UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Robustness Comparison Study on Watermarking Techniques against Compression Attack

Mohd Aliff Faiz Jeffry, Hazinah Kutty Mammi
School of Computing, Faculty of Engineering
Universiti Teknologi Malaysia
81310 UTM Johor Bahru, Johor, Malaysia
alyffpro@gmail.com; hazinah@utm.my

Submitted: 19/01/2020. Revised edition: 24/04/2020. Accepted: 25/04/2020. Published online: 20/05/2020
DOI: https://doi.org/10.11113/ijic.v10n1.251

***Abstract*—Digital watermarking technique is a way of protecting digital image from malicious attacks. Compression attack is one of the most common attacks for images uploaded into social media. Social media, such as Facebook and Twitter, implement compression method for all types of media, before it is successfully uploaded into their server. This is to reduce the network bandwidth and storage needed to store each media in their server. However, the implemented compression method tends to tarnish image properties from the image itself, which can be used to identify the image itself. This produces other problems, which are ownership and copyright issues. Digital watermark has been proposed in numerous researches, and this research is one of them, in preventing the stated problem. The chosen digital watermarking techniques must be able to withstand against compression attack done by social media. A comprehensive analysis towards the watermarking algorithms and watermarked images were done, by applying several designed experiments. Based on the results, it shows that both chosen watermarking techniques could not withstands against compression attack made by JPEG compression and social media compression. It indicates that watermarking technique was not a suitable method to be used in preserving the ownership and copyright of the image throughout social media.**

***Keywords*—Digital image, digital watermark, compression attack, image security**

I. Introduction

Social media becomes a very popular platform of sharing experiences, thoughts, and ideas. Social media is defined as a collection of online interactive communication channel, dedicated to community-based input, users' interactions, content-sharing and collaboration. The number of social media users around the world increase gradually, resulting in an instant increase of images uploaded into each social media's platforms. This situation creates some severe problems in digital world, includes ownership issues, copyright issues, identity fraud, and metadata removal [1]. These problems may be deterred by applying certain security measures, such as steganography and digital watermarking. However, there are certain consequences when having the stated security measures, and each of the consequences may develop a new different problem. Therefore, in order to attain better security protection against malicious attacks towards images, a robust technique must be used. Digital watermarking technique will be used for this research in examining robustness of selected digital watermarking technique from compression attacks of social media.

This research is done in continuing our previous research entitled A Study on Image Security in Social Media using Digital Watermarking with Metadata [1]. As been derived from our previous research, it was stated that both visible and invisible watermarking techniques cannot withstand against compression attack done by social media. Therefore, this new current research wants to re-evaluate the previous research's conclusion by applying several different robust digital watermarking techniques, by using the same methodology. This research also uses the Joint Photographic Expert Group (JPEG) image file format as the main image file format for image analysis and watermarking processes. Digital watermarking techniques exposed in this research are DCT-based Pyramid Transform [2], Two-Step Sudoku Method using LSB [3], Semi-fragile Spatial Watermarking based on Local Binary Pattern (LBP) Operator [4], and Hybrid Schur and Singular Value Decomposition (SVD) [5]. The use of metadata for preserving ownership and copyright of the image is present, but instead of using plaintext of metadata, QR code had been generated using selected unique metadata. The use of metadata for preserving ownership and copyright of the image is present, but instead of using plaintext, a QR code generated using selected, unique metadata is used. By using the techniques stated above, it is to observe whether these robust watermarking techniques could withstand against compression attack done by social media.

By using the techniques stated above, it is to observe whether these robust watermarking techniques could withstand against compression attack done by social media. This is the focus of this research. In order to support this research aim, main research objectives must be achieved. There are three main research objectives, which are; 1) to study various available robust digital invisible watermarking techniques, 2) to test and apply digital invisible watermarking techniques for robustness against compression attacks, and 3) to analyse the result of each digital invisible watermarking techniques against compression attacks. By constructing the research objectives, the main research aim could be achieved accordingly.

II. Problem Background

There are three main problems to be highlighted in this research. The problems are ownership issues, copyright issues, and identity fraud. These stumbling blocks were generated from this research's main problem, which is compression attack. Referring to previous section, every single social media platform had implemented compression technique for every media file uploaded into their server. Their main determination is to decrease the file size of each uploaded media, in order to lower the storage and network bandwidth for storing and displaying the media. However, this implemented compression technique results in an anonymous media for all media, including images and videos, uploaded into the social media. It is a result from using lossy compression technique, which will permanently deter certain useful information from the image, leaving a presentation of pixels only. Each of the images and videos uploaded into every social media were unknown and cannot be used to attain some major prime information regarding the image.

Ownership and copyright issues were supposed to be the main obstacles, as these problems were a worldwide problem. Previously mentioned, compression attacks applied by social media tends to delete all useful information that can be used to identify each images and videos, uniquely. Therefore, issues regarding ownership and copyright of the images and videos cannot be tolerated, because there is no information and proves to be used in identifying the images and videos. By applying digital watermark, it is inferred that digital watermark can preserved the image properties that are used to identify the ownership and copyright of every images.

Identity fraud is another complex problem, where attacker can use the unidentified images from social media to create a fake identity throughout social media. For some cases in digital forensic, the investigation team cannot identify the owner of the image used for identity fraud activity because lack of information referring the image itself. Therefore, by applying digital watermark, it is assumed that all image properties can be embedded inside the host image, without been tarnished by compression attack, and can preserved the image properties for computer forensic investigations.

Although this research was observed to be more into forensic area, however, this research proves that essential, back-to-basic steps in social media leads to certain degree of potential computer-related crime, as mentioned above.

III. Related Works

When it comes to the idea of protecting our digital world, the implementation of security mechanisms must be well-considered. Our digital world involved a flow of digital information, where all different types of files were transferred within the network, or as been called 'Internet'. These bunch of information were scattered in the Internet of their own purposes. For example, text-type information is normally used to send simple instructions or just a simple chat and messages. On the other hands, an image-type file is normally used to display some various information inside an image. However, these unprotected, plain messages were exposed to malicious act. There are a lot of malicious behaviors, or in other words, malicious attacks, that are waiting for any important information to be stolen, altered, and damaged. Therefore, in order to prevent these kind of attacks, numberless researches all over the world had proposing numerous techniques for deterring all possible attacks. Below shows some related works from several researches regarding image security.

