A Study on Invisible Digital Image and Video Watermarking Techniques

Farha Khan[1], M. Sarwar Raeen[2]
M.Tech Scholar[1]Professor[2]
Department of Electronics and Communication
All Saints' College of Technology,Gandhi Nagar, Bhopal

ABSTRACT: Digital watermarking was introduced as a result of rapid advancement of networked multimedia systems. It had been developed to enforce copyright technologies for cover of copyright possession. This technology is first used for still images however recently they need been developed for different multimedia objects like audio, video etc. Watermarking, that belong to the information hiding field, has seen plenty of research interest. There's a lot of work begin conducted in numerous branches in this field. The image watermarking techniques might divide on the idea of domain like spatial domain or transform domain or on the basis of wavelets. The copyright protection, capacity, security, strength etc are a number of the necessary factors that are taken in account whereas the watermarking system is intended. This paper aims to produce a detailed survey of all watermarking techniques specially focuses on image watermarking types and its applications in today's world.

Keywords: *Digital watermarking, Spatial Domain,Transform Domain, LSB, DWT, DCT, SVD.*

*****

1. Introduction

Business application has great development in multimedia system and many fields such as audio, video, text, pattern and digital data. In the last 20 years the internet has great development which provides security in the field of effectiveness and continence.In 1992 information is spread away across the globe. With the help of Jupiter research people got the uses and advantages of internet, web access, electronic mail and messaging or social networking, online messaging. It provides many advantages in various fields like education, research and development, business or medical [1].Business application is useful and increasing the growth of business process communication and digital media. There are many techniques which provide the security for digital data like audio video, text, encryption, authentication and time stamping. It is improved the protection of digital data. It is used to merge the low level signal into digital data, which is known as watermark.

Watermarking technique provides more information about host image. Watermarking is basically four step process as shown in Fig. 1 that includes: Generation, embedding, distribution and attacks and extraction [2]. Watermark generation steps generate a logo in form of audio/video/text that is unique to the content and must be such that extraction or distortion from different attacks is difficult. Embedding is a process that embeds logo or mark image into host image. Distribution is a process that can be seen as the transmission of watermarked data. And if someone tries to modify the content then it is called attacks. Extraction is the process that allows owner to be identified and provides information to the intended recipients. Extraction is same process as embedding but occurs in reverse manner. Different techniques are used for watermark embedding and extraction.

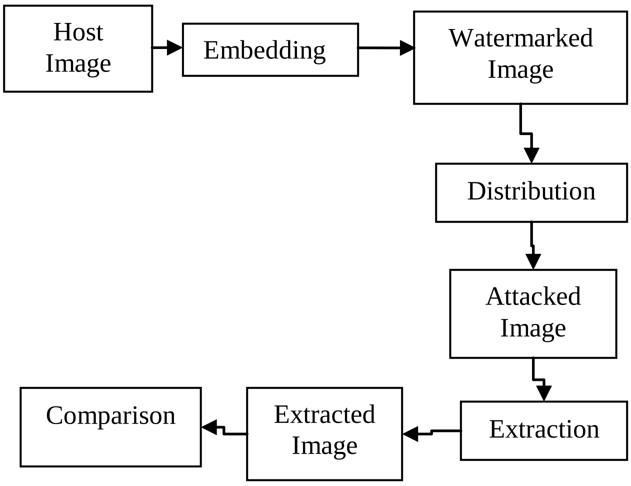

Fig.1. General Image watermarking procedure

Properties of any watermarking techniques are imperceptibility, robustness, capacity and security [3]. Each application has its own requirements. Watermarking technologies are developed according to the requirements of application and each application does not require each of the properties.

There are many types of watermarking system:

Visible Watermarking System: In this system, it is semi transparently for text or image, because it is embedded into original data. When attack is applied the image transformation visible watermarking is more robust. It provides the copyright protection for digital format visible watermarking is authenticated for data as digitally stamped document.

Invisible Watermarking System: In this system, it cannot be seen the embedded watermark by naked eyes. Electronic device is authenticated for extracted the embedded information and it is authorized for identifying the owner, creator source and multimedia data.

Blind Watermarking System: There is no need the original image if extract the watermark from watermark data it is called blind watermarking system. It is popular because the original data which is stored in memory and it reduced the cost of overheads.

