HIGH CAPACITY IMAGE STEGANOGRAPHY TOLERATING IMAGE COMPRESSION

Mr. Eittipat Kraichingrith

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science and Information Technology

Department of Mathematics and Computer Science

Faculty of Science

Chulalongkorn University

Academic Year 2017

วิทยาการอำพรางข้อมูลทางภาพความจุสูงที่ทนต่อการบีบอัดภาพ

นายอิทธิพัทธ์ ไกรชิงฤทธิ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2560

Thesis Title	HIGH CAPACITY IMAGE STEGANOGRAPHY TOLERATING IMAGE COMPRESSION
By	Mr. Eittipat Kraichingrith
Field of Study	Computer Science and Information Technology
Thesis Advisor	Assistant Professor Dr. Suphakant Phimoltares, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

.....Dean of the Faculty of Science

(Professor Polkit Sangvanich, Ph.D.)

THESIS COMMITTEE

.....Chairman

(Professor Chidchanok Lursinsap, Ph.D.)

.....Thesis Advisor

(Assistant Professor Dr. Suphakant Phimoltares, Ph.D.)

.....External Examiner

(Praisan Padungweang, Ph.D.)

อิทธิพัทธ์ ไกรชิงฤทธิ์ : วิทยาการอำพรางข้อมูลทางภาพความจุสูงที่ทนต่อการบีบอัดภาพ (HIGH CAPACITY IMAGE STEGANOGRAPHY TOLERATING IMAGE COMPRESSION) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. ดร. ศุภกานต์ พิมลธเรศ, 49 หน้า.

ในปัจจุบันความเป็นส่วนตัวของข้อมูลมีความสำคัญมากขึ้น วิธีการปกป้องข้อมูลที่มีอยู่ส่วนใหญ่บนพื้นฐานของวิทยาการรหัสลับ ไม่สามารถปกปิดการมีตัวตนอยู่ของข้อมูลลับได้ ดังนั้น วิธีการทางวิทยาการอำพรางข้อมูลมีบทบาทสำคัญในการจัดการปัญหานี้ วิทยาการอำพรางข้อมูลด้วยภาพจำแนกได้สองวิธีการบนพื้นฐานของโดเมนเชิงพื้นที่และโดเมนการแปลง วิธีการซึ่งใช้โดเมนเชิงพื้นที่มีความจุการฝังข้อมูลสูงแต่ไม่ทนทานต่อการบีบอัดภาพ ในทางตรงกันข้ามวิธีการซึ่งใช้โดเมนการแปลงโดยปกติทำงานกับการบีบอัดภาพได้แต่มีความจุการฝังข้อมูลต่ำ ในงานวิจัยวิทยาการอำพรางข้อมูลด้วยภาพเมื่อไม่นานมานี้ วิธีการซึ่งใช้โดเมนการแปลงมีพื้นฐานอยู่บนรูปแบบเจเพ็กซึ่งค่อนข้างเก่าและประสิทธิภาพการบีบอัดข้อมูลอาจจะไม่เหมาะสมในยุคคลาวด์ ในปี ค.ศ. 2010 กูเกิลได้นำเสนอเว็บพีซึ่งเป็นรูปแบบภาพใหม่ที่มีการบีบอัดคงสัญญาณหลักดีกว่ารูปแบบเจเพ็ก ในการศึกษานี้วิทยาการอำพรางข้อมูลด้วยภาพใหม่บนพื้นฐานของเว็บพีได้ถูกนำเสนอ วิธีการคำนวณใหม่และบิตที่มีความสำคัญน้อยที่สุดบนความถี่ช่วงกลางได้ถูกใช้ วิธีการที่นำเสนอให้คุณภาพของภาพดีกว่าและขนาดไฟล์ที่เล็กกว่าวิธีการบนพื้นฐานของเจเพ็กที่มีอยู่แล้วที่ความจุเดียวกัน ยิ่งไปกว่านั้นนอกจากการใช้กับภาพสเกลสีเทาแล้วการใช้กับภาพสีและภาพสีช่องแอลฟาก็ถูกนำเสนอในงานวิจัยนี้เช่นกัน

ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์	ลายมือชื่อนิสิต .....
		ลายมือชื่อ อ.ที่ปรึกษาหลัก .....
สาขาวิชา	วิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ	
ปีการศึกษา	2560	

5872631023 : MAJOR COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
KEYWORDS: IMAGE STEGANOGRAPHY / WEBP / DISCRETE COSINE TRANSFORM / DATA HIDING

EITTIPAT KRAICHINGRITH: HIGH CAPACITY IMAGE STEGANOGRAPHY TOLERATING IMAGE COMPRESSION. ADVISOR: ASST. PROF. SUPHAKANT PHIMOLTARES, Ph.D., 49 pp.

Nowadays, data privacy becomes more important. Most of the existing data protection schemes based on cryptography cannot hide the existence of secret data. Thus, a steganography approach plays an important role to handle this problem. Image steganography can be categorized into two methods which are baesd on spatial domain and transform domain. Methods using spatial domain have high embedding capacity but they are not robust to image compression. On the other hand, methods using transform domain usually work with image compression but have low embedding capacity. In recent image steganography research, many transform domain methods are based on JPEG format which is quite old and its compression efficiency may not be suitable in cloud era. In 2010, Google introduced WebP, a new image format that has better lossy compression than JPEG. In this study, the new image steganography based on WebP is presented. Re-calculation and LSB on middle-frequency method are used. The proposed scheme provides better image quality and smaller file size than the existing JPEG based method at the same capacity. Moreover, not only applying to a grayscale image but also a color image and an alpha channel color image is introduced in this research.

Department:	Mathematics and Computer Science	Student's Signature .....
		Advisor's Signature .....
Field of Study:	Computer Science and Information Technology	
Academic Year:	2017	

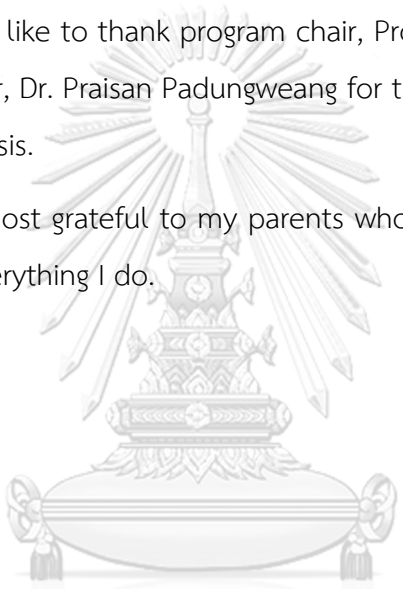
ACKNOWLEDGEMENTS

I would like to thank all of those who made it possible for me to complete this thesis.

First, I am very much obliged and grateful my research advisor, Assistant Professor Dr. Suphakant Phimoltares for suggesting and helping me understand the process of research and checking and correcting the thesis.

Also, I would like to thank program chair, Professor Chidchanok Lursinsap and external examiner, Dr. Praisan Padungweang for their valuable suggestions and comments for my thesis.

