Evaluation of Perceptual Hashing Algorithms Against Image Manipulation Over Social Media Platforms

Mohammed Alkhowaiter
Electrical and Computer Engineering
University of Central Florida
Orlando, United States
mok11@knights.ucf.edu

Khalid Almubarak
College of Computer Engineering and Science
Prince Sattam University
Al-Kharj, Saudi Arabia
k.almubarak@psau.edu.sa

Dr. Cliff Zou
Department of Computer Science
University of Central Florida
Orlando, United States
changchun.zou@ucf.edu

***Abstract*—Perceptual hash is a fingerprint of a multimedia file derived from features of its content. In defending against image-based fake news, compared with crypto hash, perceptual hash shows its advantage in detecting image manipulation while still being able to identify the same images that have different format or resolutions. However, most of prior perceptual hash research used general image datasets for testing, e.g., CASIA, without considering real application environments. Because of the rampant and serious threat of fake news in social media platforms, in this paper, for the first time we evaluate and analyze seven state-of-art perceptual hash algorithms in detecting image manipulation in three major social media platforms: Facebook, Twitter and Instagram. These platforms, like others, utilize different processing on user-uploaded images upon sharing, such as compression, scaling, etc. Our real-world image evaluation and analysis shows the contrast on the three platforms' image processing and performance comparison of those seven algorithms in detecting image manipulation. Furthermore, we present an approach to find the optimal detection threshold for each algorithm when being used for social media platforms.**

***Index Terms*—perceptual hashing, image authentication, social media, fake news defense**

I. Introduction

Social media platforms—Facebook, Instagram, Twitter, etc.—speedup the spread of information over the well-connected cyber world. However, at the same time that connection helps to forge misinformation that can quickly reach a massive number of people. Propagation of fake information and news can lead to deception, emotional distress, and influenced public opinions and actions. An investigation into the truth of news on Twitter from 2006 to 2017 showed that falsehood diffuses faster and deeper than truth [1]. The risk of misinformation increases during great events. A study on fake images on Twitter during Hurricane Sandy (2012), [2] showed that around 90 percentage of retweets were from tweets of fake images. These fake images not only mislead users but also can contain malicious URLs. Fig. 1 shows an example of a fake image that spread during Hurricane Sandy in which a shark was photoshopped in the street.

Nevertheless, most social media platform users are simply not aware of the risk of re-sharing information from unknown sources. Hence, it is impossible to prevent the spread of disinformation without an automation technique, and a solution that decreases internet misinformation is urgently needed. Today, most platforms have taken steps to reduce misinformation by verifying their user accounts and adding colored verified badge next to authentic accounts. For instance, the US 2020 presidential election and COVID-19, social platforms [3,4] labeled the misinformation posts.

Fig. 1. Faked image during Sandy Hurricane 2012

Image authentication systems were researched over past years, and they are introduced for different purposes such as image duplicates, image search engines such as TinEye [9], and digital forensics. These systems use perceptual hashing since cryptographic hashing is an avalanche effect and images upon transmission are vulnerable to a bit change. Perceptual hashing, on the other hand, are tolerated with these effects and other processing such as compression, scaling, blurring, rotation, etc. It generates a fingerprint of an image by analyzing and extracts features of the image that can be invariant under various attacks. These features then are taken to finalize the hash value, and this value is compared with the tested image hash value to make a dection whether the tested image is similar, tampered with, or different.

Social media platforms automatically altered images upon sharing for many reasons i.e. images are re-scaled and compressed for saving room on the servers and each platform shares its preferences of image sizes [7]. This means that upon sharing your image the social media platform will resize it to

fit its preference dimension. For instance, an image of the size 3000x2000 pixels will be downscaled by Facebook into 1875x1250, by Instagram into 1080x720, and by Twitter into 680x453. This diversity of scaling is one of the image attacks that distinguished systems suffer from while authenticating the images.

