Planning Document

Ng Wei Shyang
15033996
BSc (Hons) in Computer Science
Sunway University

Introduction

Steganography is technique of embeds secret messages in a cover file. The purpose of steganography is to conceal the secret messages in order to not get noticed where it get transmitted. Cover file can be anything from image, sound, video, word document, etc.

The purpose of this project is to research currenct existing steganography method and improve existing steganography method. Improved steganography method should result in higher undetectable probability in both perceptually and statistically.

The scope of this project will only be concerning about video steganography, specifically with H.264 encoding.

The proposed methodology of steganography will be concealing the data in H.264 motion estimated residual value and audio with using hiding scheme of bit plane replacement. The venue of data concealing will be decided by pseudorandom and the concealing data are encrypted before concealing it.

The proposed outcome will be a command line program that are able to both hide and retrieve data from a MP4 file with H.264 video encoding.

Literature Review

There are various method of video steganography and watermarking, each of them with different methodology and cater for different video type. There are watermarking method which do not have dependencies on any codec and as robust as able to remain watermarking after uploading to video streaming side, steganography are more concern with undetechable and capacity, therefore this project will only be concern with steganography method for H.264 codec. The reason of H.264 codec instead of others is because H.264 are one of the most widely adopted codec. According to news from encoding.com, H.264 codec has 72% of usage for both web and mobile [1].

This literature review will be seperated into 4 parts. The first part will be researching on H.264 codec methodology. In the second part, we will examine different steganography scheme. In third part, we will examine component of H.264 and opportunity of hiding data. In the last part, we will examine other part of the video which we can make use of in order to embed data into.

H.264

H.264 is a video compression standard which also known as MPEG-4 Part 10/AVC, which stands for Advance Video Coding. H.264 encoder are able to reduce the file size of a video file as much as 80% compare to Motion JPEG format and 50% reduced in file size when compared to MPEG-4 Part 2 standard [2].

H.264 or any other video compression are made up of a pair of algorithm, which is encoder or decoder, which also known as codec. Video codecs implementation from different standards are normally not compatible with each other. Encoder are used to encode raw video into an encoded video file which has smaller size than originally would by removing redundant video data, while decoder are used to decode the encoded video file back to original video format [2].

H.264 comes in with a total of 7 profiles. Usage such as network cameras and video encoder with limited computing resources are likely to use baseline profile. H.264 comes with 11 levels or degree of capability which define the bit rate and encoding rate in macroblock per second for

resolutions ranging from QCIF to HDTV. Higher level are required for higher resolution of video.

In H.264 encoding, frames are divided into several GOPs (group of pictures) [3]. Each frame will be labaled as either I (Intra), P (Predicted) or B (Bi-directional predicted). A self-contained frame that can be decode independently without any referencing to other frame are I-frame. I-frame are used for the first frame and every regular interval amount of frame. It can be used to implement fast-forward, rewind and other random access functions. P-frame is a frame which can only be decode with the reference of the previous frame. P frame usually require lesser bits than I-frame, however are more susceptible to decoding error whenever transmission error arise. Similar to P-frame, however make references to both previous and future frame are B-frames.

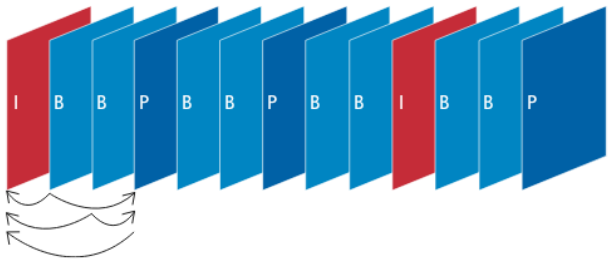

Fig. 1. *Typical sequence of I-frame, P-frame and B-frame in a video. P-frame make reference from previous I-frame or P-frame while B-frame make reference to previous and future I-frame and P-frame.*

At the beginning of the encoding process, macroblocks are form by dividing each frame into non-overlapping uniform size (16 × 16 pixels) as shown in Fig. 2. These macroblocks are further divide into smaller block, which 4 × 4 being the smallest possible block size as shown in Fig. 3. These smaller block will be applied with DCT, quantization and entropy coding. First, pixel values in macroblock will undergo DCT and Quantization process. For motion estimation and prediction purpose, the output of the process will further applied with De-Quantization and Inverse DCT. These pixel value are used make decision and coding mode and execute pixel value estimation during the stage of Intra and Inter prediction processes when decoding. Code Control as shown in Fig. 2 are used as an optimizer which regulates block sizes and coding modes selection. In order to best choose operational point between intra and inter mode for coding each macroblock, RDO (rate distortion optimization) are used. To achieve the targeted video bitrate, it also controls the Quantization Parameter.

