Multimedia Protection, Authentication and Advanced Digital Watermarking Techniques: A Survey

RanaKhudhair Abbas Ahmed
Al-Rafadian University College/ Computer Engineering Techniques Department
Baghdad, Iraq

Abstract-*Multimedia contents such as images, videos, audio, and texts are easy to available for download through internet in worldwide. Duplication of multimedia contents is to create using different software. This type of operation some time created problem of copyright and ownership authentication. Digital watermarking techniques are usedto protect multimedia contents. This paper gives various watermarking techniques in transform domain and sparse domain for protection and authentication of multimedia contents.*

Keywords - *Wavelet Transform, Copyright, Authentication, Watermarking*

I. INTRODUCTION

With multimedia data widely available on the web, a watermark could be used to provide authentication in terms of a secondary data which is overlaid on the primary data to provide protection to primary data [1, 2]. Watermarking techniques can be divided into four categories according to the type of digital to be watermarked as follows as text watermarking, image watermarking [3], audio watermarking and video watermarking. The digital watermark can be divided into noise and image according to inserted watermark type [4]. The digital watermark can be divided into visible watermark and invisible watermark according to the perceptibility [5]. The watermarking techniques can be classified according to its requirement into various ways [6, 7].

Digital watermarking is a state of art technique to put secret information behind a host medium in such a manner that the imposter can't be visualized the secret information with a naked eye and he/she perceives it as a normal host medium. There are two major domains for watermarking multimedia data namely spatial domain and transform domain. Spatial domain watermarking provides high perceptible such that the quality of the original and watermarked multimedia data is almost same. However the problem of spatial domain watermarking is that the robustness achieved is far less comparatively. Transform domain watermarking is far better than spatial domain watermarking so far as robustness is concerned and that is the reason why transform domain watermarking techniques are used to preferred for multimedia data protection. When watermark data embed into host data, watermark embedding techniques are modifying the host data according to watermark information in a perceptually invisible manner [6, 7].

II. WHAT IS MULTIMEDIA?

When different people mention the term **multimedia**, they often have quite different, or even opposing, viewpoints [8]:

- A PC vendor: a PC that has sound capability, a DVD-ROM drive, and perhaps the superiority of multimedia-enabled microprocessors that understand additional multimedia instructions.
- A consumer entertainment vendor: interactive cable TV with hundreds of digital channels available, or a cable TV-like service delivered over a high-speed Internet connection.
- A Computer Science (CS) student: applications that use multiple modalities, including text, images, drawings (graphics), animation, video, sound including speech, and interactivity.

A. Multimedia Authentication

Authenticity, by definition, means something as being in accordance with fact, as being true in substance", or as being what it professes in origin or authorship, as being genuine [9]. "A third definition of authenticity is to prove that something is actually coming from the alleged source or origin" [10,11]. For instance, in the courtroom, insurance company, hospital, newspaper, magazine, or television news, when we watch/hear a clip of multimedia data, we hope to know whether the image/video/audio is authentic. For electronic commerce, once a buyer purchases multimedia data from the Internet, she needs to know whether it comes from the alleged producer and she must be assured that no one has tampered with the content. The credibility of multimedia data is expected for the purpose of being electronic evidence or a certified product. In practice, different requirements aspect the

methodologies and designs of possible solutions [12].

B.Multimedia Authentication Objectives: Complete Authenticationv.s. Content Authentication

Based on the objectives of authentication, multimedia authentication techniques can be classified into two categories: complete authentication and content authentication. Complete authentication refers to techniques that consider the whole piece of multimedia data and do not allow any manipulations or transformation [13].

