AN INTELLIGENT SYSTEM TO DETECT AND CLASSIFY THE IMAGE FORGERY ATTACKS: FACE MORPHING AND RESIZING

Nilamba vala[1], Dr. Ravi sheth[2], Mr. JatinPatel[3]

[1]School of Information Technology, Artificial Intelligence, and Cyber Security
Rashtriya Raksha University, Gandhinagar, Gujarat, India
nilamba.vala@gmail.com
[2]School of Information Technology, Artificial Intelligence, and Cyber Security
Rashtriya Raksha University, Gandhinagar, Gujarat, India
ravi.sheth@rru.ac.in
[3]School of Information Technology, Artificial Intelligence, and Cyber Security
Rashtriya Raksha University, Gandhinagar, Gujarat, India
jatin.patel@rru.ac.in

Abstract: Image forgery means the malicious modification of digital images with the intention of fraud, which hardly leaves any detectible traces to detect a forged image; we need so much information about the image (i.e., RGB, Retouching, Resize, Checksum, file name, file creation date/time, and so on). We show two attacks on image Resizing and Face morphing attack. In this paper, we check the original image's accuracy and forged image and create a report that shows the original image and forged image information. This will help layman and forensics investigators as well and will save time. We have seen images have played a major role as evidence in many crime scenes,whichwould create a significant impact in investigation and forensics analysis. This tool could also help law enforcement agencies.

IndexTerms - Image forgery, Image resizing, automatic face morphing, face image forgery detection, morphing attack

1. INTRODUCTION

With the rise of digital technologies, as images have increased day by day in our lives, the forgery of digital images has become more and more unreachable and straightforward.

With the advent of modern and efficient computer graphics editing software, which is freely available as Photoshop, GIMP, and Corel Paint Shop, the process of creating a fake image has become enormously simple.Today, this powerful image processing software allows people to modify photos and images conveniently and unperceivable. Nowadays, it creates a significant challenge to authenticate images.

Image forgery implies that the digital image is manipulated to hide some meaningful or useful information from it. The edited region is sometimes hard to identify from the original image. The detection of a forged image is guided by the requirement for originality and the integrity of the image is maintained. As shown in the image, it will classify into two methods: Active and passive. The survey has been done on existing techniques regarding forged image, and it highlights various Resizing-Resampling, Retouching & Face morphing methods based on their powerful and computational complexity. A technique of forgery detection that exploits subtle inconsistencies in the color of image illumination. The hash value is generated through image hashing for each image in the database and it can be used for retrieval of content-based image, indexing images in the database, and authenticating, avoiding, and alleviate digital images forgery. Multimedia authentication methods have emerged to verify content integrity and prevent forgery in order to ensure trustworthiness.Experimental results show that even the slightest of image tampering can be detected with the proposed technique can lead to provide authentication as the provided image is trusty.

"Resizing" refers to the change of the image's document size.On the other hand, image resamplinghappenswhen you physically change the pixel number in the image. In fact, resampling allows you to choose and select which details you would like to include in your image.