Many academic researchers [11-17] work on image authentication using perceptual hashing approach and reached high value of robustness in preventing one or more image attacks. In the survey paper [8], Ling et al. classified the images attacks into two branches: (1) content-preserving manapulations that do not change an image's content such as compression, brightness reduction, resolution reduction, scaling, color conversion, and (2) content-changing manapulations that change an image's content i.e. removing image objects (persons, objects, etc.), moving of image elements, changing their positions, adding new objects, etc. Research to distiguash between these two attack branches are still open and most acadmic researches used known dataset such as CASIA [6] and USC-SIPI [10] as testbed.

Therefore, to our best knowledge, this paper is the first paper to evaluate state-of-art perceptual hashing algorithms over social media platforms: Facebook, Twitter, and Instagram images. This evaluation will redesign seven algorithms [11-17] and pass a set of images through these systems to check the robustness of their authentication based on a metric algorithm we introduce in this paper. The testbed of this evaluation will use real images from the platforms that we generated. This assessment will help in developing an image authentication platform for social media images in future work.

In summary, the contributions of this paper are:

- Present and apply the state-of-arts perceptual hash algorithms on social media platforms image for image authentication.
- Evaluate and compare the performance of seven state-of-art perceptual hash algorithms on three major social media platforms.
- Present approach to find optimal detection threshold for detecting image manipulation on social media platforms.

The structure of the paper is as follows: we discuss our methodologies in implementing perceptual hashing algorithms. Next section III, we discuss our evaluating method. In section IV, we show the results using different metrics. Finally in Section V, we provide summary of our work and conclude with future enhancement in image authentication.

II. METHODOLOGIES

Many researchers developed image hashing systems that defend against one or more image attacks. Different approaches and algorithms are applied in their systems to reach the best image hashing, i.e., robust against content-preserving attacks. Ling et al. classified the techniques of image hashing based on five approaches proposed in the publications: (1) Invariant feature transform methods that extract image features from transform domains and then make use of the coefficients to create the hash; (2) Local feature points such as corners, edges, salient regions, etc.; (3) Dimension reduction method where robust features are extracted from embedding the low-level features of the high dimensional space into a lower dimension, (4) Statistical feature-based approach where calculation of image statistics, such as histogram and mean, are the feature from the image; and (5) Learning-based method that applies machine learning for image feature extracting and authentication.

Based on reviewing selected papers and approaches, we pipelined the perceptual hashing processes into three stages represented in Fig. 2.

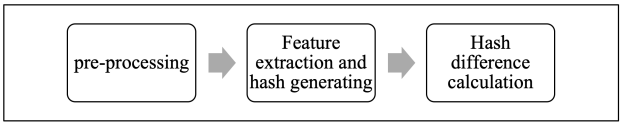

Fig. 2. Scheme of any perceptual hash system for image authentication

A. Preparing the images: (pre-processing) stage

efore images are followed on the above approaches, they pass through different enhancement lines to normalize the images in the best representation and for robust features. The common enhancement is resizing the image into fixed and small sizes to speed up the operation. Usually, it is resized into square MxM with the size of $128x128$ using the bilinear interpolation method. Another enhancement is converting the color space domain from one form to another, such as from RGB to CIE $L*a*b*$ [16], and $L*$ is only used for feature extraction because it matches human perception of lightness and is more stable. The grey-scale conversion is desirable for most developments due to its simplicity when dealing with $1-D$ instead of $3-D$ channels in RGB. Filters sometimes are applied such as Gaussian and bilateral [17] filters to remove regular noises.

B. Feature extraction and hash generating stage

Choosing among the best of state-of-arts perceptual hash algorithm modules [11-17], we focus on reviewing and re-developing these seven modules that cover state-of-art algorithms DCT, Marr-Hildreth, Wavelet, SVD, RPIVD, QFT. Each of the algorithms is adaptive in an image hashing scheme design to generate the hash value that will be used at the next stage, and respectfully short definitions are provided below.

1) DCT: Discrete Cosine Transform (DCT) [11] is one of the popular algorithms that was well implemented for image compression and hashing in the last two decades. This method is invariant feature transform-based, i.e., it can represent the image in uniqueness with small data. Basically, DCT operates on a function at a finite number of discrete data points. These data were evaluated in terms of the sum of cosine functions with different frequencies to convert it from the spatial domain to the frequency domain.