Early works of multimedia authentication were mostly in this category. Because the non-manipulable data are like messages, many existing message authentication techniques can be directly applied. For instance, digital signatures can be placed in the LSB of uncompressed data, or the header of compressed data. Then, manipulations will be detected because the hash values of the altered message bits will not match the information in the digital signature. In practice, fragile watermarks or traditional digital signatures may be used for complete authentication. Content Authentication refers to a different objective that is unique for multimedia data. The meaning of multimedia data is based on their content instead of the bit streams. In some applications, manipulations on the bit streams without changing the meaning of content are considered as acceptable [14, 15].

Compression is an example. Today, most digital multimedia data are stored or distributed in compressed forms. To satisfy various needs of broadcasting, storage and transmission, transcoding of compressed digital videos may also be required [14].

For instance, digital video clips are usually shot and stored in the compressed format with a pre-determined bitrate, but distributed with a different bitrate in transmission. Transcoding processes change the pixel values of the digital video but not its content. Therefore, videos that are obtained by transcoding the original one should be considered as authentic [14].

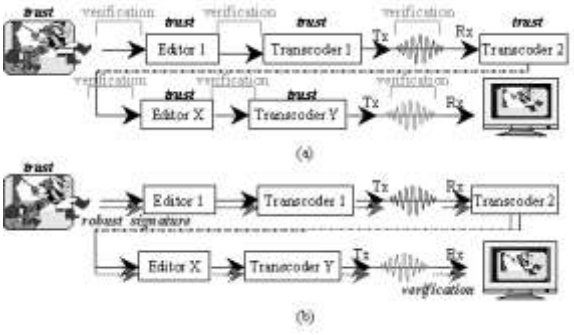

Fig. 1-1: (a) Complete Authentication: multimedia data have to be examined in each transmission, and each intermediate stage must be trustworthy; (b) Content Authentication: multimedia data are endorsed by the producer and verified only in the last stage [14].

Figure 1-1 shows the benefit of the Multimedia Content Authentication (MCA). It represents the complete process of multimedia data, from being produced to being consumed. With complete verification, we have to verify the data at every transmission stage and trust all the interim entities. However, with content verification, we can transmit the robust signature with the data and only verify it at the last stage. Therefore, we do not need to verify the data at each stage and question the trustworthiness of the intermediate people. This enhances the authenticity of the data. As in Figure 1-1, if the producer is a trustworthy camera, it can somehow provide credibility of reality to the data, i.e., proving that the multimedia data are real". This is especially useful for those multimedia data that are needed as electronic evidence [14].

C. Multimedia Authentication Sources: Raw Data v.s. Compressed Data

Multimedia compression standards have been designed and widely adopted by various applications: JPEG in the WWW, MPEG-1 in VCD, MPEG-2 format in DVD, and H.261 and H.263 in video conferencing. The source of a multimedia authentication system may be raw data or compressed data. In practical applications, the raw format of multimedia data may not be available [14]. For instance, a scanner generates temporary raw images but only saves them in their compressed format; a digital camera which captures image/video produces compressed lossless only, without generating any raw data. Therefore, an authentication system which can only authenticate raw data may have limited uses in practice. However, exceptions exist in [14]:

1. Non-standard data such as 3D objects, and
2. Medical images which usually do not tolerate lossy compression.
3.

D. Multimedia Authentication Methods: Watermarking v.s. Digital Signature

Since the meaning of multimedia data is based on its content, we can modify the multimedia bit stream to embed some codes, i.e., watermarks, without changing the meaning of the content. The embedded watermark may represent either a specific digital producer identification label (PIL) or some content-based codes generated by applying a specific rule. In the authenticator, the watermarks are examined to verify the integrity of the data [14].

For complete authentication of uncompressed raw multimedia data, watermarking may work better than digital signature methods because [14]:

- the watermarks are always associated with the data and can be conveniently examined, and
- There are many spaces in the multimedia data in which to embed the watermarks with negligible quality degradation (known as invisible watermarks).

