Elsevier Editorial System(tm) for Journal of Network and Computer Applications
Manuscript Draft

Manuscript Number:

Title: Metadata Hiding for UAV Video Based on Digital Watermarking in DWT Transform

Article Type: Research Paper

Keywords: UAV; Drones; Metadata hiding; Video watermarking; Copyright protection; Image scrambling.

Corresponding Author: Dr. Nasr addin Ahmed Salem Al-maweri, Ph.D

Corresponding Author's Institution: Faculty of Computer Science and Information Technology, University of Malaya

First Author: Nasr addin Ahmed Salem Al-maweri, Ph.D

Order of Authors: Nasr addin Ahmed Salem Al-maweri, Ph.D; Aznul Qalid Md Sabri, PhD; Ali Mohammed Mansoor, PhD; Unaizah Hanum Obaidellah, PhD; Erma Rahayu Mohd Faizal, PhD; Joan Lai P C, PhD

Abstract: As the advent of the Unmanned Aerial Vehicles (UAVs) has been increased, the protection of the information within the transmitted or stored video has become a big challenge. Most known drone systems attach metadata of the recorded video in separate files or in the header of the video. Current techniques make the metadata unsecure and easy to get lost and removed as well as it occupies more storage and bandwidth. In this paper, an efficient method is proposed to hide the metadata of UAVs video using the technology of digital watermarking. Discrete Wavelet Transform (DWT) is used to implement the embedding of the information robustly. The middle frequencies coefficients reside on CH3 sub-band are utilized to hide the watermark bits. In addition, a new scrambling algorithm is proposed to secure the information before hiding. The adaption of the proposed video watermarking algorithm to hide the metadata of the UAV video is achieved. The experimental results prove the high performance of the proposed method. The method had unnoticeable impact on the video quality where the PSNR of 44 dB is attained. The experiments show that the method achieves high robustness under various attacks and provides enough capacity for metadata hiding of UAV video.

Cover Letter

Dear Sir\Madam,

Regarding the paper titled:

'Metadata Hiding for UAV Video Based on Digital Watermarking in DWT Transform'

We would like to inform you that to the best of our knowledge:

1. Currently, the paper has not been submitted for publication anywhere, and it will not be submitted until a decision has been made.
2. The paper presents original material which has not previously published, completely or in part, in another journal.
3. Furthermore, this paper does not previously published in conference proceedings and does not submitted for publication anywhere.

It is our pleasure to submit our article to your respectful journal, Journal of Network and Computer Applications. To further share our knowledge with this new article as an addition to our previously published article in your journal by the part of our team titled
" Fair Uplink Bandwidth Allocation and Latency Guarantee for Mobile WiMAX Using Fuzzy Adaptive Deficit Round Robin"
Additionally, the authors would like to express their grateful to your estimated journal to support and serve the knowledge's.

Sincerely,

Nasr addin Ahmed Salem Al-maweri

Corresponding Author

***Suggested List of Potential Referees**

Suggested Reviewers List:

1- PIERANGELA SAMARATI,
pierangela.samarati@unimi.it,
Department of Information Systems,
Università degli Studi di Milano, Italy
2- Yuh-Jong Hu,
jong@cs.nccu.edu.tw,
Department of Computer Science,
National Chengchi University, Taiwan
3- SUKUMAR SENTHILKUMAR,
ssshivani1974@yahoo.co.in,
School of Mathematical Sciences,
Universiti Sains Malaysia, Malaysia

Metadata Hiding for UAV Video Based on Digital Watermarking in DWT Transform

Nasr addin Ahmed Salem Al-maweri[1]*, Aznul Qalid Md Sabri[1], Ali Mohammed Mansoor[1], Unaizah Hanum Obaidellah[1], Erma Rahayu Mohd Faizal[1], Joan Lai P C[2]

[1]*Faculty of Computer Science and Information Technology,*
[2] *UM Centre of Innovation and Commercialization*
University of Malaya, Malaysia

***Abstract*— As the advent of the Unmanned Aerial Vehicles (UAVs) has been increased, the protection of the information within the transmitted or stored video has become a big challenge. Most known drone systems attach metadata of the recorded video in separate files or in the header of the video. Current techniques make the metadata unsecure and easy to get lost and removed as well as it occupies more storage and bandwidth. In this paper, an efficient method is proposed to hide the metadata of UAVs video using the technology of digital watermarking. Discrete Wavelet Transform (DWT) is used to implement the embedding of the information robustly. The middle frequencies coefficients reside on CH3 sub-band are utilized to hide the watermark bits. In addition, a new scrambling algorithm is proposed to secure the information before hiding. The adaption of the proposed video watermarking algorithm to hide the metadata of the UAV video is achieved. The experimental results prove the high performance of the proposed method. The method had unnoticeable impact on the video quality where the PSNR of 44 dB is attained. The experiments show that the method achieves high robustness under various attacks and provides enough capacity for metadata hiding of UAV video.**

***Keywords*—UAV; Drones; Metadata hiding; Video watermarking; Copyright protection; Image scrambling.**

1. Introduction

Innovations involving Unmanned Aerial Vehicles (UAVs), or commonly known drones have recently progressed rapidly through innovative developments. In recent years (T.Lilien et al., 2014, Saleem et al., 2015) unlike the common assumption, the UAVs are used for military missions, but have been incorporated into various civilian applications. The services this device offer can often outperform human capabilities across various places. Nowadays, the UAVs' product specifications have reached sophisticated functionalities. For example, UAVs that can fly up to 50,000 feet can be controlled remotely from thousands of miles from its flying location (Lowenthal, 2015). Hence, the availability in the market is advantageous. This includes eliminating danger among workers who perform high-risk and life-threatening duties such as those involved in disaster management. The UAVs is increasingly impacting a large contribution in our daily life, organizations and governments. Among the common applications of UAVs are used in the following areas: security and control, military missions, air reconnaissance, traffic monitoring, forest and water search and rescue, firefighting, disaster monitoring and management (i.e., floods, earthquakes), surveys, 3D environment modeling, delivery services, farming and ranching, media reporting and news, border patrol, atmosphere sensing, map guidance, and many more (Rango et al., 2006; Nex and Remondino, 2013; Quaritsch et al., 2010; Mohammed et al., 2014).

Although, the advancement in UAVs technology and specifications have shown development of their products rapid progress, issues related to security information to UAV still needs further development and enhancement. By far, developers have added encryption systems and firewalls to achieve trusted transmission. This form of security is considered as the commutation security.

However, once the information is transferred on the drone or transmitted to the Air Traffic Control (ATC), it becomes unsecure. Thus, this situation is considered as the information security issue.

One of the most important tasks of a UAV is to record images or videos during its mission before transferring these data to the ATC. Commonly, UAV will essentially collect the information in the form of videos data that it has captured. This kind of information is called *Metadata*. Metadata contains highly sensitive and valuable information such as the location of the video, the GPS coordinates, the, time and date, the camera angles and what the video is taken for. This type of set of information is notoriously confidential for disclosure especially in areas such as security control, military and maritime.