2) Wavelet: the introduction of the DCT led to the development of wavelet coding DWT that also takes a large volume of researches. Many researchers use one of those frequency domains for feature extraction such as Tang et al.[11] and

Venkatesan et al. [13].

3) Marr- Hildreth: Marr-Hildreth is an edge detection based on local feature points. The technique of extracting the edges has different approaches, but Haldo et al. [12] implemented it by convolving the image with a Gaussian kernel and then approximating the second derivative (Laplacian) with a 33 kernel. Afterward, they found the zero crossings of the filtered image in order to generate a binary image.

4) SVD: Singular Value Decomposition (SVD is another algorithm implemented by Kozut et. al. [14] that follows the dimension reduction method. Kozut et al. introduced a pseudo-random (PR) signal representation scheme that views images as linear matrices [A1, ..., Ap]. Each Ai is represented as a matrix corresponding to the PR location chosen from that image that will be decomposed later to generate the secondary image that consists of invariant feature vectors that are used to create the hash value. The image hashing is created by SVD against multiple attacks like rotation, crop, and compression.

5) Visual Model-Based: Wang et al. [15] in their paper propose a perceptual image hash method for content authentication. They combine a statistical feature-based approach with visual perception using Watson's visual model theory. Watson's visual model is used in order to preserve sensitive features that are important for humans perceiving image content processing. On the other hand, key-point-based features and image-block-based features are used to generate the intermediate hash by extracting key-point-base features using input image to SIFT algorithm. To achieve this, the proposed method comprises two main stages: 1) Hash Generation Algorithm and 2) Tampering Detection and Tampering Localization. The module is against different image attacks, including geometric attacks. *6) RPIVD:* Tang et al. [16] designed a robust image hashing using Ring Partition and Invariant Vector Distance (RPIVD) that is considered a statistical feature-based approach. Basically, their module is processed in three stages: (1) preparing the image by bilinear interpolation resizing into MxM, low pass filtering, and converting the color space from RGB to CIE $L*a*b*$ in order to take $L*$, (2) partitioning the image into equal rings which they choose 512 rings, (3) applying four statistical measures (mean, variance, skewness, and kurtosis) to each ring. This paper provides robust image hashing against several attacks but most strongly against rotation.

7) QFT: Yan et al., in their paper [17], introduced another perceptual hashing approach that used Quaternion Fourier Transform (QFT) to construct feature hash, and QFMT to construct geometric hash. QFT is considered an invariant feature transform-based method that extracts image features from both color and structural information to form a quaternion image to produce the hash. QFT is capable of defending against common image attacks and performs excellently at detecting and locating various types of attacks.

C. Hashes difference: (Similarity metric) stage

After the generation of perceptual hashing, images can be authenticated based on the different values. There are multiple metrices for perceptual hashing comparison, however most of the above-mentioned approaches follow one of two metrics for measuring: Hamming distance [11-14] and Euclidean distance [15-17]. The threshold T is set by each algorithm to distinguish whether the distance value is less or equal to the threshold value and images are similar or images are tampered with or different. Smaller T is better and more secure, especially for image revising over huge datasets to reduce collision probability. Therefore, the best system algorithms are those that can authenticate the received image with a small T and give the malicious images a high distance value.