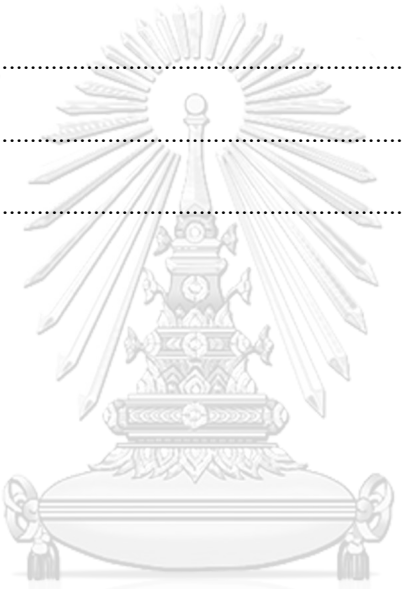
Finally, I'm most grateful to my parents who have always supported and encouraged me in everything I do.



CONTENTS

Page

Page



Content of Tables

Content of Figures

Chapter 1. Introduction

Nowadays, digital data is widely used for computation and communication. Using digital representation results in many benefits such as accuracy, portability or efficiency but not much advantage on security. To ensure data security, data hiding techniques are recommended. In data hiding, there are two methodologies which are widely used. The first methodology is called cryptography which transforms secret data into a non-understandable form. The other methodology is steganography which conceals the presence of secret data. The main advantage of steganography over cryptography is that it does not show any sign of secret data existence.

Hiding secret data inside a media can be confused with digital watermarking. Digital watermarking and steganography are different in terms of their purpose. Steganography is used for secret communication which needs to be invisible while digital watermarking is used to declare its ownership. Digital watermarking can be visible or invisible depending on the need of application. In case of invisible watermarking, steganography techniques can be adapted to create invisible digital watermarking.

The image steganography plays important roles in privacy protection. Many techniques have been invented to enhance information security. The major criteria for choosing techniques are quality of host image after embedding and quantity of secret data that are able to be embedded into the host image. The image quality metric is measured by peak signal-to-noise ratio (PSNR) or structural similarity index (SSIM) whilst the amount of embedded secret data is usually measured by bits per pixel (BPP). By using these metrics, any steganography research can be compared.

In recent research approaches, Bhowmik, Islam, and Yang proposed new steganography methods based on least significant bit (LSB) technique on the spatial domain [1-3]. Their experimental results showed high embed data quantity with acceptable image quality. Unfortunately, none of them mentions about robustness to transformation or attacking. For the transform domain, new discrete cosine transform (DCT) based methods were introduced. Lin proposed the integer-to-integer based DCT to solve transformation rounding problem which achieves high image quality [4].

However, as same as the above methods, the robustness performance was not mentioned. On the other hand, Zhang and Huang proposed new robustness algorithms that can be used with JPEG image compression [5, 6]. Nevertheless, the low embedded payload is still the drawback of their methods.

Inventing a new steganography method based on JPEG that can provide a good payload capacity seems to be a good idea to overcome above problems. However, the current trend of the world is changed and everything is shifting into a cloud. Many data including images are highly sent over the internet. This means, the size of host image now plays important roles when applying steganography in the real-world scenario.

JPEG compression is very old and it seems to be not good enough for cloud-era. In 2010, Google introduced the new image format called WebP. WebP claims that it produces 25-34% smaller file size compared to JPEG at the same image quality [7]. Moreover, WebP supports alpha-channel image and lossless image compression which cannot be done in JPEG. Not only feature advantage, but WebP is now currently used by high traffic websites according to statistical information from W3CTech [8].

Considering WebP image as host image is a good idea because it is suitable for cloud-era and support many compression features such as alpha-channel and lossless compression. Moreover, it is very challenging because at the time this thesis is written, there is no steganography technique based on WebP image. By above reasons, this thesis aims to introduce a new steganography algorithm that can achieve acceptable image quality and payload quantity based on Lossy WebP image.

1.1. Objective

To propose an image steganography method providing high performance in metrics and compatible with WebP lossy compression.

1.2. Scope of thesis and constraints

The proposed method is limited as follows.

1. The proposed method is based on WebP lossy compression.
2. The proposed method is based on a grayscale image with non-alpha channel. However, this method can be extended to support color image with alpha channel.
3. Performance metrics concerned in this thesis are PSNR, SSIM, Capacity, FileSize, and IncreasedFileSize.

1.3. Expected outcome

This research aims to propose an image steganography method that works with WebP lossy compression and achieves higher performance in metrics compared to existing JPEG method.

Chapter 2. Theoretical backgrounds

2.1. Lossy WebP compression algorithm

Lossy WebP compression is an image compression algorithm based on block prediction method. The important concepts are introduced first and then the overview of the compression method is presented.

Block concept - As mentioned, Lossy WebP is based on block prediction. There are two important types related to this scheme which are “Macroblock” and “Subblock”. The macroblock is sub-image with size of 16x16 pixels obtained from an input image while the subblock is sub-image with size of 4x4 pixels partitioned from a macroblock. Thus, a macroblock consists of 16 subblocks. Figure 1 shows the block concept of this scheme.

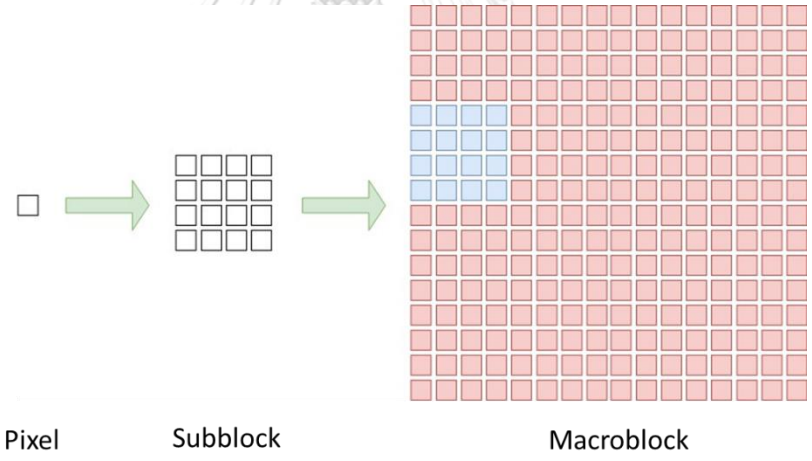


Figure 1. Block concept

Prediction concept - Lossy WebP takes advantage of a similarity between neighbor blocks. The algorithm tries to predict a block information from their neighbors to reduce some redundant information based on several prediction models. The neighbor blocks can be a left-block, a top-block, both or other blocks depending on a prediction model. After all prediction models are applied, the prediction model with most similar result will be assigned to the block. Figure 2 shows the prediction concept

of this scheme. The predicted subblock is generated from an averaging prediction model with data from its left neighbor subblock and its top neighbor subblock.