TABLE 1. Related works

Authors	Year	Domain	Techniques	Problem statement
Jeffry and Kutty Mammi [1]	2017	Image security, digital watermark	Visible watermarking, DCT	Unauthorized sharing, ownership issue, copyright issue, fraud
Maheshwari *et al.* [2]	2015	Image security, digital watermark	DCT based Pyramid Transform	Ownership verification
Chun He [6]	2016	Digital watermark, digital signature	DEW, LSB, DCT, Mp3Stego	Web resources protection
Goli and Naghsh [3]	2017	Image security, digital watermark	Two-step Sudoku Method, LSB	Cropping attacks of watermarked images
William Puech [7]	2008	Image encryption, image compression, digital watermark, medical image, image security	Crypto-watermarking	Protecting the transmission of medical images, applied to all kinds of image, videos, and 3D objects
Furqan and Kumar [8]	2015	Digital watermark, copyright	DWT-SVD domain	Copyright protection of data on Internet

IV. Digital Watermark

Digital watermarking was not a new thing in Information Technology (IT) areas. It is widely known and is currently developing in order to cater different collection of threats. As for definition, digital watermarking is a way of embedding trusted information into a medium that is used as a display. For example, an image, A, had been watermarked into another image, B, while B is used as a presentation of the image, without displaying A that had been embedded inside B.

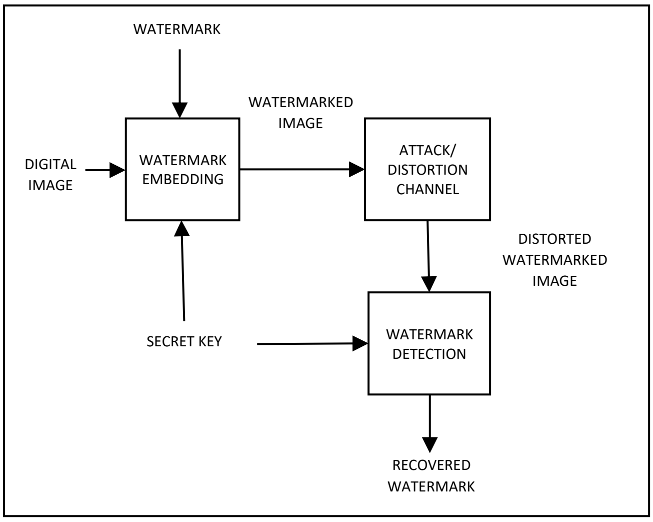


Fig. 1. Digital watermarking process

There are tremendously huge collection of digital watermarking techniques that had been proposed and proved of its functionalities in deterring a number of image attacks, such as, but not limited to, image compression, image cropping, and image manipulation. Another applications of digital watermarking includes copyright protection, fingerprinting, tracking, temper detection, broadcast monitoring, and completeness [9]. As been mentioned by us in previous paper [1], digital watermarking is best suited for preserving copyright and ownership of image. We also mentioned that by applying digital watermarking techniques to image, fraud activity also can be reduced [1]. However, in our previous research, we failed to preserve the watermarked information inside the watermarked images when all watermarked images undergo uploading and downloading processes into social media, which in another word, compression process of social media. It is been proved that DCT cannot withstand against compression attack done by social media [1]. However, there were so many other digital watermarking techniques that had not been explored yet, thus leaving us to do this comparative study for different watermarking techniques.

V. Comparative Study of Digital Watermarking Techniques

This section explains a comparison done between two types of digital watermarking techniques, which are the earlier watermarking techniques and the new robust watermarking techniques. This is to show the evolution of digital watermarking techniques. It also intends to show why the earlier version of watermarking techniques are not suitable to protect images from malicious attacks.

A. Comparison Between the Techniques

This section explains several comparisons based on the author's claims in their paper. This comparison was done to show various robustness aspects that every proposed watermarking technique may offers. There are numerous image attacks, and some of the attacks are prone to demolish every pixel inside an image. Some other image attacks targets on a certain area or certain pixels, making the image vulnerable to other image attacks, such as noise, filtering, blurring, sharpening, resampling, scaling, rotation, cropping, and JPEG lossy compression [5]. Researchers all over the world had come out with several countermeasures, and watermarking is one of them.

For this paper, there were four watermarking techniques to be explored, as been stated previously. An extensive comparative study for each watermarking technique was made, and those comparisons were recorded in this subtopic. However, the main point of doing this comparison study is to observe the robustness of each of the techniques against the compression attack. This comparison was made based on the author's claimed in their paper and does not include any actual hands-on techniques comparison using tools such as MATLAB.

DCTPT claims to has a good watermarking technique that can withstand against compression attack [2]. This technique had been proposed by five researches from Kukas Jaipur, India. They introduced a hybrid combination of previous DCT technique with the Laplacian Pyramid [2]. The result of using this technique, it is robust enough to withstand against compression attack, with a high Peak Signal-to-Noise Ratio (PSNR) value. PSNR is a common performance measurement used for calculating distortion between two images [10]. It indicates that every watermarked image that was run through DCTPT could withstand against compression attack.

TSSLSB, on the other hand, was developed to cater decent cropping attack. TSSLSB had been introduced by two researchers from Islamic Azad University [3]. This technique is a hybrid implementation of sudoku methodology with LSB technique. Based on the watermarking processes explained in [3], the watermark image will be broken up into nine parts, and each part will be randomized accordingly based on the sudoku method, and this process will be repeated once more, and the scrambled image will be embedded inside the host image. The experiment result was flabbergasted, as every part of the watermarked image contains at least one retrievable watermark image, even after a 98.8% cropping of the host image, the embedded watermark is retrievable [3]. Based on a study of the algorithm of TSSLSB, as an early hypothesis, it is assumed that this technique can withstand against compression attack by social media. However, the result may turn over our hypothesis for this technique, as the author itself did not test the technique against the compression attack.

SSWLBP was developed by two researchers from New Jersey Institute of Technology, Newark, USA. This technique is a hybrid combination of spatial watermarking technique with LBP operator. SSWLBP was claimed to be robust against several image attacks, which are additive noise, luminance change, contrast adjustment, colour balance, and JPEG compression [4]. This technique had captured our attention, as it was claimed to be robust enough against the JPEG compression attack. It fits our research need in experimenting with watermarking techniques that can withstand against compression attack. Therefore, this technique suits to be used for our research. More than that, this technique was claimed to be very fast in watermarking processes, as it involved less computational cost, where only Boolean functions are applied to this technique [4].

The last technique is HSSVD. HSSVD is a hybrid combination of Schur factorization and SVD transform. It had been proposed and developed by three researchers from Jawaharlal Nehru Technological University Hyderabad, India [5]. These researchers focused on the insusceptibility of their proposed watermarking technique against various image attacks, and compression is one of them. Schur and SVD algorithms were widely known as those techniques were hard to be penetrated by various attacks [5], [11]. This hybrid technique offers good security measures against various image attacks, but in terms of performance-wise, it requires a lot more time compared to the other techniques as it is a resource-hunger process [5]. It involved numerous complex computations; thus it requires more processing time. However, security is the most important element to be discussed in this research. This technique was claimed to be robust against compression attack. Therefore, this technique had been chosen to be studied and experimented in this research.

