Robust Watermarking Techniques against Compression Attack

To cite this article: Mohd Aliff Faiz Jeffry and Hazinah Kutty Mammi 2020 IOP Conf. Ser.: Mater. Sci. Eng. 884 012058

View the article online for updates and enhancements.

You may also like
- A Zero-Watermark Hybrid Algorithm for Remote Sensing Images Based on DCT and DFT
  SiMing Xing, Tong Yi Li and Jing Liang
- Remote Sensing Image Zero-Watermark Algorithm Based on Remd
  SiMing Xing, Zhilin Cheng, ChunYu Ji et al.
- An Improved Mapping Pattern for Digital Watermarking using Hilbert-Peano Pattern
  Mohamad Nazmi Nasir, Syifak Izhar Hisham and Mohd Faizal Ab Razak
Robust Watermarking Techniques against Compression Attack

Mohd Aliff Faiz Jeffry¹ and Hazinah Kutty Mammi²
¹,²School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, Skudai, Johor, MALAYSIA

E-mail: alyffpro@gmail.com, hazinah@utm.my

Abstract. Digital watermarking is a way to protect digital images from malicious attacks. Compression attack is one of the most common attacks on images uploaded to social media. Social media, such as Facebook and Twitter, have implemented a compression method for all types of media before being successfully uploaded to their server. It is designed to reduce the network bandwidth and storage needed to store each media on their server. However, the compression method used tends to tarnish the image properties of the image itself, which can be used to identify the image itself. This causes another problem, namely ownership and copyright issues. The use of digital watermarks was therefore proposed for this research to avoid the problem identified. The selected digital watermarking techniques, which are DCT-based Pyramid Transform (DCTPT), Two-Step Sudoku Method using LSB (TSSLSB), Semi-fragile Spatial Watermarking based on Local Binary Pattern Operator (SSWLBP) and Hybrid Schur and Singular Value Decomposition (HSSVD), theoretically must be able to withstand compression attacks by social media. These techniques have been simulated using the default MATLAB image dataset, but the use of photos taken by smartphones is a must for us to obtain useful metadata for real-world implementations. Some comprehensive analyses of the watermarking algorithms were done, and the findings were recorded in this paper.

1. Introduction
Social media becomes a very popular platform for sharing experiences, thoughts, and ideas. Social media is defined as a collection of an online interactive communication channel, dedicated to community-based input, users’ interactions, content-sharing, and collaboration. The number of social media users around the world increases gradually, resulting in an instant increase of images uploaded into each social media platform. This situation creates some severe problems in our 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 issue. Therefore, to attain better security protection against malicious attacks towards images, a robust technique must be applied. Digital watermarking were used for this research in examining the robustness of selected digital watermarking techniques 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 [2]. 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 two 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 [3], Two-Step Sudoku Method using LSB [4], Semi-fragile Spatial Watermarking based on Local Binary Pattern (LBP) Operator [5], and Hybrid Schur and Singular Value Decomposition (SVD) [6]. 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 can withstand against compression attack done by social media.

2. Problem background
There are three main issues to be highlighted in this research. The issues are ownership issues, copyright issues, and identity fraud. These stumbling blocks were produced from this research’s main problem, which is a compression attack. Referring to the previous section, each social media platform had implemented a 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 of using a 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 was 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 tend to delete all useful information that is used to identify each image and videos, uniquely. Therefore, issues regarding ownership and copyright of the images and videos cannot be tolerated, as there is no information and proves to be used in identifying both images and videos. By applying digital watermark, it is inferred that digital watermark can preserve the image properties that are used to identify the ownership and copyright of every image.

Identity fraud is another complex problem, where an attacker can use 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 to 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 preserve the image properties for forensic investigations.