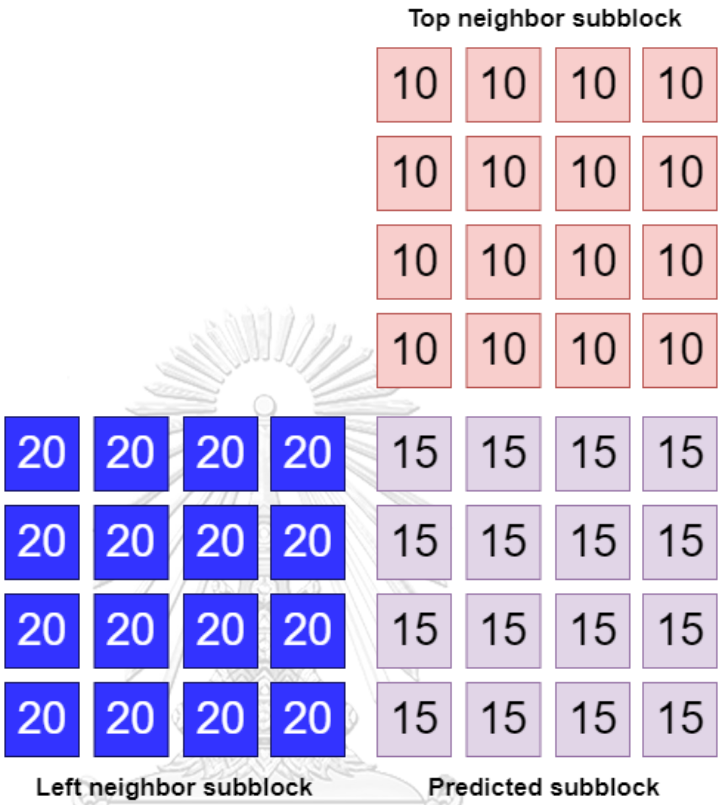


Figure 2. Prediction concept

Overview of the algorithm - The compression algorithm can be group into three major processes which are prediction, quantization, and encoding. First, an input image is divided into smaller pieces to form a macroblock structure. Then, each macroblock is sent to prediction process to find the best prediction model of their 16 subblocks. In prediction process, current block image will be constructed by several prediction models. The results of the predicted image can be viewed as redundant image data as shown in Figure 2. The most similar predicted image will be subtracted from original block image results in “residual” data. The residual is then sent to quantization process for data compression. The quantization process is very similar to JPEG compression, DCT is applied to those residual data and then all coefficients are quantized to make lossy compression. At this point, the compressed block will be restored and sent back

to the prediction process if another macroblock requires current block as a neighbor for its prediction model. After quantization process, all quantized coefficient will be arranged in ZigZag order and encoded by entropy encoding method.

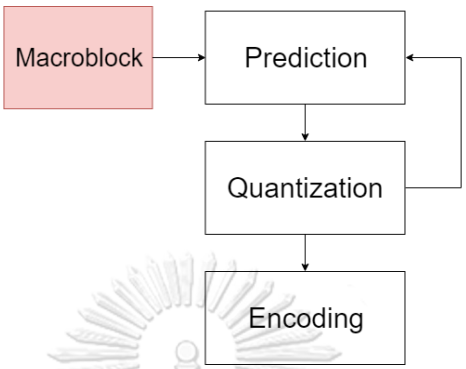


Figure 3. Lossy WebP flowchart

2.2. Data hiding process discussion

This section shows the discussion on where data hiding process should be placed on lossy WebP compression process. Considering JPEG based steganography schemes [5, 6], all schemes are manipulated the quantized DCT coefficients to make a room for hiding data. Because WebP and JPEG are very similar scheme, applying the same JPEG approach on WebP seem to be a reasonable idea. Thus, a test experiment was set up to check whether the idea is good.

The test data hiding experiment on WebP was set up by adding data hiding process after quantization process. The flowchart of modified WebP algorithm for this experiment is shown in Figure 4. The LSB of quantized coefficients was changed to hide secret data. Lena image was used in this test and secret data were randomly generated.

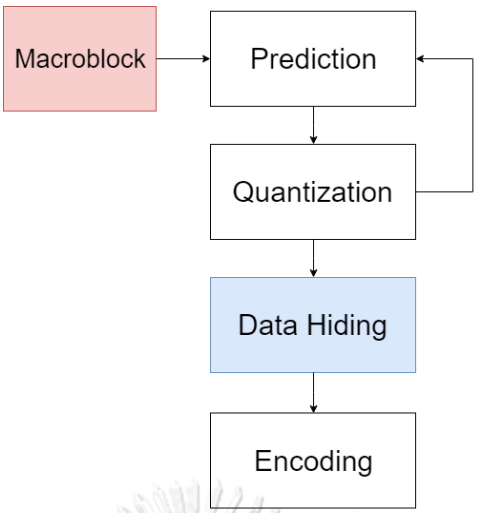


Figure 4. Modified Lossy WebP flowchart

Surprisingly, the experimental result was not good as expected. PSNR is approximately 10.93 dB and SSIM is approximately 0.44. Figure 5 shows a comparison between original WebP image and embedded WebP image. The host image's quality was really low compared to original lossy WebP image. An investigation is needed to figure out what causes the dramatic distortion on the image quality.

(a) (b)

Figure 5. Experimental result (a) Original WebP (b) Embedded WebP

According to WebP process, the quantized coefficients are restored to an image and taken by prediction process to predict a model for next block. This means block's

coefficients are related to some previous block's coefficients. To decode image, WebP blocks must be decoded in order, from left to right and top to bottom. When block's coefficients are changed by data hiding process, the decoder will produce a distorted sub-image. The distorted sub-image is then used for decoding the next block. The composition of the distorted sub-image causes the dramatic drop in image quality as the result.

To solve this problem, one way is to move the data hiding process into the quantization process. Considering the source code of WebP encoder/decoder provided by Google [9], modifying the quantization or prediction process is very complicated. Moreover, changing those process should be done carefully because it can affect image quality or decoding process. Thus, this solution is not practical and can cause more problems than solving the existing one. However, another solution to address this problem has been found and will be introduced in Chapter 4.

Chapter 3. Related Works

Since the steganography emerged, many kinds of techniques have been developed to enhance information security. Although these techniques are widely used in many media types such as text, audio, image or video, in this study, only image steganography techniques are focused and considered. The image steganography can be split into two major categories based on domain used in the process. The first category corresponds to the spatial domain while the transform domain is employed in the second category.

For the spatial domain, data hiding based on the spatial domain usually directly embeds secret data into pixel values. The main advantage of the spatial domain is the preservation of image quality.

A new data hiding technique using edge areas of images was proposed by Yang, C.H., et al. [3]. The researcher exploited the benefits from the fact that edge areas can tolerate more changes than the flat areas [3]. Edge areas are calculated by pixel value differencing and divided into three different levels which are low level, middle level, and high level. The k-bit LSB substitution is used to embed secret data which k depends on its pixel-differencing level. Even though the result ended up with the high capacity (BPP ≈ 2.25) and high image quality (PSNR ≈ 43.66), the main drawback of this work is that it uses LSB bits to embed secret data, which is quite sensitive to noise and image compression. So this algorithm is not practically used in real-world applications.

Islam, A.U., et al. proposed a new technique to embed secret data on the most significant bit (MSB) of an image [2]. Their method used bit-differencing of MSB No. 5 and MSB No.6 to hide secret data. Zero-bit is supposed to be embedded if the difference between MSB No.5 and No.6 is 0. However, One-bit is supposed to be embedded if the difference between MSB No.5 and No.6 is 1. From their experiment, this method can achieve high image quality (PSNR ≈ 51.18 dB) but average capacity (BPP = 1.00). Moreover, the method does not guarantee to operate with an image compression algorithm. However, the MSB bit is less affect by noise than LSB bit. This

scheme has some potential to work with image compression with acceptable error rate.