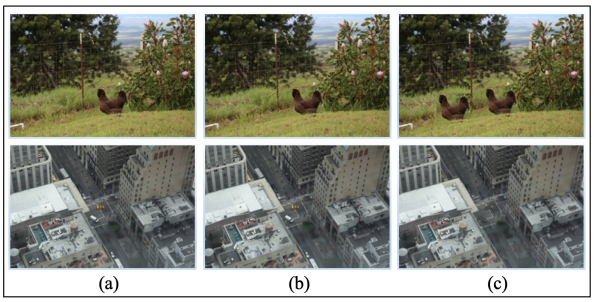

Fig. 3. Samples of images in the dataset for evaluation: (a) original images; (b) posted and then downloaded as is; (c) images tampered, posted, and then downloaded

III. PROPOSED IMAGE EVALUATION

Social network platforms: Facebook, Instagram, and Twitter apply such image enhancements as scaling, compression, brightness reduction, and contrast. Each platform has different image effects upon posting for storage preference and transmission. To analyze the processing on each platform, we upload an image, and then we download the image again. From these steps, we found out that each downloaded image has different sizing, different scale, different smoothness, different quality. From the visualization, Facebook effects the image less than other platforms from first analysis.

The scheme of the evaluation approach that we follow is shown in Fig. 3, and seven approaches are applied to each test for comparison. The first step of evaluation is collecting the dataset for testing by preparing a collection of images from their original sources (cameras). Samples of the dataset represented in Fig. 4, and they are scaled down to ease the uploading process to the platforms. Each image is shared on each platform, and then it is downloaded. The downloaded images are manipulated by adding some content and then they are shared again to each social media platform. Again, the manipulated images are downloaded. Now, we collect nine images as original, nine images downloaded from social media as they are posted, and nine altered images that are reposted and downloaded. There is a limitation in collecting images because each image has to go through multiple processes starting by using real accounts in social media platforms, uploading/downloading, altering, uploading/ downloading again, which it will take a while to generate a massive dataset.

The second step of the approach is preparing the algorithms that will generate the perceptual hash for images. We choose seven modules based on state-of-art approaches [11-17], most

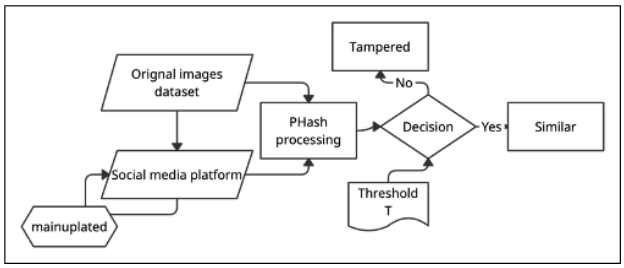

Fig. 4. Scheme of social networking images evaluation

recognized algorithms for the last decade and the technique that the algorithms follow among five approaches that Ling et al [8] classified, excluding the learning-based approach. The majority of approaches are reverse-engineered and [11-13] are provided as open sources [5] [18]. The decision making is chosen based on the thresholds set by the original founders [15-17] which are 0.25, 0.25, 0.004, 0.0008, 5.0, 200, and 0.8, respectfully. Afterward, the evaluation of the proposed methods measured by the division of altered images hashing over similar images hashing as shown by equation (1):

$$diff = ph_{alter}/ph_{similar} \tag{1}$$

The perceptual hash distance, phsimilar in Equation (1) refers to the Hamming distance or Ecludian distance value between the original image (Fig.4a) and social media downloaded and unaltered image (Fig.4b). The smaller value of phsimilar is better, which means the perceptual hash algorithm is able to detect that the downloaded image from the social media platform is unaltered from the original image besides the image processing that social media platforms add upon posting such as compression and resizing. On the other hand, the perceptual hash distance, phalter refers to the Hamming distance or Ecludian distance value between the original image (Fig.4a) and social media downloaded and altered image (Fig.4c). The larger value of phalter is better, which means the perceptual hash algorithm can detect an altered image used in the social media platform.

The diff value calculated in Equation (1) reflects how well the perceptual hash algorithm can detect image alteration when an image is used in a social media platform. A good perceptual hash algorithm should have a large diff value for a better decision-making whereas the small diff value will make it hard to choose the threshold. Therefore, it will create wrong decision-making, hence, increasing the false-negative and false-positive rate.

