frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 21 June 2023
DOI 10.3389/fcomp.2023.981933

OPEN ACCESS

EDITED BY
Kiran Raja,
Norwegian University of Science and Technology, Norway

REVIEWED BY
Xinwei Liu,
Zhejiang Wanli University, China
Kishor Upla,
Sardar Vallabhbhai National Institute of Technology Surat, India

*CORRESPONDENCE
Ilias Batskos
✉ i.batskos@utwente.nl

RECEIVED 29 June 2022
ACCEPTED 30 May 2023
PUBLISHED 21 June 2023

CITATION
Batskos I, Spreeuwers L and Veldhuis R (2023) Visualizing landmark-based face morphing traces on digital images.
Front. Comput. Sci. 5:981933.
doi: 10.3389/fcomp.2023.981933

Visualizing landmark-based face morphing traces on digital images

Ilias Batskos*, Luuk Spreeuwers and Raymond Veldhuis

Data Management and Biometrics Group, Department of Electrical Engineering, Mathematics and Computer Science, University of Twente, Enschede, Netherlands

This paper focuses on an identity sharing scheme known as face image morphing or simply morphing. Morphing is the process of creating a composite face image, a morph, by digitally manipulating face images of different individuals, usually two. Under certain circumstances, the composite image looks like both contributors and can be used by one of them (accomplice) to issue an ID document. The other contributor (criminal) can then use the ID document for illegal activities, which is a serious security vulnerability. So far, researchers have focused on automated morphing detection solutions. Our main contribution is the evaluation of the effectiveness and limitations of two image forensics methods in visualizing morphing related traces in digital images. Visualization of morphing traces is important as it can be used as hard evidence in forensic context (i.e., court cases) and lead to the development of morphing algorithm specific feature extraction strategies for automated detection. To evaluate the two methods, we created morphs using two state-of-the-art morphing algorithms, complying with the face image requirements of three currently existing online passport application processes. We found that complementary use of the visualization methods can reveal morphing related traces. We also show how some application process-specific requirements affect visualization results by testing three likely morphing attack scenarios with varied image processing parameters and propose application process amendments that would make forensic image analysis more reliable.

KEYWORDS

morphing, forensics, visualization, identity, detection

1. Introduction

Image morphing is a special effect often used in motion pictures and animations that changes/morphs one image or shape into another through a seamless transition (Steyvers, 1999). A well-known movie that heavily used morphing techniques is the 1991 movie Terminator 2: Judgement Day, where the shape-shifting terminator could transform or morph into different individuals. Face morphing is a special case of image morphing which focuses on faces. Using computer software, one can create a composite face image from the faces of, usually, two individuals. The similarity between the morph and either of the contributors can be controlled and under the right circumstances, the composite image can look like both contributors and can be used by one of them (accomplice) to obtain an otherwise legitimate ID document. The other contributor (criminal) can then use the ID document for illegal activities. This is known as a Morphing Attack (MA), an

identity sharing scheme between two or more individuals and a serious security vulnerability (Scherhag et al., 2017a,b; Batskos et al., 2021). Morphing examples are shown in Figure 1.

The earliest morphing research appeared in the early 2000s (Hancock, 2000; Tiddeman et al., 2001). Later, Ferrara et al. (2014) reexamined the issue in the context of identity documents making it more widely known to the scientific and security communities and a burst of research effort to better understand and deal with this vulnerability has followed.

The root of the problem is the fact that in most countries, authorities accept face images for ID document applications without a verifiable, trusted source. It is extremely hard, if not impossible, to ascertain that a printed face image brought to a police station or municipality by a passport applicant has not been manipulated. Printing the face image on photographic paper is "the nail in the coffin" of image manipulation detection. Some, if not all, potential traces of digital image manipulation are eliminated. Most countries still accept only printed face images in ID document applications, even though it has proven to be highly problematic.

Live enrolment in controlled environments (applicants visiting the authorities and having their photo taken there) solves the problem of potential prior image manipulation and trust. There is a handful of countries that have already transitioned to live enrolment or plan to transition in the near future like Norway, Portugal and Germany. However, the transition is costly, takes time and it is not always possible (emergency situations in remote locations). For many countries an intermediate stage before the transition to live enrolment is to only accept digital face images instead of printed ones. This is also relevant and highly desirable for banking institutions and other online service providers that require identity verification. In Estonia, the UK and Ireland for example, passport applicants can electronically submit digital face images that satisfy some criteria. Although the risk of prior image manipulation remains, our ability to reliably detect manipulation traces using image forensics techniques becomes significantly higher than with printed images.