3. Digital watermark
Digital watermarking was not a new thing in Information Technology (IT) areas. It is widely known and is currently developing to cater different collections of threats. As for definition, digital watermarking is a way of embedding trusted information into a medium that is used as a display, as shown in Figure 1. 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.
There is a tremendously huge collection of digital watermarking techniques that had been proposed and proved of its functionalities in deterring several image attacks, such as, but not limited to, image compression, image cropping, and image manipulation. Another application of digital watermarking includes copyright protection, fingerprinting, tracking, temper detection, broadcast monitoring, and completeness [7]. As been mentioned in our previous paper [1], digital watermarking is best suited for preserving copyright and ownership of the image. We also mentioned that by applying digital watermarking techniques to the image, fraud activity also can be reduced [1]. However, in 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 is in other words, the 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 against compression attack.

4. Compression attack

Every file format in the computer system is prone to be compressed by a certain compression algorithm. It can be compressed by using either a lossy compression format or a lossless compression format. Both compression format furnishes the same concept of compression, but with different techniques. Lossy compression would squeeze everything inside the file, by using a mathematical algorithm, thus produces a very small file size. But here are the cons; it tends to tarnish certain useful information regarding the compressed file. For example, in our case, an image had been compressed, resulting in very small file size, but with certainly visible pixels gone in the compression process. This technique is good, in terms of reducing the file size to save storage spaces, but it is not in terms of preserving the properties of the image. The example of a lossy compression format is JPEG. On the other hand, lossless compression format does the same compression as lossy compression, but without tarnishing every single bit of the information. The algorithm preserved everything, and the file size of the compressed file is reduced. The example of a lossless compression format related to this research is Portable Network Graphic (PNG).

This research focusses on the compression technique applied by two main platforms of social media, which are Facebook and Twitter. Both social media uses certain compression algorithms, that acts as a medium to compress every media, including photos, videos, and audios. Based on my previous research in [1] and [2], each image uploaded into Facebook and Twitter will be compressed into an average of 87% and 91% smaller than the original image, respectively. The image presentation comparison between original and uploaded images was different [2], as the compression rate used by both Facebook and Twitter high. This is measured using Error-Level Analysis (ELA), where it shows differences between two visibly identical images. It shows a vast different between original and compressed image.

Therefore, the attention of this paper is to demonstrate other watermarking techniques that are claimed to be robust enough against compression attack, either JPEG compression attack or social media compression attack.

**Figure 1. Digital watermarking process**
5. Comparison of each technique against several image attacks

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 [6]. 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 [3]. 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 [3]. 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 [8]. 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 [4]. This technique is a hybrid implementation of sudoku methodology with LSB technique. Based on the watermarking processes explained in [4], 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 [4]. 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 [5]. 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. 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 [5].

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 [6]. 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 [6][9]. 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 [6]. 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 1 and Table 2. Table 1 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 1. Performance-wise versus security-wise offered by each watermarking techniques

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

Based on Table 1, 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 2 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 2. Robustness comparison against several image attacks for each watermarking techniques

| Techniques | Cropping | Noise | Blurring | Sharpening | Compression |
|------------|----------|-------|----------|------------|-------------|
| DCTPT      |          | -     |          | -          | ✓           |
| TSSLSB     |          | ✓     |          | ✓          |             |
| SSWLBP     |          | ✓     |          | ✓          | ✓           |
| HSSVD      | ✓        | ✓     | ✓        |            | ✓           |

By referring to Table 2, 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 2, 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 2, it is observed that only DCTPT, SSWLBP, and HSSVD that are robust enough compression attack.