Non-Blind Watermarking System: In this technique it needs to original data so that it can extract the watermark it is called non- blind watermarking system. It is robust than blind watermarking.

Fragile Watermarking System: In fragile watermarking the watermark is embedded in such a way that any modification or manipulation of the image would alter or destroy the watermark. It provides the legitimacy of multimedia system knowledge after we are embedding the delicate watermark into multimedia system data. If any modification happens into multimedia knowledge the delicate watermarking is employed to distort the watermark data. If we have a tendency to extract the watermark knowledge from original watermark once examination it's simply known whether or not multimedia data is manipulated or altered.

Semi-fragile watermark: It provides robustness and characteristics between robust and fragile watermark. It can detect information alteringtransformations.

2. Watermarking Application

Watermarking applications is an explosion in the use and distribution of digital media. Personal computers with Internet connections (broadband) have become more common and have made the distribution of data and multimedia applications much easier and faster. E-commerce applications and online services are rapidly developing. Even home video and analog audio devices are quickly replaced by digital successors. As a result, digital mass storage devices for multimedia data have entered the mainstream market today. Digital data has many advantages over analog data. However, this also opens up the possibility of unlimited duplication and modification of copyrighted material.

In [4] Garima et al. discussed about watermarking, that belong to theinformation hiding field. There's a lot of work begin conducted in numerous branches in this field. The image watermarking techniques might divide on the idea of domain like spatial domain or transform domain or on the basis of wavelets. The copyright protection, capacity, security, strength etc. are a number of the necessary factors that are taken in account whereas the watermarking system is intended.In order to prevent unauthorized access or manipulation of digital multimedia data, two complementary techniques can be used, namely cryptography and digital watermarking. Encryption techniques can be used to protect digital data during transmission from the sender to the recipient. Once the recipient has received and decoded the data, the data is identical to the original data and is no longer protected. The tattoo techniques complete the cryptography by integrating a secret, imperceptible signal, a watermark, in the original data so that they always exist. This watermark is used for the following purposes:

- Copyright Protection: A watermark is used to provide copyright information as evidence in the event of a copyright or property dispute.
- Fingerprints: Unique information directly related to user identification is incorporated into the data as a watermark. In case of copyright infringement, this watermark can be used to track the source of illegal copies.
- Broadcast monitoring: a watermark is embedded in the data, such as advertising or protected material, to allow automatic tracking of data in transmission channels. The results of this monitoring can be used for licensing or copyright purposes.
- Indexing: indexing of video mail where comments can be incorporated into video content: indexing of movies and news, where markers and comments from search engines can be inserted and used.
- Medical application: inserting patient's date and name into medical images could be a useful security measure.
- Data embedding: digital tattoo techniques can incorporate messages into the data. Data can be secret or private, but it can also be public.

Compression: In this scheme, image color information is incorporated as a watermark in luminance data to reduce data storage requirements

3. Related Work

Watermarking method can be categorized into two groups, namely spatial domain and transform domain. In the spatial domain, the host image pixels are manipulated and the watermark information is directly inserted into them. Although the spatial domain methods have lower computational complexity and higher capacity, they are vulnerable to various attacks and have worse robustness. On the other hand, transform domain methods not only tolerate various attacks but have good performances. Although transform domain methods need predefined transformation and inverse transformation, and the watermark information is distributed over the whole range of pixels of the host image instead of local parts, transform domain methods are more robust to various attacks [5].

At present, the watermarks used in colour image watermarking techniques are most pseudo-random sequence, binary or grayscale image and only few watermarking schemes used the colour image as watermark [6].

Imane Assini et al. [1] proposed a discrete wavelet transform (DWT), fast Walsh-Hadamard transform (FWHT) and singular value decomposition (SVD) technique is used for two image watermarking. The result analysis shows better compromise invisibility capacity robustness with low PSNR value.

Divjot Kaur Thind [2] proposed a digital video watermarking scheme which combines Discrete wavelet transform (DWT) and Singular Value Decomposition (SVD). The simulation result provide robustness against attacks such as frame dropping, frame averaging and lossy compression. The main drawback of this scheme was that its complexity translates in this case into more resources required to perform the computation - more memory and/or processor cycles and/or time.