The current implementation of video systems in UAVs sends the metadata as, either, a separate file or saves the data within the header file of the video. Both techniques do not give concern on the security issues of the metadata. As a result, the data are susceptible to loss or deletion. Recently, a *zombie drone* supported by a system called SkyJack was introduced. The purpose of this type of drone is to hack the systems of other drones enabling it to take advantages of their information and control them (Paganini, 2014). This alarming situation strengthens the importance of addressing the security issues pertaining to the UAVs information.

Therefore, to protect the metadata from being hijacked, leaked and revealed, we propose a method to hide the metadata using an efficient and robust technique via digital watermarking based on Discrete Wavelet Transform (DWT). Digital

watermarking concerns with embedding some information namely called watermark into another digital signal of data file such as text, video, audio or image. Digital watermarking has always been implemented as three main components watermarks generation, embedding and extraction (Al-maweri et al., 2016). Furthermore, a new scrambling method is developed to encode the metadata before hiding it in the video. The proposed video watermarking algorithm tries to enhance the video watermarking performance in terms of imperceptibility, robustness and capacity compared to the existing video watermarking methods. In addition, we intend to adopt the watermarking technique on the UAVs video metadata.

The rest of the paper is organized as follows: the second section reviews the recent video watermarking algorithms. The third section discusses the DWT transform. The fourth section explains the proposed algorithm. The fifth section presents the experiments and results of evaluating the proposed video watermarking. Finally, the sixth section concludes the paper.

2. Related Work

Security challenges and vulnerabilities related to the UAVs development worries air drones vendors since the beginning of the UAVs discovery. For this matter, researchers in the field began to think about solutions in various ways to address these challenges. One research that focused on securing the metadata of the transmitted video was introduced by (Marcinak and Mobasseri, 2005). In their research, they proposed sending the metadata information within the video by embedding the metadata using digital watermarking. Their method used VLC representation to build the pair trees where the watermark bits are embedded by either changing the specific bits in some blocks to indicate embedding '1' or leaving the block unchanged to indicate embedding '0'. However, the VLC approach in watermarking is now considered obsolete. Researchers in this field have stopped using this method as indicated by no recent contributions offered to improve this mechanism. That is largely influenced by the complexity in the implementation of such technique. Moreover, (Marcinak and Mobasseri, 2005) have not reported any positive results on the robustness of using VLC trees for the purpose of watermarking. Nevertheless, a previous study by (Alattar et al., 2003) reported some results of using VLC trees for video watermarking. The reported results showed very low performance in term of its robustness compared to the recent works on video watermarking.

Digital video watermarking has evolved rapidly and research improvements in the field are still ongoing. (Faragallah, 2013) developed an approach for video watermarking using Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT). He transformed the video into DWT using two levels of decomposition. The coefficients such as CH2, CV2 and CD2 sub-bands were then transformed into an SVD form before the embedding was performed. The Error Correction Code was integrated to the method to enhance its robustness against any attack. The reported results showed some improvements to the imperceptibility and robustness. However, the Bit Error Rate (BER) was high under some attacks such as median filtering, frame averaging, JPEG compression and scaling. This indicates that the algorithm is not resilient to potential attacks. Another algorithm was proposed by (Masoumia and Amirib, 2013). In this algorithm, the DWT with three levels of decomposition was used after applying motion detection based on scene change analysis. The watermark bits were embedded using the spread spectrum technique on CH3, CV3 and CD3 sub-bands. This approach showed lower performance compared to (Faragallah 2013). In this result, the Low Peak Signal to Noise Ration (PSNR) about 35 with low robustness under attacks such as frame dropping, frame averaging, frame swapping and noise, indicate degraded overall performance.

A different approach was proposed by (Thanh et al., 2014). In this approach, the embedding was achieved in low frequency coefficients of DCT domain. DCT was applied to only specific regions in the video sequence. These regions were generated based on the matching regions between the frames using the *frame patch matching technique*. The algorithm was concerned to tolerate geometrical attacks. Hence, the KAZE feature matching method was used before extraction is executed to recover the distorted video scene from the original scene. Although the algorithm intends to increase the robustness against geometrical attacks and had survived rotations, it showed low robustness under scaling, frame dropping and frame insertion. Another method for video watermarking that used DCT was proposed by (Ahuja and Bedi 2015). In their method, DCT was obtained from each frame for the luminance part only after converting the video into the YUV color space. The embedding of the watermark bits was executed diagonally in the coefficients in each block obtained from 8x8 blocks of the DCT transformation. This algorithm showed low PSNR value less than 35. However, it showed some enhancement under certain attacks such as frame swapping. Nevertheless, it showed lower robustness under other attacks such as noising, filtering and geometrical attacks.

(Agilandeeswari and Ganesan, 2015) proposed a hybrid video watermarking method which utilized Contourlet Transform (CT), DWT and SVD. In this method, the embedding was performed on DWT coefficients of both middle frequency sub-bands CH and CV. Before embedding, the detection of non-motion frames using histogram difference and applying CT transform for the chosen frames is performed. The watermark image was scrambled using the Arnold transform and sliced into 24 slices using bit plane slicing algorithm. This watermarking approach attained good perception quality with high PSNR values about 60 dB. However, the robustness showed degraded performance under various attacks such as Gaussian noise, salt and pepper noise, frame swapping, and rotation.

Recently, a real-time video watermarking algorithm for surveillance networks was proposed by (Liu et al., 2015). In this algorithm, the video frames were segmented into candidate-scenes-based after transforming the frames into

DCT domain. These selected scenes are obtained by finding the relationships between the frames. The VLC run level pairs are changed to embed the bits in the macro blocks. The experiments showed an acceptable PSNR value of 42 dB. However, the robustness was still close to the previous mentioned works, if not less, in many situations. Their results were reported using bit correction rate (BCR) in the chosen frames. As reported, the BCR under no attack was negligible between 0.85 and 1 in rare situations.

The lack of works in the field of UAVs security issues and the current threats for the critical data transmitted with UAVs videos as well as the gap in the performance level of the current video watermarking schemes motivates further research and investigation to protect UAVs systems.

3. Discrete Wavelet Transform

Practically, the techniques of digital video watermarking perform the embedding of the information in the sequence of images that construct the video scene. The embedding is executed either in the spatial domain or in the frequency domain. In spatial domain, the embedding is implemented to modify the pixel values. While, in frequency domain, the media is converted first into another transform and the embedding is executed by modifying the frequency coefficients. However, most of the available works prefer using frequency domain due to providing high robustness, capacity. In addition, this type of domain promotes fewer defects to the visual quality of the watermarked data (Gupta et al., 2015; Al-maweri et al., 2015). The Discrete Wavelet Transform (DWT) is one of the most common frequency forms that can contribute to the digital watermarking technique. It converts the image data from its pixels representation into another coefficients representation using some mathematical equations. For an image *I* as input for the DWT transform, the transform can be executed by dividing the original image into four equal size matrices, each matrix contains the coefficients of specific features on the images according to frequency level, starting from low frequency to high frequency. Four coefficients representations produce one level of decomposition - Approximations, (CA), Horizontally CH, Vertically (CV) and Diagonally (CD). This level can be further decomposed to multiple levels as shown in Figure 1. The proposed method is developed based on a DWT which uses the *daubechies* 'db1' filtering family. The CA3 and CV3 coefficients were utilized to perform the embedding in CH3 sub-band as highlighted in Figure 1.

