

# A New Robust Video Watermarking Technique Using H.264/AAC Codec Luma Components Based On DCT

Nazia Azeem<sup>1\*</sup>, Iftikhar Ahmad<sup>2\*</sup>, Syed Roohullah Jan<sup>3</sup>, Muhammad Tahir<sup>4</sup>, Farman Ullah<sup>5</sup>,  
Fazlullah Khan<sup>6</sup>

<sup>1,2,3,4,6</sup> Department Of Computer Science, Abdul Wali Khan University Mardan, KPK, Pakistan

<sup>5</sup> Department Of Computer Science, Bacha Khan University, Charsadda, KPK, Pakistan

## ABSTRACT

Video watermarking is well known as the process of embedding copy right information in video bit streams. It had been proposed in recent years to solve the problem of illegal manipulation and distribution of digital video. In this study, an effective, robust DCT transform using MATLAB. In the proposed method, first the video frames are extracted from the host video. Then, each frame gets watermarked with multi-level discrete cosine transform which is also known as embedding. After that each watermarked video frame gets reconstructed. Watermarked video is obtained after reconstruction of watermarked video frame. Experimental results shows that the proposed algorithm is imperceptible as well as robust against wide variety of signal and video processing attacks like Gaussian noise, cropping, geometric attack, , over writing etc. The technique is fairly acceptable and watermarked video is of good quality, achieves high PSNR and other results.

**Keyword** :- Watermark, video watermarking, video frames, frequency domain etc....

## 1. INTRODUCTION

Video Watermarking is a young and rapidly evolving field in the area of multimedia. There has been an explosive growth in use of internet and World Wide Web and also in multimedia technology and its applications recently [1]. This has facilitated the distribution of the digital contents over the internet. Digital multimedia works (video, audio and images) become available for retransmission, reproduction, and publishing over the Internet. A large amount of digital data is duplicated and distributed without the owner's consent [2][3]. This arises a real need for protection against unauthorized copy and distribution. Hence it became necessary to build some secure techniques for legal distribution of these digital contents. Watermarking helps us to identify the true owner of the digital information. This technology is one of the possible methods to protect digital information [9]. Digital Watermarking has proved to be a good solution to tackle these problems. It discourages the copyright violation and help to determine the authenticity and ownership of the data. In the literature, different schemes are proposed to achieve more robustness and imperceptibility [13]. Growing popularity of video based applications such as Internet multimedia, wireless video, personal video recorders, video-on-demand, videophone and videoconferencing have a demand for much higher compression to meet bandwidth criteria and best video quality as possible. Different video Encoder Decoders (CODECs) have evolved to meet the current requirements of video application based products. Watermark embedding may bring in diminutive distortion into the audible or visible components of the watermarked signal. If the watermark cannot be easily removed from the watermarked signal even after applying common watermarking

attacks then it is referred as robust embedding [17]. The basic components involved in robust watermarking are watermark embedding, attack, and watermark detection. In watermark embedding, a watermark signal (Text, image or audio etc) is constructed and then embedded into an original signal (Video) to produce the watermarked signal. Once embedding is done, the watermarked video can be subjected to various attacks. During watermark detection, the watermark detector is given a test signal that may be watermarked, attacked or not. The watermark detector reports whether the watermark is present or not on examining the signal at its input [21]. Among various available standards H.264/Advanced Audio Codec (AAC) is becoming an important alternative regarding reduced band width, better image quality in terms of peak-signal-to-noise-ratio (PSNR) and network friendliness, but it requires higher computational complexity [5]. Different watermarking techniques have been proposed for different video CODECs, but only a few works on H.264/AAC can be found in the literature [18]. H.264/AAC uses different transformation and block sizes than MPEG series, so development of new algorithms is required to integrate robust watermarking techniques for different profiles of H.264/AAC. The watermarking procedure for the audio, video and digital images is approximately similar, it is performed within the digitally transformed or original data. Various PCA-based, DCT-based and wavelet-based transforms can be applied for the watermarking purposes [7]. These transform-domain techniques are popular due to convenient compatibility with well-known compression algorithms and quality of result data comparing with other techniques.

## 2. PROBLEM STATEMENT

Our aim is to watermark any given digital video without any degradation in the quality of the video considering the HVS (Human Visual System).

### 2.1 RESULTS

For the experimental results, i have considered various approaches: H.264 compression, geometric distortions and noising. Results showed a good performance in the proposed method.