Previous works in [18, 13] have shown effective watermarking methods for these applications. However, there is no advantage to using the watermarking method in compressed multimedia data for complete verification. Compression standards, e.g., MPEG or JPEG, have user-defined sections where a digital signature can be placed. Because multimedia data are stored or distributed in specific file format instead of pixel values, the digital signature can be considered as being embedded" in the data.

Once the multimedia data is modified, the user-defined section of the original data is usually discarded by the editing software. Even if the digital signature can be preserved by the software, we can easily detect the modification, since the hash values of the modified data will not be the same as the original. Moreover, compressed multimedia data over less space for hiding watermarks [14].

Visual quality of the data may be compromised in order to ensure that enough watermarking bits for adequately protecting the data. For content authentication, compression should be distinguished from other manipulations. Previous watermarks are either too fragile for compression or too extensible to detect malicious manipulations. The performance of an authenticator should be simultaneously evaluated by two parameters: the probability of false alarm and the probability of missing manipulations. Fragile watermarks, which have low probability of miss, usually fail to survive compressions such that their probability of false alarm is very high. Previous researchers have attempted to modify the fragile watermark to make it more robust with compression [13, 19, 20].

However, such modifications failed to distinguish compression and tampering. When they lower the probability of false alarm, the probability of miss in their systems increases significantly. On the other hand, robust watermarks are robust to most manipulations, but are usually too robust to detect malicious manipulations. Their probability of miss is usually too high [14].

Digital signatures can be stored in two different ways. If the header of the compressed source data remains intact through all processing stages, then the digital signature can be saved in the header. Otherwise, it can be stored as an independent file. Anyone who needs to authenticate the received multimedia data has to request the source to provide the signature [14].

III. COPYRIGHT AND MULTIMEDIA

The task of applying copyright law to a new technology is a hauntingly familiar problem. The history of copyright jurisprudence has largely consisted of the attempt to apply a threadbare set of rules to new technological offspring. Like hand-me-down clothes, their fit is less than perfect. Multimedia programs, like any computer programs, have two components: data (input and output) and processing (coded logic). This section explains that copyright law affords disparate protection to these components, and discusses why the disparity will significantly impact the development of the multimedia industry [21].

IV. DIGITAL WATERMARKING TECHNIQUES IN SPATIAL DOMAIN

The basically two watermarking techniques, namely as LSB modification and correlation of different noise sequences are available in spatial domain. These techniques are easy to implement without prior knowledge of digital watermarking technique concept.

1) LSB Modification Based Watermarking Technique

In Least significant bit (LSB) modification technique [22, 23, 24], most significant bits of the watermark are replaced with the least significant bits of the host digital data. The visual degradation of host digital data is very less in this technique because of important data of the host digital data are less affected due to modification.

2) Correlation Based Watermarking Technique

The other watermarking technique in the spatial domain is to exploit the correlation properties [7, 25, 26, 27] of the pseudo-random noise patterns and white Gaussian noise patterns which are additive in nature. These patterns are utilized for the purpose of watermarking because of they have low amplitude like noise, great correlation property and less affect by interference. These noise sequences are utilized for the purpose of watermarking due to the following reasons.

1. These noise sequences are random in nature. An initial seed is required for generation of sequences.
2. It becomes very difficult to predict these sequences by imposter until and unless there is a prior knowledge of the seed as well as the knowledge of technique.

In correlation based watermarking technique, two noise sequences are generated using the same private key. One will be used when the watermark data is bit 1 and the other is used when it is bit 0.

V. DIGITAL WATERMARKING TECHNIQUES IN TRANSFORM DOMAIN

In transform domain watermarking techniques [7, 28], frequency domain version of the image is used for watermark information embedding. The Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are two of most frequently image transform used for transform watermarking techniques [17]. In this technique, an image is transformed from the spatial to frequency domain. Then, according to the human visual system, transform coefficients are arranged into various priorities. Then the magnitudes of transform coefficients are changes according to watermark data bits. The watermarking technique in transform domain is performed mainly in three steps. The first step is to perform forward transform which converts the spatial domain data into the frequency domain and get the transform coefficients. The second step is to modify the transform coefficients according to the watermark data. The last step is performing the inverse transform to get watermarked data. There are basically two watermarking techniques such as Discrete Cosine Transform (DCT) based technique and Discrete Wavelet Transform (DWT) based technique is available in transform domain which are explained below.