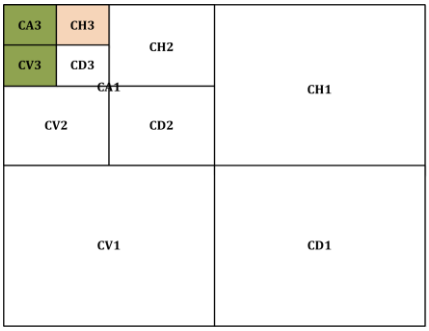


Figure 1: Chosen DWT Sub-bands

The principle of utilizing more than one sub-band coefficients for embedding purposes is adopted from (Yanxia Zhao and Zenghui Zhou, 2012). The proposed algorithm is expected to enhance the performance in term of imperceptibility and robustness as well as security by proposing new mathematical embedding equations and mechanism and adapting it to metadata hiding.

4. The Proposed Watermarking Algorithm

The main purpose of developing the proposed digital video watermarking algorithm is to adapt it to the metadata protection and hiding for the videos taken by UAVs systems. This proposed algorithm can be integrated with the videoing system in UAVs either before transmitting the video or once information are received by the data centres, commonly known as the Air Traffic Control (ATC). The proposed video watermarking algorithm is developed in a way that suits hiding the collected data from the UAVs such as the date and time the video is taken, the location where the video is taken, the GPS coordinates of the important scene, altitudes and angels of the camera. These data are sensitive and confidential. Thus, exposure of such data is highly risky. The developed watermarking algorithm will manage scrambling the metadata of the video using two secret keys before generating images of the metadata. This is followed by hiding these images within the recorded video using the DWT domain. Figure 2 illustrates the concept of the proposed metadata hiding application.

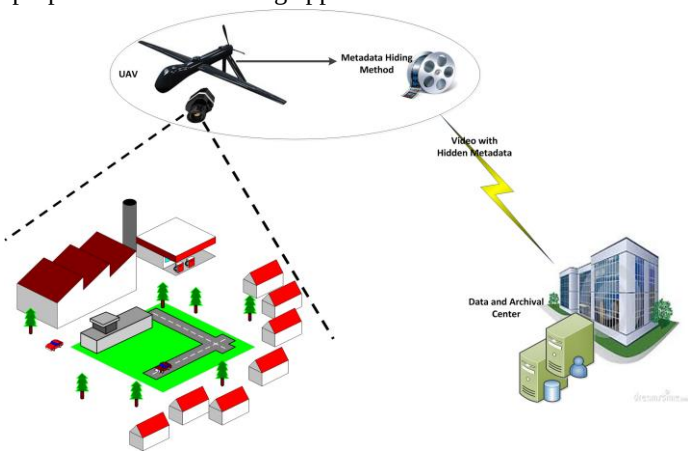


Figure 2: Metadata Hiding in UAVs Video

4.1. Metadata Scrambling and Generation

Given that the metadata is confidential, sensitive and susceptible to the recent threats of zombie drones (i.e., UAVs hack systems), it is imperative to encode the metadata before hiding them it in the video. This is achieved in the proposed algorithm by proposing a new scrambling technique. This technique differs from the conventional scrambling mechanisms which have been used in previous watermarking systems. The proposed

scrambling technique takes two keys as input and the metadata as image of size (128x128) pixels. It scrambles the image of the metadata according to the keys using the proposed mathematical equations. The output from the scrambling process will be in the form of 16 generated and encoded watermarks. These 16 watermarks are generated to adapt the watermarking process for the metadata and video of the UAVs. Figure 3 presents a description of how scrambling of the metadata and generation of the watermarks are performed.

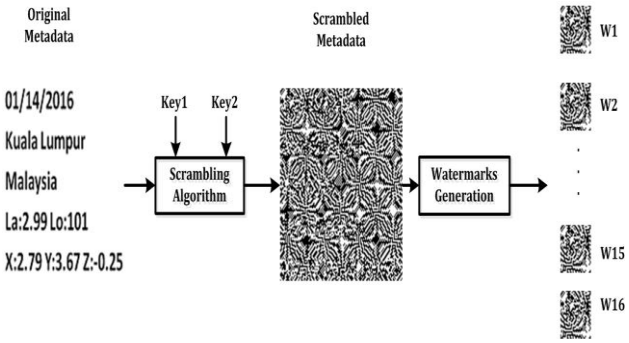


Figure 3: Metadata Scrambling and Watermarks Generation

The following steps describe the process of scrambling the metadata and generating the watermarks:

Step1: Input Key1, Key2, OriginalDataImage (128x128).
Step2: Create Matrix1(128x128) as:

$$\text{Matrix1}(i,j) = \frac{\text{round }(\text{Key 1} * (i+j))}{\sqrt{\text{Key 1}}} \quad (1)$$

Step3: Create Matrix2 as:

$$\text{Matrix2}(i,j) = \frac{\text{round }(\text{Key 2} + (i*j))}{\sqrt{\text{Key 1}}} \quad (2)$$

Step4: From Matrix1, generate BinaryImage1 as:

$$BinaryImg1(i,j) = \begin{cases} 1, & Matrix1(i,j)\ is\ even \\ 0, & Matrix1(i,j)\ is\ odd \end{cases} \quad (3)$$

Step5: From Matrix2, generate BinaryImage2 as:

$$BinaryImg2(i,j) = \begin{cases} 1, & Matrix2(i,j)\ is\ even \\ 0, & Matrix2(i,j)\ is\ odd \end{cases} \quad (4)$$

Step6: Convert OriginalDataImage to Binary.
Step7: Perform XOR operation for OriginalDataImage and BinaryImg1.
Step8: Perform XOR operation for Step7 output and BinaryImg2.
Step9: Divide the scrambled image into 16 equal images of size (32x32).
Step10: Return the scrambled 16 watermarks from Step9.

4.2. Video Watermarks Embedding

After generating the scrambled watermarks from the previous process, the embedding of the watermarks in the video taken by the UAV camera is performed. This phase pre-processes the video in which the entire video is split into image sequences or frames. The embedding of the scrambled watermarks is then achieved, and finally, the watermarked frames are reconstructed together to build the watermarked video containing the hidden metadata. Figure 4 shows the proposed video watermarking process.