Based on the overall readings, it can be summarized in both Table 2 and Table 3. Table 2 explains the comparison between performance-wise and security-wise furnished by each watermarking technique. The comparison is based on claimed written by authors of each watermarking techniques, and it does not include any hands-on on all of the techniques yet.

TABLE 2. Performance-wise versus security-wise offered by each watermarking techniques

Techniques	Performance-wise	Security-wise
DCTPT	×	✓
TSSLSB	✓	×
SSWLBP	✓	✓
HSSVD	×	✓

Based on Table 2, it shows that only SSWLBP provides a good measurement in both performance and security aspect. It is such that it offers a good processing time at a low computational cost, plus issues a good security measurement against several image attacks. It makes SSWLBP robust enough to be used in this research, for furthering in our next research that will be discussed in the next topic. However, it is not to mention that other watermarking techniques are not robust against certain image attacks. Every watermarking technique offers a different function in preserving information of an image against different image attack. Nevertheless, this research's focal point is to simulate watermarking techniques that are claimed robust enough against compression attack by social media. At least two techniques will be chosen for running the experiments of this research.

Table 3 shows a comparison of those techniques that robust against several image attacks. It summarizes overall image attacks that each of the watermarking techniques can withstand with.

TABLE 3. Robustness comparison against several image attacks for each watermarking techniques

Technique	Cropping	Noise	Blurring	Sharpening	Compression
DCTPT	-	-	-	-	✓
TSSLSB	✓	-	-	-	-
SSWLBP	-	✓	-	✓	✓
HSSVD	✓	✓	✓	✓	✓

By referring to Table 3, it shows that HSSVD offers great image protection against several image attacks, including compression attack. It is the same with SSWLBP and DCTPT. As can be observed in Table 3, DCTPT was developed to cater compression attack. While TSSLSB was designed for preventing cropping attack. And for SSWLBP, it was designed to withstand against noise attacks, sharpening attack, and compression attack. Based on the overall comparison recorded in Table 3, it is observed that only DCTPT, SSWLBP, and HSSVD that are robust enough compression attack.

VI. Compression Attack

Compression is a process of transforming data to another form of data by removing all redundancies that occurs in the data itself [12]. Based on the definition, by applying compression technique, it will change data into unreadable form, as well as reducing the size of the data file [12]. However, in our scope, compression technique or compression attack used by social media does not changed the presentation of image, however it does reduce the file size of uploaded images.

In social media, every media, including images, videos, and sounds; that will be uploaded into social media must be compressed first. As previously mentioned, compression is done for reducing the bandwidth and storage size of all media. Compression is good in terms of removing redundancy and reducing the file size, however, it also removes some important elements inside an image. Metadata is the most important attributes in an image, which stored all crucial information about the image's properties. As can be seen in previous research [1], metadata was fully tarnished from the image after a successful upload process into social media. Therefore, it is proven that compression technique used by every social media will exactly remove all metadata from an image, which leaves the image in an anonymous state. In this research, digital watermarking techniques are used to preserve the metadata of the image, by embedding all metadata of the image into the host image. After that, the watermarked image will go through compression technique of social media, and the images will be downloaded back for watermark detection. If the watermarked information can be detected from the downloaded watermarked images, it is proven that the digital watermarking technique used is robust enough to withstand against compression attack of social media.

Besides social media compression attack, there are various compression attacks available for experimental purposes. As for comparing the compression attack done by social media, another compression attack is introduced for this research. JPEG is not only an image file format. It is a compression method used for compressing images. JPEG compression method is a lossy compression format, where for each compression process, some of image properties, including metadata and pixels value will be partially tarnished from the image itself. It is useful in reducing some redundancy in an image, thus reducing the file size, without visibly affecting the presentation of the image. The theory of compression method or compression attack is the same for all types of compression methods. Therefore, JPEG compression method is used for this research in order to observe and analysed the robustness of chosen watermarking techniques against both compression attacks.

VII. Proposed Methodology

For this research, DCT-based Pyramid Transform technique and Two-step Sudoku Method using LSB technique will be used for the entire research. However, as been expressed by both watermarking technique's researchers, both techniques were using image as the information to be embedded inside a host image. This research's main intention is to preserve the originality and ownership of image by applying metadata into the host image. Therefore, some watermarking processes must be altered in order to follow the research needs.

VIII. Experiment Design

There are eight different experiments that will be conducted for this research. Three of them are for image analysis, and another five will be experiments based on watermarked images. Figure below shows a list of experiments that will be conducted.

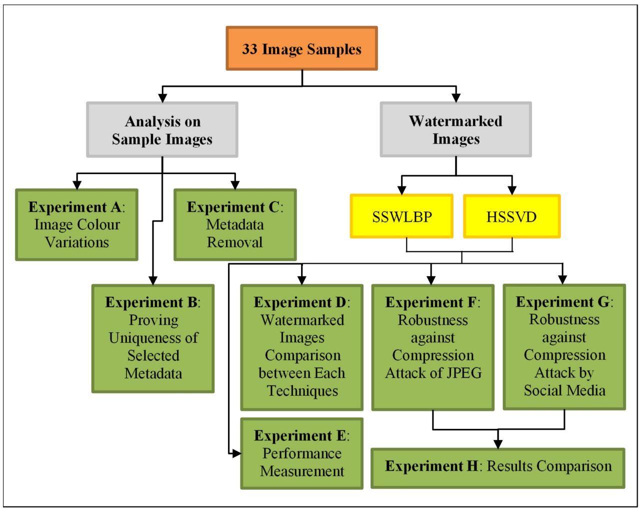

33 Image Samples
Analysis on Sample Images
Watermarked Images
Experiment A: Image Colour Variations
Experiment C: Metadata Removal
SSWLBP
HSSVD
Experiment B: Proving Uniqueness of Selected Metadata
Experiment D: Watermarked Images Comparison between Each Techniques
Experiment F: Robustness against Compression Attack of JPEG
Experiment G: Robustness against Compression Attack by Social Media
Experiment E: Performance Measurement
Experiment H: Results Comparison

Fig. 2. Experiment design

An approximate of thirty-three image samples will be used for every experiment done in this research. Each of the images are absolutely different, in terms of objects in the image, the pixel values, and the image properties. All images will be taken using a smartphone. All results will be recorded and will be analysed based on the research needs. The following sub-sections will introduce each of the proposed experiments for this research.