Aparna J R et al. [3] proposed a block based image watermarking algorithm which uses cryptographic algorithm to find out the positions of the cover image in which the watermark is to be embedded. The result shows that this scheme is robust enough to withstand scaling, blurring and sharpening attacks. The drawback is that PSNR values are not much improved.

Adamu Muhammad et al. [4] proposed a human visual system based watermarking algorithm for spatial scalable coding based on the H.264/SVC standard. The minimal watermark detection rates after re-encoding, recompression and Gaussian filtering attacks are 0.96, 0.94 and 0.66, respectively. Drawbacks are that visual quality degradation and bit rate overhead.

Rohit Thanki et al. [6] proposed a scheme that utilizes various image processing transforms and Compressive Sensing (CS) to achieved Security for multimedia data which are embedded with embedding factor into the hybrid coefficients. High payload capacity, faster execution time and used for multimedia data authentication. PSNR value is quite low in this scheme.

Venugopala P S, et al. [7] discusses about the bit stream watermarking techniques in spatial and temporal domain. Watermark embedding is performed by embedding binary bits in the random positions of the video as per the random numbers generated. Insertion time approx 150 sec and extraction time is approx 100 sec. Power consumed by videos is between 400-700 mW. The drawback is that the watermarking bits are embedded into the random position as well as Bit error rate is high.

Makbol et al [8] bestowed a medical image watermarking theme which mixes DWT and DCT. The watermark is inserted into DCT of high-frequency sub-band (HH) of the cover medical image. the standard of the projected theme is evaluated by the peak signal to noise ratio (PSNR) for various gain.

Zear et al. [9], presented a multiple watermarking for health care applications using mixtures DWT-DCT-SVD. two watermarks are inserted within the singular price of the first medical image once its decomposition till the third level DWT and transformation by DCT and SVD. The results demonstrate that this technique is ready to resist against varied attacks.

Gunja et al. [10] proposed a comparative analysis of DWT and DWT-FWHT-SVD. The cover image is divided into four sub bands and then transformed by DWT-FWHT and SVD. The proposed algorithm DWT-FWHT-SVD is strongly robust to various attacks compared with DWT.

Emon Dey et al. [11] proposed a semi blind watermarking scheme utilizing both Discrete Wavelength Transform (DWT) and Singular Value Decomposition (SVD). To embed the watermark, we transformed the host image into wavelet domain and generated a secondary host image using directive contrast. By remodeling the SVD coefficients of the watermark with the SVD coefficients of secondary image we inserted the watermark into the secondary image. A genuine extraction scheme has also been developed to recover the watermark from the cover image. The scheme has been employed using horizontal sub band. In addition to, evaluations have been added in terms of vertical and diagonal sub bands to compare the performance of the algorithm on the basis of specific sub bands. Experimental evaluations in terms of Normalized Correlation (NC) and Peak Signal to Noise Ratio (PSNR) give proof that our procedure is durable and imperceptible under variety of attacks.

Dimple Bansal et al. [12] performed watermarking by the combining the features of DWT (Discrete wavelet transformation) and Discrete Cosine Transformation (DCT). Red color component of the image is used for applying the DWT for embedding the watermark. After this, DCT is implemented on the 8X8 block of the image. Using this functionality a more secure and robust image is found.

Swagata Mawande et al. [13] proposed a digital video watermark scheme based on discrete wavelet transformation and on the singular value decomposition. A sketch of this scheme with Matlab is suggested. The built-in watermark is robust against various attacks that can be performed on the video with watermarks.

Jayprakash Upadhyay et al. [14] proposed an algorithm based on DWT transformations. The LSB method is used to hide data in the least significant bit of the "original video" pixels. The imperceptibility, embedding and robustness are the parameters of this technique. The results of the simulation show that the proposed algorithm reaches these parameters within their acceptable range, i. H. The level of non-perception is high, the ability to integrate is high even in a noisy environment and against a wide range of attacks, for example. Salty and pepper noise, rotation, cropping and median filtration compared to existing tattoo methods.

Hannes Mareen et al. [15] proposed a watermarking approach to protect videos from copyright violations based on implicit distortions generated by a video encoder, rather than the artifacts used in the prior art. These distortions are imperceptible and robust against video manipulation.