Equations (2) and (3) represent the false-negative rate (FNR) and false positive rate (FPR) respectfully. FN calculates by dividing FN over the summation of FN and true positive (TP). On contrast FP calculates by dividing FP over the summation of FP and true negative (TN). The smaller rate of either FN or FP indicate the robustness of the authentication of each algorithm.

$$FNR = FN/(FN + TP) \tag{2}$$

$$FPR = FP/(FP + TN) \tag{3}$$

IV. EXPERIMENTAL RESULTS

In this section, we use our above proposed evaluation scheme to evaluate those algorithms. We implemented and tested the scheme using Python (3.8.5) and famous libraries such as OpenCV [18]. DCT, DWT, and Marr-Hildreth are provided in the library, where the four remaining approaches are re-implemented as they are described in these publications [14-17]. We ran the tests on a computer with Dual-Core CPU, Intel i5 @ 2.7GHz, 4.0G RAM.

A. Evaluation based on algorithms' original decision thresholds set by their authors

Following the scheme in Fig. 3, we generated 378 tests equally distributed by the seven perceptual hash algorithm modules [11-17]. These tests are calculated by using the 9 images since each platform perceptually twice hashes these 9 images: one to calculate the Phsimilar (Fig.4a Vs Fig.4b) and the second for Phalter (Fig.4a Vs Fig.4c) in total of 54 tests for the three platforms. Afterward, these outputs are summarized and shown at Tables II and III. The minimum score, (min) in the following tables means the lowest perceptual hashes value among the nine tests at each approach and platform. The average, (avg) indicates the average of nine tests under each algorithm and platform, and finally the maximum, (max) refers to the highest perceptual hash among the nine evaluations at each algorithm and platform.

The summarization of the perceptual hashing distance of seven algorithms modules is shown in Table I. This table shows the evaluation of phsimilar of images group (A&B) in Fig 4. In addition, the perceptual hashing difference values for the altered images using groups (A&C) in Fig 4 is represented too. The threshold in table T directly brought from the original papers presenting those perceptual harsh algorithms [11-17]. If the perceptual hash value exceeds the threshold, it produces a false-positive since the image is supposed to be authentic. Among these modules, DCT, Wavelet, and SVD broke the threshold limits in some tests. On the other hand, Marr-Hildreth (Mar-Hld), Visual Model-Based (Vsul M-B), RPIVD, and QFT kept remaining under their threshold values. Also, in the table we can obviously note that Facebook in all tests has the least gap values with the threshold compared to others. Overall, SVD is the worst in the table at authentication since the remainder of algorithms are partially or completely successful such as Visual Model-Based. Table III shows excellent measurements of false-negative and false-positive at each approach.

Fig. 5 represents the percentage values of different images hashes (A&C) from Tables II-IV to similar image hashes (A&B) using Equation (1). From the chart, Facebook has the highest percentage gap at the seven algorithms since it creates lowest manipulation to user-uploaded images upon sharing. Instagram and Twitter show the same average differences at most algorithms and show little difference at DCT, RPIVD, and QFT. The percentage at QFT reaches the top particularly at Facebook and this is due to the perceptual hashing results of A&B images.

TABLE I
PERCEPTUAL HASHING COMPARISON BETWEEN THE ORIGINAL IMAGES (FIG.4A), THE POSTED IMAGS (FIG.4B), AND ALTERED IMAGES (FIG.4C) ON SOCIAL MEDIA PLATFORMS

Algorithm	T	Facebook						Instagram						Twitter					
		min		*avg*		*max*		*min*		*avg*		*max*		*min*		*avg*		*max*	
		a-b	a-c	a-b	a-c	a-b	a-c	a-b	a-c	a-b	a-c	a-b	a-c	a-b	a-c	a-b	a-c	a-b	a-c
DCT	0.25	0	0.125	0.04	0.444	0.25	0.75	0	0.125	0.20	0.402	0.37	0.75	0	0	0.08	0.458	0.25	0.75
Mar-Hld	0.25	0	0.083	0.02	0.201	0.05	0.347	0.02	0.097	0.07	0.205	0.15	0.375	0.02	0.069	0.10	0.232	0.20	0.402
Wavelet	0.004	0	0	0.031	0.003	0.093	0.031	0	0	0.031	0.003	0.093	0.031	0	0	0.003	0.031	0.031	0.093
SVD	0.0008	0.001	0.004	0.003	0.010	0.008	0.023	0.004	0.004	0.004	0.009	0.015	0.023	0.005	0.004	0.004	0.012	0.007	0.023
Vsul M-B	5	1.02	6.80	1.44	8.98	2.40	10.75	1.41	6.80	2.09	8.99	3.02	10.77	1.17	6.78	2.15	8.98	3.57	10.74
RPIVD	200	2	57	8	243.33	20	601	5	57	19.33	243.33	46	602	6	59	28.55	244.66	74	613
QFT	0.8	0	0.03	0.007	0.3611	0.02	1.51	0.01	0.03	0.024	0.366	0.05	1.51	0	0.03	0.017	0.362	0.03	1.51