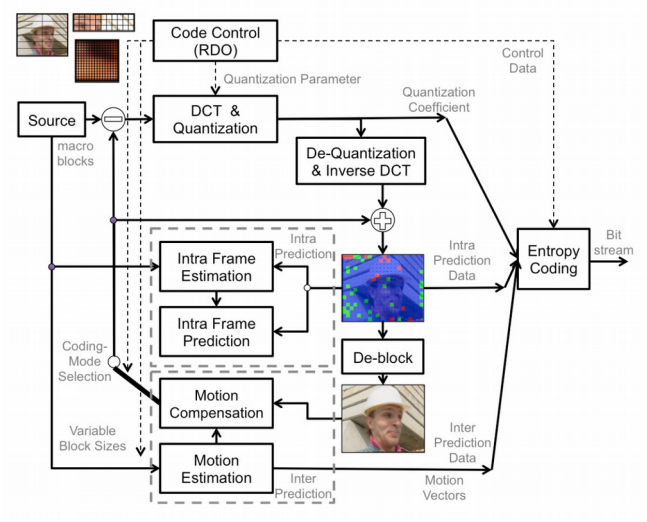

Fig. 2. *H.264 hybrid video encoder.*

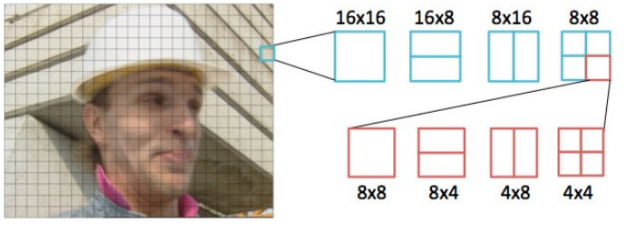

Fig. 3. Macroblock being divide into smaller block to embed information

For the case for I-frame, coefficients in transformed domain are used to encode the pixel values. To exploit the spatial redundancies within a frame, it also uses intra prediction with neighboring blocks for encoding the pixel values. For P-frame to reduce redundancies, motion estimation between two frames are implemented. For motion estimation, previous frame which can be used as motion compensated frame but

previously encoded, is decoded and its prediction errors, if any, are decoded and added to the decoded frame. B-frame in contrast, uses up to 2 frame for motion estimation purposes.

Lastly, entropy coding are applied to control data from RDO, results of the DCT & Quantization process, prediction data and motion vectors. Two entropy coding methods, namely CABAC (Context-Adaptive Binary Arithmetic Coding) and CAVLC (Context-Adaptive Variable Length Coding), are used in H.264 compression standard to encode quantized transform coefficients. CAVLC works by processing a macroblock in the form of run-level pairs. Diversely, entities are binarizes for further processing in CABAC. Best probability model and table are choosen for both of the entropy coding method based on the local context to encode syntax such as motion vector information, quantized transform coefficients, etc. Due to the ability of permits the adaptation to statistics of non-stationary symbol and assignment of a non-integer number of bits to each symbol of an alphabet which offered by CABAC, it has higher computational complexity as relative to CAVLC. However, CABAC always achieve higher compression gain. The output of entropy coder is a series of compressed video contents in binary stream which can be then either stored in various mediums or transmitted.

Steganography Scheme

Steganography is technique of embeds secret messages in a cover file. Conceptually, steganography scheme is scheme that used in embedding secret messages in a cover file depending on the type of cover file. In this section, we examine a total of 5 scheme, which include bit plane replacement, spread spectrum, histogram manipulation, mapping rule and divisibility.

A. Bit Plane Replacement

Bit plane replacement is scheme in which secret message are embed into a particular bit plane in the cover file, where the choice of bit plane are agreed upon both sender and receiver. This scheme are commonly used to data types such as audio sample, raw image pixels value, raw video pixels value and motion vector information, etc. These data types can be inserted one bit of value without having perceptual impact significantly. The benefit of this scheme is low distortion, high payload and relatively easy implementation.

Bit plane replacement is also known as LSB (least significant bit), which embed data by replacing the right most bit of the data, which has the lowest weightage in term of numerical value. As shown in Fig. 4, secret message “Hello” are embed into the container data by replacing the least significant bit of every container data with the bit sequence of the secret message. By replacing one least significant bit, the numerical value of the container data are affected by at most 1_2 (1_{10}). Subsequently, replacing last two significant bit will affect the numerical value by at most 11_2 (3_{10}). Receiver of the embedded data can then obtain the secret message by retrieving the least significant bit of every embedded data and reconstruct it back to original form.

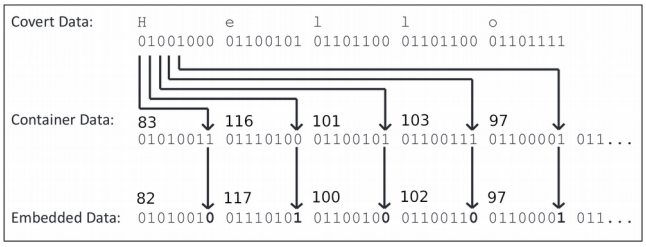

Fig. 4. LSB scheme in embedding word “Hello” into container data

B. Spread Spectrum

In spread spectrum scheme, secret message are embedded within a range of acceptable changes in which is not perceptible to human visual system.

This scheme are widely adopted for watermarking purposes. Example of watermarking technique based on spread spectrum can be found in Cox et al. [4]. The technique can be formulated as below:

$$v'_i = v_i + aw_i \qquad \text{— (1)}$$

$$v'_i = v_i(1 + aw_i) \qquad \text{— (2)}$$

$$v'_i = v_i(e^{aw_i}) \qquad \text{— (3)}$$

where $w_i \in \{0, 1\}$ is the secret message, v_i is the input value, v'_i is the output value, and a is the scaling parameter which decides to what extend w alters v_i. In equation (1), it shows that by adding information to the input data, it generate the output, which is invertible. In contrast, equation (2) and (3) are generated based on multiplication and exponential operations. Therefore, it is invertible only when $v_i \neq 0$.