Jantana Panyavaraporn and Paramate Horkaew [16] proposed an invisible digital watermarking algorithm on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) domains is presented. Herein, a binary watermark image was embedded in the middle sub-band coefficients of a video stream. The experimental results of proposed algorithm indicates that the PSNR values of the watermarked videos were as high as almost up to 37 dB with the optimal watermarking strength

4. DifferentWatermarking Techniques

A. Spatial Domain Techniques

Spatial Domain Techniques Here, watermark signal is embedded to the message video directly. It is done by changing the pixel values of original video. A number of spatial domain watermarking methods are explained by researchers. Some of these methods are least significant bit coding technique, predictive coding technique, spread spectrum coding technique and patchwork watermarking technique.

Least Significant Bits Method

This is the most widely used method for embedding and extraction in spatial domain. In this method image is first divided into subset of images. Encoder first selects the subset of images and then selects the number of bits to be replaced. It replaces LSB of host image with MSB of watermark image. In this method size of host and watermark image must be same. Embedding is done in LSB of pixels because change in LSB of pixels cannot be easily detected by human eyes. Visibility of watermark in host image depends on the number of bits that is replaced.This method may not resistant to different types of attacks such as cropping, addition of noise or lossy compression etc. An improvement over basic LSB method will use the pseudorandom number generator to determine the pixels that is to be used for embedding based on seed point or key values. This method lacks the basic robustness that any watermarking applications require.

Predictive Coding Scheme

The disadvantage with LSB coding is that if only LSB coding is applied then the retrieval of the watermark cannot be done properly. It also contains a noise component. Therefore, predictive coding scheme is used in spatial domain for further improvement. In this technique correlation between adjacent pixels are used. Watermark is embedded in a set of pixels. Alternate pixels are replaced by the difference between the adjacent pixels. Predictive coding scheme shows better robustness as compared to LSB coding. Another method that is widely used is spread spectrum coding technique. In this method, messages are encoded with sequences of symbols. Symbols are represented by a signal referred to as chip. Typically chips are pseudo-random sequence of 0’s and 1’s. For inserting watermark, perceptually significant coefficients are more reliable.

Patchwork Based Method

Last one that is generally used in spatial domain is patchwork based method. In patchwork watermarking method, the image is divided to find the two subsets of the image. Here brightness of one subset is incremented by some factor. Also brightness of another subset is decremented by the same factor. This type of technique is mostly used for audio watermarking.

Table 1: Review on Spatial Domain Techniques

Author	Description
Manoj Kumar, Arnold Hensman [17]	Both host video and information to be embedded is divided into different frames in such a way that approximately whole video has uniform distribution of watermark to be embedded. This approach provides high robustness against common signal processing attacks
M. Jeni, S. Srinivasan [18]	In this method authors extracted feature values first from the video. As feature value is made of pixels so author use spatial domain watermarking and embed secret message in feature value
Vladimir et al. [19]	This is a 2D modulation method in time domain in which orthogonal properties of PN sequences are used. Author embeds watermark in 2 levels. First watermark is embedded in frames by PN sequence spreading and second modulation is performed with in the frames
Venugopala et al. [20]	Authors embed 8 bit-plane images, obtained from single gray scale watermark image, into different scenes of a video sequence. Method is based on blind watermarking for uncompressed video. This technique is robust against attacks such as frame dropping, temporal shifts and addition

	of noise

B. Transform Domain Techniques

Discrete Cosine Transformation based Watermarking

It is a kind of transform whose kernel is in cosine function. It works for complex numbers. It converts an image from spatial domain to transform domain and vice versa. When an image is transformed using DCT it divides given image into 8*8 blocks. Then it finds low and high frequency components by zigzag scanning. And then embeds watermark in low frequency components. This method provides high robustness against JPEG compression. DCT methods lack resistance to strong geometric attacks.

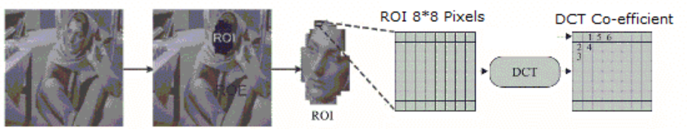

Figure 2: DCT Watermarking Technique

3.3 Discrete Wavelet Transformation based Watermarking

It is a decomposition technique that decomposes given image into set of basic wavelets. It provides spatial and transform representation of an image. DWT is suitable technique to identify the area in the image that contains secret image. DWT decompose given image into low and high frequency components and finds high frequency components and embeds an image into high frequency components. In DWT based method frequency resolution depends on frequency so when frequency is corrupted it decreases robustness. DWT multiresolution technique decomposes given image into four sub bands – LL (High scale low frequency components), LH (Vertical low scale high frequency components), HL (Horizontal low scale high frequency components), HH (Diagonal low scale high frequency components). It embeds watermark into LH and HL bands. This method does not provide strong robustness against different types of geometric and image processing attacks.