TABLE II
FALSE NEGATIVE AND FALSE POSITIVE RATES OF EACH ALGORITHM MODULE BASED ON THE ORIGINAL DECISION THRESHOLDS SET BY THEIR AUTHORS

Algorithm	FNR	FPR
DCT	12.96	11.11
Mar-Hld	0	35.18
Wavelet	5.5	16.7
SVD	38.89	0
Vsul M-B	0	0
RPIVD	0	20.37
QFT	0	50

The robust content preserving for images cares about the content that human eyes perception regardless of the little effects that happened to images without content changing such as compression. Among these algorithms, DCT, Marr-Hildreth, RPIVD, and QFT are highly affected and sensitive to the normal processing that major social media platforms apply. Therefore, they increase the gap between the platforms. On the other hand, Wavelet, SVD, and Visual Model-Based are less sensitive to the normal image processing by social media platforms indicating that they are better at image features preservation, they almost have the same gap. The highest contrast goes to QFT, RPIVD, and then DCT. Among those algorithms, Visual Model-Based shows perfect results at testing as shown in Table II and here at Fig. 5 also gives a constant flow of the three platforms.

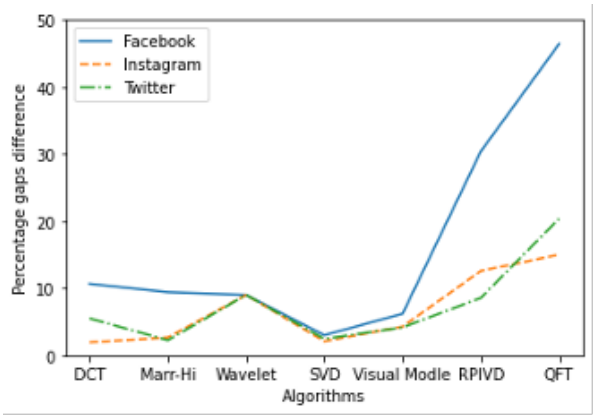

Fig. 5. Perceptual hash gaps (diff defined in Equation (1)) between similar images and tampered images

B. Finding optimal decision thresholds for social media platforms

The seven perceptual hash algorithms under study were well designed by their authors with carefully-set decision thresholds in detecting image manipulation based on specific dataset [6] [10]. However, their authors determined the decision thresholds based on general modification/manipulation operation on images. In the specific social media platform scenario under study in this paper, we want a perceptual hash algorithm to detect any deliberate image manipulation, while at the same time, not treating the image resizing/compression operation by social media platform as image manipulation. Therefore, for each perceptual hash algorithm, there should exist better decision threshold for the social media platform environment. In this section, we present the method in finding the optimal decision threshold, and then verify that the performance will be better comparing with those original decision thresholds.