By using this technique, the secret message is hidden and spread throughout the entire video content. Therefore, with only part of the video, it hardly able to reconstruct the secret message. However, it has higher computational complexity compare to bit plane replacement scheme because it needs to process the entire video.

C. Histogram Manipulation

A histogram of pixels in a compressed still image are shown in Fig. 5. In general, one particular pixels value are usually associated with another pixel value to hide secret message. Example of such technique can be found in Ni et al. which utilize the zero and peak of the pixel value in histogram [5]. First, it determine the peak point of histogram, which is '10' in Fig. 5. After determine peak point, for every $c \geq T$ (T being the peak point where c is the value), it increase by 1 in order to zero out the pixel value next to the peak. It then embed data with either '10' or '11', in which '10' indicating binary '1' and vice versa. It can also be in reverse order where the it should follow the same when retrieving secret message.

Both spatial domain and frequency domains can be applied with histogram manipulation sceheme. By using histogram manipulation, it can also able to achieve reversible data embedding. Here, reversible are meant by the ability of perfectly recover the original content after retrieving secret message. However, histogram manipulation often face with underflow or overflow problems. Histogram manipulation are also more expensive due to pre-processing required such as vacating a bin for data embedding.

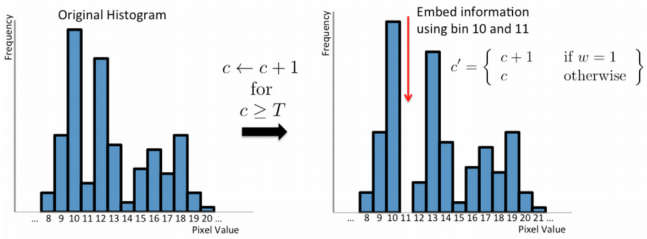

Fig. 5. Hiding secret message with histogram

D. Mapping Rules

Mapping rules is a steganography scheme where it map a certain entity in the cover file with a meaning. The mapping rule are required to agreed by both sender and receiver. Choice of the entity will be choosen depending on the secret message instead of the original decision. Fig. 8 is mapping rules technique implemented by Kapotas et al [6]. In this implementation, it map possible macroblock size with '00', '01', '10' and '11'. During encoding, it changes the original block size choices to the block-combination which generated from the secret message. Despite offering high payload, this method often face with severe bitstream size increase.

Commonly, this scheme provide high flexibility in applying to different component depending on

target file type. In H.264, it can be applied to block size, prediction type, etc.

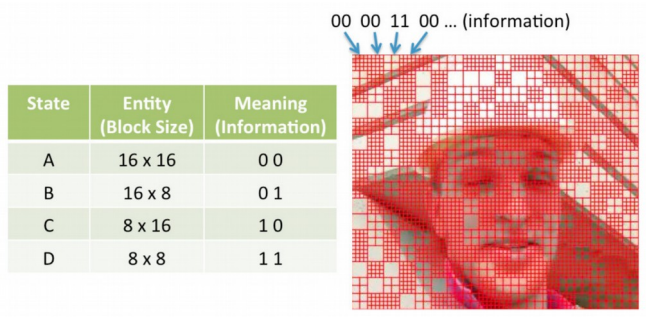

Fig. 6. Mapping rules using macroblock size to hide secret message

E. Divisibility

In this scheme, it utilize the property of cover data value, which is it's divisibility to embed secret message into it. An example can be found by Wong et al., which when '1' is to be embedded, it scale the magnitude of each coefficient in the macroblock by a prime number, or leave them as they are otherwise [7]. In this method, it need to check the divisibility of all number by the choosen prime number in order for it to works.

Originally, this method are invented for reversible steganography. With this scheme, perceptual quality of embedded video can be maintained. However, it require high computational complexity. It also often need a location map for decoding and reconstruction purposes.

Opportunity in H.264

We had examine H.264 encoding in the first section of literature review. We had also examine various steganography scheme in the second part of literature review. In this part, we shalt examine the opportunity to embed data in H.264 and suitable steganography scheme to be used.

As we had examine earlier, H.264 is a hybrid video encoding standard which made up of several major procedure. As shown in Fig. 7, it consist of prediction, transformation, quantization and entropy coding. Each of these major procedure produce entity which can be utilize to embed information. There had been numbers of steganography method proposed for H.264 encoding standard, and it will be review in each respective segment.

Most of these proposed method perform data embedding during the video encoding process. This is because data embedding that done prior to video encoding often lost information during video encoding process which lead to incomplete secret message reconstruction.

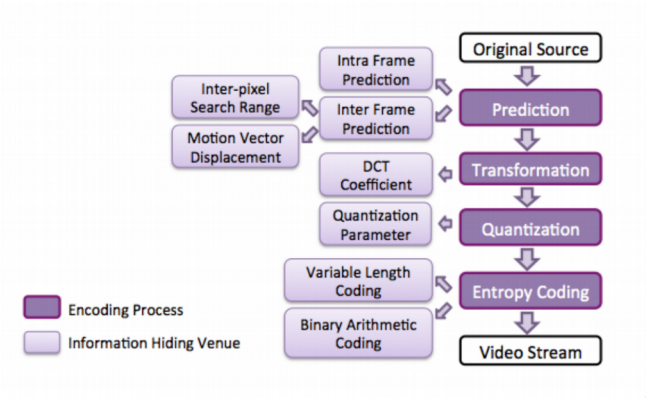

Fig. 7. H.264 encoding process and entities for information hiding

A. Prediction

During prediction process, there are a total of 4 entities which can utilize for data embeding, namely intra frame prediction, inter frame prediction, inter pixel search range and motion vector displacement.