1) Discrete Cosine Transform (DCT) Based Watermarking Technique

Discrete Cosine Transform [3, 17, 21, 22, 23, 24, 25, 26, 27]) converts host digital data from the spatial domain into the frequency domain. DCT converts a spatial domain 2D representation into its frequency domain equivalent. The output of DCT is that the size of the transformed frequency domain data is exactly equal to that in the spatial domain. The DC coefficient of the DCT transformed data is situated at the upper left side and contains very important of information of data because of it is low frequency coefficients. All coefficients other than DC coefficients are called as AC coefficients. The DC DCT coefficients are always an integer and the range of coefficients would be in between -1024 to 1023 while AC DCT coefficients may be integer or non-integer.

2) Discrete Wavelet Transform (DWT) Based Watermarking Technique

In most of applications such as compression, digital watermarking, image fusion of the field of image processing, the wavelet transform has very important contributions to make the application smooth and fruitful. Waves are periodic in nature and are oscillating with respect to time or space. Actually the DWT performed convolution operation between 1D or 2D signals with particular instances of wavelets at various time scales and positions. The Discrete Wavelet Transform [36, 37, 38, 39, 40, 41, 42, 43, 44] is based on sub band coding, is easy to implement, does require limited time and resources and yield fast computations of wavelet transform. In wavelet analysis two words such as approximations and details are frequently used. The approximations wavelets are the high-scale, low frequency coefficients of the signal. The details wavelets are the low-scale, high frequency coefficients of the signal. For a 2D image I (x, y), the forward and reverse decomposition can be done by discrete wavelet transform (DWT) and inverse discrete wavelet transform (IDWT) first on dimension x and then the same procedure can be performed for the other dimension y. This result in the representation of the image which is pyramidal in nature.This kind of 2D DWT decomposition the image into four sub bands, namely, approximation sub band, horizontal sub band, vertical sub band and diagonal sub band [17].

VI. ADVANCED DIGITAL WATERMARKING TECHNIQUES

There are various limitations of above all watermarking techniques in term of less computational security and less payload capacity, less ability to embed grayscale and color watermark data. To overcome these limitations of watermarking techniques, inventors are proposed new watermarking techniques for protection of multimedia data. The inventors described watermarking techniques such as Singular Value Decomposition (SVD) based watermarking technique for hiding grayscale watermark data; hybrid watermarking technique using various images transform such as DCT, DWT, SVD for protection of digital video data; DWT based watermarking technique for hiding color watermark data; compressive sensing (CS) theory and curvelet based watermarking technique for protection of digital image. The more details on these watermarking techniques are given below.

a. *Singular Value Decomposition (SVD) Based Watermarking Technique for hiding Grayscale Watermark Data*

Singular value decomposition [45, 31, 46, 47, 48, 49, 50] is a numerical technique based on the linear algebra and it is used to diagonal matrices in numerical analysis. There are lots of areas where SVD finds its application. When SVD is applied to an image with size of M×N, three matrices are found, namely U, V and S. The U and V matrices are called unitary matrices having size of M×M and N×N respectively. S matrix is called diagonal matrix

having size of M×N. The singular matrix is very important for watermarking purpose and entries in this matrix are arranged diagonally and in ascending order. One of the most important properties of the singular values is that they are very much stable and hence if a small change is made in the value of host digital data its singular values do not have any significant change.

b. Hybrid Watermarking Technique using Various Image Transform such as DCT, DWT, SVD for Protection of Digital Video Data