Instead of using a grayscale image, Bhowmik, S., and A.K. Bhaumik proposed an algorithm that applied to a color image [1]. The two-consecutive blocks are grouped together. The LSB bits of both blocks are used to control the direction of k-bit LSB substitution which is usual order, complement order, reverse order, and complement reverse order. The number of k-bit is calculated by the decimal value of the six MSB bits of pixel value modulo by 4. The performance of the method achieves high capacity (BPP ≈ 3.00) and high image quality (PSNR ≈ 44.03). This is caused by the benefit of using the color image which contains more space to store information than a grayscale image. Unfortunately, the drawback of the method is that file size is larger than that of the grayscale image. Moreover, the algorithm cannot be used with any transformation or compression which are mentioned in their research.

For better understanding, the summary results of spatial domain based methods are shown in Table 1.

Table 1. Summary of spatial domain based methods

Method	PSNR (dB)	Capacity (bpp)
Bhowmik's method	44.03	3.00
Islam's method	51.18	1.00
Yang's method	43.66	2.25

For the transform domain, the traditional concept is to transform an image into another domain using transformation method such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). Then, secret data are embedded in the transformed coefficients.

In 2014, Lin, Y.-K. proposed steganography algorithm that directly embeds secret data into coefficients of the DCT transformation [4]. Generally, DCT transformation produces a real number as its coefficients which causes a problem in data hiding. In their research, Integer-to-Integer DCT transformation is used and secret data are hidden into high-frequency range coefficients. The result showed that the method has a high capacity (BPP = 1.75) and high image quality (PSNR ≈ 43.98). Unfortunately, applying the algorithm with image compression was not mentioned. Moreover, for the further consideration, a high-frequency range which is used to embed secret data is usually noise-stored location. It is possible that the algorithm cannot well operate with an image compression.

In 2015, Zhang, Y., et al. proposed the new algorithm that can be resistant to JPEG compression by using a relative relationship between DCT coefficients [5]. Reed Solomon (RS) Coding is used in this method to minimize the error of extracted secret data. A single bit of secret data is embedded into each four consecutive quantized coefficient blocks. Even though their method can work with JPEG compression, their experimental result shows low performance in terms of capacity (BPP ≈ 0.10) with some error. To get error-free secret data, more of the capacity must be preserved for error-correction.

In 2016, Huang, F., et al. proposed a new method that can be used with JPEG images [6]. Histogram shifting and block selection strategy were used in this method. To avoid image distortion, the quantized blocks are selected if the number of zero coefficients is greater than some threshold. To maximize embedding capacity, the most non-zero coefficients which are 1 and -1 are used to embed secret data. This algorithm can preserve JPEG image quality (PSNR ≈ 50.00 compared to original JPEG) and file size but low embedding capacity (BPP ≈ 0.02).

A JPEG based method with high capacity has been proposed by Vongurai, N and S. Phimoltares [10]. This method customizes standard quantization table from 8x8 to 32x32 by interpolation scheme. Secret data are embedded into the middle-frequency of quantized coefficients. The larger quantization table and the selected embedding area result in high image quality (PSNR ≈ 39.60) and high capacity (BPP ≈

0.98). However, this method uses customized quantization table. Thus, a special software may be required to open the embedded image.

For better understanding, Table 2. shows summary results of transform domain based methods.

Table 2. Summary of transform domain based methods

Method	PSNR (dB)	Capacity (bpp)
Lin's method	43.98	1.75
Zhang's method	-	0.10 (with error)
Huang's method	50.00	0.02
Vongurai's method	39.60	0.98

According to the literature review, spatial and transform domains provide different strength and weakness. For spatial domain techniques, the capacity of each technique usually is higher than a transform domain technique, but it has low chance to resist image compression which is difficult to use in the real world applications. Conversely, most transform domain methods can be used in the real world applications. However, their capacities are quite low compared to the spatial domain methods. In order to create more useful image steganography method that can be used in the real-world scenario, the transform domain based method is more suitable.

In 2010, Google introduced WebP technology, the new image format that can surpass the JPEG compression scheme. Moreover, WebP is used by high traffic websites according to report from W3CTech [8]. Thus, this technology is very advantageous and has a sense of future-proof when considering the growth of internet traffic in cloud-era. Not only the benefit mentioned above, but WebP is also similar to JPEG compression. Considering WebP as host image is very practical. For this reason, the new image steganography method based on WebP is proposed in this thesis.

Chapter 4. Proposed method

This chapter proposes a new image steganography scheme based on Lossy WebP in both embedding process and extracting process along with the solution to the problem mentioned in Chapter 2.2.

4.1. Re-calculation process

The solution to address the problem in Chapter 2.2 is called “Re-calculation” process. Due to several discussed reasons, the data hiding process cannot be moved to another location in the whole process. In order to correct wrong quantized coefficient, Re-calculation process simulates prediction and quantization process to re-calculate quantized coefficients of the current block before using in data hiding process. As shown in Figure 6, Re-calculation process consists of dequantization, prediction, and quantization process. Not only is those processes, a separated memory added for store modified compressed macroblocks.

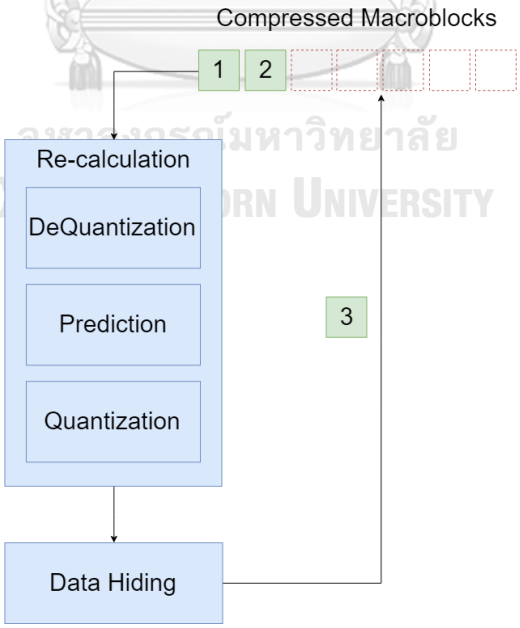


Figure 6. Re-calculation process

Even though the prediction process is ran twice, the performance cost is not double because the prediction parameter such as the best prediction models for each subblock are already obtained. Those result can be pass-through to the re-calculation process. Thus, an analysis part of the second prediction process can be skipped. The overall process of the proposed algorithm is shown in Figure 7. The re-calculation process is added after quantization process followed by data hiding process.

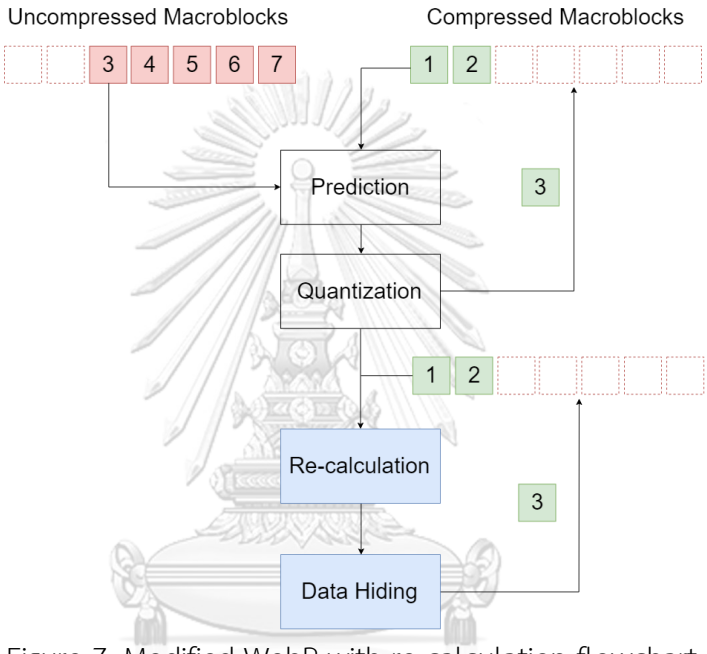


Figure 7. Modified WebP with re-calculation flowchart

To validate this solution, two experiments A and B were set up. In experiment A, secret data were hidden into WebP image without re-calculation process. On the other hand, experiment B applied re-calculation process before hiding data. To clearly see effect of re-calculation process, only the first block of both experiments were modified and set to extremely value by directly modify the coefficeint value. Both experimental results are shown in Table 3.