1. Intra frame prediction

In a macroblock, one of the 14 prediction modes are used to encode the block if it is encoded with intra-mode. A total of 9 prediction mode available for 4 × 4 blocks and 4 prediction mode for 16 × 16 blocks as shown in Fig. 8 and Fig. 9 respectively. The remaining one mode is the skip mode.

Hu et al. propose an information hiding method with mapping rules in 4 × 4 blocks [8]. In the method, it seperate 9 prediction mode available for 4 × 4 blocks into 2 group. The former group indicating ‘0’ while the latter indicating ‘1’. The group are determined by measuring the probability of original mode to assigned mode. It then able to retrieve information by comparing assigned mode with original mode which can be obtain be re-encode the video after decoding. Similar method are also proposed by [9] which utilize logistic function in creating embedding sequence and [10] which utilize chaotic sequence.

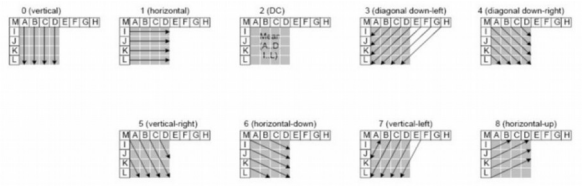

Fig. 8. 9 prediction mode available for 4 × 4 blocks

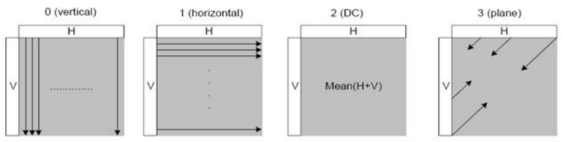

Fig. 9. 4 prediction mode available for 16 × 16 blocks

2. Inter-Frame prediction

In H.264, 7 type of block sizes are adopted, namely 4 × 4, 4 × 8, 8 × 4, 8 × 8, 8 × 16, 16 × 8, and 16 × 16. Motion estimation are to be applied to every block size and block size which result in smaller output bit size will be choosen. As discuss earlier in the mapping rules scheme segment, a method utilizing mapping rules which each block size are map to a meaning are proposed by Kapotas et al. [11]. In this method, every block size are map with 2 bits, which as shown in Fig. 6. 4 × 8 and 8 × 4 are being assigned with the same meaning, and the same goes to 16 × 8 and 8 × 16. During video encoding, it will force the encoder to choose block size which equivilent to the bit stream of the secret message. With this method, secret message can be retrieve with reading all the block size of the video and reconstruct the bitstream with using the bit representation that map to the block size.

3. Motion vector displacement

Motion compensation and motion estimation in inter-prediction will generate a total of 3 entity, namely phase angel, horizontal and vertical magnitudes. These entity are utilize by Jordan et al. for watermarking purpose [12]. It is done by adopting bit plane replacement scheme to change the phase angle, horizontal and vertical magnitudes to hide information. It is further improve by [13] and [14] by only embed information when it has low phase angel or high horizontal and vertical magnitude. With the improvement, visual degration are greatly improve compare to the former method.

4. Inter pixel search range

To achieve high compression efficiency, hierarchical based motion estimation are used in H.264 codec in order to support a range of block sizes and quarter pixel precision. Motion estimation is the process of finding a match of pixel blocks in inter frame coding. Motion estimation start with searching all macroblock in order to find the best macroblock in the integer pixel level, and subsequently continue with sub pixel level and quarter pixel level.

Zhu et al. propose a method utilizing inter pixel process to hide secret message with using mapping rule scheme [15]. As indicate in Fig. 10, pixel point are seperate into 2 group, one group indicating ‘0’ and the rest indicating ‘1’. Pixel point are choosen depending on the sequence of bitstream from the secret message. The pixel point will be reflected in motion

vector and the secret message can be reconstruct later by reading the motion vector.

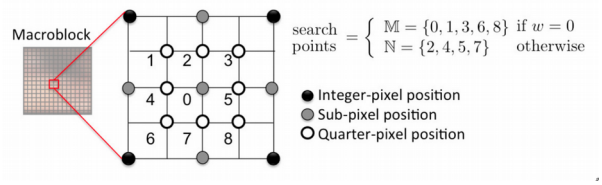

Fig. 10. information hiding with quarter pixel search point

B. Transform process

Luminance based DCT coefficient are often being utilize for hiding information in steganography. It can be utilize to hide information by using bit plane replacement. In [16], the researcher propose method which utilize I-frame in H.264 for data hiding. It hide information into quantized luminance DCT coefficients of I-frame. In their method, they eliminate I-frame distortion drift, low visual distortion and high payload by pairing coefficient for data embedding and distortion adjustment based on the analysis of the relation between the DCT coefficients and the distortion incurred in pixel values.

In [17], Meuel et al. had introduced technique to hide information in edge pixels represented in quantized DCT coefficients by using edge detection and multi-directional interpolation algorithm. Spread spectrum scheme are utilize in this technique and it take error concealment application at the decoder into consideration when designing the method.