### 2.2 CONCLUSION

The presented technique was applicable not only to avi video, but also to other DCT coding videos like MPEG-1, MPEG-2, H261 and H263.

## 3. OBJECTIVES

- i. To end watermark using H.264/AAC video format.
- ii. To embed watermark in H.264/AAC video format is more robust.
- iii. The embedded watermark should be imperceptible.

## 4. DIGITAL WATERMARKING

Now Digital watermarking technology is an emerging field in computer science, cryptography, signals processing and communications [2]. Digital Watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection. Watermarking technique is to hide secret information into the digital signals so as to discourage unauthorized copying or attest the origin of the media. The watermark is a digital code embedded in the image data and is invisible [5]. A digital watermark is permanently embedded in the data, that is, it remains present within the original data after any distortion process. A watermark could be used to provide proof of authorship of a signal.

## 5. LITERATURE SURVEY

Here two basic ways to embed data in a binary image are by changing the values of individual pixels and by changing a group of pixel [4]. The second approach modifies such features as thickness of strokes, relative position etc. The sudden increase in watermarking interest is most likely due to the increase in concern over copyright protection of content. In the early days, encryption and control access techniques were used to protect the ownership

of media. Nowadays watermarks have been investigated as a complementary technology [17]. Digital watermarking has recently been extended from still images to video. Many algorithms have been introduced. Initially designed for still images [8] to the definition of specific video watermarking scheme. Open path still remain in video watermarking [12]. This technology is indeed in its infancy and is far from being as mature as for still image [10]. Video watermarking is a process of watermark the sequence of video frames. Video can be considered as a stream of individual images. Hence all image watermarking techniques are equally applicable to video, when the individual frames are treated as images. Such techniques do not make use of the availability of the temporal domain apart from the spatial domain which image provide. This can lead to the design and use of sophisticated techniques, exploiting the presence of temporal domain. In general, watermark can be embedded in Spatial domain or Transform domain. There are many type approaches for spatial domain techniques such as LSB Correlation-Based, Patchwork, Random function, Image checksum, M-frame, SST, and Kodak Technique [19]. For Transform Domain the techniques available are DCT, DWT, DFT Continuous Transform and Random. The spatial technique inserts the watermark in the least significant bits of the image. This allows a watermark to be inserted in an frame without affecting the value of the video. LSB is the simplest example of a spatial domain watermarking techniques to insert data into digital signals in noise-free environments is least significant bit (LSB) coding. This technique essentially involves embedding the watermark by replacing the least significant bit of the video data with a bit of the watermark data [3]. An advantage of the spatial techniques is that they can be easily applied to any image, regardless of subsequent processing. A possible disadvantage of spatial techniques is they do not allow for the exploitation of this subsequent processing in order to increase the robustness of the watermark. This spatial watermarking technique is not very secure and not very robust to processing techniques because the least significant bit plane can easily be replaced by random bits, effectively removing the watermark bits [22]. In the transform domain approach, some sort of transforms is applied to the original image first. The transform applied may be (DCT), (DFT), (DWT), etc. The watermark is embedded by modifying the transform domain coefficients. The transform domain approaches are more robust against noise or attack. DCT is classic and still most popular domain for image processing. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The first step of the embedding method is that the host image has to be divided into 8 x 8 blocks. One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. Discrete Cosine Transform (DCT) is a classic and quite an important method for video watermarking. A lot of digital video watermarking algorithms embed the watermark into this domain. The usability of this transform is because that most of the video compression standards are based on DCT and some other related transforms. In this domain some DCT coefficients of the video are selected and divided into groups, and then the watermark bits are embedded by doing adjustment in each group [7][9].

## 6. APPLICATIONS OF VIDEO WATERMARKING

The major applications of digital video watermarking includes copyright protection, video authentication, broadcast monitoring, copy control, video tagging, ownership identification and enhance video coding [8].

## 7. PHASES OF WATERMARKING

All Watermarking is the procedure of embedding the owner's identification or information within digital image, audio, video, and texts, by considering various features of the digital media like the limitations of the human perception, histogram shifting, etc. The overview of different phases of watermarking system is shown in Figure-1 [12]. A watermark is designed and embedded to exist in the host media permanently. The watermark can be a sequence of copyright logos / messages, ownership identifiers marks, gray or binary images or any other digital information formats. After watermarking is performed on an original digital media data, it can be distributed on internet and may undergo certain manipulations like unintentional or intentional attacks, so as to degrade the watermark to disappear. Ideally, the watermark must remain intact or safely detectable after the digital data has undergone some attacks. Only when there is a question of ownership or as a proof of intellectual property rights, the embedded information from the host is extracted [13]. There are two different types of watermarking systems by considering the embedded watermark at the detection or extraction stage.