We recalculate the threshold for each algorithm based on the perceptual hashes outputs through the conducted tests. Based on [17], the optimal threshold can be determined using the probability of true authentication (POTA), which essentially calculates the probability distribution of phsimilar and phalter results using the true-positive and true-negative decisions as it appears at Equations (4) and (5). Based on the threshold value, which begins with zero, the probability of true authentication for similar images, i.e., POTAsimilar, is represented by the blue line at Fig. 6 will be zero since all the images recognize as tampered, and therefore, tampered images probability, i.e., POTAtempered, is shown by the orange dashed line is one.

$$POTA_{similar} = \frac{no.\,of\,true\,positive\,results}{no.\,of\,similar\,images\,tests} \tag{4}$$

$$POTA_{tampered} = \frac{no.\,of\,true\,negative\,results}{no.\,of\,tampered\,images\,tests} \tag{5}$$

With each increase in the threshold value, the rate of true authentication for both states will change until they intersect at a certain point, as it is shown in Fig. 6, e.g., DCT with a red dot and value of 0.23. This point is selected to represent the new threshold NT where it balanced the performance of FPR and FNR. Table IV at the end shows the comparison of false-positive and false-negative rates for original thresholds OT and the new thresholds NT for all seven algorithms. The outcomes of NT show little enhancements at DCT and

TABLE III
ORIGINAL THRESHOLDS (OT) AND NEW THRESHOLDS (NT) PERFORMANCE COMPARISON

	Original Thresholds OT			New Thresholds NT		
	OT	***FPR***	***FNR***	***NT***	***FPR***	***FNR***
DCT	0.25	0.25	0.24	0.23	0.25	0.22
Mar-Hld	0.25	0	0.41	0.11	0.20	0.16
Wavelet	0.004	0.14	0.27	0.008	0.14	0.27
SVD	0.0008	0.43	0	0.0066	0.28	0.31
Vsul M-B	5	0	0	5	0	0
RPIVD	200	0	0.28	55.26	0.035	0
QFT	0.8	0	0.5	0.038	0.07	0.10

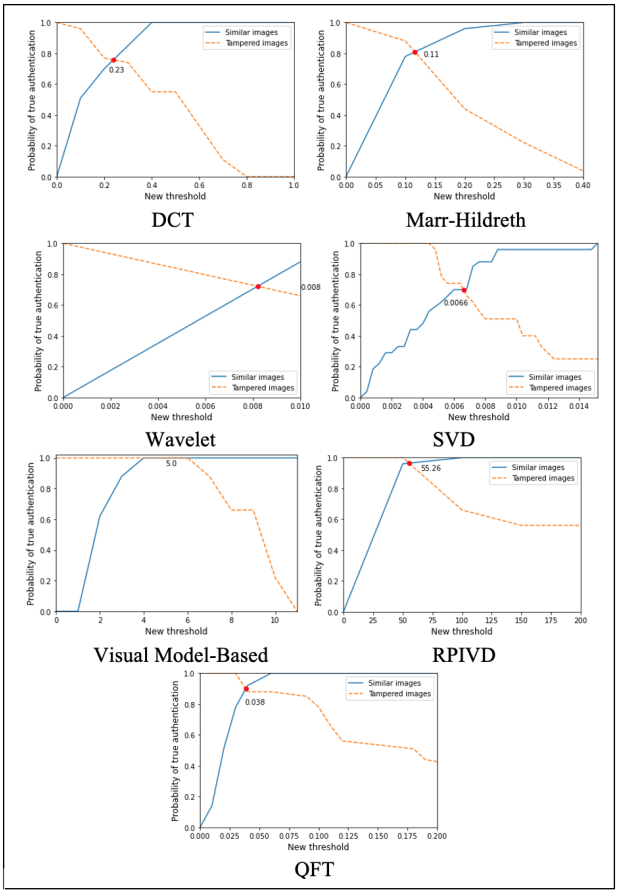

Fig. 6. The new threshold calculation for each approach

Wavelet algorithms, moderate enhancement at Marr-Hildreth and SVD, huge enhancement at RPIVD and QFT. Visual Model-Based remains the same since the performance of the original decision threshold is already fantastic.

V. CONCLUSION

We have evaluated seven approaches in the field of image authentication and perceptual hashing. This evaluation used social media platforms, Facebook, Instagram, and Twitter, as real environments to figure out the robustness and weakness of each of the seven approaches. Results show that each platform employed different image processing to the shared images and different processing factors, i.e., compression. Facebook is the least platform that applies effects on the image upon sharing whereas Twitter is the worst. On the other hand, among these approaches, Visual Model-Based is the best approach that shows great results at all platforms with zero failure, in contrast, SVD represents the worst with a high percentage of false-negatives at all platforms.