C. Quantization Process

Various steganography method are develop for H.264 quantization process. The first method is porposed by Wong et al., which utilize macroblock's quantization scale for information hiding [18]. Matrix encoding scheme are used in this method to embeded information. This method claim to be able to maintain video bitstrean size with low embedding complexity. Additional, another method claim to maintain exact video quality to the original video after data embedding are proposed by Wont et al. by utilizing divisibility [7]. In this method, no change are applied to the macroblock if the bit to be embed is '0'. Otherwise, each quantization scale and non-zero DCT will be respectively divide and multiply by specific prime number in the macroblock.

Another method proposed by Su et al. which hide secret message in non-zero DCT coefficients in which that represent prediction residuals [19]. To determine amount of information that can be embed into each coefficient, this method uses quantization step that is based on Just Noticeable Difference (JND) to manipulates DCT coefficients.

D. Entropy Coding

In H.264, there are two type of entropy coding method, namely CAVLC and CABAC. There are various steganography and watermarking method developed to utilize these two entropy coding for hiding information.

To compactly represent strings of zeros in CAVLC, run-level coding mark the last three ±1 coefficients by refer to trailing ones (T1s) table. In [20], T1s table are utilized to carry information by mapping rules as follow:

$$\widetilde{T1s} = \begin{cases} 2, & \text{if } w = 0 \text{ and } T1s \geq 3, \\ 1, & \text{if } w = 1 \text{ and } T1s = 2 \text{ or} \\ & \text{if } w = 1 \text{ and } T1s = 0, \\ 0, & \text{if } w = 0 \text{ and } T1s = 1, \\ \text{unchanged}, & \text{otherwise} \end{cases}$$

$\widetilde{T1s}$ is the manipulated codeword of T1s and w is the bit to be embed. In this method, perceptual video quality degration after data embedding cannot be avoided. However, this method has low complexity and it result in narrow range of bit length variant. Therefore, it can be used in real time streaming. Similar method

introduced by Kim et al. where it manipulate sign and number of non-zero DCT coefficients in a I4MB block[21].

CABAC entropy encoding generate significant coefficient (*sig_vtx*) during context mapping. A method propsoed by Seo et al., hide information in *sig_vtx* using bit plane replacement [22]. It replace the least significant bit of the *sig_ctx* (absoulte value) with the bit to be embed. Another method proposed by Wang et al. also uses bit plane replacement, but embed data in syntax elements which generated during binarization process of CABAC [23]. This method are created mainly for watermarking purposes.

Other opportunity in video

A total of 2 component are made up of a video namely visual component and sound component. In previous section, we had examine visual component of a video, which is moving image, specifically with H.264 encoding standard and it's opportunity for embedding secret message. In this section, we will examine steganography technique to embed data into uncompressed PCM (Pulse-code modulation) audio format, such as WAV.

WAV is a audio file format, with file extension of *.wav* or *.wave*. WAV store directly the waveform of the digital audio file. Generally, there are 2 parameter for PCM audio, namely sampling rates and sampling bit depth. Sampling rate are frequency of the computer collect audio sample. Common sampling rate are 44.1 kHz, which is the sampling rate of audio CDs standard. Another common sampling rate is 48 kHz which used in DVDs. Sampling bit depth is the number of bit used to represent sample collected. The higher the bit depth, the more accurate it get. Common sampling bit depth for audio are 16-bit for normal audio and 24-bit for extreme quality audio.

1. Bit Plane Replacement

Most common steganography method for audio file is bit plane replacement. This is done by converting cover file into bit stream, and replace the least significant bit of audio to the bit stream of cover file. This technique does not cause significant quality degration given the higher the bit depth of the audio sampling, such as 24-bit audio sample.

2. Parity Coding

The second steganography method is parity coding [24]. Instead of embed data in every individual audio sample, it group audio sample into a group. If the parity bit for the region is '1' and the data to embed is '0', it will flip all the lsb of the particular region. However, if the parity bit match the bit to embed, it does nothing. This steganography method is based on bit plane replacement.

3. Phase Coding

Phase coding is the third steganography method to be examine here. In this method, an audio file are seperated into smaller segment, where the size of segments are to be the same with the size of message to be embedded. Then, DFT (Discrete Fourier Transform) are used in order to create matrox of the phase. After phase differences between neighbouring segment are calculated, the secret information will be embedded at the initial segment with following formula:

$$\widetilde{phase} = \begin{cases} \pi/2 & if\ message\ bit = 0 \\ -\pi/2 & if\ message\ bit = 1 \end{cases}$$

Lastly, inverse DFT are used with the new phase matrix generated from first segment and magnitude matrix to reconstruct the sound signal and concatenating the sound segment back together. Relative phase difference between neighbouring are to be preserve. In this method, noticeable scattering of phase happen if there is huge modification in the phase relation between

each frequency component [24]. However, imperceptible coding can be achieve by having sufficiently small change in phase relation [25] [26].

4. Spread Spectrum

Spread spectrum is spreading secret message across the whole file. Spread spectrum had been examine in the second part of literature review. Different from earlier part, the technique are only to be applied to frequency spectrum of audio signal [24]. However, spread spectrum are susceptible to introduce noise into the audio file.

5. Echo Hiding

Echo is the reflection of sound that arrive to the listener at a delay time. Echo hiding method are done by introducing echo into an audio file. There are 4 total parameter introduced, which is initial amplitude, delay rate, ‘0’ offset and ‘1’ offset. Secret message are later to be hidden in every echo generated [27]. The secret message can be hidden as shown in Fig. 11.