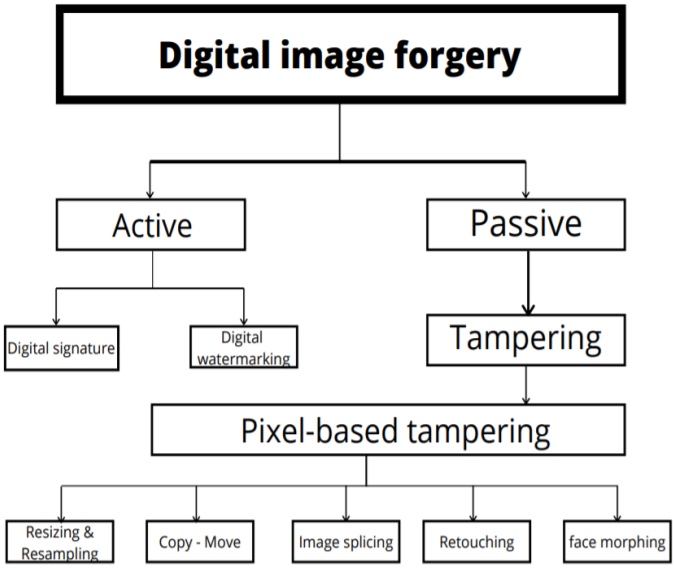

Image Retouching is known to be a less risky form of digital image forgery than other forms.In the case of image retouching,the original image does not significant changes, but there is an enhancement or reduces certain features of the original image. This technique is popular among magazine photo editors(as shown in below figure1). This type of image forgery is present in the almost all-magazine cover that would employ this technique to enhance an image's featuresto be more attractive. The fact is that such amplifications are ethically wrong.

Fig.1.Image Retouching

The idea behind Face morphing attack is to create one synthetic face image which contains characteristics of two different individuals, and to use this image on a document or as reference image in a database. Using this image for authentication, a biometriatta recognition system accepts both individuals, shown in figure2.

Fig.2. Face morphing Attack

2. LITERATURE REVIEW

In paper[1]**(Transferable Deep-CNN features for detecting digital and print-scanned morphed face images),** They suggest a novel approach to detect both digital and print-scanned morphed face images using the transferable features from a pre-trained Deep Convolutional Neural Networks. Therefore, the proposed method is based on the fusion of the first completely connected layers at the feature stage. Two D-CNN (VGG19 and AlexNet) use the morphed face picture database to be precisely fine-tuned.The proposed approach is thoroughly tested on the newly developed database for both digital and print-scanned morphed face images corresponding to bona fide and morphed data representing a real-life scenario. The results obtained consistently indicate the proposed device detection's improved performance over previously proposed techniques on both the optical and the print-scanned morphed face image database.

In paper[2] **(Accurate and Robust Neural Networks for Security-Related Applications Exampled by Face Morphing Attacks),**This paper studies the impact of various changes in training data that restrict the quantity and location of the information available for decision-making. For the specific instance of morphing attacks, they test the accuracy and robustness against semantic and black box attacks on the networks that were trained on various training data modifications. A morphing attack is an attack on a biometric facial recognition system where two different individuals with the same synthetic face picture are manipulated to match the system.

In paper[3]**(A Robust Type-I11 Data Hiding Technique Against Cropping** &**Resizing Attacks),** They propose an underrated hiding method of information that makes Watermark recovery for signals subjected to successive cropping and resampling. Using a Form - III data hiding approach with better robustness vs. rate trade-off than the standard methods under the mean square error distortion measure, they use multiple embedding of a watermark signal. The cropped-resampled signal's cyclic autocorrelation features are used to estimate the cropping quantity. They analytically showed that it is possible to restore the resampled cropped signal to the cropped signal within a limited error range. By designing white noise such as watermark signals uncorrelated with their shifted replicas, watermark detection synchronization in the cropped stego-signal is achieved. They use all-pass filters that are orthogonal to all of their cyclic shifts for this reason. By modulating the process of the cyclic all-pass filters, freedom to hide data is achieved. In addition, for both adding redundancy and achieving synchronization, they use Reed-Solomon error-correcting codes. They also address the issue of multiple cropping attacks concealing data.

In paper[4]**(Detecting Morphed Face Images),**they present a novel model to detect morphed face images. The approach proposed is based on micro-texture observation using Binarised Statistical Image Features (BSIF). A linear Support Vector Machine (SVM) is used to identify.This is the first work that uses BSIF features to solve morphed face detection to the best of our knowledge. On our newly built large-scale morphed face database with 450 different morphed face samples, comprehensive tests are performed. The database is constructed with 110 subjects of different races, ages, and gender.