Table 3. Test experimental result

Metrics	Experiment A	Experiment B	Original WebP
PSNR	23.9040	44.5689	47.4899
SSIM	0.9750	0.9934	0.9936

According to Table 3, both image quality metrics were highly gained in experiment B. Moreover, considering pixel value difference between the embedded image from both experiments and original WebP image shown in Figure 7a and Figure 7b. It is clear that Re-calculation process can decrease error caused by data hiding process. For these reasons, applying Re-calculation process before Data hiding process can improve image quality.

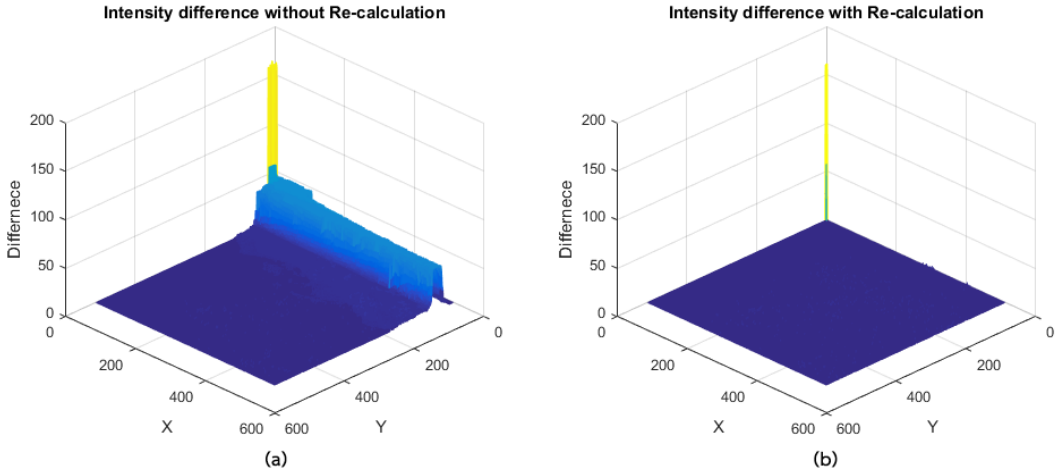


Figure 8. Intensity difference (a) Intensity difference without Re-calculation (b) Intensity difference with Re-calculation

4.2. Coefficients Selection

Generally, any quantized coefficients can be used for embedding secret data. However, the additional study is required to improve data security and preserve image quality.

Discrete Cosine Transform (DCT) converts an image from the spatial domain into the frequency domain resulting in coefficients matrix. The coefficients matrix can be grouped into 3 parts which are low-frequency part, middle-frequency part, and high-frequency part. According to [11], the low-frequency part is used to store the important coefficients. Any modification on the low-frequency part can degrade image quality. In case of the high-frequency part, this location is related to noise on the image. Thus, embedding data on both parts should be avoided. Considering [10, 11], the middle-frequency part is used for embedding secret data on JPEG based method. WebP and JPEG are both used Discrete Cosine Transform in their algorithm. Thus, the same approach should be used in this research.

Unlike JPEG, WebP's coefficients matrix is 4x4 instead of 8x8. The location of middle-frequency on [11] cannot directly apply on WebP. A new region of middle-frequency part needs to be obtained. Table 4 shows the region of middle-frequency part for WebP coefficients matrix. The value 1 represents coefficient positions of the middle part. These positions were manually selected from all possibilities and will be used for embedding secret data.

Table 4. Location of middle-frequency part

0	0	0	0
0	0	1	1
1	1	1	1
1	0	0	0

4.3. Embedding process

Embedding process is a process to embed secret data into lossy WebP image. This process uses LSB substitution technique together with the Re-calculation process to perform data hiding. The Embedding process can be described as follows.

For each macroblock,

1. Run encoding process till all quantized coefficients are obtained.
2. Apply Re-calculation process.

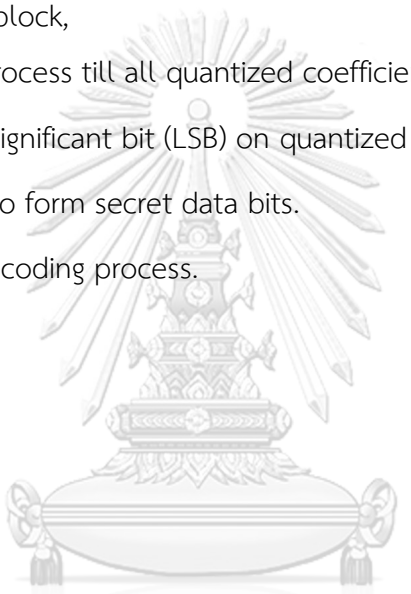
3. Substitute the least significant bit (LSB) on quantized coefficients of the middle-frequency part with secret data bits.
4. Continue the encoding process.

4.4. Extracting process

Extracting process is a process to extract secret data from lossy WebP image. This process is very simple and can be described as follows.

For each macroblock,

1. Run decoding process till all quantized coefficients are obtained.
2. Copy the least significant bit (LSB) on quantized coefficients of the middle-frequency part to form secret data bits.
3. Continue the decoding process.



Chapter 5. Experiments and Results

5.1. Experimental Setup

This study uses images from Kodak dataset [12]. Kodak dataset contains 23 non-alpha channel color images. All images are converted to grayscale before using in this experiment. The Huang, F., et al.'s scheme [6] is used as a competitive method because it is a recent method that performs better than other JPEG based methods. As in Huang, F., et al.'s research [6], this experiment is set as four configurations based on encoder quality parameter (Q) which is 70, 80, 90, and 100 where Q=100 implies highest image quality. There are five performance metrics used in this test, which are PSNR, SSIM, Capacity, FileSize, and IncreasedFileSize. PSNR and SSIM are used for measure image quality. Capacity is defined as number of secret bits per pixels of host image. FileSize and IncreasedFileSize are used for measure compression performance. This experiment is run on a machine with Windows 10 x64, Intel Core i5-2500K 3.7 GHz and 12 GB non-ECC DDR3 memory.

5.2. Experimental Results

There are 23 test images. Some images were dropped from experimental results. The selected JPEG based method yields various capacity, depending on quantized coefficients matrices on each image which related to both image context and quality level. Thus, only images that reach target capacity were included in the results.

The experiment results are presented in charts, which are averaged PSNR vs Capacity, averaged SSIM vs Capacity, averaged FileSize vs Capacity, and averaged IncreasedFileSize vs Capacity. Not only the performance of embedded JPEG and embedded WebP are shown, but the original performance of JPEG and WebP are also added in the chart. Thus, comparing embedded image performance against original performance is also provided. However, IncreasedFileSize is zero for an original image. Hence, the chart of averaged IncreasedFileSize vs Capacity includes only embedded

JPEG and embedded WebP. Moreover, these charts are shown under the predefined quality parameter Q which is 70, 80, 90, and 100 in chapter 5.2.1, 5.2.2, 5.2.3, and 5.2.4 respectively.