Up to this point it had been seen that individual DCT and DWT based watermarking technique is better in perceptibility as compare to correlation based watermarking technique while SVD based watermarking technique is better than correlation, DCT or DWT based watermarking technique because it is able to embed grayscale watermark data into the digital data. So in this technique, hybridization of the two transforms namely DCT and DWT and one linear algebra named SVD is used for achieving high perceptible watermarked video data. A 2D DCT is applied to the Y plane of the frame. Then 3rd level DWT is applied on the DCT transformed Y plane of the frame. Singular value decomposition is applied to DWT transformed Y plane of the frame.

c. DWT based Watermarking Technique for Hiding Color Watermark Data

Up to this point it had been seen that all above watermarking techniques are used for embedding monochrome and grayscale watermark data into the host digital data. So in this technique, DWT is used for embedding color watermark data into color host digital image. This technique is visible watermarking technique and used for owner identification.

d. Compressive Sensing (CS) theory and Curvelet based Watermarking Technique for Protection of Digital Image

Up to this point it had been seen that all watermarking techniques are embedded direct watermark data into the host digital data. Then imposter or unauthorized people can easily get watermark data by applying various manipulations on watermarked data. So in this technique, compressive sensing (CS) theory [51, 52, 53] has provided protection for watermark data before embedding into the host digital data. This technique adds two procedures such as CS theory acquisition procedure and CS theory recovery procedure in traditional watermarking technique.

In this technique, watermark data are first converted into its sparse measurement using CS theory acquisition procedure at embedder side and at detector side, watermark data are reconstructed from extracted sparse measurements using the CS theory recovery procedure. There is necessary condition is application of CS theory on image is that the image must be sparse in its own domain. In this technique, sparse measurements of watermark data are embedded into transform coefficients of host digital data to generate watermarked digital data. In this technique, fast discrete curvelet transform (FDCT) coefficients of host digital data is used for watermark data embedding.

In 2005, Candès, Demanet and Donoho described new image transform, namely curvelet transform based on sparsity theory. Curvelet transform is calculated the inner relationship between the image and its curvelet function to realize sparse representation of the image. There are two types of curvelet transform such as continuous curvelet transform and discrete curvelet transform available in the literature. Discrete fast curvelet transform is used most of image processing applications such as compression, watermarking, sparse representation and edge detection [52]. There are two types of fast discrete curvelet transform, namely unequispaced fast Fourier transform (USFFT) and frequency wrapping. The frequency wrapping based discrete curvelet transform technique is easy to implement, less computation time and easy to understand compared to the USFFT technique [52]. Therefore, frequency wrapping based curvelet transform technique is used in many image processing applications. When the frequency wrapping based curvelet transform [52] applied to an image, then the image is converted into low frequency coefficients and high frequency coefficients. The curvelet decomposition of image by frequency wrapping based curvelet transform with 4 scales and 16 orientation parameter are given as C {1, 1}; C {1, 2}; C {1, 3}; C {1, 4}. Given the decomposition scale 4, the curvelet coefficients C {1, 1} is the low frequency coefficients and the other coefficients C {1, 2}; C {1, 3}; C {1, 4} is the high frequency coefficients.

VII. CONCLUSION AND FUTURE DIRECTION

Watermarking techniques are used for multimedia data protection. The LSB technique is not a very good technique for digital watermarking because of limited robustness against watermarking attack. In correlation based techniques, when the noise power increase, then the perception of recovered watermark data is increasing. The spatial domain watermarking techniques are easy to be applied on any multimedia data and provide high payload capacity. But the limitation of spatial domain watermarking techniques is that there are not robust against watermarking attacks.

The transform domain watermarking techniques based on DCT and DWT provide more robustness against watermarking attacks. But the limitation of transform domain watermarking techniques can't be applied for larger size watermark data. The limitation of spatial and transform domain watermarking techniques can be overcome by using a hybrid approach of watermarking. The perceptibility of multimedia data using the hybrid watermarking technique is higher than spatial and transform domain watermarking techniques at the same gain factor. The robustness of hybrid watermarking techniques is considerably higher than spatial and transform domain watermarking techniques.