In paper[5] **(Detection of Face Morphing Attacks by Deep Learning),**They recommend an approach to detecting morphing attacks based on convolutionary neural networks. They present an automated morphing pipeline based on this data to generate morphing attacks, train neural networks, and analyze their data—only precision. Compared with the accuracy of various well-known network architectures, the value of using pre-trained networks compared to networks learned from scratch is studied.

In paper[6] **(Automatic Generation and Detection of Visually Faultless Facial Morphs),**An approach to automatic visually faultless facial morph generation along with a proposal on how to automatically detect such morphs. It is attempted that with the naked eye, the generated morphs can not be recognized as such, and a reference automatic face recognition (AFR) method generates high similarity scores when matching a morph with the faces of people involved in morphing.Automatic morph generation allows for the generation of abundant experimental data, which is necessary (i) for the performance evaluation of morph rejection AFR systems and (ii) for the training of morph detection forensic systems. In this first experiment, human output reveals that it is similar to random guessing to differentiate between morphed and genuine face pictures.At the decision threshold of a 1 percent false acceptance rate in this second experiment, the reference AFR device checked 11.78 percent of morphs against any genuine images. These findings suggest that facial morphing is a significant challenge to AFR-aided access control systems and identifies the need for morphed detection approaches. The third experiment shows that this distribution of Benford features derived from JPEG compressed morphs quantized DCT coefficients is the automated detection of morphs is significantly different from that of genuine images.

In paper[7] **(Seeing is Not Believing: Camouflage Attacks on Image Scaling Algorithms),** They show an automated attack against standard scaling algorithms in this paper, i.e., to generate camouflage images automatically whose visual semantics change dramatically after scaling.They choose several computer vision applications as targeted victims to demonstrate the threats from such camouflage attacks, including multiple image classification applications based on common deep learning frameworks and mainstream web browsers.Their experimental results show that after scaling, such attacks can cause distinct visual results and thus generate an effect of evasion or data poisoning on these victim applications. They also present an algorithm that can effectively make attacks on standard cloud-based image services and trigger apparent misclassification effects, even if the image processing details are hidden in the cloud.This paper suggests a few possible countermeasures, from attack prevention to detection, to protect against such attacks.

In paper[8] **(Evading Classifiers by Morphing in the Dark),** They investigate a much more restricted and practical scenario of attacks that do not presume any of the information listed above. The goal classifier is minimally exposed to the opponent, exposing its final judgment on classification (e.g., reject or accept an input sample). In addition, by using a black box morph, the opponent can only exploit malicious samples.That is, by morphing malicious samples in the dark, the opponent must evade the target classifier. They present a scoring system that can assign a real-value score that represents progress in evasion to each sample based on limited available

knowledge.They propose a hill-climbing approach, dubbed EvadeHC, which operates without the aid of any domain-specific experience and evaluates it against two PDF malware detectors, namely PDFrate and Hidost, using such a scoring mechanism. The experimental assessment shows that their dataset's proposed evasion attacks are successful, achieving a 100 percent evasion rate.Interestingly, the known classifier evasion system that operates based on classification scores performed by the classifiers is outperformed by EvadeHC. Even though their assessments are carried out on PDF malware classifiers, domain agnostic methods are suggested and broader to other learning-based systems.

In paper[9] **(Resampling Forgery Detection in JPEG-Compressed Images),** An efficient method to discern the periodicity introduced by resampling and JPEG compression has been proposed in this paper. Initially, using the expectation-maximization algorithm, the probability map of an image was obtained.Then, to detect whether the image was resampled, JPEG-compressed, or both, it was Fourier-transformed and balanced with affine transformation templates and a scaled JPEG template. In different types of digital tampering when resampling and JPEG compression occurred, experimental results are provided to show that the given method is reliable and effective.In addition, improved results are better compared to the current approaches obtained by them.

In paper[10] **(Image Resampling Detection),** This paper explores the techniques of image resampling detection proposed in recent years, gives detailed differences in their efficiency, and reveals the critical difficulties that have arisen in a few significant issues, such as rotating image detection, noise reduction in the resampled image, and productivity improvement. In addition, this paper reviews the existing trends and brings up new hotspots in this area. They agree that this analysis will give researchers from critical research zones some guidance, giving them a general and novel perspective.