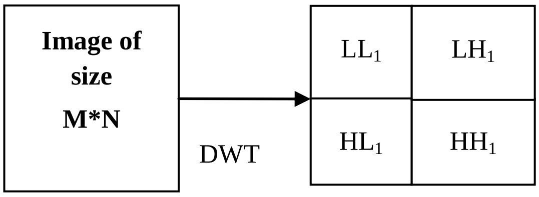

Figure 3: DWT Watermarking Technique

3.4 Discrete Wavelet Transform-Discrete Cosine Transform based Watermarking

In this method hybrid watermarking technique is used that combines DWT and DCT. In this method first DWT is applied on the host image up to different levels followed by DCT and then applies different types of attacks. As the number of level increases size of watermark decreases and PSNR increases. In this method mark image is multiplied with deviation of host image so quality degrades very slowly. This method provides high PSNR and can extract high quality and large marks. It does not change the view of host image. This method satisfies the requirements of robustness.

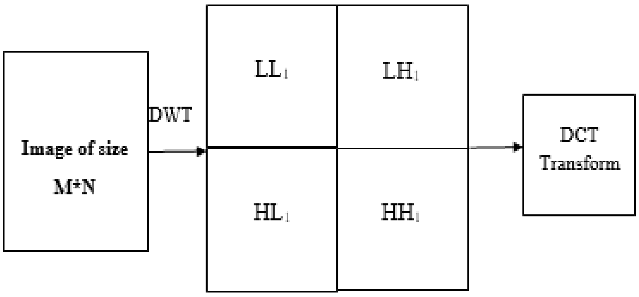

Figure 4: DWT-DCT Watermarking Technique

3.5 Discrete Wavelet Transform(DWT)-Discrete Cosine Transform(DCT)-Singular Value Decomposition(SVD) based Watermarking

DWT, DCT and SVD are combined in a zigzag way to satisfy the requirement of robustness. First DWT is applied on host image which decomposes the given image into four bands. And then DCT is applied on HH band and map the DCT coefficient using zigzag scanning and then applies SVD to get singular value coefficients. Same procedure is then applied on watermark image. Extraction is same as embedding but works in reverse manner. This method provides good robustness. But complexity increases as process of application of DWT, DCT, SVD and IDWT, IDCT, and inverse SVD.

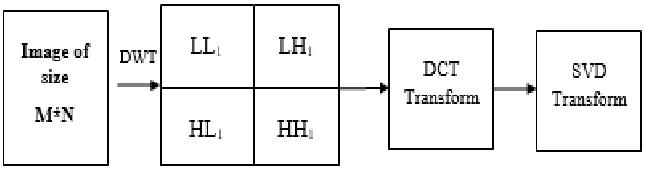

Figure 5: DWT-DCT-SVD Watermarking Technique

5. Performance Measures

Robustness of watermark means that the after intentional or unintentional attacks thewatermark is not destroyed and it can be still used to provide certification and it is measured using correlationcoefficient. It is measured “after attack”. For the robust capability, mean absolute error (MSE) measures the mean ofthe square of the original watermark and the extracted watermark from the attacked image. The lower the value ofthe MSE lower will be the error. It is represented as:

$$MSE = \frac{1}{XY[\sum_{i=1}^{X}\sum_{j=1}^{Y}(c(i,j) - e(i,j))}$$

X and Y are height and width respectively of the image. The c (i, j) is the pixel value of the cover image and e (i, j)is the pixel value of the embed image.

PSNR represents the degradation of the image or reconstruction of an image. It is expressed as a decibel scale.Higher the value of PSNR higher the quality of image. PSNR is represented as:

$$PSNR = 10log10(\frac{(L * L)}{MSE}$$

Correlation coefficient(CC) measures the robustness of the watermark. It correlates the extracted watermark with theoriginal watermark. More the value of CC, more robust is the scheme.