- i. Known watermark
- ii. Unknown unique watermark

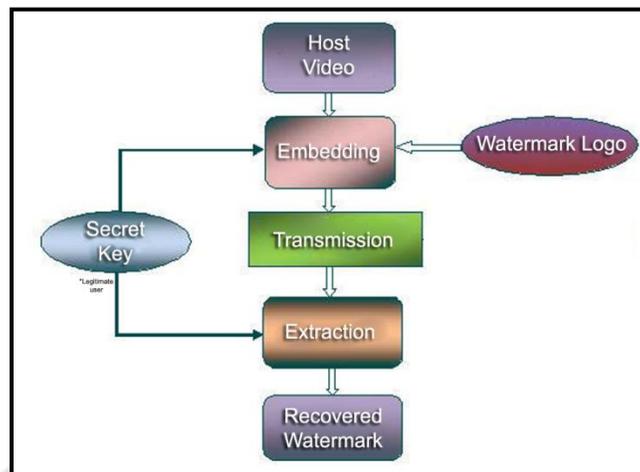


Fig -1: Phases Of Watermarking

## 8. WATERMARK EMBEDDING PROCESS

According to the working domains of watermark algorithms, video watermarking techniques are classified into different two domains: spatial domain and frequency domain. In frequency domain the watermark information is embedded into the transform domain of the host signal for example DCT or wavelet domain [16].

## 9. PROPOSED METHOD

In this scheme, a video is decomposed into different parts and the watermark is embedded in corresponding frames of U or V in the original video. This ensures the proposed method to achieve robustness against the attack of frame dropping, averaging, cropping and lossy compression [13]. For every motionless scene in the video, the algorithm embeds an identical watermark. Independent watermarks are used for successive but different scenes. All watermarks are embedded in the V channel frames. In the detection phase, the embedded watermark will be extracted from the video channel through reverse process.

## 10. EMBEDDING ALGORITHM

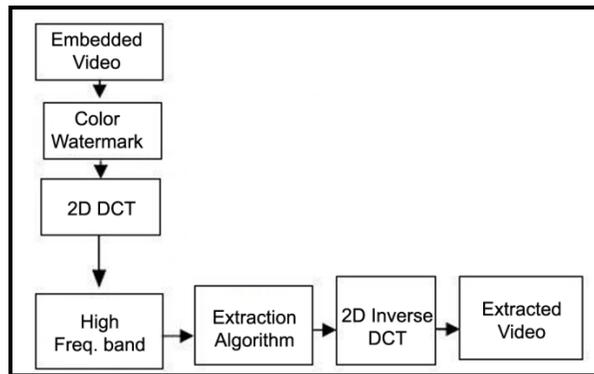
The block schematic representation of the proposed embedding algorithm to watermark a video data for the copy right protection purpose is as follows:

Applying watermark to video is different from image, such as video object and redundancy of the large amount video data, researchers have make use of those characteristics to develop different schemes. In the proposed approach shown in figure 2, watermark is embedded in the desired DCT coefficient of video sequence. Watermark generation and embedding is performed in matlab.

i. Take cover video of size  $m \times n$  and watermark logo of size  $m \times n$  is also taken as an input. ii. All frames of video are decompose into 3 components: Y, U and V.

iii. Select one luma component for watermark embedding from U or V.

iv. 2D-DCT is applied is applied to all blocks of each frame in V luminance.



**Fig -2:** Watermark Embedding

v. Combine modified Y, U and V components to create watermarked video frame.

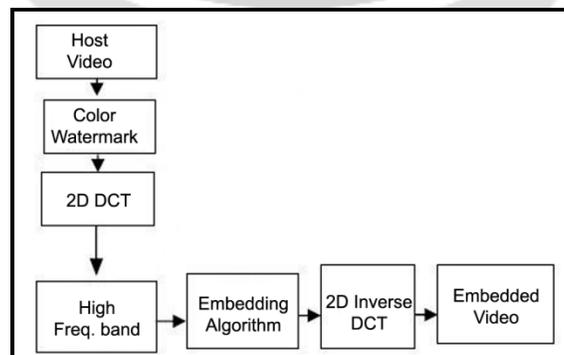
By this procedure all the frames will be embed with color watermark.