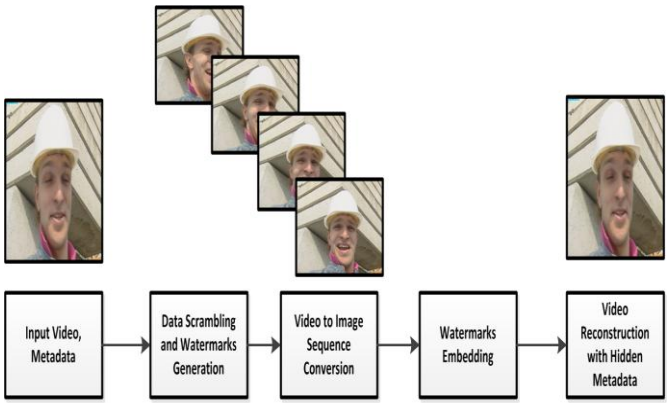


Figure 4: Video Watermarks Embedding Process

The embedding of the watermarks in the video frames is executed by embedding 16 watermarks, each in one frame. The process is repeated specific times for another 16 frames, obtained from the original metadata as in Figure 3, to increase the robustness of the extraction. The algorithm is made flexible to repeat the embedding process multiple times according the video length. The following steps explain the embedding procedure in the video:

Step1: Input Video, OriginalDataImage.
Step2: Scramble and generate 16 watermarks of size (32x32) from OriginalDataImage.
Step3: Read the video and convert it into frames (image sequence)
Step4: Set *i*=1. *Stop*= length (video).
Step5: Read watermarks from *W1* to *W16*.

4.3. **Step6:** Call *Frame Watermark Embedding* to embed each watermark in each *ith* frame until *W16*.
Step7: *i=i+16*.
Step8: Save the watermarked frames.
Step9: Loop until Stop, or prior specified *ith* frame.
Step10: Reconstruct the video from the watermarked frames.
Step11: Return the watermarked video.

4.4. Frame Watermark Embedding

During embedding the watermarks in the video sequence images, each watermark embedding in each frame is

performed by calling the frame watermarking procedure as in step 6 in section 4.2. The frame embedding procedure purpose is to insert the bits of the watermark sized as (32x32) pixels to the *ith* frame on the image sequences. It takes the frame image as RGB and the scrambled watermark, performs the embedding in YCbCr color space using DWT transform then produces the watermarked frame with the hidden metadata in RGB again. As explained previously, the watermarking is achieved in the middle frequency coefficients, specifically, in CH3, to enhance both visual quality impact and tolerance of the hidden data to survive attacks and video distortions. Figure 5 describes the frame watermarking process.

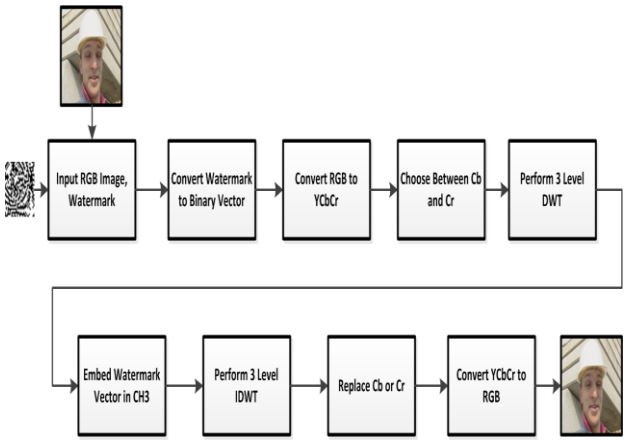


Figure 5: Frame Watermarking Process

The frame watermark embedding is executed according to the following steps:

Step1: Input RGB image, Watermark, Scaling factors (α, β).
Step2: Convert Watermark to Binary Vector (1024 bit).
Step3: Convert RGB to YCbCr color space.
Step4: Calculate Average Chrominance Red (Cr) and Chrominance Blue (Cb) where:

$$I = \begin{cases} Cb, & Cr < 3 \\ Cr, & Cr > 3 \end{cases} \quad (5)$$

Step5: Perform 3 Level DWT for image I using 'db1'.
Step6: Embed Watermarks Bits one by one in CH3 sub-band as follow:

- *k*=1;
- Compute Δ_1 and Δ_2

$$\Delta_1 = \frac{|CA3(i,j)| - |CV3(i,j)|}{\beta} \quad (6)$$

$$\Delta_2 = \frac{|CA3(i,j)| - |CH3(i,j)|}{\Delta_1} \quad (7)$$

- Modify CH3 coefficients where:

$$\mathrm{CH3(i,j)} = \begin{cases} \frac{\Delta_2 + CH3(i,j)}{\alpha}, & Watermark(k) = 1 \\ CH3(i,j), & Watermark(k) = 0 \end{cases} \quad (8)$$

- *k=k+1*.
- Negate back Negative coefficients.

Step7: Loop in CH3 until all watermarks bits are embedded.
Step8: Perform the inverse 3 Level IDWT for modified image I.
Step9: Convert YCbCr to RGB.
Step10: Return the watermarked frame.

4.5. Video Watermarks Extraction

Since the proposed watermarking algorithm is developed to have blind extraction scheme, which means that there is no need for the original video to be available upon extraction. The archived watermarked video which contains the hidden metadata can be used on the extraction algorithm in a blind way in order to extract the hidden data in the video. The video extraction procedure is performed by splitting the video into image sequence, where the hidden 16 watermarks are extracted. Then the watermarks are reconstructed to form the 128x128 pixels image and finally the metadata are descrambled. Figure 6 shows the process of video watermarking extraction.

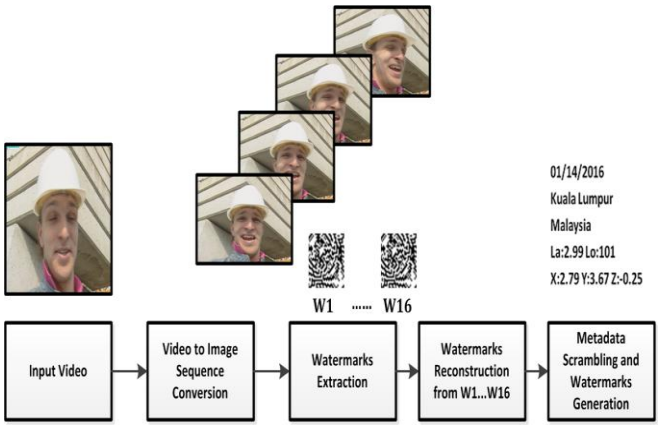


Figure 6: Video Watermarks Extraction Process

The following steps explain how the extraction procedure from the video is implemented:

Step1: Input Video.
Step2: Read the video and Convert it into frames (image sequence)
Step3: Set *i*=1. *Stop*= length (video).
Step4: Call *Frame Watermark Extraction* to extract each watermark from each *ith* frame until *W16*.
Step5: Reconstruct the Extracted Watermark from *W1 ... W16*, then, Descramble the extracted Watermark (128x128).

Step6: Save the Extracted Watermark (Hidden Data).
Step7: *i=i+16*.
Step8: Loop until Stop, or prior specified *ith* frame.

4.6. Frame Watermark Extraction

To extract each watermark from each watermarked frame, a *Frame Watermark Extraction* is implemented and being called by the main video extraction procedure as in step 4, section 4.4. The watermarked frame in RGB color space and the two scaling factors β and α values used in the embedding process are used again with the same values in the extraction procedure. The RGB image is converted to YCbCr color space and the extraction is done in DWT domain from CH3 sub-band as shown in Figure 7.