The SVD based watermarking technique is used for embedding grayscale watermark data into host digital data. This chapter has also given watermarking technique for embedding of color watermark data. Also watermarking technique for grayscale watermark data embedding into host digital data is described using new signal processing theory namely CS theory and curvelet transform. In future, We can apply watermarking techniques to other multimedia data such as audio and text.

VIII. REFERENCES

[1] Mahmoud El-Gayyar., "Watermarking Techniques – Spatial Domain Digital Rights Seminar. Media Informatics", University of Bonn, Germany, May 2006.

[2] Reena, Vandera."Modified Approach of Digital Image Watermarking Using Combined Dct and Dwt Modified Approach of Digital Image Watermarking Using Combined Dct and Dwt", Volume 3, Issue 7, July, 2013.

[3] Munesh Chandra "A DFT-DWT Domain Invisible Blind Watermarking Techniques for Copyright Protection of Digital Images", Advances in Wavelet Theory and Their Applications in Engineering, Physics and Technology 2015.

[4] HamzaA. Ali, Sama'a A. K. khamis, World of Computer Science and Information Technology Journal (WCSIT) Vol. 2, No. 5, 163-168, 2012 ,Robust Digital Image Watermarking Technique Based on Histogram Analysis.

[5] International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014) 218 Vol. 2, Issue 2, Ver. 2 (April - June 2014) ISSN : 2347 - 8446 (Online) ISSN : 2347 - 9817 (Print) © 2014, IJARCST All Rights Reserved www.ijarcst.com Digital Watermarking: Comparing Two Techniques I Jyoti Rani, IIAnupam

[6] Wolfgang, R. &Podilchuk, C., "Perceptual Watermarks for Digital Images and Video". Proceedings of the IEEE, 87(7), 1277 – 1281, July 1999.

[7] Langelaar, G., Setyawan, I. &Lagendijk, R., "Watermarking of Digital Image and Video Data – A State of Art Review", IEEE Signal Processing Magazine, 20 – 46, Sept. 2000.

[8] Li &Drew., "Fundamentals of Multimedia, Chapter 1, Introduction to Multimedia", Prentice Hall, 26. M. Wu and B. Liu, "Watermarking for Image Authentication", IEEE Proc. Of ICIP, Chicago, 2003.

[9] The Oxford English Dictionary, 2nd Ed., Oxford Univ., pp. 795-796, 1989.

[10] The Webster's New 20th Century Dictionary.

[11] Dattatherya , S. VenkataChalam , Manoj Kumar Singh, A Generalized Image Authentication Based On Statistical Moments of Color Histogram, Int. J. on Recent Trends in Engineering and Technology, Vol. 8, No. 1, Jan 2013.

[12] D. Bearman, and J. Trant, "Authenticity of Digital Resources: Towards a Statement of Requirements in the Research Process", D-LibMagazine, June 1998.

[13] M. Yeung and F. Mintzer. "An Invisible Watermarking Technique for Image Verification", IEEE International Conf. on Image Processing, Santa Barbara, Oct. 1997.

[14] Ching-Yung Lin. " Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection", Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Graduate School of Arts and Sciences Columbia University, 2000.

[15]Clara Cruz Ramos, R. Reyes, Mariko Nakano-Miyatake, He?ctor Manuel Pe?rezMeana, "Watermarking-Based ImageAuthentication System in the Discrete Wavelet Transform Domain", Discrete Wavelet Transforms: Algorithms and Applications, 2011.