### 11. WATERMARK DETECTION AND EXTRACTION

In the detection phase, video is checked for the presence of the watermark. There are two somehow related ways to look at watermark extraction, first is to determine to whom this watermark belongs and second is to determine whether this is the correct watermark being seemed. In a blind video watermarking scheme, it does not need the original video while detecting the watermark. The video frames from the watermarked video are extracted. The video frames will be processed to get the video watermark [16].

As an identical watermark is used for all frames within a luminance, multiple copies of each part of the watermark may be obtained. The watermark is recovered by averaging the watermark extracted from different frames. This reduces the effect if the attack is carried out at some designated frames. If enough scenes are found and all parts of the watermark are collected, the original large watermark image can be reconstructed [21-35]. The recovery of the watermark is done by applying the extraction algorithm IDCT to the part of the watermarked video. Extract the reference luminance from the video Y,U or V, apply the inverse discrete cosine transform to the target luminance component. After extracting and refining the watermark, the user can compare the results with the referenced watermark subjectively.

The generalized block representation of proposed extraction algorithm from the marked reference frames of watermarked video is given in Fig-3.



**Fig -3:** Watermarking Detection Extraction

## 12. EXPERIMENTS AND RESULTS



a) Original Frame

b) Watermark Frame

c) Watermark Logo

## 13. COMMON ATTACKS

### 13.1 Common Attacks:

The common attacks of video watermarking are frame dropping, frame averaging, statistical analysis, lossy compression, cropping and various signal processing and geometrical attacks.

### 13.2 Intentional attacks:

The intentional watermark attack includes Single frame attacks like filtering attacks, contrast and color enhancement and noise adding attack. Or statistical attacks.

### 13.3 Unintentional attacks:

The unintentional attacks may be due to Degradations that can occur during lossy copying, or due to compression of the video during re-encoding or because of change of frame rate and Change of resolution [15].

### 13.4 Compression attack:

The most used video compression is definitely AVI [6]. In MATLAB, for compressing a video to different quality factors, the video should be created from frames and be reread.

### 13.5 Noise Attack:

Adding noise in MATLAB is simply done by “movnoise” command. Gaussian, Poisson, Salt & Pepper and Speckle are among the noises that could be used applied.

### 13.6 Cropping:

Cropping attack is simply cutting off parts of the video. If the algorithm is non-blind, it is better to bring back those parts from the original video for a better recovery of the message [6].

### 13.7 Geometric Attacks:

Geometric attacks are related to the videos and images. These attacks actually do not eliminate the watermark which can be manipulated the watermark so that Watermark information cannot be observed by the detector. Examples are translation, rotation of image, cropping warping and line/column removal. The watermark quality can be degraded by these types of attacks. Mosaic attack is another example of this attack [15] [36-43].

### 13.8 Removal/Over Write Attacks:

Removal attacks can be affected in such a way the watermark, which can be absolute or almost about to altered or over written the watermark information. Examples are averaging, quantization, re-modulation, lossy compression collision attacks. This attack is that in which the watermarked object can be remove

the watermark data. Interference attacks are that in which the watermark information has an additional noise. The attack if any occurs in the data that degraded the quality of data [15].

**Table-1** Various image quality measures of watermarked frame

Video Quality Measurement	PSNR Y'UV	MSE Y'UV	VQM
Watermarked	48.94565	1.24235	1.32437

**Table 1**

**Table-2** Various image quality measures after various attacks performed on frame

Operations on frames and/or video	PSNR	MSE	VQM	DFM	SCD
Cropping	47.68218	1.42822	1.55739	0.000	0.000
Rotation	46.58419	2.28809	1.73929	0.000	0.000
Compressed	47.22145	1.85425	1.52896	0.000	1.000
Noise	47.54133	1.96735	1.43543	0.000	0.000

**Table 2**

**Table-2** shows the values for the quality measures check for video frames after performing various attacks against video frames. This task is performed to check the robustness of frames and compared to paper [16] in references.