A. Experiment A: Image Colour Variation

Every image consists of different colour variations and pixel density. This colour is based on RGB or CMYK. For JPEG images, it supports ICC colour profile or colour space, which include sRGB and Adobe RGB. For this experiment, thirty-three image samples were classified into three different image colour categories, which are mostly one colour, few colours, and many colour. Each of the categories will have an approximate ten image samples, where each of them is classified in order to observe the compression process and watermarking processes. This category-based images will be used for the following experiments, and each of the results will be observed.

The main intention of doing this experiment is to observe the difference between those three image variations categories against compression attack by both JPEG compression and social media compression. As an early hypothesis, it is assumed that the lower the colour variation in an image, the higher the compression applied to the image. In order to prove this hypothesis, several experiments involving the JPEG compression and social media compression were made.

B. Experiment B: Proving Uniqueness of Selected Metadata

This experiment is designed to observe the differences for every image's metadata. It is to prove that every images used in this research were different and unique. Therefore, it can be used to prove originality and copyright of every images used for this research.

C. Experiment C: Metadata Removal

This experiment is conducted to distinguish the percentage of metadata inside every sample images. It is to see whether the metadata inside an image makes any difference towards the image size. The results will be recorded, together with some analysis.

D. Experiment D: Watermarked Images Comparison between Each Techniques

This experiment is a comparison experiment for each of the watermarked images between SSWLBP and HSSVD watermarking techniques. This experiment will observed the watermarked images properties. There are four parameters that will be measured for this comparison experiment. The parameters are image presentation, pixels value, size of the watermarked images, and resolution of watermarked images. This experiment focuses on the visual representation of watermarked images by comparing them with the original image sample. In order to help identify and measure the robustness of each technique against compression attack, Mean-Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) were calculated. MSE measures the cumulative squared error between the watermarked image and the original image, while PSNR measure the peak error of each of the image. The lower the MSE, the lower the error rate. However, for PSNR, the higher the PSNR value, the better the quality of the image itself.

This comparison experiment will be conducted, as to observe any differences between SSWLBP's watermarked images with HSSVD's watermarked images. Based on reading, an early hypothesis can be made, which is the image presentation for both watermarking techniques will have some difference, in terms of pixels values. A further analysis for every watermarked image by both techniques must be done.

E. Experiment E: Performance Measurement

Performance of each of watermarking techniques must be analysed. Each of the watermarking techniques will be measured in terms of time taken for watermarking processes, and the size of watermarked images. It is to see the effectiveness of each of watermarking algorithms in processing and producing the watermarked images. A comparison between the size of original image with the size of watermarked image will also be done.

F. Experiment F: Robustness against Compression Attack by JPEG Compression

This experiment will be conducted after a successful watermarking process done by each of the chosen watermarking techniques. Each of the watermarked images will undergo JPEG compression, in order to detect the presence of embedded watermark information inside the watermarked images, after the JPEG compression attack. Basically, JPEG has several compression rates, starting from 0% to 100%. Therefore, for this experiment, each of the watermarked images will go through several JPEG compression attack, by using several compression rates. Each compression rates will determined whether the embedded watermark information inside watermarked images can withstand against JPEG compression attack. If the embedded watermark information are presence in every JPEG compression attack's rates, therefore it can be concluded that the watermarking technique used is robust enough against JPEG compression attack.

G. Experiment G: Robustness against Compression Attack by Social Media

This experiment is the most important experiment in this research. thirty watermarked images will undergo through compression attack by social media, which is the uploading process into social media. Each of the uploaded watermarked images will be downloaded back to the computer, and those downloaded images will go through watermark detection phase. If the watermarked information can be retrieved back from the downloaded images, then the watermarking technique used for the watermarked images is considered robust enough against compression attack. However, if no watermarked information detected from the downloaded images, it is assumed that the watermarking algorithm used for the particular watermarked images is weak against compression attack. Each of the results will be recorded, and analysis on each of the result will be done.

H. Experiment H: Results Comparison of Experiment F and G

This experiment is a combination experiment of the results from Experiment F and Experiment G, where this experiment will compare results from both experiments. It is to observe the robustness of watermarked images against JPEG compression attack with social media's compression attack, by analyzing the presence of embedded watermark for each watermarking technique. Each of the results will be compared.

IX. Results and Discussion

This section explains the results and analysis of all of the constructed experiments. Each experiment was briefly explained below.

A. Experiment A: Image Colour Variation

This experiment was conducted to identify colour variation of each of the image in the dataset. TinEye, a colour extraction tool helps us to analyse the colour variation in each image. All sample images will be categorized into three main colour variation categories, which are one colour variation, few colour variations, and many colour variations. A simple condition-based algorithm had been constructed, and can be seen in Eq. (1), (2), and (3) below.

(1)

(2)

(3)

The reason why only the first colour was chosen is that it indicates major colour percentage in an image. If the first colour percentage is 45% and above, then the image is considered as a one colour variation image. If the first colour percentage is between or equal to 44% and 35%, then the image falls under few colour variations. For many colour variations, the percentage of the first colour must be under or equal to 35%. Based on this constructed range colour, every image samples were correctly categorised into their own colour variation categories, and the result is shown below.

TABLE 4. Results of Experiment A

Image Colour Variations		
One colour	Few colours	Many colours
13	10	10

By referring to the image colour variations, it is assumed that every result produced by each following experiment will have some correlations with the result in this experiment. It includes the size of image, pixel values, resolution, compression rates, etc. Each of those results from upcoming experiments will be compared with results generated from this experiment.

B. *Experiment B: Proving Uniqueness of Selected Metadata*

This experiment was constructed to observe the differences and functionality of each metadata, whether it is useful for determining ownership and copyright or not. The most valuable metadata were chosen, and those chosen metadata were used for watermark embedding processes.

Based on several analysis regarding each of the metadata, a list of selected metadata was produced, as shown in

Fig. 3 below.

Final chosen metadata						
Original Filename	Camera Model	DateTime	Resolution	File Size	Exposure	MD5

Fig. 3. Chosen metadata

The summary and description of the chosen metadata were described in table below, with the value that those metadata hold.

TABLE 5. Summary of the description of chosen metadata

Chosen metadata	**Preserved?**	**Description**
Original Filename	Copyright	Stores filename that includes a combination of file type, date, sequence number, and file format.
Camera Model	Ownership	Indicates the smartphone's camera used to take the photo.
DateTime	Ownership	Records date and time the photo taken.
Resolution	Copyright	Store the resolution of the photo (in pixel).
File Size	Ownership Copyright	Store the original size of the photo.
Exposure	Copyright	Present the exposure of the photo taken.
MD5	Copyright	Protect from the alteration towards the original image

Based on the chosen metadata structure shown in

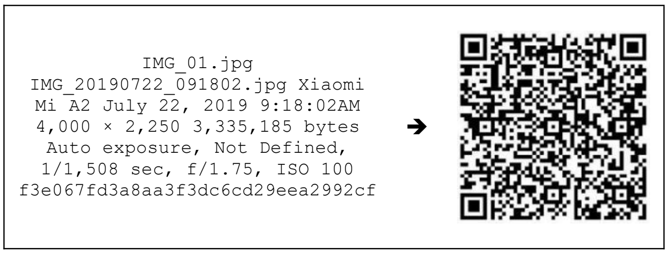
Fig. 3, table below shows the metadata value extracted from a sample image. It shows the original filename, camera model, datetime, resolution, file size, exposure, and MD5 value of the image. All information were extracted from the sample images, and been carefully stored aside, in order to preserve the originality and confidentiality of the information.