BER is the ratio that describes how many bits received in error over the number of the total bits received.

$$BER = \frac{P}{(H * W)}$$

Table 2: Review on Transform Domain Techniques

Author	Description
Sonjoy Deb Roy et al. [21]	Authors presented a hardware implementation of digital watermarking system that can insert invisible, semi-fragile watermark information into compressed video streams in real time.
DawenXu et al. [22]	In this paper authors embed watermark after compressing the video by bit substitution method, provided the video file size is strictly preserved. Since data hiding is completed entirely in the encrypted domain.
Thomas Stütz et al. [23]	In this method embedding is done after H.264 compression by simple bit substitution. It offers significantly increased marking space and high robustness to re-compression.

Table 3 summarizes the evaluation of the performance of each watermarking technique in terms of robustness, imperceptibility (invisibility), and Blindness. As seen, none of them is ideal due to the nature of watermarking which is a tradeoff among these criteria. Whenever a criterion is increased, other criteria are decreased. Although the result for the proposed watermarking systems seems to be good, they are still reported under their assumption. In real environment condition, there is still a huge gap to use an efficient watermarking technique to embed the voice feature in digital image.

Table 3: Comparative Review on Image and Video Watermarking Methods

Techniques	Robustness (BER %)	Imperceptibility (PSNR)	Blindness
Histogram [24]	0.003	48.34	Semi Blind
Spatial domain [25]	0.002	47.54	Non-blind
DFT [26]	0.260	60.52	Blind
DCT [27]	0.004	60.24	Semi Blind
DWT [28]	0.00001	48.07	Blind
SVD [29]	0.001	73.65	Blind
DWT-DCT-SVD [30]	0.001	113.42	Blind
DWT+ spatial [31]	0.05	N/A	Blind
DWT+NN [32]	0.02	39.08	Blind

6. Conclusion

Watermark embedding and extraction algorithms are required for providing copyright protection and ownership identification.For the protection of the copyright and the identification of the property, algorithms of incorporation and extraction in watermark are necessary.

In this paper a number of image and video watermarking techniques have been studied. In some techniques watermark is inserted in the raw video before compression either in spatial or transform domain.It has been concluded that to minimize distortions and to increase capacity, techniques in frequency domain must be combined with another techniques which has high capacity and strong robustness against different types of attacks.

References

[1] Imane Assini, Abdelmajid Badri, Khadija Safi, Aicha Sahel, Abdennaceur Baghdad, “Hybrid multiple watermarking technique for securing medical image using DWT-FWHT-SVD”, IEEE, 2017.

[2] Divjot Kaur Thind, Sonika Jindal, "A Semi Blind DWT-SVD Video Watermarking", Procedia Computer Science, Vol. 46, pp. 1661-1667, 2015.

[3] Aparna J R, Sonal Ayyappan, "Image Watermarking using Diffie Hellman Key Exchange Algorithm", International Conference on Information and Communication Technologies, 2014.

[4] Bhargava, G., & Jhapate, A., "A Study on Digital Watermarking Techniques", International Journal Online of Science, 4(3), 2018. Available at: http://ijoscience.com/ojsscience/index.php/ojsscience/article/view/130 . DOI : https://doi.org/10.24113/ijoscience.v4i3.130.

[5] Lamia Rzouga Haddada, Bernadette Dorizzi, Najoua Essoukri Ben Amara, "A combined watermarking approach for securing biometric data", Image Communication, 2017.

[6] Rohit Thanki, Vedvyas Dwivedi, Komal Borisagar, "A hybrid watermarking scheme with CS theory for security of multimedia data", Journal of King Saud University – Computer and Information Sciences, 2017.

[7] Venugopala P S, Dr. Sarojadevi H, Dr.Niranjan.N.Chiplunkar, "An Approach to Embed Image in Video as Watermark Using a Mobile Device", Elsevier, 2017.

[8] Makbol, nasrin m., khoo, bee, rassem, taha. "Block-based Discrete wavelet transform-singular value decomposition image Watermarking scheme using human visual system characteristics", IET Image processing, vol. 10, pp. 34-52, 2016.

[9] Zear, aditi, singh, amit kumar, pardeep kumar, "Multiple Watermarking for healthcare applications", Journal of intelligent Systems, 2016.