[16]JasniZain, and Malcolm Clarke, 3rd International Conference:Sciences of electronic, Technologies of Information andTelecommunications, March 27-31, 2005 –, Mohammad Faizal Ahmad Fauzi, RajasvaranSecurity In Telemedicine: Issues In WatermarkingMedical Images , SETIT 2005

[17] Hadamard Transform ArisMarjuni, International Journal of Computer and Electrical Engineering, Vol. 5, No. 3, June 2013, An Improved DCT-Based Image Watermarking Scheme Using Fast Walsh, Logeswaran, and Swee-HuayHeng.

[18] R. G. van Schyndel, A. Z. Trikel, and C. F. Osborne. "A Digital Watermark", IEEE International Conf. on Image Processing, Austin, Texas, Nov. 1994.

[19] B. Zhu, M. D. Swanson, and A. H. Tewk. "Transparent Robust Authentication and Distortion Measurement Technique for Images", The 7th IEEE Digital Signal Processing Workshop, pp. 45-48, Sep 1999.

[20] R. B. Wolfgang and E. J. Delp. "A Watermark for Digital Images", IEEE International Conf. on Image Processing, Laussane, Switzerland, Oct. 1996.

[21] Heather J. Meeker., "Multimedia and Copyright", Rutgers Computer and Technology Law Journal, 1994.

[22] Lee, Y. & Chen, L, "High Capacity Image Steganographic Model", IEEE proceedings of Vision Image and Signal Processing, 288 – 294, June 2000.

[23] Chan, C. & Cheng, L., "Hiding Data in Images by Simple LSB Substitution", Pattern Recognition, 37, 469 – 474, 2004.

[24]Ramalingam, M., Stego, "Machine – Video Steganography using Modified LSB Algorithm", World Academy of Science, Engineering and Technology, 74, 502 – 505, 2011.

[25] Arena, S., Caramma, M. &Lancini, R., "Digital Watermarking Applied to MPEG-2 Coded Video Sequences Exploiting Space and Frequency Masking", Proceedings of International Conference on Image Processing, 2, 796 – 799, 2000.

[26] Bangaleea, R. &Rughooputh, H., "Performance Improvement of Spread Spectrum Spatial Domain Watermarking Scheme Through Diversity and Attack Characterization", IEEE Conference Africon, 293 – 298, 2002.

[27] Thanki, R., Trivedi, R., Kher, R. &Vyas, D., "Digital Watermarking Using White Gaussian Noise (WGN) in Spatial Domain", Proceedings of International Conference on Innovative Science & Engineering Technology (ICISET), 38 – 42, 2011.

[28] Dajun, H., Qibin, S. &Tian, Q., "A Semi-fragile Object based Video Authentication System", Proceedings of the International Symposium on Circuits and Systems, 814 – 817, 2003.

[29] Hernandez, J., Amado, M. & Perez-Gonzalez, F., "DCT domain Watermarking Techniques for Still Image: Detector Performance Analysis and a New Structure", IEEE Transactions on Image Processing, 9, 55 – 68, Jan 2000.