TABLE 6. Sample chosen metadata extracted from a sample image

Attributes	**Value**
Filename	IMG_20190722_091802.jpg
Camera Model	Xiaomi Mi A2
DateTime	July 22, 2019 9:18:02AM
Resolution	4,000 × 2,250
File Size	3,335,185 bytes
Exposure	Auto exposure, Not Defined, 1/1,508 sec, f/1.75, ISO 100
MD5	f3e067fd3a8aa3f3dc6cd29eea2992cf

QR code will be generated for each image based on their own chosen metadata value. Therefore, in order to achieve that, an online QR Code Generator is used, where it can be reached on the link https://goqr.me. The entire chosen metadata were run through the QR code generator, by inserting a line of fully combined chosen metadata and generate the QR code based on the text, as shown in

Fig. 4. The same process was done to all sample images.



```
IMG_01.jpg
IMG_20190722_091802.jpg Xiaomi
Mi A2 July 22, 2019 9:18:02AM
4,000 × 2,250 3,335,185 bytes
Auto exposure, Not Defined,
1/1,508 sec, f/1.75, ISO 100
f3e067fd3a8aa3f3dc6cd29eea2992cf
```

Fig. 4. Generating QR code from a single line of finalized metadata

The use of QR code in this research is significance in increasing the security aspect of the watermarking process. This is to ensure that the embedded metadata are well preserved, and impenetrable by attacker. Another reason on implementing QR code for watermarking process is that the QR code is more robust against physical or direct attack.

Imagine the use of only a plain text of chosen metadata instead of using the generated QR code, the tendency of the plaintext getting penetrated by attacker is higher. The attacker may intercept the embedded watermarking and change the metadata attribute stored inside the watermarked image, thus making the integrity of the watermarked image down. Other consideration is to use a screenshot of the chosen metadata instead of using QR code. The tendency of getting penetrated by the attacker is very low, since all of the chosen metadata attributes were saved in an image. However, as to be mentioned, images are prone to compression. The possibilities of pixels presented by the chosen metadata attributes on the image prone to compression is higher than the use of QR code. It is because the text inside the image is only represented by a small number of pixels, thus making it prone towards compression attack. The metadata attributes could be retrieved back, but in a bad form, and the metadata attributes stored on the image might be unreadable. Therefore, it is confirmed that the use of QR code is much better compared to plaintext and the screenshot of chosen metadata.

As for the conclusion of this experiment, it was a success in proving the uniqueness of chosen metadata, with some security aspect added into the QR code.

C. Experiment C: Metadata Removal

Main intention of conducting this experiment is to distinguish the percentage of metadata inside every sample image. Therefore, a special tool must be used for removing embedded metadata of every image in our dataset. JPEG & PNG Stripper was used to make our experiment successful.

For this experiment, all sample images were going through this tool, and all information regarding the difference between original sample image with the new sample image are carefully recorded. The image resolution remains the same for the new sample image, however, the size of image shows the most obvious difference between original image and new image.

Below is the summary result of this experiment, which includes all 33 sample images.

TABLE 7. Average metadata removal result

Comparison with original image	**Average size reduction**	
	Bytes	**%**
Smaller	9,124	0.25

Based on the indicated results, it shows a slight difference between original image and new no-metadata image. The difference is only at the file size, which that the new image sizes are reduced at an average of 9,124 bytes, which is 0.25% from the original image sizes. It is a very small difference between both types of images. This experiment shows that metadata only occupies a small number of bytes in a single image, but it consists of all information that explains the image itself.

D. Experiment D: Watermarked Images Comparison between Each Techniques

This research focuses on two main watermarking techniques, which are SSWLBP and HSSVD. Both techniques were run by using MATLAB, and every sample image were run through each technique. All analysis regarding the watermarked images produced by both watermarking techniques are discussed in this subsection.

The extracted watermark from SSWLBP watermarked image is in a good condition, but with some visible noise appeared on the lower left side of the extracted watermark image. The noise only occupies a small amount of the QR code, and it does not interfere with the reading of the QR code.

For HSSVD watermarking technique, it also been considered as a favourable outcome since all sample image were successfully watermarked, and all embedded watermark can be retrieved back, but in a small size.

On the other hand, the watermarked image generated by HSSVD is completely different from SSWLSB. The HSSVD watermarked image is in a grayscale form, and the image resolution decreases to be 512 × 512 pixels. It is because the algorithm of HSSVD were built like that. The intention of the authors of the algorithm was to preserve the embedded watermark inside the watermarked image, without hedging the image presentation and image resolution. The watermarked image had completely compressed from the original image of 4,000 × 2,250 into 512 × 512, which is about 97% smaller than the original image.

The changes of pixels value between original image with watermarked image can be evaluated by recording the value generated from imageDiff. It shows the percentage of pixel difference between those types of image. Besides that, PSNR value can be used to calculate the quality of image produced from the watermarking technique. The higher the PSNR value, the better the quality of compressed or reconstructed image.

From the overall result, it can be concluded by using an average value of PSNR value and pixel changed percentage. The average value of PSNR and pixel changed percentage for SSWLBP and HSSVD were shown in TABLE 8 below.

TABLE 8. Average PSNR value and pixel changed percentage comparison between SSWLBP with HSSVD

	SSWLBP	**HSSVD**
PSNR Value	48.62397	38.6652
Pixel changed	0.88%	undefined

SSWLBP and HSSVD claimed to be robust against various image attacks, and PSNR is one of the parameters that shows the robustness of each techniques from image attacks. Both techniques claimed to have a high RSNR reading, which was 42.67 for SSWLBP, and HSSVD with 65.123. This experiment can be used to check for the claim made by the authors of both watermarking techniques. The equipment used is adequate for us to experiment with the result claimed by the authors. Therefore, the result of PSNR value for both watermarking techniques were recorded and shown as in TABLE 9 below.