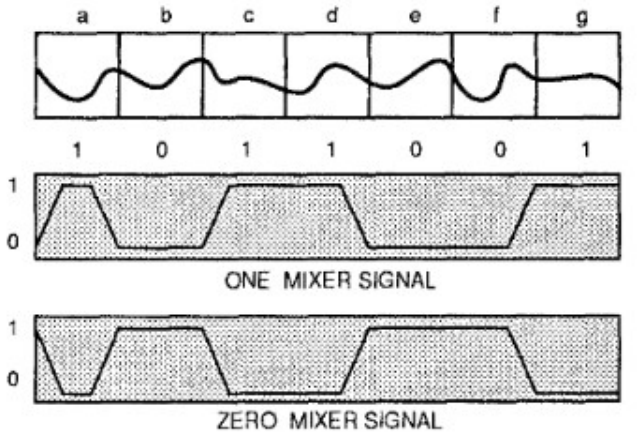

Fig. 11. Echo parameter and data embedded

Technical Plan

In this section, technical detail of proposed steganography will be discuss here. We had examine various element within H.264 codec standard, steganography scheme and method. There will be a total of 4 part. First part is embedding secret message into cover file and the second part is retrieving secret message. The third part will include proposed method in testing validity of proposed steganography method. The last part will be the tools used in this project.

1. Secret Message Embedding

In secret message embedding, 3 input are required. The first input is the secret message. Secret message can be any file type, from text to binary file. This is because the program will read secret message as byte stream so it can hide any file type instead of specific file type (eg. text, image). The second input is the cover video. There are requirement for cover video, namely moving image being encoded with H.264 and audio being either uncompressed or encoded with loseless compression. The last input is password for steganography. This password will be used to determine pseudorandom sequence and act as a key for encryption. The password that used to embedding information are required for retrieving secret message.

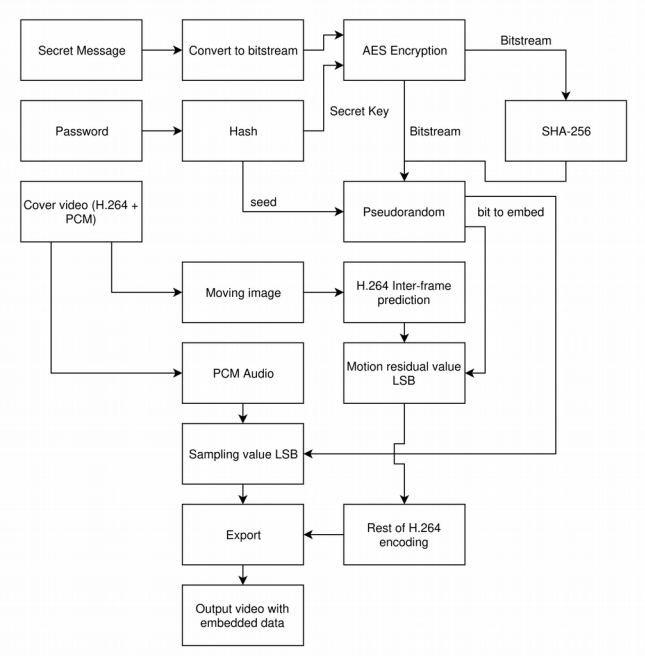

Fig. 12. Proposed steganography message hiding block diagram

After getting the input, the algorithm will first hash the password to get a certain number of bits for AES encryption key. It will then encrypt the secret message bitstream and the output is encrypted secret message. Encrypted secret message will be applied with SHA-256 hash for integrity checking during retrieval. A pseudorandom will be used, and it will first be seeded with a number that get from output of hash password. After that, algorithm will run through H.264 inter-frame prediction to know the number of block being divided. Being known the number of blocks and audio sample, algorithm will used pseudorandom and modular function to determine the venue for the bit to embed. The algorithm will then encode the video and replace respective lsb of moving residual prediction value and lsb for audio signal. The output will be video file embedded with secret message The embedding process can be shown in Fig. 12.

The bitstream for embedding will be embed in following manner as shown in Fig. 13. The first block being the size in bit for the file name, and will be represented with 16 bit unsigned integer. The second block being the size in bit for payload, and is represented with 64 bit unsigned long. The third block is hash encrypted payload for integrity checking purpose. It follow by the file name and payload with respective size from previous 2 block. This enable easy message retrieving for the file name, extension and size without the need of user input.

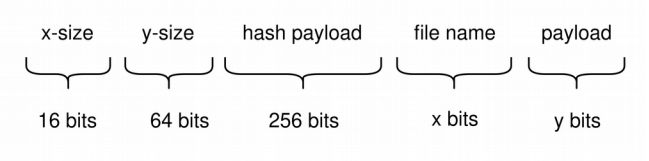

Fig. 13. Structure of bitstream being embedded

2. Secret Message Retrieval

For message retrieval, there are a total of 2 input. The first input is password. The password are used to get secret key for decryption and pseudorandom sequence. The password need to match the data embedding password in order to retrieve embedded data that scattered around the video with correct sequence and decrypt embedded data. The second input is video with embedded data.