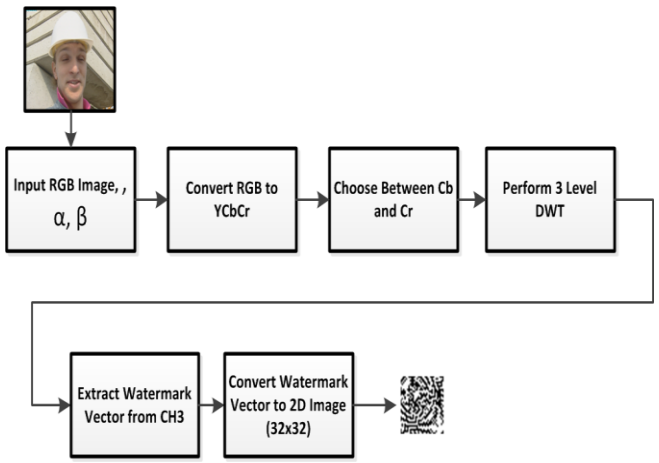


Figure 7: Frame Watermarks Extraction Process

Using the scaling factors in the proposed mathematical embedding and extraction formulas made it possible to enhance the trade-off between imperceptibility and robustness of the watermarking. The following steps explain the implementation of the extraction procedure for specific frame:

Step1: Input RGB image, α, β.
Step2: Convert RGB to YCbCr color space.
Step3: Calculate Average Chrominance Red (Cr) and Chrominance Blue (Cb) where:

$$\bar{I} = \begin{cases} Cb, & Cr < 3 \\ Cr, & Cr > 3 \end{cases} \quad (8)$$

Step4: Perform 3 Level DWT for image I using 'db1'.
Step5: Extract Watermarks Bits one by one from CH3 sub-band as follow:

- *k*=1;
- Compute Δ_1, Δ_{1ex} and Δ_{2ex} such that:

$$\overline{\Delta_1} = \frac{|CA3(i,j)|-|CV3(i,j)|}{\beta} \quad (9)$$

$$\Delta_{2ex} = |CH3(i,j)| * \alpha - |CH3(i,j)| \quad (10)$$

$$\Delta_{1ex} = \frac{|CA3(i,j)|-|CH3(i,j)|}{\Delta_{2ex}} \quad (11)$$

- Extract Watermark Bit from CH3 coefficients where:

$$\text{Watermark}(k) = \begin{cases} 0, & \overline{\Delta_1} - \Delta_{1ex} > x \\ 1, & \overline{\Delta_1} - \Delta_{1ex} < x \end{cases} \quad (12)$$

Where $x = 1, \ldots 10$ according to the attack strength

- *k=k+1*.

Step6: Loop in CH3 until all watermarks bits are extracted.
Step7: Convert the watermark vector (1024 bit) to 2D binary image (32x32).
Step8: Return the Extracted Watermark.

4.7. Metadata Descrambling

By the end of the extraction process from each 16 frames and the reconstruction of the scrambled watermark, the scrambled data image is taken as input to a proposed descrambling technique. This procedure will reverse the encoded data to its original form. The following steps clarify the steps of the implemented descrambling procedure.

Step1: Input *Key1*, *Key2*, *ScrambledDataImage* (128x128).
Step2: Create $Matrix1_{EX}$ (128x128) as:

$$Matrix1_{EX}\ (\mathrm{i},\mathrm{j}) = \frac{\text{round (Key 1}*(\mathrm{i}+\mathrm{j}))}{\sqrt{\text{Key 1}}} \quad (13)$$

Step3: Create $Matrix2_{EX}$ as:

$$Matrix2_{EX}\ (\mathrm{i},\mathrm{j}) = \frac{\text{round (Key 2}+(\mathrm{i}*\mathrm{j}))}{\sqrt{\text{Key 1}}} \quad (14)$$

Step4: From $Matrix1_{EX}$, generate $BinImg1_{EX}$ as:

$$BinImg1_{EX}(i,j) = \begin{cases} 1, & Matrix1_{EX}\ (i,j)\ is\ even \\ 0, & Matrix1_{EX}\ (i,j)\ is\ odd \end{cases} \quad (15)$$

Step5: From Matrix2, generate $BinImg1_{EX}$ as:

$$BinImg2_{EX}(i,j) = \begin{cases} 1, & Matrix2_{EX}\ (i,j)\ is\ even \\ 0, & Matrix2_{EX}\ (i,j)\ is\ odd \end{cases} \quad (16)$$

Step6: Convert *ScrambledDataImage* to Binary.
Step7: Perform XOR operation for *ScrambledDataImage* and $BinImg2_{EX}$.
Step8: Perform XOR operation for Step7 output and $BinImg1_{EX}$.
Step9: Return the *DescrambledDataImage* from Step8.

5. Experiments and Results

5.1. Experiments Setup

An experiment was performed to evaluate the performance of the proposed video watermarking

algorithm. This is done 1) to validate the goal of attaining optimal trade-off between keeping the visual quality of the watermarked (after metadata hiding) video as close as to the quality of the original video, and 2) to evaluate the robustness of the proposed algorithm against malicious attacks. This is also to ensure that both capacity and security metrics are taken into consideration.

Four different standard videos known as Foreman, News, Akiyo and Bus with resolution of (352x288), 10 seconds long and 30 frame/sec frame rate are used to execute the experiments. Another video was downloaded from WolFang Digital, a video production studio, taken by a UAV of the Kuala Lumpur City, named as UAVVideo is used to repeat the same assessment to validate the measured metrics on actual UAV video.

To measure the imperceptibility and the data invisibility, every video is watermarked with the metadata represented in image of size 128x128 pixels as illustrated in Figure 3. The original video sequence and the watermarked video are used to measure the average Peak Signal to Noise Ration (PSNR) value and similarity percentage according to the following formulas:

$$PSNR = 20\log_{10}\frac{MAX(O_{imseq})}{RMSE} \quad (12)$$

Such that:

$$RMSE = \sqrt{\frac{1}{mxn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[O_{imseq}(i,j) - W_{imseq}(i,j)]^2} \quad (17)$$

where *mxn* is the size of the image, *(i,j)* is the pixel location, O_{imaseq} is the original image sequence and W_{imseq} is the watermarked image sequence.

$$Similarity = \left(1 - \frac{RMSE}{MAX(O_{imseq})}x100\right)\% \quad (18)$$

To measure the extraction accuracy and the robustness of the proposed algorithm, every watermarked video was used to extract the hidden metadata. The accuracy of the extracted watermarks considering various attacks such as salt and pepper noise, Gaussian noise, scaling, frame dropping frame swapping, frame averaging and compression is evaluated by measuring both Bit error Rate (BER) and Normalized correlation (NC) according to the following formula:

$$NC = \left(\frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}O(i,j) - E(i,j)}{\sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}O^2(i,j)} \times \sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}E^2(i,j)}}\right) \quad (19)$$

Where, *O* is the original watermark and *E* is the extracted watermark.