**Table-3**, from paper [16] with which our results are compared

Test Carrier Videos	Average PSNR of Watermarked Frames	MSE of Watermarked Frames
News	46.0135	1.6425
Ice	45.6489	1.7848
Crew	46.6249	1.4256
Soccer	46.5829	1.4394

**Table 3**

The experimental results showed that there is no perceptible Distortion in the embedded video. The main advantage of this method is that it is robust. In the experiments, various .avi and .mpg videos are used as the host whereas .jpg,

.png images are used as watermark images. The performance evaluation of algorithm is summarized in Tables. If different size of images are used as a watermark image, then the value of psnr and other average values are shown in below tables. From this tables we have observe that if the size of image & video is different than we got different values [44-54].

## 14. CONCLUSION

This paper focuses on the digital watermarking techniques performed on video using 2-D Discrete Cosine transform. The algorithm presented in this paper is robust video watermarking technique for the color watermark video. This watermarking technique is used to make a video more secure for copyright protection and content authentication. The algorithm is fairly robust against attacks like image cropping and noise like Gaussian noise, removal attack.

In future, the algorithm can be improved to resist these attacks especially geometric attack. And to evaluate the effectiveness of video frame various tasks is performed. This work could further be extended for the watermarking purpose of content like movie.

## 15. REFERENCES

- [1] Mr.Krunal R. Patel Mr.Parimal A. Patel, "A Survey on Digital Video Watermarking", Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X
- [2] Mr. Rashel Sarkar, Ms. Smitha Ravi, "A Survey of Digital Video Watermarking", Volume 1, No. 2, April 2012 ISSN – 2278-1080  
The International Journal of Computer Science & Applications (TIJCSA)
- [3] Sourav Bhattacharya, T. Chattopadhyay and Arpan Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC"
- [4] Jing Zhang, Student Member, IEEE, Anthony T. S. Ho, Senior Member, IEEE, Gang Qiu, and Pina Marziliano, Member IEEE, "Robust Video Watermarking of H.264/AVC", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS, VOL. 54, NO. 2, FEBRUARY 2007 205
- [5] Mohd Shahidan Abdullah, Azizah Abd Manaf, "An Overview of Video Watermarking Techniques", University Technology of Malaysia (Postgraduate Annual Research Seminar 2007 (3-4 July 2007))
- [6] Pooya Monshizadeh Naini *University of Tehran Iran*, "Digital Watermarking Using MATLAB
- [7] Aditi Agarwall, Ruchika Bhadana<sup>2</sup> and Satishkumar Chavan, "A Robust Video Watermarking Scheme using DWT and DCT", (Aditi Agarwal et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1711-1716)
- [8] Ankita A. Hood ,Prof. N.J. Janwe,"A Review on Video Watermarking and Its Robust Techniques", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 1, January- 2013 ISSN: 2278-018
- [9] Tahani Al-Khatib, Ali Al-Haj, Lama Rajab and Hiba Mohammed, "A Robust Video Watermarking Algorithm", (Journal of Computer Science 4 (11): 910-915, 2008 ISSN 1549-3636 © 2008 Science Publications)
- [10] Chetan K.R Raghavendra K. "DWT Based Blind Digital Video Watermarking Scheme for Video Authentication", *International Journal of Computer Applications (0975 – 8887) Volume 4– No.10, August 2010* 19
- [11] N Leelavathy, E V Prasad, Mylavaram. India, S Srinivas Kumar "Video Watermarking Techniques – A Review", International Journal of Computer Applications (0975 – 8887) Volume 104 – No.7, October 2014 24
- [12] Rini T Paul, "Review of Robust Video Watermarking Techniques", IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011 90
- [13] A paper by Prabhishkek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks" "Embedding, Extraction and Detection of Digital watermark in spectral images", lappeenranta university of technology department of information technology
- [14] Shivanjali Kashyap, "Digital Watermarking Techniques and Various Attacks Study for Copyright Protection", © 2015, IJARCSSE All Rights Reserved Page | 737  
Volume 5, Issue 3, March 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