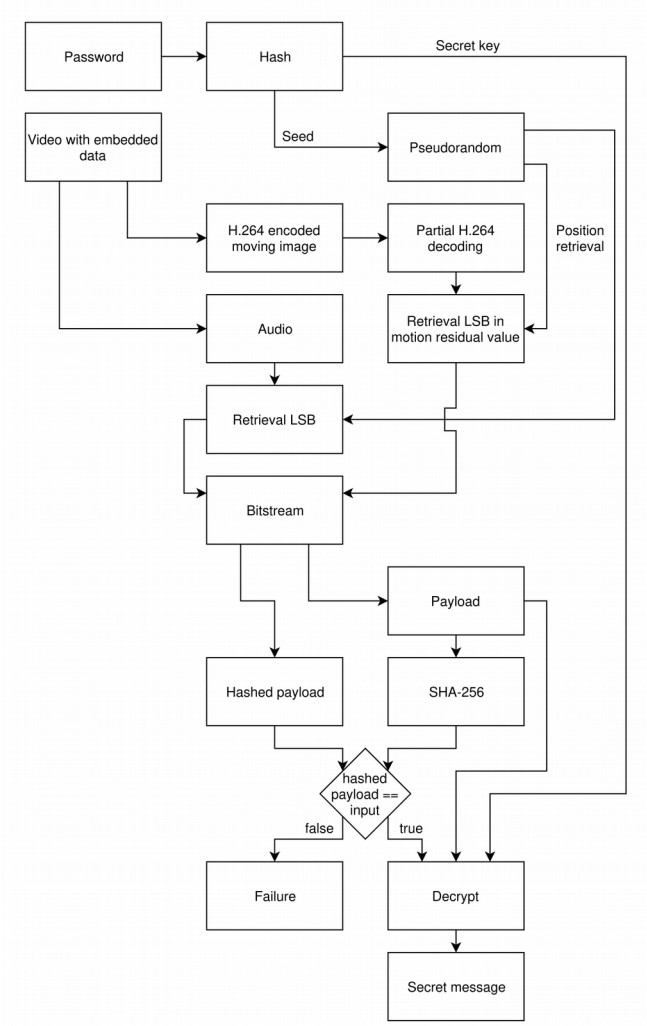

Fig. 14. Proposed steganography message retrieval block diagram

After getting the input, the algorithm first seperate H.264 encoded moving image and audio. After that, it will partially decode the encoded H.264 moving image and retrieve LSB of motion residual value and keeping their position for later use. The password will be hash and act as seed for pseudorandom sequence. The algorithm will then follow the pseudorandom sequence to reconstruct

the bitstream embedded into the video. The first 16 bits of bitstream will determine the size of file name in bit and following 64 bits will determine size of encrypted payload. It will follow by retrieving hash encrypted payload with the size of 256 bits. After that, it will reconstruct the remaining of number of bits specify by the first 80 bits. After finish reconstruct, encrypted payload will hash with SHA-256 and compare the output with hash encrypted payload obtain from the 3rd block. If both of them matcg, encrypted payload will be decrypt by using the secret key generated from hash password. The last step is to write the decrypted payload into a file with the file name specify at the 3rd block of embedded bitstream. However, if hash encrypted payload and hash of last block of bitstream does not match, it indicate either no data being embedded or error retrieving data.

3. Steganography validiation

Validation of proposed steganography method will be concerned with 3 category, namely integrity of proposed steganography algorithm, perceptual detectability and statistical detectability.

For validation of integrity of proposed steganography, test will be run throughout different type of secret message. Secret message shall include text, image, uncompressed pcm audio, unexecutable binary and executable binary. Different type of file will be tested to ensure correctness of steganography method, which able to extract original file after embedding without error.

For perceptual detectability, samples of particular frame in original video and embedded video will be choosen and compare side by side. Further, we will also use visualization method to visualize differences between two frame. Differences can be absolute differences or relative differences. Histogram will also be used to examine different between pixel value spread of original frame and embedded frame.

For statistical detectability, lsb of audio or frame moving residual value will be extract and reconstruct in emulating environment where password are not known. Different secret message file will be used and test to ensure detectability is low and reconstruction of extracted bitstream shall be random bitstream.

4. Tools

Tools that involved in this project are rather straight forward. This is because it only involve specific media type. As the program will be command line, no GUI framework will be used. Libraries that will be used for manipulating audio, video and H.264 codec are ffmpeg and x264. For encryption and hash algorithm, Crypto++ library will be used. Random library will be used for pseudorandom usage.

Work Plan

Activities / Tasks	Week																											
	Capstone Project 1														Capstone Project 2													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Plan template and SAF																												
Literature Review																												
Draft of methodology																												
Finalize methodology																												
Draft of planning documents																												
Finalize planning documents																												
Documentation study																												
Steganography implementation																												
Steganography testing																												
steganography validation																												
Thesis Writing																												
Viva presentation																												

The current milestone had been achieve up until finalize planning documents. Plan template and SAF had been submitted in the 2nd week of Capstone Project 1. In this planning document, it consist of literature review, methodology and planning document. The activities documentation study is studying documentation of libraries that will involved in this project. No result will be generated in this activities and the dedicated time for documentation study are required due to long documentation of x264 libraries. Steganography implementation activities are consist of implementing proof of concept of proposed steganography method. This algorithm will be tested with integrity testing before moving on to steganography validation, which required steganography algorithm passing integrity test. Thesis writing comes after validation of steganography method and propsoed steganography method and result will be recorded in the thesis.

References

[1] Grivalsky, D. (2016). Encoding.com Publishes its 2016 Global Media Format Report. Encoding.com. [online] Available at: https://www.encoding.com/blog/2016/01/27/encoding-com-publishes-its-2016-global-media-format-report/ .