TABLE 9. PSNR value comparison between claimed made by authors and results generated from this experiment

	SSWLBP		HSSVD	
	Claimed	Result	Claimed	Result
PSNR value	42.67	48.6240	65.123	38.6652

Based on the findings, it shows the PSNR value of SSWLBP is proven of its claimed made by the authors. However, for HSSVD, the PSNR value of this experiment were lower than claimed been made by the authors, for almost 40% lower than the expected PSNR value. It might be caused by the environment, the image sample used, and all other expect that need to be considered. However, the PSNR gathered from this experiment shows a lower reading. The lower the reading, the higher the chances of getting attacks by various image attacks. However, it is just a hypothesis made after doing this experiment. More experiments need to be done in order to prove the hypothesis.

This experiment had successfully watermarked all sample images using two different watermarking techniques, which were SSWLBP and HSSVD, resulting two types of watermarked images. A comprehensive comparison and analysis regarding the presence of the embedded watermark, the image presentation, file size comparison, and image resolution had been done.

E. *Experiment E: Performance Measurement*

This experiment exposed two main criteria of performance measurement computed from SSWLB and HSSVD watermarking techniques, which are time taken for watermarking processes, that includes embedding and extracting processes, and file size comparison for watermarked images with original images.

The time taken for embedding and extracting processes for both watermarking techniques were carefully recorded. The time were taken by using command 'tic' and 'toc' available in MATLAB. Based on the command, an average value of embedding and extracting time for both watermarking techniques were recorded, as in TABLE 10 below.

TABLE 10. Average time taken for embedding and extracting for both SSWLBP and HSSVD

	Watermarking techniques			
	SSWLBP		HSSVD	
	Embedding	Extracting	Embedding	Extracting
Average time taken for watermarking process (seconds)	27.634	37.683	0.148	0.191

Based on the table above, it shows that SSWLBP requires a longer time for both embedding and extracting watermarking processes, compared to HSSVD. Although stated that SSWLBP does not requires any computational algorithm thus making it to be faster than HSSVD, it is, however, was slower than HSSVD. It is because SSWLBP load and process all available pixels in each image sample, making it to take a longer time to be processed. SSWLBP also produced an exact image resolution from the original image resolution, which in this research, it preserved 4,000 × 2,250 pixels. HSSVD, however, do entertain all the pixels in the sample image, but it tends to compress all images into 512 × 512 pixels.

The increased file size for watermarked image compared to the original image is acceptable, since we literally add an image to be watermarked into a host image, making the size of the image increase rapidly. This was shown by SSWLBP watermarking technique, where all watermarked images increased rapidly, at an average of 185.64% larger than the original image. While for HSSVD, it demonstrated a compression method for all watermarked images, where all image sample will be transformed into a smaller image resolution, thus creating a smaller file size for the watermarked image. The watermarked image produced by HSSVD is at an average of 96% smaller than then actual file size of the original image sample. The embedded watermark was preserved but had been transformed into a smaller size, which is 64 × 64 pixels. For SSWLBP, the size of the embedded watermark is constant, at 400 × 400 pixels.

TABLE 11. Average percentage difference between original image sample with watermarked images for both SSWLBP and HSSVD watermarking techniques

SSWLBP		HSSVD	
%	Difference with original	%	Difference with original
185.64%	Larger	96.00%	Smaller

The experiment shows that SSWLBP requires a lot more time for embedding and extracting watermarks compared to HSSVD. This happened because of the file size produced by each watermarking technique differ from each other. The file size for SSWLBP watermarked images were larger from the original image sample, while the file size were smaller for all HSSVD watermarked images.

F. *Experiment F: Robustness against Compression Attack by JPEG Compression*

This experiment was done in investigating the presence of embedded watermark information inside every image after been compressed by a lossy compression, which is JPEG compression. In addition, several observations together with analysis regarding the image presentation, pixel value, file size comparison, and image resolution were done.

Based on the extracted watermark of SSWLBP watermarked images that been compressed into five different compression quality, it shows that the extracted watermarked are unreadable, and cannot be used to retrieve back the embedded metadata inside the QR code. It is visible, but the retrieved watermark is unreadable by the QR code reader, making it unidentified. The quality of retrieved watermarked images decreased when the value of Q decreased. The noise in every watermarked image increase gradually, which makes the watermarked images impossible to be read by QR code. Therefore, it can be concluded that SSWLBP is not robust against JPEG compression attack. The only reason on why the embedded watermark unreadable is because of JPEG compression. Since JPEG is a lossy compression, it tends to remove any pixels inside the image, making it presentable, yet loses some valuable information.

For HSSVD, it was observed that all retrieved watermark was unreadable, and does not present the QR code embedded inside the watermark image, visibly. In addition, the extracted watermarks seem to have been corrupted by the compression, thus leaving it to be in that form. Therefore, it can be concluded that HSSVD watermarking technique is prone to JPEG compression attack.

Those results can be compared with all claimed made by the authors of both SSWLBP and HSSVD watermarking techniques. TABLE 12 shows the comparison for both watermarking techniques between the claimed made by the authors of each watermarking technique with the results gathered from this research.

TABLE 12. Claimed made by authors versus experimented results

SSWLBP		HSSVD	
Claimed	**Result**	**Claimed**	**Result**
Robust against compression attack, with proven results	Cannot withstands against compression attack	Robust against compression attack, with proven results	Cannot withstands against compression attack

From the table above, it shows that the claimed made by the authors of both watermarking techniques were not applicable for this research, as all watermarked images that went into JPEG compression attack did not preserved the embedded watermark. It is because JPEG compression tends to tarnish and scramble all pixel values in an image, making it readable and presentable, but in a compressed file. The claimed made by the authors of each watermarking techniques shows that they experimented the watermarked images with the JPEG compression by using the MATLAB environment. The watermarked images used by the authors were not been stored physically inside the storage media, such as the disk. All watermarked images used by them were stored logically inside the memory, thus making all pixel value fresh and unsusceptible from any file compression formatting. That makes the watermarked images used by the authors robust against compression attack.

The percentage of pixel changes increases as the percentage of Q decreases. The average of the percentage of pixel changed for compressed SSWLBP watermarked images against JPEG compression attack were shown below.

TABLE 13. Average pixel changed for SSWLBP watermarked images against JPEG compression

	Q				
	100%	**90%**	**80%**	**70%**	**60%**
Average pixel changed for SSWLBP watermarked images against JPEG compression	28.15%	77.78%	84.12%	89.30%	93.84%

It shows a significant increase of the pixel changed percentage when the percentage of Q decreases. The percentage of pixel changed has a relationship with the PSNR value. The PSNR value of the compressed images of different percentage of Q can be summarized by calculating the average of the PSNR value for all images that went through different JPEG compression attacks, as in TABLE 14.