- [15] *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727* Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 83-90 “A New DCT based Color Video Watermarking using Luminance Component” Jaya Jeswanil, Dr. Tanuja Sarode2  
“A Blind and Robust Video Water Marking Technique in DCT Domain” D.Niranjan babu, D.Jagadeesh International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 1, January- 2013 ISSN: 2278-0181
- [16] “Hardware realization of DC embedding video watermarking technique based on FPGA” CONFERENCE PAPER · JANUARY 2012 DOI: 10.1109/ICM.2010.5696189
- [17] “DCT Domain Video Watermarking Technique for AVI Video” International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 4, April 2015 Copyright to IJRCCCE 10.15680/ijrccce.2015.0304083 3001 Manoj Kumar1, Dolley Shukla2
- [18] ] “A Review on Video Watermarking and Its Robust Techniques” Ankita A. Hood Ballarpur Institute of Technology, Ballarpur. Prof. N.J. Janwe Rajiv Gandhi College of Engg. Research & Technology, Chandrapur
- [19] Hui-Yu Huang, Member, IEEE, Cheng-Han Yang, and Wen-Hsing Hsu, “A Video Watermarking Technique Based on Pseudo-3-D DCT and
- [20] Quantization Index Modulation”, IEEE transactions on information forensics and security, vol. 5, no. 4, December 2013
- [21] Khan. F., Bashir, F. (2012). Dual Head Clustering Scheme in Wireless Sensor Networks. in the IEEE International Conference on Emerging Technologies (pp. 1-8). Islamabad: IEEE Islamabad.
- [22] Syed Roohullah Jan, Farman Ullah, Hashim Ali, Fazlullah Khan, " Enhanced and Effective Learning through Mobile Learning an Insight into Students Perception of Mobile Learning at University Level", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.674-681, March-April 2016. URL : <http://ijsrset.com/IJSRSET1622209.php>
- [23] Khan. F., Nakagawa. K. (2012). Cooperative Spectrum Sensing Techniques in Cognitive Radio Networks. in the Institute of Electronics, Information and Communication Engineers (IEICE), Japan , Vol -1, 2.
- [24] Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015). A Dynamic Key Length Based Approach for Real-Time Security Verification of Big Sensing Data Stream. In Web Information Systems Engineering–WISE 2015 (pp. 93-108). Springer International Publishing.
- [25] M. A. Jan, P. Nanda, X. He, Z. Tan and R. P. Liu, “A robust authentication scheme for observing resources in the internet of things environment” in 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 205-211, 2014, IEEE.
- [26] Khan. F., Nakagawa, K. (2012). Performance Improvement in Cognitive Radio Sensor Networks. in the Institute of Electronics, Information and Communication Engineers (IEICE) , 8.
- [27] Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015, August). DPBSV--An Efficient and Secure Scheme for Big Sensing Data Stream. In Trustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 246-253). IEEE.
- [28] M. A. Jan, P. Nanda and X. He, “Energy Evaluation Model for an Improved Centralized Clustering Hierarchical Algorithm in WSN,” in Wired/Wireless Internet Communication, Lecture Notes in Computer Science, pp. 154–167, Springer, Berlin, Germany, 2013.
- [29] Khan. F., Kamal, S. A. (2013). Fairness Improvement in long-chain Multi-hop Wireless Adhoc Networks. International Conference on Connected Vehicles & Expo (pp. 1-8). Las Vegas: IEEE Las Vegas, USA.
- [30] Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). A dynamic prime number based efficient security mechanism for big sensing data streams. Journal of Computer and System Sciences.
- [31] M. A. Jan, P. Nanda, X. He and R. P. Liu, “Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network”, 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC & EUC), pp. 1400-1407, 2013.
- [32] Jabeen. Q., Khan. F., Khan, Shahzad, Jan. M. A., Khan. S.A (2016). Performance Improvement in Multihop Wireless Mobile Adhoc Networks. in the Journal Applied, Environmental, and Biological Sciences (JAEBS), Print ISSN: 2090-4274 Online ISSN: 2090-4215
- [33] Khan. F., Nakagawa, K. (2013). Comparative Study of Spectrum Sensing Techniques in Cognitive Radio Networks. in IEEE World Congress on Communication and Information Technologies (p. 8). Tunisia: IEEE Tunisia.
- [34] Puthal, D., Sahoo, B., & Sahoo, B. P. S. (2012). Effective Machine to Machine Communications in Smart Grid Networks. ARPN J. Syst. Softw. © 2009-2011 AJSS Journal, 2(1), 18-22.

