996. Secure spread spectrum watermarking for images, audio and video. International Conference on Image Processing, 234–246.
61. Cox, I.J., Kilian J., Leighton, F.T., and Shamoon, T.,1997. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing,6(12), 1673–1678.
62. Craver S., Memon N., Yeo B.L., Yeung M.M., 1997. Can invisible watermark resolve rightful ownerships Fifth Conference on Storage and Retrieval for Image and Video Database. 3022:310–321.
63. Deguillaume F., Csurka G., Pun T., 2000. Countermeasures for unintentional and intentional video watermarking attacks. IS&T/SPIE Electronic Imaging.