[10] Gunja, baisa. Et mali, suresh, "Comparative performance Analysis of digital image watermarking scheme in dwt and DWT-FWHT-SVD domains", IEEE, 2014.

[11] Emon Dey, Sharmin Majumder, Arnab Neelim Mazumder, "New Approach to Color Image Watermarking Based On Joint DWT-SVD Domain In YIQ Color Space", IEEE, 2017.

[12] Dimple Bansal and Manish Mathuria, "Color Image Dual Watermarking using DCT and DWT Combine Approach", IEEE, 2017.

[13] Swagata Mawande, Hemlata Dakhore, "Video Watermarking using DWT-DCT-SVD Algorithms", IEEE, 2017.

[14] Jayprakash Upadhyay, Bharat Mishra, Prabhat Patel, "A modified approach of video watermarking using DWT-BP based LSB algorithm", IEEE, 2017.

[15] Hannes Mareen, Johan De Praeter, Glenn Van Wallendael, "Peter Lambert A novel video watermarking approach based on implicit distortions", IEEE, 2018.

[16] Jantana Panyavaraporn and Paramate Horkaew, 'DWT/DCT-based Invisible Digital Watermarking Scheme for Video Stream", IEEE, 2018.

[17] Manoj Kumar, Arnold Hensman, "Robust Digital video watermarking using reversible data hiding and visual cryptography," Proceedings of 24th IET Irish Conference on Signals and Systems (ISSC 2013), pp: 1–6, 2013.

[18] M. Jeni, S. Srinivasan, "Reversible Data Hiding in Videos Using Low Distortion Transform" Proceeding of IEEE conference on Information Communication and Embedded Systems (ICICES), pp. 121–124, 2013.

[19] Vladimír BÁNOCI, Martin BRODA, Gabriel BUGÁR, Dušan LEVICKÝ, "2D - Spread Spectrum Watermark Framework for Multimedia Copyright Protection," Proceeding of 24th IEEE Conference on Radioelektronika (RADIOELEKTRONIKA), pp. 1–4, 2014.

[20] Venugopala P S, H. Sarojadevi, Niranjan N. Chiplunkar, Vani Bhat, "Video Watermarking by Adjusting the Pixel Values and Using Scene Change Detection," Proceeding of IEEE fifth International Conference on Signals and Image Processing, pp. 259–264, 2014.

[21] Sonjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander Fish, "Hardware Implementation of digital watermarking system for video authentication," IEEE transactions on circuits andsystems for video technology, vol 23, no. 2, pp. 289–301, Feb. 2013.

[22] Dawen Xu, Rangding Wang, and Yun Q. Shi, "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution," IEEE transactions on information forensics and security, vol. 9, no. 4, pp. 596–606, April 2014.

[23] Thomos Stutz, Florent Autrusseau, Andreas Uhl, "Non blind structure preserving substitution watermarking of H.264/CAVLC inter frames," Proceedings of IEEE on multimedia, vol. 16, no. 5, pp. 1337–1349, August 2014.

[24] Zong, T., "Robust histogram shape based method for image watermarking", 2014.

[25] Cheung, W., "Digital image watermarking in spatial and transform domains", In Proceedings of the TENCON, IEEE, 2000.

[26] Li, J., "An adaptive secure watermarking scheme for images in spatial domain using fresnel transform", In Information science and engineering (ICISE). IEEE, 2009.

[27] Wang, Y., and A. Pearmain, "Blind MPEG-2 video watermarking in DCT domain robust against scaling", IEEE Proceedings-Vision, Image and Signal Processing 153(5): 581–588, 2006.

[28] Ma, B., "Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking", Multimedia Tools and Applications 72(1): 637–666, 2014.

[29] Ghazy, R.A., "Block-based SVD image watermarking in spatial and transform domains", International Journal of Electronics 102(7): 1091–1113, 2015.

[30] Navas, K., "DWT-DCT-SVD based watermarking", International conference on communication systems software and middleware and workshops,IEEE, 2008.

[31] Huai-Yu, Z., L. Ying, and W. Cheng-Ke., "A blind spatial-temporal algorithm based on 3D wavelet for video watermarking", IEEE international conference on multimedia and expo, 2004.

[32] Li, X., and R. Wang., "A video watermarking scheme based on 3D-DWT and neural network", IEEE international symposium on multimedia workshops, IEEE, 2007.