5.2. Results and Discussion

5.2.1. Imperceptibility

The impact on the perceptual quality of the watermarked video was tested on all videos mentioned previously. Figure 8 and 9 shows the PSNR and Similarity Values, VS the watermarked frames from 10th to 27th frame in Forman video. PSNR showed high value of 44 in all frames and similarity above 99.32%. This indicates high imperceptibility of the proposed algorithm.

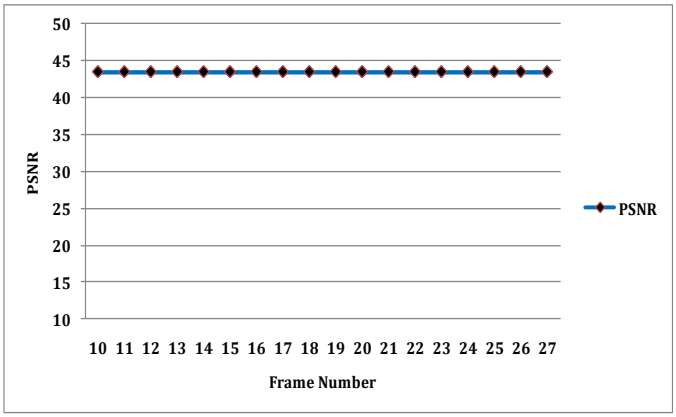


Figure 8: PSNR for Watermarked Video Frames

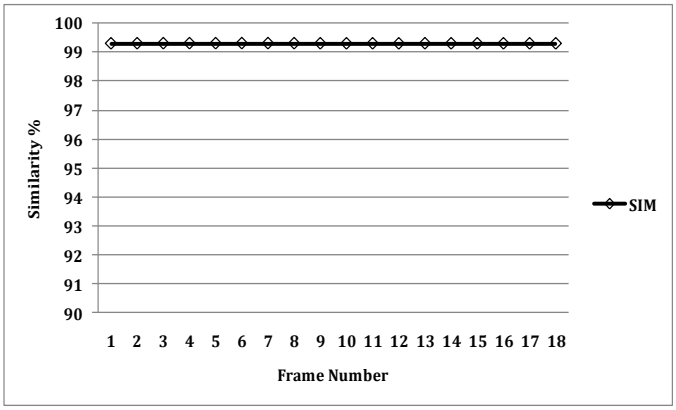


Figure 9: Similarity Measure for Watermarked Frames

The average PSNR and Similarity Values for different videos are measured and reported in Figure 10 and Figure 11. As observed, the performance of the proposed algorithm in terms of imperceptibility is stable with different kind of videos. The PSNR value attained is higher compared to the current algorithms in video watermarking as shown in Table 1.

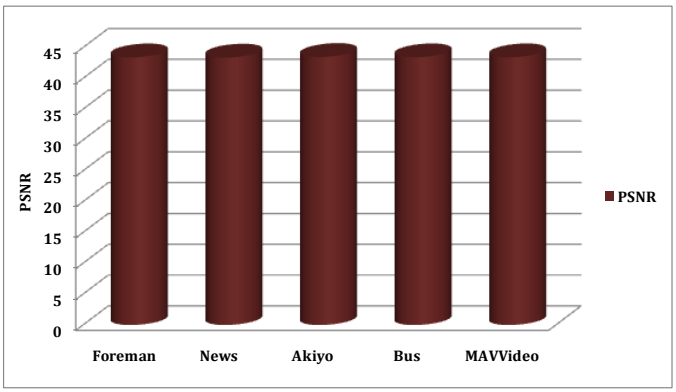


Figure 10: Average PSNR for various Watermarked Videos

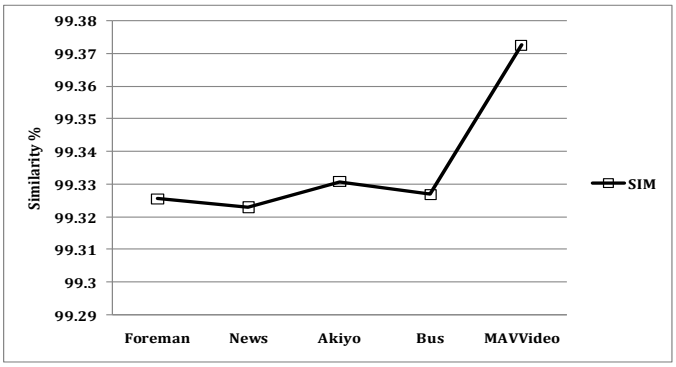


Figure 11: Average SIM for Various Watermarked Videos

Table 1: PSNR VS NC and BER

Algorithm	PSNR	NC	BER	Video
T. M. Thanh	37.14	1	0.00	Akiyo
Rakesh	36	0.997	0.003	Akiyo
M. Masoumi	35	0.994	0.007	Suzie
S. Liu	42	0.970	0.040	Bus
Proposed Algorithm	**44**	**1**	**0.000**	**All**

5.2.2. Robustness

The goal of the proposed algorithm is to achieve optimal performance by obtaining the trade-off between both PSNR and NC or BER values. The NC values measure the accuracy of the extracted watermarks compared to the original ones that carry the metadata. Figure 12 shows the robustness of the proposed algorithm from the watermarked frames. The NC values were always '1' which indicate perfect accuracy. Table 2 shows the extracted watermarks from different videos with their associated values of NC and BER. As observed, all the NC values are 1 and BER value are 0.000.

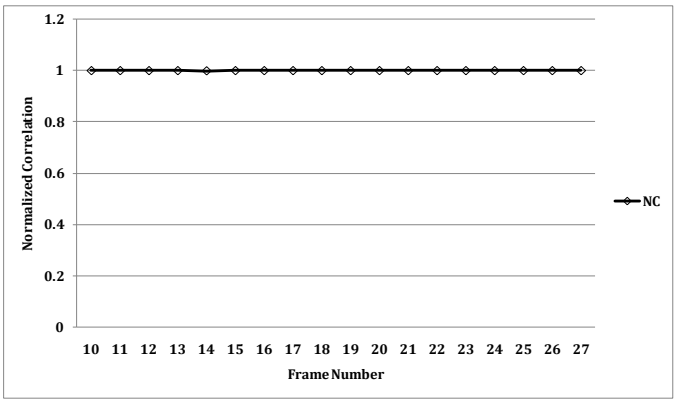


Figure 12: NC values for Extracted Watermarks from Watermarked Frames

Table 1: Accuracy of the Proposed Algorithm

Video	Extracted Watermark	NC	BER
Foreman	01/14/2016 Kuala Lumpur Malaysia La:2.99 Lo:101 X:2.79 Y:3.67 Z:-0.25	1	0.000
News	01/14/2016 Kuala Lumpur Malaysia La:2.99 Lo:101 X:2.79 Y:3.67 Z:-0.25	1	0.000
Akiyo	01/14/2016 Kuala Lumpur Malaysia La:2.99 Lo:101 X:2.79 Y:3.67 Z:-0.25	1	0.000
Bus	01/14/2016 Kuala Lumpur Malaysia La:2.99 Lo:101 X:2.79 Y:3.67 Z:-0.25	1	0.000
UAVVideo	01/14/2016 Kuala Lumpur Malaysia La:2.99 Lo:101 X:2.79 Y:3.67 Z:-0.25	1	0.000