5.2.1. Q=70

For Q=70, the experimental results are shown in Figure 8. The proposed WebP based method performs better than JPEG based method in averaged PSNR ($\overline{\text{PSNR}}$) vs Capacity, averaged SSIM ($\overline{\text{SSIM}}$) vs Capacity and averaged FileSize ($\overline{\text{FileSize}}$) vs Capacity. For averaged IncreasedFileSize ($\overline{\text{IncreasedFileSize}}$) vs Capacity, JPEG based method achieves better performance than the proposed method.

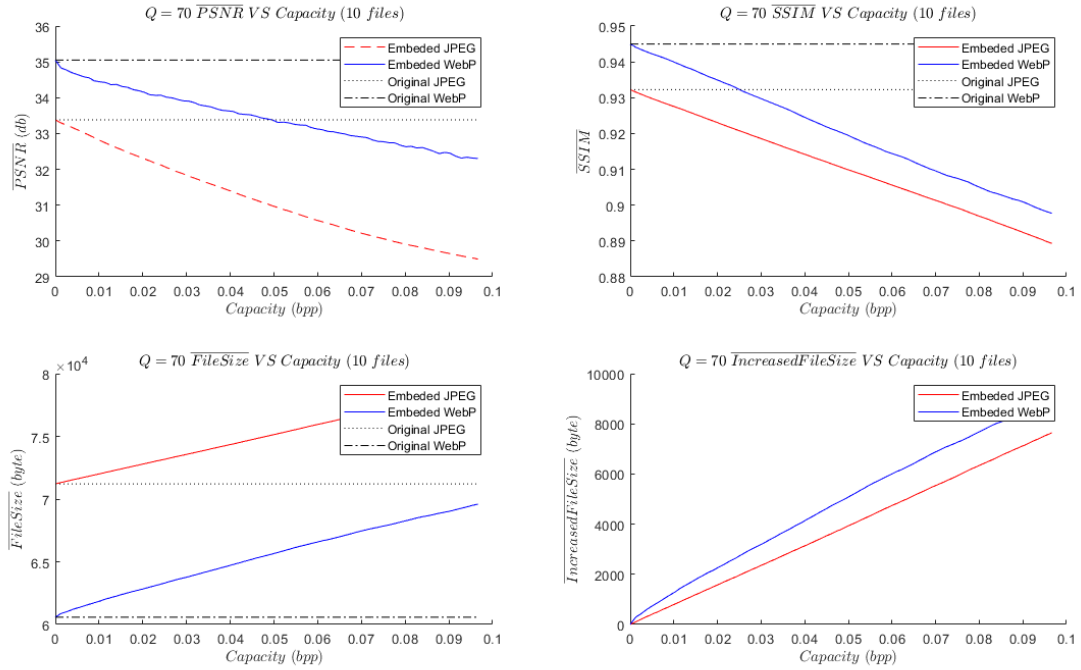


Figure 9. Experimental results for Q=70 (a) averaged PSNR vs Capacity (b) averaged SSIM vs Capacity (c) averaged FileSize vs Capacity (d) averaged IncreasedFileSize vs Capacity

5.2.2. Q=80

For Q=80, the experimental results are shown in Figure 9. The WebP based method achieves better performance than the competitive method in averaged PSNR ($\overline{\text{PSNR}}$) vs Capacity, averaged SSIM ($\overline{\text{SSIM}}$) vs Capacity, and averaged FileSize ($\overline{\text{FileSize}}$) vs Capacity. For IncreasedFileSize ($\overline{\text{IncreasedFileSize}}$) vs Capacity, WebP based method and JPEG based method achieve almost the same performance.

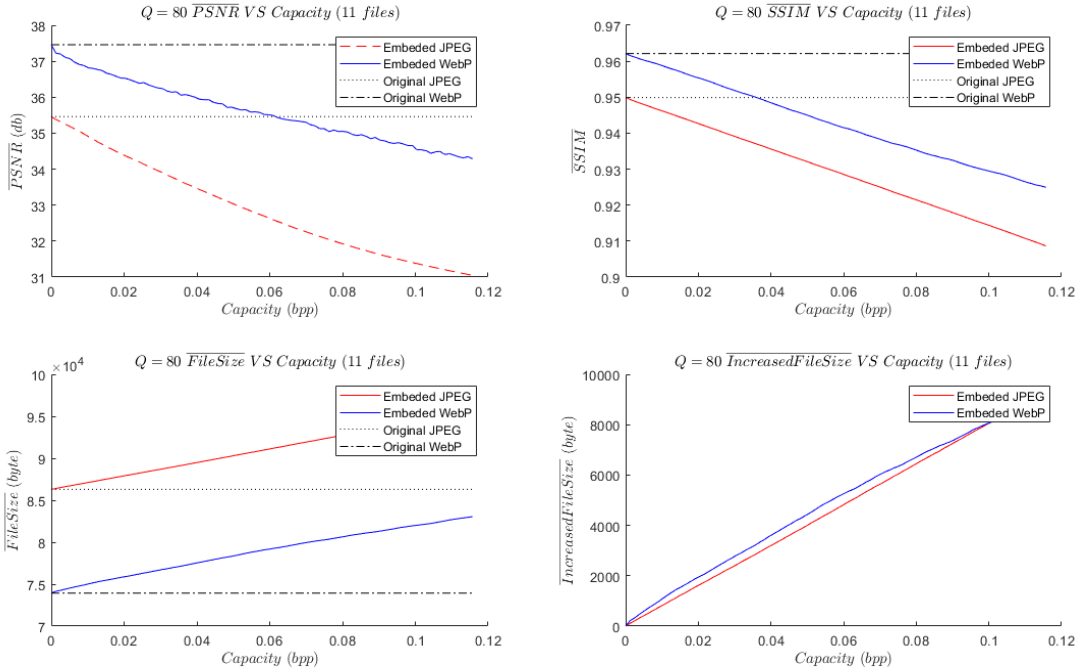


Figure 10 Experimental results for Q=80 (a) averaged PSNR vs Capacity (b) averaged SSIM vs Capacity (c) averaged FileSize vs Capacity (d) averaged IncreasedFileSize vs Capacity

5.2.3. Q=90

For Q=90, the experimental results are shown in Figure 10. The proposed method performs better than JPEG based method in all metrics which are averaged PSNR ($\overline{\mathbf{PSNR}}$) vs Capacity, averaged SSIM ($\overline{\mathbf{SSIM}}$) vs Capacity, averaged FileSize ($\overline{\mathbf{FileSize}}$) vs Capacity, and IncreasedFileSize ($\overline{\mathbf{IncreasedFileSize}}$) vs Capacity.