6. Proposed experiment design

This research focusses on experimenting with chosen watermarking techniques that were claimed to be robust enough against compression attack. This will be done to prove the claimed made by those watermarking techniques authors. Therefore, for this research, after a comprehensive comparison study of all watermarking techniques, two from four techniques were chosen, which are SSWLBP and HSSVD. Both watermarking techniques offer good protection against compression attack, thus making us choose both techniques for our research.
Several experiment designs that had been constructed, including analysis of sample images and analysis on watermarked images. However, the main experiment is to observe the compression attack of social media onto watermarked images, by watermarking a set of 30 images using two different watermarking techniques, and then upload it into two most popular social media, which are Facebook and Twitter. All uploaded watermarked images will then be downloaded back and save into the computer for the watermarking extraction process. If the embedded watermark is present, then the watermark technique is considered robust against the social media compression attack. However, if the embedded watermark is damaged and cannot be extracted from the watermarked image, then it can be concluded that those watermarking techniques do not robust against the compression attack, leaving several questionable thoughts against their claimed statements. Although it might happen in our incoming phases of this research, a thorough analysis of those results must be done.

Parameters used to measure robustness against compression attack are Mean-Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). Both MSE and PSNR will compute compression between two visually identical images. The MSE measures the cumulative squared error between the compressed image and the original image, while the PSNR is a measure of the peak error. The lower the MSE value, the lower the error rate. In order to compute PSNR as been shown in Equation (2), we must calculate the MSE of the first block of the image, as in Equation (1) below.

\[
MSE = \frac{\sum_{M,N}[l_1(m,n) - l_2(m,n)]^2}{M \times N}
\]  

\[
PSNR = 10 \log_{10} \left( \frac{R^2}{MSE} \right)
\]  

The higher the PSNR, the better the quality of the compressed image. As been claimed by authors of both watermarking techniques, SSWLBP produces a high value of PSNR, which is 42.67 [5], and PSNR or 65.123 for HSSVD [6]. Based on both PSNR values from both techniques, it is assumed that those techniques may withstand against compression attack.

7. Expected outcomes
As for our first observation of the chosen watermarking techniques, it is assumed that both SSWLBP and HSSVD could withstand an attack on social media compression. Authors of both techniques believed and guaranteed that their techniques are robust against a compression attack. All techniques must, therefore, be carried out through MATLAB and the robustness against the compression attack for both watermarking techniques must be reported and analysed.

8. Conclusion
A comparison of four watermarking techniques was discussed. Two robust watermarking techniques were chosen, based on the characteristics and robustness offered against the compression attack. Further analysis and practice of the chosen watermarking techniques will be carried out next, following the proposed design of the experiment, as previously stated.
References

[1] M. A. F. Jeffry and H. Kutty Mammi, “A study on image security in social media using digital watermarking with metadata,” 2017 IEEE Conf. Appl. Inf. Netw. Secur., pp. 118–123, 2017.

[2] M. A. F. Jeffry, “A Study on Image Security in Social Media using Digital Watermarking with Metadata,” 2017.

[3] J. P. Maheshwari, M. Kumar, G. Mathur, R. P. Yadav, and R. K. Kakerda, “Robust Digital Image Watermarking using DCT based Pyramid Transform via image compression,” pp. 0–4, 2015.

[4] M. S. Goli and A. Naghsh, “Two-Step Sudoku,” no. Ipria, pp. 237–242, 2017.

[5] Z. Wenyin and F. Y. Shih, “Semi-fragile spatial watermarking based on local binary pattern operators,” Opt. Commun., vol. 284, no. 16–17, pp. 3904–3912, 2011.

[6] K. Meenakshi, C. Srinivaso, and K. S. Prasad, “A Fast and Robust Hybrid Watermarking Scheme Based on Schur and SVD Transform,” Int. J. Res. Eng. Technol., vol. 03, no. 16, pp. 7–11, 2014.

[7] R. Kumar, D. Kumar, and M. J. Alam, “Experimental Studies of LSB Watermarking with Different Noise,” Procedia - Procedia Comput. Sci., vol. 54, pp. 612–620, 2015.

[8] S. Kumar and A. Dutta, “A Study on Robustness of Block Entropy Based Digital Image Watermarking Techniques with respect to Various Attacks,” pp. 1802–1806, 2016.

[9] G. S. Ammar and W. B. Gragg, “The generalized Schur algorithm for the superfast solution of Toeplitz systems,” pp. 315–330, 1987.