TABLE 14. Average PSNR value for SSWLBP watermarked images against JPEG compression

	Q				
	100%	**90%**	**80%**	**70%**	**60%**
Average PSNR value for SSWLBP watermarked images against JPEG compression	53.1840	44.6903	42.7514	41.6996	40.6989

Those are the discussion for the SSWLPB watermarked images that went through JPEG compression attack. The discussion continued with the JPEG compression applied to all HSSVD watermarked images.

As the percentage of Q decreases, the number of white pixels appeared tends to increase. It shows that the quality of the compressed watermarked images became poorer when the value of Q decreases. It can be briefly precis into an average value, as shown in TABLE 15 below.

TABLE 15. Average pixel changed for HSSVD watermarked images against JPEG compression

	Q				
	100%	**90%**	**80%**	**70%**	**60%**
Average pixel changed for HSSVD watermarked images against JPEG compression	9.11%	67.94%	74.26%	77.90%	80.29%

The PSNR value calculated between compressed HSSVD watermarked images with original HSSVD watermarked images seems to be decreased as the value if Q decreased. It is because the compression rate increase when the value of Q decreased. Therefore, the quality of compressed images tends to become poorer as the quality of JPEG compression decrease. The result was shown in TABLE 16 below.

TABLE 16. Average PSNR value for HSSVD watermarked images against JPEG compression

	Q				
	100%	90%	80%	70%	60%
Average PSNR value for HSSVD watermarked images against JPEG compression	61.5660	44.4829	40.8545	39.1980	38.2048

Based on the results gathered from the experiment, it shows a significance decreased of the file size for both watermarking techniques when the compression quality decreased. TABLE 17 shows the average difference between SSWLBP watermarked image with JPEG compressed SSWLBP watermarked image.

TABLE 17. Average difference between SSWLBP watermarked image with JPEG compressed SSWLBP watermarked image

Q	100%	90%	80%	70%	60%
Average compressed SSWLBP watermarked image file size (bytes)	5,077,916	1,683,457	1,104,702	873,291	740,604
Smaller / Larger	Smaller				
Average difference with SSWLBP watermarked images (bytes)	51.30%	83.85%	89.41%	91.62%	92.90%

It shows that the file size of the compressed SSWLBP watermarked images decrease gradually as the value of Q decreased. It explains that the lower the JPEG quality, the lower the file size of the image. It is because the percentage of compression been applied to the watermarked images increase as the value of Q decreased.

The discussion continues with the difference in file size of HSSVD watermarked images against JPEG compression attack. It shows an average file size comparison between compressed HSSVD watermarked image with HSSVD watermarked image. Table below shows the average file size comparison between two types of image.

TABLE 18. Average difference between HSSVD watermarked image with JPEG compressed HSSVD watermarked image

Q	100%	90%	80%	70%	60%
Average compressed HSSVD watermarked image file size (bytes)	163,848	66,997	46,142	36,790	30,694
Smaller / Larger	Larger	Smaller			
Average difference with HSSVD watermarked images (bytes)	14.63%	53.13%	67.72%	74.26%	78.53%

As can be seen on the previous table, the compressed HSSVD watermarked images had an increase in file size when Q equal to 100%, where the compressed image became larger, at an average of 14.63% compared to the original watermarked image. It was assumed that when Q=100%, JPEG algorithm will try it best to preserved as much information as it can, as there will be only a small percentage of compression going on in the image when the JPEG quality is set to 100%. Therefore, the increase of files ize of the compressed watermarked image when Q=100% is acceptable. However, as the value of Q decreases, the file size of compressed watermarked images decreased gradually.

The demonstration of JPEG compression towards watermarked images had been done. It shows that the compression tends to tarnish all important information from the image, and embedded watermark is one of them. It is because JPEG compression tends to manipulate the whole binary values inside the image in order to compress the image into a certain percentage or rate of compression, even at a very low compression rate. Both watermarking techniques claimed to be robust against compression attack, but however, those claimed was false, since this experiment proved that all watermarked images generated from both watermarking techniques were prone to compression attack. Therefore, it can be concluded that both watermarking techniques were not robust against JPEG compression attack.

G. *Experiment G: Robustness against Compression Attack by Social Media*

This experiment is the core of this research. This experiment was constructed to analyse the robustness of selected watermarking techniques against compression attack done by social media. As been stated previously, both SSWLBP and HSSVD were penetrable by JPEG compression attack. Since JPEG compression and social media compression required a different platform for compressing the image, it was then constructed. The watermarked images went through the uploading and downloading processes into two different social media, which are Facebook and Twitter. After all watermarked images been successfully uploaded into both social media, all uploaded watermarked images were downloaded back in order to do further analysis regarding the presence of embedded watermark and others.

The analysis regarding the presence of the embedded watermark inside the watermarked image after being compressed by two different social media, which are Facebook and Twitter were analysed. Other aspects including the presentation of the image, the different of file size and image resolution were also been discussed onwards.

Both watermarking techniques could not withstand against compression attack made by both Facebook and Twitter. The embedded watermark inside the watermarked image could not be extracted, leaving the watermarked image prone to compression attack made by both social media.

Based on the justification about the downloaded watermarked images from Facebook, the PSNR value and the percentage of pixel changed are undefined. It is a result from the different image resolution of the downloaded watermarked images from Facebook. Nevertheless, the PSNR value and the percentage of pixel changed for downloaded watermarked images from Twitter can be recorded.

TABLE 19. Average PSNR value and percentage of pixel changed for SSWLBP watermarked images that went through compression by Facebook and Twitter

Facebook		Twitter	
PSNR value	**% of pixel changed**	**PSNR value**	**% of pixel changed**
Undefined	Undefined	43.5699	81.09%

Based on the table above, it shows that the average PSNR value for watermarked image downloaded from Twitter is 43.5699 with an average percentage of pixel changed of 81.09%. The quality of the downloaded watermarked images was well-preserved, but the amount of pixel change was very high, that the embedded watermark could not withstand against the compression.

This report continued with the observation towards the HSSVD watermarked image that had been downloaded from Facebook and Twitter.

For this time, the comparison for Facebook compressed watermarked images can be done, because the compressed image resolution was the same as the original watermarked images. The comparison of PSNR value and percentage of pixel changed were shown in table below.

TABLE 20. Average PSNR value and percentage of pixel changed for HSSVD watermarked images that went through compression by Facebook and Twitter

Facebook		Twitter	
PSNR value	**% of pixel changed**	**PSNR value**	**% of pixel changed**
45.2810	67.36%	27.0394	0%

The PSNR value of Facebook compressed watermarked image is at an average of 45.2810, where this value indicates that the quality of the compressed watermarked image had become poorer, thus increases the percentage of pixel changed to be at an average of 67.36%. The higher the percentage of pixel changed, the lower the PSNR value. However, the claimed that had been made earlier cannot been applied to the next analysis regarding the PSNR value and percentage of pixel changed for Twitter compressed watermarked image. As can be seen on the table above, it is mentioned that the percentage of pixel changed for all compressed watermarked images by Twitter were at 0%, where there is no single pixel been changed for the compressed images. However, the PSNR value indicates that the quality of the compressed images was at a lower level, which is at an average of 27.0394. The PSNR value is very low that the quality of the compressed images becomes very poor.