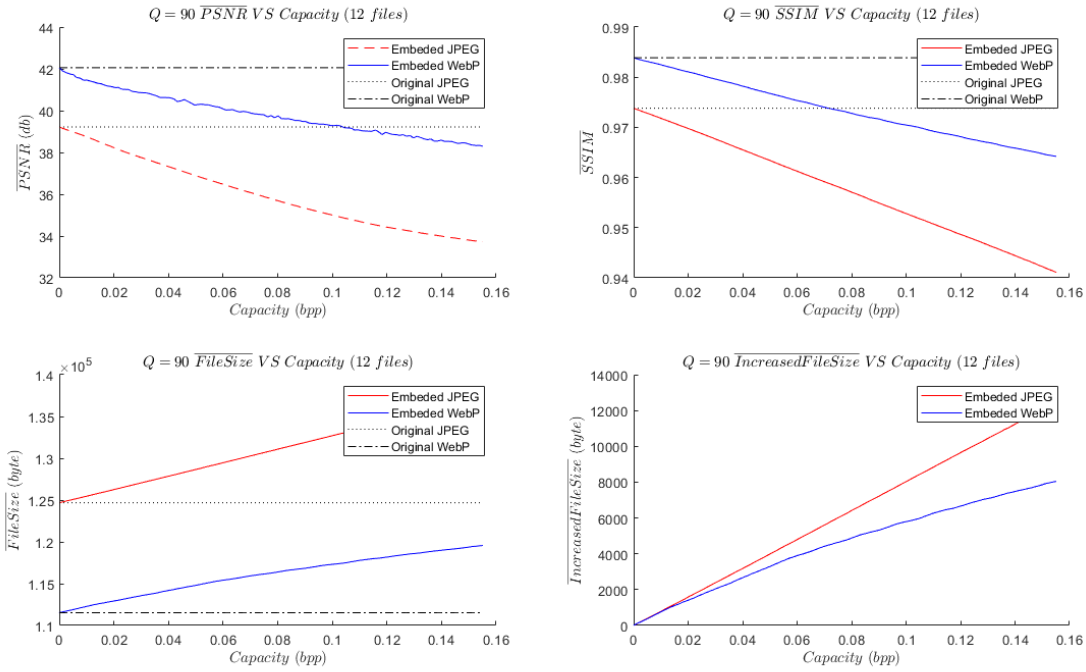


Figure 11. Experimental results for Q=90 (a) averaged PSNR vs Capacity (b) averaged SSIM vs Capacity (c) averaged FileSize vs Capacity (d) averaged IncreasedFileSize vs Capacity

5.2.4. Q=100

For Q=100, the experimental results are shown in Figure 11. The JPEG based method performs better than WebP based method in averaged PSNR ($\overline{\mathrm{PSNR}}$) vs Capacity and averaged SSIM ($\overline{\mathrm{SSIM}}$) vs Capacity. However, the proposed method achieves better performance in averaged FileSize ($\overline{\mathrm{FileSize}}$) vs Capacity and IncreasedFileSize ($\overline{\mathrm{IncreasedFileSize}}$) vs Capacity.

.

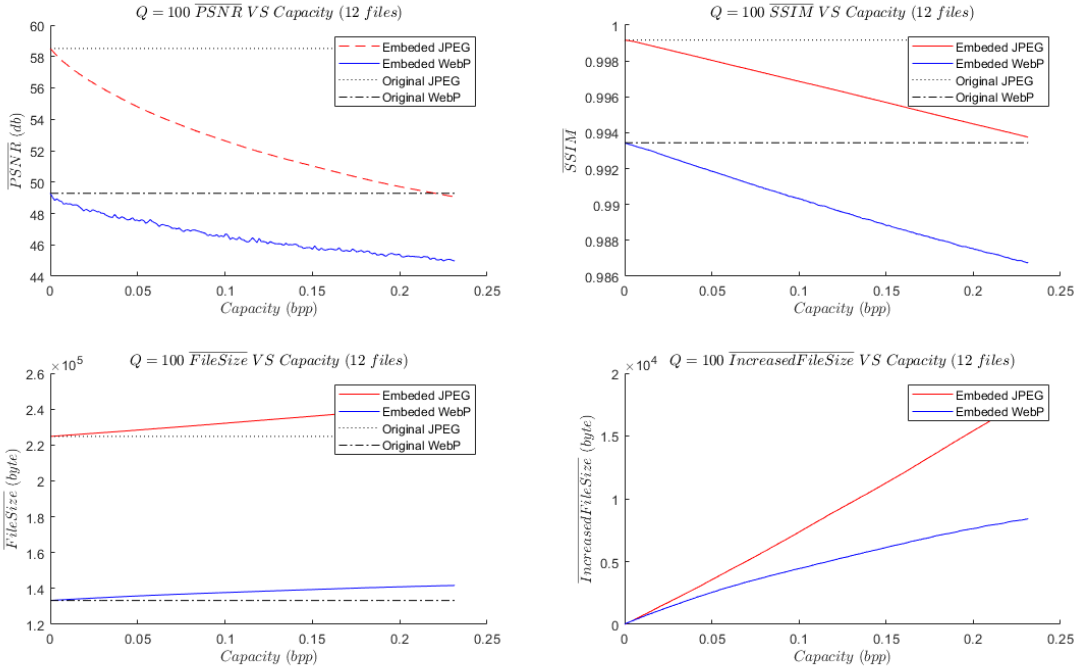


Figure 12. Experimental results for Q=100 (a) averaged PSNR vs Capacity (b) averaged SSIM vs Capacity (c) averaged FileSize vs Capacity (d) averaged IncreasedFileSize vs Capacity

5.3. Discussion

In terms of PSNR and SSIM, these metrics represent image quality. The proposed method provides better image quality than JPEG base method at Q=70, Q=80, and Q=90 except for Q=100 at the same capacity. The embedded image quality usually depends on its original image quality. Even though WebP achieves better image quality than JPEG in most cases, JPEG has higher quality than WebP for Q=100. However, the WebP based image quality at Q=100 seems to be better than JPEG based image if the capacity is more increasing according to the trend of averaged PSNR ($\overline{\text{PSNR}}$) vs Capacity.

In terms of Capacity, the proposed method provides better image quality than JPEG based method at Q=70, Q=80, and Q=90 except for Q=100 at the same capacity. In another word, the proposed scheme can provide higher capacity compared to JPEG based method if both image qualities are equal.

In terms of FileSize, the proposed method provides smaller embedded file size in all cases compared to the JPEG based method. This result can be considered as one of the benefits gained from using WebP as host image. However, the proposed embedding method is also important because our embedd method can preserve original WebP compression performance.

In terms of IncreasedFileSize, this metric indicates compression performance on both WebP and JPEG algorithms. The more IncreasedFileSize means less performance in compression algorithm. One factor that affects compression performance is the number of zero coefficients in each block. In case of Q=70, the JPEG based method performs better in IncreasedFileSize metric than proposed method. Considering the way each method embed secret data, the JPEG based scheme avoids embedding secret data into non-zero coefficients while the proposed method embeds secret data regardless the coefficient value. This means the number of zero coefficients is changed by the proposed method more than JPEG based method especially when Q=70 which zero coefficients are more produced than higher parameter Q. This effect is less impact when the parameter Q is higher or the quantized zero coefficients are lower. That is why the proposed method can perform better in

Q=80, Q=90, and Q=100. However, the proposed method still performs better in terms of FileSize metric which is more important than IncreasedFileSize metric.

Figure 13. Embedded color images

One benefit of adding Re-calculation and data hiding process after quantization process is that the main process of lossy WebP compression remains untouched. Therefore, the proposed method can immediately apply on a color image and an alpha channel color image. The preliminary result on color images and alpha channel color images are shown in Figure 12 and Figure 13 respectively.