In paper[11]**(Simple Black-Box Adversarial Attacks on Deep Neural Networks),** Their attacks treat the network as an oracle (black-box) and presume only that the network output can be observed on the inputs being checked. In order to create a numerical approximation to the network gradient, their attacks use a new local-search-based technique, which is then carefully used to generate a small collection of pixels in a disturbing image.They show how to adapt this fundamental idea to accomplish many powerful misclassification concepts.

In paper[12] **(Deep Face Representations for Differential Morphing Attack Detection),**They explain and demonstrate different aspects of face morphing in this article. Attacks, including numerous techniques for producing morphed face pictures, and the state-of-the-art algorithms for Morph Attack Detection (MAD) based on a strict taxonomy, and finally, the availability of public databases enable reproducible benchmarking of new MAD algorithms. The effect of competitions / benchmarking, tests of vulnerability metrics for performance assessment, and performance assessment are also given systematically. In addition, in this emerging biometrics area, they discuss the open issues and possible future work that need to be tackled.

In paper[13] **(One Pixel Attack for Fooling Deep Neural Networks),** In an incredibly restricted situation where only one pixel can be changed, they analyze an attack. They suggest a new way to produce one-pixel adversarial disturbances based on differential evolution (DE). Due to the inherent characteristics of DE, it needs less adversarial information (a black box attack) and can fool more types of networks.The results show that 67.97 percent of the natural images in the Kaggle CIFAR-10 test dataset and 16.04 percent of the ImageNet (ILSVRC 2012) test images can be perturbed to at least one target class by modifying just one pixel with 74.03 percent and 22.91 percent confidence on average. They also show the same vulnerability on the original CIFAR-10 dataset.Therefore, in an extremely restricted example, the proposed attack explores a particular approach to adversarial machine learning, demonstrating that existing DNNs are also prone to such low-dimensional attacks.

TABLE 1 : LITERATURE REVIEW

Paper	Techniques Proposed by	Publication Year	Features Extracted	Classifier Used	Dataset Used	Accuracy	Limitation
1	R. Raghavendra , Kiran B. Raja, Sushma Venkatesh, Christoph Busch	2017	AlexNet be FA and VGG19 be FV	P-CRC	Digital HP Print-Scan RICOH Print-Scan	DEER -> 8.23:17.64:12 .47 APCER=10% 7.53 : 32.87 : 16.43 APCER=5% 14.38 :41.78 :28.76	-
2	Clemens Seibold1, Wojciech Samek1, Anna Hilsmann1, and Peter Eisert1;2	2018	-	Softmax	ILSVR C	True +ve:95% True-ve:98% EER: 3.1% For naïve	Fewer artifacts are presented to the network during the training.