As mentioned, it was necessary to attain optimal performance while achieving the trade-off between imperceptibility and robustness. Table 1, also describes the results of PSNR vs. NC and BER for the proposed algorithm and compares it with other algorithms. As shown in Table 1, the proposed algorithm performs better than the other reported works, where the

PSNR attained from the current work is higher than all of them. At the same time, the NC values reached the highest value 1 and BER was 0.000. Other algorithms attained lower PSNR and NC but higher BER. Although other studies tried to increase the PSNR values, their method affected the NC and BER values. The reasons behind getting better performance in our algorithm can be summarized as follow: Firstly, using the middle frequency coefficients from CH sub-band had fewer defects to the visual quality. Secondly, the proposed modification of the mathematical equations enabled the trade-off and control of the robustness and imperceptibility. Finally, the strategy of splitting the metadata over 16 frames and repeating the embedding in other frame blocks added high imperceptibility and provided more chance to detect the watermarks in case of malicious attacks.

To validate the resistance of the proposed algorithm against malicious attacks and video distortions, it was tested under certain attacks and the results are reported in Table 3. The extracted watermarks from the attacked videos are shown with each video, the NC and BER values are listed. From the results, it is proven that the algorithm survived most of the attacks with NC value 1 and BER 0.000. The algorithm continued to perform with high NC values around 0.99 on the other attacks such as noising, frame averaging and compression.

In order to prove the high performance of the proposed algorithm, it was compared with the other algorithms as listed in Table 4. It is obvious from the result that the proposed algorithm worked better than the other algorithms in surviving various attacks. Figure 13 also presents the comparison with the other algorithms (with and without attacks).

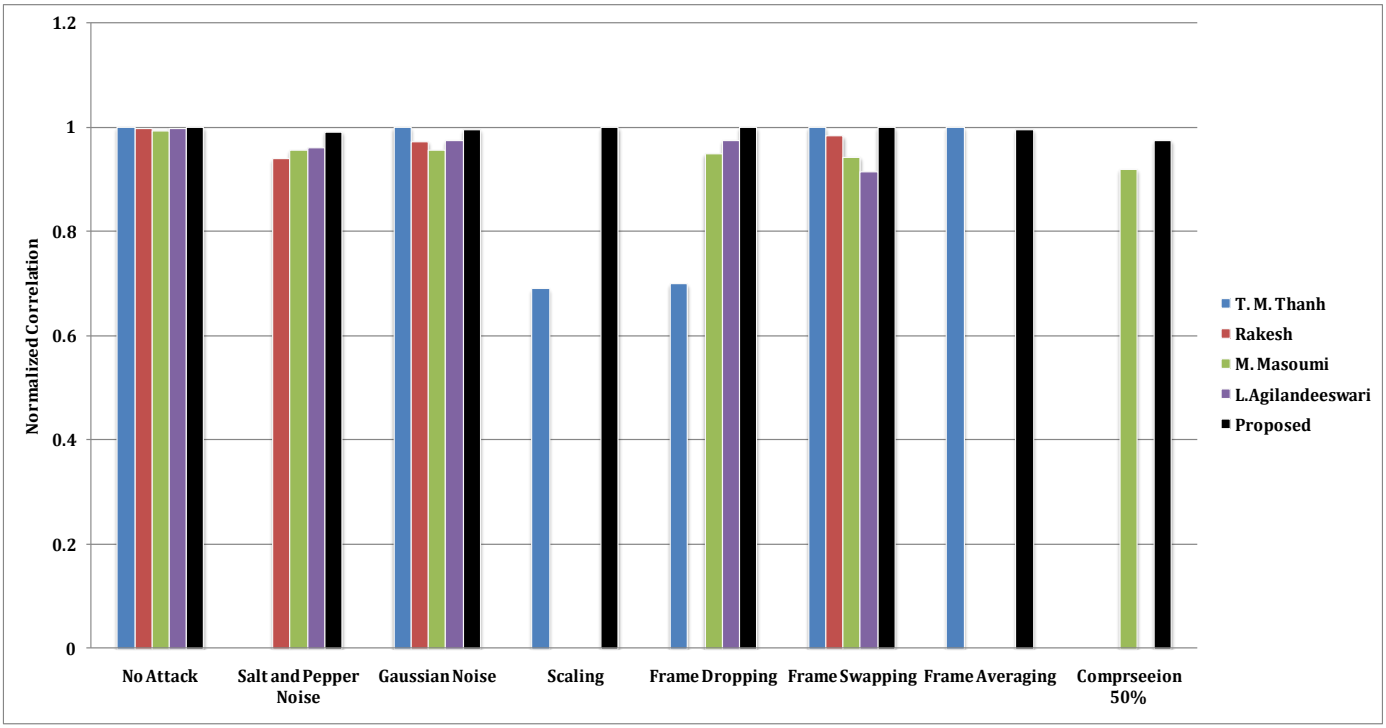


Figure 13: Comparison of the Robustness with Various algorithms

5.2.3. Capacity and Security

As contributed to enhancing imperceptibility and robustness metrics, the capacity and security issues for the proposed video watermarking algorithm is not neglected. The capacity of the algorithm is able to embed a payload size of 128x128 pixels, which means, it is able to hide a total of 16384 bits using 16 frames. In each frame, 32x32 pixels, which means 1024 bit, can be embedded. Setting up the capacity parameters in such manner helped in attaining high performance on the other side for both imperceptibility and robustness.

The security of the algorithm, as discussed in sections 4.1 and 4.6, is achieved by scrambling the metadata using two secret keys. Without knowing the keys, the hidden data cannot be revealed.

Table 3: Robustness against Various Attacks

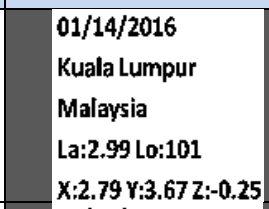
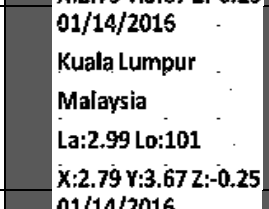
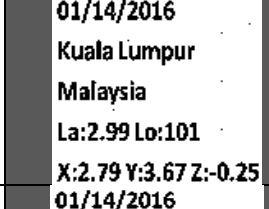
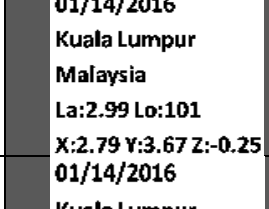
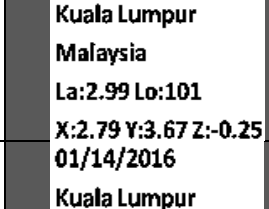
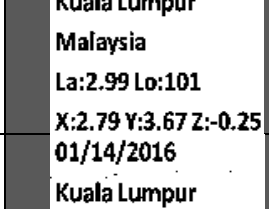
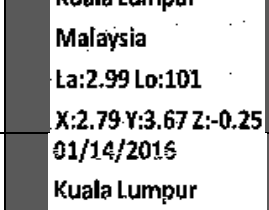
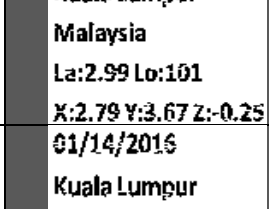
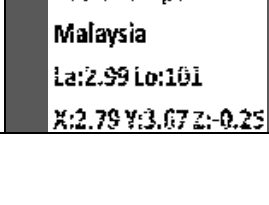
Attack Type	Extracted Data Image	NC	BER
No Attack		1	0.000
Salt and Pepper Noise		0.992	0.001
Gaussian Noise		0.996	0.003
Scaling		1	0.000
Frame Dropping		1	0.000
Frame Swapping		1	0.000
Frame Averaging		0.996	0.005
Compression 10%		0.995	0.005
Compression 50%		0.975	0.03