- [35] Khan. F. (2014). Secure Communication and Routing Architecture in Wireless Sensor Networks. the 3<sup>rd</sup> Global Conference on Consumer Electronics (GCCE) (p. 4). Tokyo, Japan: IEEE Tokyo.
- [36] M. A. Jan, P. Nanda, X. He and R. P. Liu, "PASCCC: Priority-based application-specific congestion control clustering protocol" *Computer Networks*, Vol. 74, PP-92-102, 2014.
- [37] Khan. F. (2014). Throughput & Fairness Improvement in Mobile Ad hoc Networks. the 27<sup>th</sup> Annual Canadian Conference on Electrical and Computer Engineering (p. 6). Toronto, Canada: IEEE Toronto.
- [38] Mian Ahmad Jan and Muhammad Khan, "A Survey of Cluster-based Hierarchical Routing Protocols", in *IRACST-International Journal of Computer Networks and Wireless Communications (IJCNCW)*, Vol.3, April. 2013, pp.138-143.
- [39] Khan. S., Khan. F., (2015). Delay and Throughput Improvement in Wireless Sensor and Actor Networks. 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW) (pp. 1-8). Riyadh: IEEE Riyad Chapter.
- [40] Khan. Shahzad, Khan. F., Jabeen. Q., Arif F., Jan. M. A., Khan. S.A (2016). Performance Improvement in Wireless Sensor and Actor Networks. in the *Journal Applied, Environmental, and Biological Sciences* Print ISSN: 2090-4274 Online ISSN: 2090-4215
- [41] Puthal, D., & Sahoo, B. (2012). Secure Data Collection & Critical Data Transmission in Mobile Sink WSN: Secure and Energy efficient data collection technique.
- [42] Mian Ahmad Jan and Muhammad Khan, "Denial of Service Attacks and Their Countermeasures in WSN", in *IRACST-International Journal of Computer Networks and Wireless Communications (IJCNCW)*, Vol.3, April. 2013.
- [43] Qamar Jabeen, Fazlullah Khan, Muhammad Nouman Hayat, Haroon Khan, Syed Roohullah Jan, Farman Ullah, " A Survey : Embedded Systems Supporting By Different Operating Systems", *International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET)*, Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.664-673, March-April 2016. URL : <http://ijsrset.com/IJSRSET1622208.php>
- [44] M. A. Jan, P. Nanda, X. He and R. P. Liu, "A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network" in *Trustcom/BigDataSE/ISPA*, Vol.1, PP-318-325, 2015, IEEE.
- [45] Jabeen. Q., Khan. F., Hayat, M.N., Khan, H., Jan., S.R., Ullah, F., (2016) A Survey : Embedded Systems Supporting By Different Operating Systems in the *International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET)*, Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.664-673.
- [46] Syed Roohullah Jan, Syed Tauhid Ullah Shah, Zia Ullah Johar, Yasin Shah, Fazlullah Khan, " An Innovative Approach to Investigate Various Software Testing Techniques and Strategies", *International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET)*, Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.682-689, March-April 2016. URL : <http://ijsrset.com/IJSRSET1622210.php>
- [47] M. A. Jan, P. Nanda, X. He and R. P. Liu. 2016. A Lightweight Mutual Authentication Scheme for IoT Objects, *IEEE Transactions on Dependable and Secure Computing (TDSC)*, "Submitted".
- [48] M. A. Jan, P. Nanda, X. He and R. P. Liu. 2016. A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application, *Elsevier Future Generation Computer Systems (FGCS)*, "Submitted".
- [49] M. A. Jan, M. Usman, P. Nanda and X. He. 2016. PAWN: A Payload-based mutual Authentication scheme for Wireless Sensor Networks, in 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-16), "accepted".
- [50] M. Usman, M. A. Jan and X. He. 2016. Cryptography-based Secure Data Storage and Sharing Using HEVC and Public Clouds, *Elsevier Information sciences*, "accepted".
- [51] Khan. F., Khan. F., Jabeen. Q., Jan. S. R., Khan. S., (2016) Applications, Limitations, and Improvements in Visible Light Communication Systems in the *VAWKUM Transaction on Computer Science* Vol. 9, Iss.2, DOI: <http://dx.doi.org/10.21015/vtcs.v9i2.398>
- [52] Syed Roohullah Jan, Fazlullah Khan, Muhammad Tahir, Shahzad Khan., (2016) "Survey: Dealing Non-Functional Requirements At Architecture Level", *VFAST Transactions on Software Engineering*, (Accepted 2016)
- [53] M. A. Jan, "Energy-efficient routing and secure communication in wireless sensor networks," Ph.D. dissertation, 2016.

- [54] Syed Roohullah Jan, Faheem Dad, Nouman Amin, Abdul Hameed, Syed Saad Ali Shah, " Issues In Global Software Development (Communication, Coordination and Trust) - A Critical Review", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.660-663, March-April 2016.  
URL : <http://ijsrset.com/IJSRSET1622207.php>