3	HusrevT. Sencar, MahalingmRamkuma, Ali N. Akansu	2017	Cropped-resampled signal are used to estimate the amount of cropping.	-	-	-	The system performs well, only if the attack is low.
4	R. Raghavendra Kiran B. Raja Christoph Busch	2016	A normalized face image using BSIF filters	SVM	-	MFCN:3.46% NFCM : 0% ACER: 1.73%	Neurotechnology Verilook face recognition SDK on morphed face images.
5	Clemens Seibold1, Wojciech Samek1, Anna Hilsmann1 and Peter Eisert1;2	2017	DCT coe_cients of JPEG-compressed morphs.	CNN	ILSVRC	FRR:16.2% FAR:1.9% From scratch FRR:11.4% FAR:0.9% From pretrained (AlexNet)	-
6	Andrey Makrushin, Tom Neubert, and Jana Dittmann	2017	quantized DCT coefficients of JPEG-compressed morphs is substantially different from that of authentic images enabling the automatic detection of morphs.	SVM	Utrecht ECVP face dataset	98.44%	After inverse wrapping, the blended face has the same geometry as the face wrapped in it. Therefore, the morph has a mutual texture.
7	QixueXiao,Yufei Chen, Chao Shen, Yu Chen and Kang Li	2019	The color histogram and the color scattering distribution	Deep learning classifiers	sourceImg	-	size and brightness, of source and target images.
8	Jiawei Su, Danilo Vasconcellos Vargas and Kouichi Sakurai	2019	-	Softmax classifier	CIFAR-10 dataset	NiN:35.20% & VGG:31.40% Success Rate	
9	Shu-ping Li, Zhi Han, Yi-Zhen Chen, Bo Fu, Chunhui Lu, Xiaohui Yao	2016	-	-	-	-	this approach is high computation load and the fact that it only detects one specific type of tampering.
10	Rachna Mehta, Navneet Agarwal	2019	interpolation occurs before compression with the digital zoom feature.	SVM	-	-	-
11	Hung Dang, Yue Huang, Ee-Chien Chang	2017	Such malware the detection mechanism is usually a classifier that makes	PDFrate Hidost	Contagio dataset	-	-

			decision-based on some extracted features				
12	Ulrich scherhag 1, christian rathgeb1,2, johannes merkle2, Ralph breithaupt3, and christophbusch 1	2019	texture descriptors can be further processed.	SVM CNN	-	-	the new network has to be trained for each subject
13	Ulrich Scherhag, Christian Rathgeb, Johannes Merkle and Christoph Busch	2020	-	SVM	FERET	-	-

3. CONCLUSION

In this paper, we introduced an efficient and robust model for detecting resizing and face morphing attacks in both grayscale and color images using traditional techniques and hand-crafted functions. Experimental results in terms of detection accuracy and CPU time on different publicly available datasets and our newly developed techniques of forgery dataset confirm the superiority and robustness of our proposed method over existing methods found in the current literature. Results also show that our proposed method is more effective and consistent in detecting resizing and face morphing image forgery attacks. We will investigate the efficiency of deep learning-based forgery detection techniques in the future. As per the dataset, the accuracy of the forgery detection of our method may vary slightly.

REFERENCES

[1] R. Raghavendra, "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images," *IEEE explore*, p. 9, 2017.

[2] C. Seibold, "Accurate and Robust Neural Networks for Security Related Applications Exampled by Face Morphing Attacks," *researchgate publication*, p. 16, 2018.

[3] H. T. Sencar, "A ROBUST TYPE-I11 DATA HIDING TECHNIQUE AGAINST CROPPING & RESIZING ATTACKS," *IEEE explore*, p. 4, 2002.

[4] R. Raghavendra, "Detecting Morphed Face Images," *researchgate publication*, p. 7, 2016.

[5] C. Seibold, "Detection of Face Morphing Attacks by Deep Learning," *researchgate publication*, p. 13, 2017.

[6] A. Makrushin, "Automatic Generation and Detection of Visually Faultless Facial Morphs," *sitepress publication*, p. 12, 2017.

[7] Q. Xiao, "Seeing is Not Believing: Camouflage Attacks on Image Scaling Algorithms," *usenix.org*, p. 19, 2019.

[8] H. Dang, "Evading Classifiers by Morphing in the Dark," *arxiv.org*, p. 16, 2017.

[9] S.-p. Li, "Resampling Forgery Detection in JPEG-Compressed Images," *IEEE explore*, p. 5, 2010.

[10] R. Mehta, "Image Resampling Detection: A Review," *IEEE explore*, p. 8, 2019.

[11] N. Narodytska, "Simple Black-Box Adversarial Attacks on Deep Neural Networks," *arxiv.org*, p. 9, 2016.

[12] U. Scherhag, "Deep Face Representations for Differential Morphing Attack Detection," *arxiv.org*, p. 15, 2020.

[13] J. Su, "One Pixel Attack for Fooling Deep Neural Networks," *arxiv.org*, p. 15, 2019.