[2] I. Richardson (2007). White paper: an overview of H.264 advanced video coding [Online]. Available: http://www.vcodex.com/files/H.264overview_Jan11.pdf

[3] Tew, Y. and Wong, K. (2014). An Overview of Information Hiding in H.264/AVC Compressed Video. *IEEE Transactions on Circuits and Systems for Video Technology*, 24(2), pp.305-319.

[4] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[5] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354-362, Mar. 2006.

[6] S. Kapotas, E. Varsaki, and A. Skodras, "Data hiding in H.264 encoded video sequences," in *IEEE 9th Workshop on Multimedia Signal Process.*, pp. 373-376, Oct. 2007.

[7] K. S. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete video quality - preserving data hiding," *IEEE Trans. Circuits Syst. Video Technol*., vol. 19, no. 10, pp. 1499–1512, Oct. 2009.

[8] Hu, Y., Zhang, C. and Su, Y. (2007). Information Hiding Based on Intra Prediction Modes for H.264/AVC. *Multimedia and Expo, 2007 IEEE International Conference on*.

[9] Zhu, H., Wang, R., Xu, D. and Zhou, X. (2010). Information hiding algorithm for H.264 based on the predition difference of intra_4×4. *2010 3rd International Congress on Image and Signal Processing*.

[10] D. Xu, R. Wang, and J. Wang, "Prediction mode modulated data-hiding algorithm for H.264/AVC," *J. of Real-Time Image Process.*, pp. 1–10, Aug. 2010.

[11] S. Kapotas and A. Skodras, "A new data hiding scheme for scene change detection in H.264 encoded video sequences," in *IEEE Int. Conference on Multimedia and Expo*, pp. 277–280, Apr. 2008.

[12] F. Jordan, M. Kutter, and T. Ebrahimi, "Proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video," in *ISO/IEC JTC1/SC29/WG11 Coding of Moving Pictures and Audio,* 1997.

[13] J. Zhang, J. Li, and L. Zhang, "Video watermark technique in motion vector," in *Proc. of XIV Brazilian Symp. on Comput. Graph. and Image Process.*, pp. 179–182, Oct. 2001.

[14] Y. Dai, L. Zhang, and Y. Yang, "A new method of MPEG video watermarking technology," in *Int. Conference on Commun. Technol*., vol. 2, pp. 1845–1847, Apr. 2003.

[15] Zhu, H., Wang, R. and Xu, D. (2010). Information hiding algorithm for H.264 based on the motion estimation of quarter-pixel. *2010 2nd International Conference on Future Computer and Communication*.

[16] X. Ma, Z. Li, H. Tu, and B. Zhang, “A data hiding algorithm for H.264/AVC video streams without intra-frame distortion drift,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 20, no. 10, pp. 1320–1330, Oct. 2010.

[17] P. Meuel, M. Chaumont, and W. Puech, “Data hiding in H.264 video for lossless reconstruction of region of interest,” in *EUSIPCO 07: 15th European Signal Process. Conference*. Poznan, Poland: EURASIP, pp. 2301–2305, Sep. 2007.[18] K. Wong and K. Tanaka, “A data hiding method using Mquant in MPEG domain,” *IIEEJ Proc. of Image Electron. and Visual Computing Workshop*, 2007.

[19] Andrew B. Watson, "DCT quantization matrices visually optimized for individual images," *Human Vision, Visual Processing, and Digital Display IV*, Bernice E. Rogowitz, Editor, Proc. SPIE 1913-14, 1993.

[20] K. Liao, S. Lian, Z. Guo, and J. Wang, “Efficient information hiding in H.264/AVC video coding,” *Telecomm. Syst*., vol. 49, no. 2, pp. 261–269, Jun. 2010.

[21] S. Kim, S. Kim, Y. Hong, and C. Won, “Data hiding on H.264/AVC compressed video,” in *Image Analysis and Recognition*, ser. Lecture Notes in Comput. Science, M. Kamel and A. Campilho, Eds. Springer Berlin Heidelberg, 2007, vol. 4633, pp. 698–707.

[22] Y.-H. Seo, H.-J. Choi, C.-Y. Lee, and D.-W. Kim, “Low-complexity watermarking based on entropy coding in H.264/AVC,” *IEICE Trans. on Fundamentals of Electron., Commun. And Comput. Sci*., vol. E91-A, no. 8, pp. 2130–2137, Aug. 2008.

[23] R. Wang, L. Hu, and D. Wu, “A watermarking algorithm based on the CABAC entropy coding for H.264/AVC,” *J. of Computational Inform. System*, vol. 7(6), pp. 2132–2141, Jun. 2011.

[24] Jayaram, P., Ranganatha, H. R. and Anupama, H. S. 2011. Information Hiding Using Audio Steganography – A Survey. International Journal of Multimedia and Its Application, 3(3), pp. 86-96.

[25] Nedeljko Cvejic, Tapio Seppben “Increasing the capacity of LSB-based audio steganography ” *FIN-90014 University of Oulu*, Finland ,2002.

[26] Yin-cheng qi, liang ye, chong liu “Wavelet domain audio steganalysis for multiplicative embedding model” *Proceedings of the 2009 International Conference on Wavelet Analysis and Pattern Recognition*, Baoding, 12-15 July 2009.

[27] Gruhl, D., Lu, A. and Bender, W. (1996). Echo hiding. *Information Hiding*, pp.295-315.