Facebook compressed all watermarked images at an average rate of 95.10%, which means that all watermarked images became smaller in size, at an average of 95.10% smaller than the original watermarked images. The compression rate applied to all images that been uploaded into Facebook were high, thus making it to be susceptible against compression attack. The same goes with Twitter. Twitter tends to compress all uploaded images until it becomes at an average of 88.93% smaller than the original watermarked image file size. Those values were recorded in the table below.

TABLE 21. Average file size comparison between the compressed watermarked images against Facebook and Twitter with the original watermarked image of SSWLBP

Facebook			Twitter		
Filesize (bytes)	**Difference**	**% difference**	**Filesize (bytes)**	**Difference**	**% difference**
530,920	Smaller	95.10%	1,208,441	Smaller	88.93%

TABLE 22. Average file size comparison between the compressed watermarked images against Facebook and Twitter with the original watermarked image of HSSVD

Facebook			Twitter		
Filesize (bytes)	**Difference**	**% difference**	**Filesize (bytes)**	**Difference**	**% difference**
66,104	Smaller	55.44%	198,827	Larger	41.43%

HSSVD watermarked images also been compressed, but here are some twist. The watermarked images that went through uploading and downloading processes by using Facebook were reduced in file size, at an average of 55.44% smaller than the original watermarked image. However, the watermarked image that went through the uploading and downloading processes by using Twitter had increased in the file size. It became larger, at an average of 41.43%. These were a result of the reconstruction process of JPEG compression.

On the other hand, SSWLBP watermarked images downloaded from Facebook were having some difficulties, where the downloaded watermarked images tend to lose their crucial properties, which is image resolution. It was shown that the downloaded watermarked images were having 2,048 × 1,152 pixels of image resolution, at about 73% smaller than the original 4,000 × 2,250 pixels for SSWLBP watermarked image. The image resolution had been cut down by Facebook is because that the original watermarked image had a huge number of pixels inside it, making Facebook to compress each image into a maximum resolution set-up by Facebook itself.

Facebook wants to reduce the bandwidth required for those images to be displayed on the web page, thus increasing the performance of Facebook.

Compression is everywhere. It is a noble act to reduce the image size into a smaller size, without interfering the presentation of the pixels. However, this method has a tendency on corrupting the most valuable information embedded inside the image. It is not focusing only to the embedded watermark, but it applies to all aspect of information stored inside the image itself. For example, the metadata stored inside the image. The compression implemented by social media tends to remove all of the valuable information in order to save the storage and to reduce the bandwidth. It is a good measure, but in terms of preserving ownership and copyright of the image, it is bad. Therefore, it is assumed that all social media could not preserved the originality of the uploaded image, thus making all of the image presence inside their server to be unknown, and no one could ever claim that those images are theirs.

H. Experiment H: Results Comparison of Experiment F and G

This experiment is an analysis experiment, which includes the comparison of results gathered between Experiment F with Experiment G. It is to observe the difference between the results accomplished by both experiments.

From both experiments, it is observed that both experiments had successfully abolished the embedded watermark inside every watermarked image. It is because the compression made by both JPEG compression and social media compression tends to compress everything inside the image, thus messed up with the embedded watermark. Both JPEG and social media compressions falls into the same compression category, which is lossy compression. As been well-known, lossy compression will remove all values inside the file, but preserving the presentation of the image. Table below shows the summary of the presence of the embedded watermark inside the compressed watermarked image.

TABLE 23. Summary of the presence of the embedded watermark inside the compressed watermarked image

	Experiment F		**Experiment G**	
	SSWLBP	**HSSVD**	**SSWLBP**	**HSSVD**
Presence of embedded watermark inside the compressed watermarked image	×	×	×	×

Therefore, it can be concluded that both watermarking techniques could not withstand against compression attack done by both JPEG and social media.

X. CONCLUSION

The first objective of this research had been resolved by briefly explained the literature review of robust digital watermarking techniques against compression attack. The second objective also had been successfully done by testing and applying the chosen digital watermarking techniques that were robust against compression attack, which are SSWLBP and HSSVD. The watermarking processes that involved both techniques were done in the MATLAB environment. All other experiments were done outside MATLAB environment. The third objective was also achieved, where the analyses of the results of each experiment using both watermarking techniques were done.

REFERENCES

[1] M. A. F. Jeffry and H. Kutty Mammi. (2017). A Study on image Security in Social Media Using Digital Watermarking with Metadata. *2017 IEEE Conf. Appl. Inf. Netw. Secur.* 118-123.

[2] J. P. Maheshwari, M. Kumar, G. Mathur, R. P. Yadav, and R. K. Kakerda. (2015). Robust Digital Image Watermarking using DCT based Pyramid Transform via image compreSSIon, 0-4.

[3] M. S. Goli and A. Naghsh. (2017). Two-Step Sudoku, no. Ipria, 237-242.

[4] Z. Wenyin and F. Y. Shih. (2011). Semi-fragile Spatial Watermarking Based on Local Binary Pattern Operators. *Opt. Commun.*, 284(16-17), 3904-3912.

[5] K. Meenakshi, C. Srinivaso, and K. S. Prasad. (2014). A Fast and Robust Hybrid Watermarking Scheme Based on Schur and SVD Transform. *Int. J. Res. Eng. Technol.*, 03(16), 7-11.

[6] C. He. (2016). Research of Web Resources Protection Based on Digital Watermarking and Digital Signature.

[7] W. Puech. (2008). Encryption and Compression for Medical Image Security, 8-9.

[8] A. Furqan and M. Kumar. (2015). Study and Analysis of Robust DWT-SVD Domain Based Digital Image Watermarking Technique Using.

[9] R. Kumar, D. Kumar, and M. J. Alam. (2015). Experimental Studies of LSB Watermarking with Different Noise. *Procedia -Procedia Comput. Sci.*, 54, 612-620.

[10] S. Kumar and A. Dutta. (2016). A Study on Robustness of Block Entropy Based Digital Image Watermarking Techniques with respect to Various Attacks, 1802-1806.

[11] G. S. Ammar and W. B. Gragg. (1987). The Generalized Schur Algorithm for the Superfast Solution of Toeplitz Systems, 315-330.

[12] M. Salleh, S. Ibrahim, and I. Isnin. (2012). Image Encryption Algorithm Based on Chaotic Mapping, *J. Teknol.*, 39(D), 1-12.