Figure 14. Embedded alpha channel color images

Chapter 6. Conclusion

In this research, the new WebP based image steganography scheme is proposed. For most value of image quality parameter Q, the proposed scheme has higher averaged PSNR, averaged SSIM, and averaged Capacity compared to the JPEG based method. The proposed method has lower averaged FileSize and averaged IncreasedFileSize compared to the JPEG based method. These mean the proposed method achieves better image quality and higher secret bits per image while provides smaller image file size compared to JPEG based method. Moreover, the proposed method can be used with grayscale image, color image, and alpha channel color image which are not applicable to JPEG based method. In addition, the proposed method provides future-proof communication using WebP as file format of host image.

Nevertheless, there are still some WebP features waiting for investigation such as Animated WebP, Lossless WebP and WebM (video format). Extending the proposed method to cover all these features are very interesting.

REFERENCES

1. Bhowmik, S. and A.K. Bhaumik. *A new approach in color image steganography with high level of perceptibility and security*. in *2016 International Conference on Intelligent Control Power and Instrumentation (ICICPI)*. 2016.
2. Islam, A.U., et al. *An improved image steganography technique based on MSB using bit differencing*. in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*. 2016.
3. Yang, C.H., et al., *Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems.* IEEE Transactions on Information Forensics and Security, 2008. **3**(3): p. 488-497.
4. Lin, Y.-K., *A data hiding scheme based upon DCT coefficient modification.* Computer Standards & Interfaces, 2014. **36**(5): p. 855-862.
5. Zhang, Y., et al. *A JPEG-Compression Resistant Adaptive Steganography Based on Relative Relationship between DCT Coefficients*. in *2015 10th International Conference on Availability, Reliability and Security*. 2015.
6. Huang, F., et al., *Reversible Data Hiding in JPEG Images.* IEEE Transactions on Circuits and Systems for Video Technology, 2016. **26**(9): p. 1610-1621.
7. *WebP Compression Study | WebP | Google Developers*. 2018; Available from: https://developers.google.com/speed/webp/docs/webp_study.
8. *Usage Statistics of WebP for Websites, March 2018*. 2018; Available from: https://webcache.googleusercontent.com/search?q=cache:2a0v0okKdEkJ:https://w3techs.com/technologies/details/im-webp/all/all+&cd=1&hl=en&ct=clnk&gl=th.
9. *v0.6.0 - webm/libwebp - Git at Google*. 2018; Available from: https://chromium.googlesource.com/webm/libwebp/+/v0.6.0.
10. Vongurai, N. and S. Phimoltares. *Frequency-Based Steganography Using 32x32 Interpolated Quantization Table and Discrete Cosine Transform*. in *2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation*. 2012.

11. Chang, C.-C., T.-S. Chen, and L.-Z. Chung, *A steganographic method based upon JPEG and quantization table modification.* Information Sciences, 2002. **141**(1): p. 123-138.

12. Franzen, R.W. *True Color Kodak Images*. 2018; Available from: http://r0k.us/graphics/kodak/.

APPENDIX

Table 5. Tested images in each experiment

Image	Q=70	Q=80	Q=90	Q=100
1	✓	✓	✓	
2		✓	✓	✓
3				✓
4				✓
5	✓	✓	✓	
6	✓	✓	✓	
7				✓
8	✓	✓	✓	
9				✓
10				✓
11	✓	✓	✓	
12				✓
13	✓	✓	✓	
14	✓	✓	✓	
15				✓
16				✓
17				✓
18	✓	✓	✓	
19	✓	✓	✓	
20				✓
21			✓	
22	✓	✓	✓	
23				✓

Figure 15. Kodak image 1

Figure 16. Kodak image 2

Figure 17. Kodak image 3

Figure 18. Kodak image 4

Figure 19. Kodak image 5

Figure 20. Kodak image 6

Figure 21. Kodak image 7

Figure 22. Kodak image 8

Figure 23. Kodak image 9

Figure 24. Kodak image 10

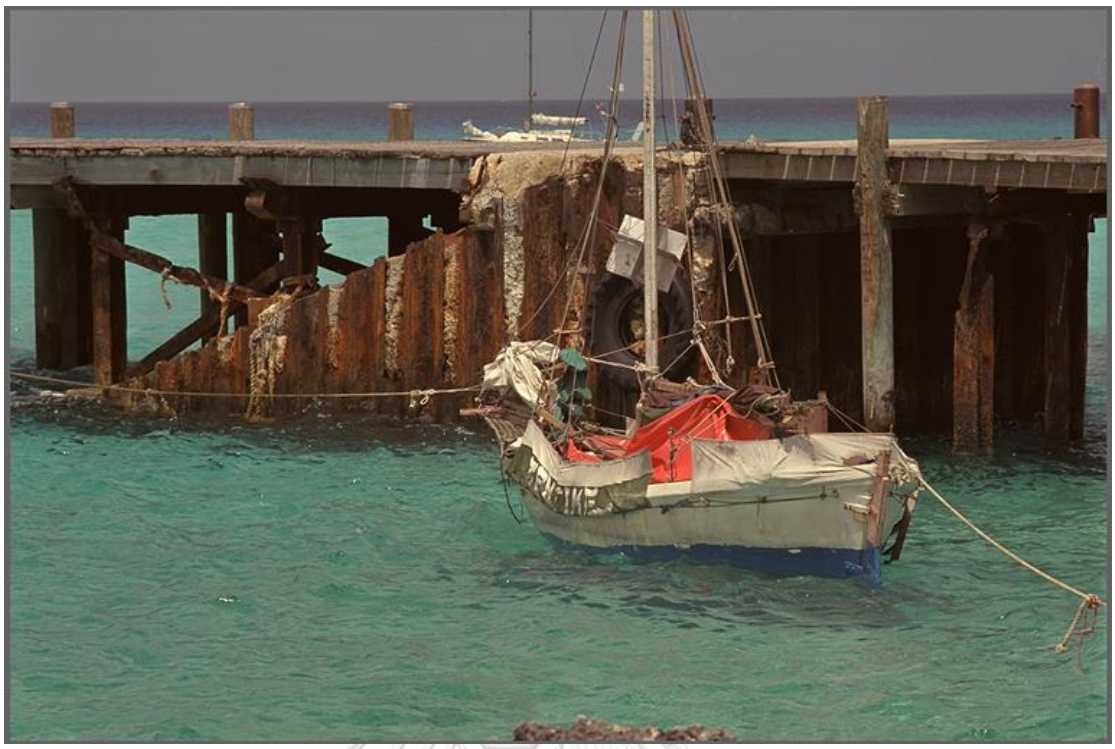


Figure 25. Kodak image 11

Figure 26. Kodak image 12

Figure 27. Kodak image 13

Figure 28. Kodak image 14

Figure 29. Kodak image 15

Figure 30. Kodak image 16

Figure 31. Kodak image 17

Figure 32. Kodak image 18

Figure 33. Kodak image 19

Figure 34. Kodak image 20

Figure 35. Kodak image 21

Figure 36. Kodak image 22

Figure 37. Kodak image 23

VITA

Name: Eittipat Kraichingrith

Affiliation: Advanced Virtual and Intelligent Computing (AVIC) Center, Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University.

Country: Thailand

Biography: Mr. Eittipat Kraichingrith was born on December 13, 1992 in Thailand. He received a Bachelor's Degree in Computer Science from Chulalongkorn University. Now he is a Master's degree student in Computer Science and Information Technology, Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University.