Table 4: Comparison between the Proposed Algorithm and Previous Works

Attack Type	T. M. Thanh	Rakesh	M. Masoumi	L.Agilandeeswari	Proposed
No Attack	1	0.997	0.994	0.999	**1**
Salt and Pepper Noise	N/A	0.939	0.956	0.96	**0.992**
Gaussian Noise	1	0.973	0.956	0.975	**0.996**
Scaling	0.69	N/A	N/A	N/A	**1**
Frame Dropping	0.7	N/A	0.949	0.9751	**1**
Frame Swapping	1	0.983	0.943	0.915	**1**
Frame Averaging	1	N/A	N/A	N/A	**0.996**
Compression 50%	0	N/A	0.9192	N/A	**0.975**

6. Conclusion

In this paper, the problem of disclosing, leaking or revealing the metadata of UAV recorded videos was solved by developing an enhanced video watermarking algorithm to be adapted to UAVs metadata hiding application. The proposed algorithm was implemented in DWT transform and the middle frequency coefficients were utilized. A new scrambling mechanism was implemented to secure the hidden metadata. The imperceptibility and robustness of the algorithm was enhanced to provide an optimal trade-off. The performance of the algorithm has been proven by testing it against various attack and video distortions. Testing and enhancing the algorithm under other geometrical attacks such as rotation is ongoing. Future research and test can be conducted with government agencies like the police force that will be using the drone or organizations using drone as their service like surveyors etc.

7. Acknowledgement

This work is funded under the Fundamental Research Grant Scheme; grant number FP061-2014A for the period of July, 2014 until end of June, 2016.

8. References

Agilandeeswari, L. and K. Ganesan (2015). A robust color video watermarking scheme based on hybrid embedding techniques. *Multimedia Tools and Applications, Springer*.

Ahuja, R. and R. Ahuja (2015). Copyright protection using blind video watermarking algorithm based on mpeg-2 structure. In *International Conference on Computing, Communication and Automation (ICCCA2015)*, pp. 1048–1053. IEEE.

Al-maweri, N. a. A. S., R. Ali, W. A. W. Adnan, A. R. Ramli, and S. M. S. A. A. Rahman (2016). State-of-the-Art in Techniques of Text Digital Watermarking: Challenges and Limitations. *Journal of Computer Science*. DOI**:** 10.3844/ofsp.10508.

Al-maweri, N. a. A. S., W. A. Wan Adnan, A. R. Ramli, K. Samsudin, and S. M. Syed Ahmad (2015). A hybrid digital image watermarking algorithm based on dct-dwt and auto-thresholding. *Security and Communication Networks 8*(18), 4373–4395.

Alattar, A. M., E. T. Lin, and M. U. Celik (2003). Digital watermarking of low bit-rate advanced simple profile mpeg-4 compressed video. *IEEE TRANSACTIONS ON Circuits and Systems For Video Technology 13*, 787–800.

Faragallah, O. S. (2013). Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain. *{AEU} - International Journal of Electronics and Communications 67*(3), 189 – 196.

Gupta, M., G. Parmar, R. Gupta, and M. Saraswat (2015). Discrete wavelet transform-based color image watermarking using uncorrelated color space and artificial bee colony. *International Journal of Computational Intelligence Systems 8*(2), 364–380.

Liu, S., D. B.-W. Chen, L. Gong, W. Ji, and S. Seo (2015). A real-time video watermarking algorithm for authentication of small-business wireless surveillance networks. *International Journal of Distributed Sensor Networks, Hindawi*.

Lowenthal, M. M. (2015). *Intelligence: From Secrets to Policy* (6 ed.). USA: CQ Press, SAGE Publication.

Marcinak, M. P. and B. G. Mobasseri (2005). Digital video watermarking for metadata embedding in uav video. In *Military Communications Conference*. IEEE.

Masoumia, M. and S. Amirib (2013). A blind scene-based watermarking for video copyright protection. *International Journal of Electronics and Communications (AEÜ),Elsevier 67*, 528– 535.

Mohammed, F., A. Idries, N. Mohamed, J. Al-Jaroodi, and I. Jawhar (2014, May). UAVs for smart cities: Opportunities and challenges. In *Unmanned Aircraft Systems (ICUAS), 2014 International Conference on*, pp. 267–273.

Nex, F. and F. Remondino (2013). UAV for 3d mapping applications: a review, springer. *Applied Geomatics 6*(1), 1–15.

Paganini, P. (2014). Privacy and security issues for the usage of civil drones. *Infosec Inistiute*.

Quaritsch, M., K. Kruggl, D. Wischounig-Strucl, S. Bhattacharya, M. Shah, and B. Rinner (2010). Networked as aerial sensor network for disaster management applications. *e & i Elektrotechnik and Informationstechnik 127*, 56–63.

Rango, A., A. Laliberte, C. Steele, J. E. Herrick, B. Bestelmeyer, T. Schmugge, A. Roanhorse, and V. Jenkins (2006, 9). Using unmanned aerial vehicles for rangelands: Current applications and future potentials. *Environmental Practice null*, 159–168.

Saleem, Y., M. H. Rehmani, and S. Zeadally (2015). Integration of Cognitive Radio Technology with unmanned aerial vehicles: Issues, opportunities, and future research challenges. Journal of Network and Computer Applications 50, 15 – 31.

Thanh, T. M., P. T. Hiep, T. M. Tam, and K. Tanaka (2014). Robust semi-blind video watermarking based on frame-patchmatching. *International Journal of Electronics and Communications (AEÜ),Elsevier 68*, 1007–1015.

L., L. ben Othmane, PelinAngin, AndrewDeCarlo, RaedM.Salih, and B. Bhargava (2014). A simulation study of adhoc networking of with opportunistic resourceutilization networks. *Journal of Network and Computer Applications 38*, 3–15.

Yanxia Zhao and Zenghui Zhou (2012, Sept). Multipurpose Blind Watermarking Algorithm for Color Image Based on DWT and DCT. In *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM),*, pp. 1–4.