[30] Lu, C. & Liao, H., "Video Object based Watermarking: A Rotation and Flipping Resilient Scheme", Proceedings of International Conference on Image Processing, 2001.
[31] Huang, F. & Guan, Z., "A Hybrid SVD-DCT Watermarking Method Based on LPSNR", Pattern Recognition Letters 25, 1769 – 1775, 2004.
[32] Preda, R. &Vizireanu, D., "Blind Watermarking Capacity Analysis of MPEG2 Coded Video", Proceedings of Conference of Telecommunications in Modern Satellite, Cable and Broadcasting Services, Serbia, 465 – 468, Sept. 2007.
[33] Koz, A. &Alatan, A., "Oblivious Spatio-Temporal Watermarking of Digital Video by Exploiting the Human Visual System", IEEE Transactions on Circuits and Systems for Video Technology, 18(3), 326 – 337, March 2008.
[34] Sridevi, T., Krishnaveni, B., Vijayakumar, V. &Ramadevi, Y., "A Video Watermarking Algorithm for MPEG Videos", A2CWiC 2010 – Amrita ACM-W Celebration of Women in Computing, Sept. 2010.
[35] Ding, Y., Zheng, X., Zhao, Y. & Liu, G., "A Video Watermarking Algorithm Resistant to Copy Attack", Proceedings of 3rd International Symposium on Electronic Commerce and Security, July 2010,.
[36] Ejima, M. & Miyazaki, A., "A Wavelet Based Watermarking for Digital Images and Videos", IEEE International Conference on Image Processing, 678 – 681, August 2000.
[37] Serdean, C., Ambroze, M., Tomlinson, M. & Wade G., "Combating Geometrical Attacks in a DWT based Blind Video Watermarking System", IEEE Region 8 International Symposium on Video/Image Processing and Multimedia Communications, Zadar, Croatia, 263 – 266, June 2002.
[38] Raval, M. &Rege, P., "Discrete Wavelet Transform Based Multiple Watermarking Scheme", Proceedings of the Convergent Technologies for the Asia-Pacific Region, 3, 935 – 938, 2003.
[39] Fan, L. &Yanmei, F., "A DWT based Video Watermarking Algorithm Applying DS-CAMA", IEEE Region 10 Conference TENCON 2006.
[40] Elbasi, E., "Robust MPEG Video Watermarking in Wavelet Domain", Trakya University Journal of Science, 8(2), 87 – 93, 2007.
[41] Essaouabi, A. &Ibnelhaj, E., "A 3D Wavelet based Method for Digital Video Watermarking", Proceedings of the 4th IEEE Intelligent Information Hiding and Multimedia Signal Processing, July 2009.
[42] Raghavendra, K. &Chetan, K., "A Blind and Robust Watermarking Scheme with Scrambled Watermark for Video Authentication", Proceedings of IEEE International Conference on Internet Multimedia Services Architecture and Applications, Dec. 2009.
[35] Hussein, J. & Mohammed, A., "Robust Video Watermarking using Multiband Wavelet Transform", IJCSI International Journal of Computer Science Issues, 6(1), 44 – 49, 2009.
[44] Mostafa, S., Tolba, A., Abdelkader, F. &Elhindy, H., "Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform", IJCSNS International Journal of Computer Science and Network Security, 9(8), 45 – 52, Aug. 2009.
[45] Ganic, E. &Eskicioglu, A., "Secure DWT-SVD Domain Image Watermarking Embedding Data in All Frequencies", ACM Multimedia and Security Workshop 2004, 1 – 9, 2004.
[46] Dili, R. &Mwangi, E., "An Image Watermarking Method Based on the Singular Value Transformation and the Wavelet Transformation", Proceedings of IEEE AFRICON, 1 – 5, 2007.
[47] Mansouri, A., Mahmoudi, A., Aznaveh, &Azar, F., "SVD based Digital Image Watermarking using Complex Wavelet Transform", Sadhana, 34(3), 393 – 406, June 2009.
[48] Santhi, V. &Thangavelu, A., "DWT SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space", International Journal of Computer Theory and Engineering. 1(4), Oct. 2009.
[49] Kamlakar, M., Gosavi, C. &Patankar, A., "Single Channel Watermarking for Video Using Block based SVD", International Journal of Advances in Computing and Information Researches, 1(2), April 2014.
[50] Gupta, A. &Raval, M., "A Robust and Secure Watermarking Scheme Based on Singular Value Replacement", Sadhana, 37(4), 425 – 440, Augst 2012.
[51] Donoho, D., "Compressed Sensing. IEEE Transaction on Information Theory", 52(4), 1289 – 1306, April 2006.
[52] Candès, E., "Compressive Sampling. Proceedings of the International Congress of Mathematicians, Madrid", Spain, 2006.
[53] Baraniuk, R., "Lecture notes on Compressive Sensing", IEEE Signal Processing Magazine, 24, 118 – 124, July 2007.