In future work, we intend to design a more robust system to verify content authentication. One interesting approach is to use a machine learning algorithm as the backbone of perceptual hashing in content authentication. In recent years, many state-of-the-art results in image classification, restoration, and denoising are achieved by applying machine learning algorithms. Most traditional perceptual hashing algorithms capture global features only, which present a vulnerability to small content alterations. However, the recent advancement in machine learning to use a convolutional neural network that considers both local and global features solves the issue. The convolutional neural network has been applied to content authentication in perceptual hashing. However, room for improvement is still applicable.

REFERENCES

[1] S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," in American Association for the Advancement of Science, 1200 New York Avenue NW, Washington, DC, 2018, pp.1146–1151.

[2] A. Gupta, H. Lamba, P. Kumaraguru, and A. Joshi, "Faking Sandy: characterizing and identifying fake images on Twitter during Hurricane Sandy," WWW 2013 Companion - Proceedings of the 22nd International Conference on World Wide Web, 2013, pp.729-736.

[3] "Facebook's Third-Party Fact-Checking Program", Facebook's Third-Party Fact-Checking Program, 2021. [Online]. Available:https://www.facebook.com/journalismproject/programs/third-party-fact-checking

[4] Y. Roth and N. Pickles, "Updating our approach to misleading information," Twitter product, 2020 [Online]. Available:https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information.

[5] "pHash.org: Home of pHash, the open source perceptual hash library", Phash.org, 2021. [Online]. Available: https://www.phash.org.

[6] CASIA, accessed on Sep. 1, 2015. [Online]. Available:http://forensics.idealtest.org/.

[7] K. Olafson and T. Tran, "Social Media Image Sizes 2021: Cheat Sheet for Every Network," Hootsuite blog, 2020, [Online]. Available:https://blog.hootsuite.com/social-media-image-sizes-guide/.

[8] L. Du, A. Ho, and R. Cong. (2019). Perceptual hashing for image authentication: A survey. Signal Processing: Image Communication.

[9] "What is Tineye," Tineye website, [Online]. Available: https://tineye.com/faq#what.

[10] (2007). USC-SIPI Image Database. [Online]. Available:http://sipi.usc.edu/database/

[11] Z. Tang, F. Yang, L. Huang, X. Zhang, "Robust image hashing with dominant DCT coefficients," Optik, Volume 125, Issue 18, 2014.

[12] H. Spontón and J. Cardelino, "A Review of Classic Edge Detectors," Image Processing on Line, Uruguay, 2015, ISSN 2105–1232c

[13] R. Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin, "Robust image hashing," Proceedings 2000 International Conference on Image Processing (Cat. No.00CH37101), 2000, pp. 664-666, vol.3.

[14] S. S. Kozat, R. Venkatesan, and M. K. Mihcak, "Robust perceptual image hashing via matrix invariants," 2004 International Conference on Image Processing, 2004. ICIP '04., 2004, pp. 3443-3446, Vol. 5.

[15] X. Wang, K. Pang, X. Zhou, Y. Zhou, L. Li, and J. Xue, "A Visual Model-Based Perceptual Image Hash for Content Authentication," in IEEE Transactions on Information Forensics and Security, July 2015.

[16] Z. Tang, X. Zhang, X. Li, and S. Zhang, "Robust Image Hashing With Ring Partition and Invariant Vector Distance," in IEEE Transactions on Information Forensics and Security, Jan 2016.

[17] C. Yan, C. Pun and X. Yuan, "Quaternion-Based Image Hashing for Adaptive Tampering Localization," in IEEE Transactions on Information Forensics and Security, Dec 2016.

[18] "Home - OpenCV", OpenCV, 2021. [Online]. Available: https://opencv.org. [Accessed: 26- Jun- 2021].