The aim of this paper is two-fold. First, we evaluate the effectiveness of two well known image forensics techniques to visualize face morphing traces on digital images under certain conditions. Visualization (and interpretation) of morphing traces is very important as it can be used as evidence in a forensic context. Moreover, it offers valuable insight into the inner workings of different morphing software. This insight can be used to extract morphing algorithm specific features and explicitly train automated single image morphing attack detection (SMAD) algorithms (Raja et al., 2021). To the best of our knowledge visualization of face morphing related has not received much attention, although it is a very important from a forensics point of view.

Second, we evaluate to what extent we can effectively apply these forensic techniques to the three online passport application processes mentioned above, given their specific requirements. This will help determine application process amendments that are necessary to increase our chances to detect morphing traces.

In Section 2, we first describe the visualization methods in more detail, then analyze the aforementioned online passport application processes and their face image requirements and finally we describe our datasets and bona fide and morphing attack scenarios.

In Section 3, we present and analyze visualization results of both methods for the different scenarios and in Section 4 we discuss about the limitations of the examined methods given the requirements of the online passport application processes and recommend some amendments to these processes. The main limitations of the evaluated image forensics methods are the following:

- Methods require calibration due to strong influence by image characteristics (quality, size, format).
- Generally accepted image processing before submission (rotation, resizing, compression) affect robustness of results.
- Automation is not trivial and expert opinion is necessary.

2. Materials and methods

2.1. Materials

2.1.1. Online passport applications and face image requirements

As mentioned in the introduction we are interested in online passport applications like those of Estonia, Ireland and the UK which allow applicants to submit their own face image as long as the images are compliant with some requirements. It is important to analyze the requirements to understand the reasoning behind the selection of the images we decided to analyze and the difficulty of the task.

Partial ICAO compliance is required like looking straight to the camera, no hair in front of eyes, face not covered, light and uniform background, neutral expression, no shadows or flashes among other things (Ferrara M., et al., 2012). Partial because there is no requirement of specific inter-eye distance, head/image ratio, width/height ratio. In essence, submitted images should be such that the remaining criteria can be satisfied by the authorities (aligning, cropping, resizing, compressing). Model examples of accepted images are shown in Figure 2.

The main technical requirements are presented below.

Estonia (Police and Border Guard Board, 2022):

- Color
- Unedited
- Between 1 and 5 MB.
- Resolution must be 1,300 × 1,600.
- No scans or screenshots.

Ireland (Photo Guidelines - Department of Foreign Affairs, 2022):

- Color
- No scans.
- Resolution at least 715 pixels wide and 951 pixels in height.
- JPEG format.
- Uncompressed, without loss or compression artifacts.
- Not digitally enhanced or changed.
- Not larger than 9 MB.

FIGURE 1
Examples of tested morphs. In each row from left to right, the first morphing contributor, a morphed image created with our morphing algorithm (UTW), with the algorithm of the University of Bologna (UBO) and the right most image is the second morphing contributor. The contributing images in the first row come from the FRGC database, contributing images in the second row were captured in house with a smartphone and in the third and fourth row with a DSLR camera.

UK (Get a passport photo GOV.UK, 2022):

- Color
- Unaltered by computer software.
- Resolution at least 600 pixels wide and 750 pixels tall.
- Between 50 KB and 10 MB.
- No cropping.

We observe that the range of accepted image characteristics is quite wide. Characteristics may vary both within and between countries in terms of image resolution, size and format but there is a common theme. Images should not be edited, processed, altered by computer software. This includes, or at least should include, any compression other than the internal camera compression. In Ireland this is explicit. In the UK however, the minimum size requirement is 50 KB. For a color image of at least 600 × 750 pixels with 3 bytes per pixel, this size implies heavy compression which is contradictory to the requirement that an image should be unaltered by computer software. Heavy compression on applicant's side is not only unnecessary but also detrimental to effective and reliable forensic image examination. Similarly, Estonia has two requirements that contradict each other, namely the exact resolution and no editing. We are not aware of a digital camera or a smartphone that directly captures 1,300 × 1,600 images as Estonia requires. This could be achieved either by scaling or cropping and resaving. Both processes require editing with software. Both scaling and resaving (JPEG to JPEG or PNG to JPEG) will alter image content and introduce artifacts in an image which might conceal manipulation traces.

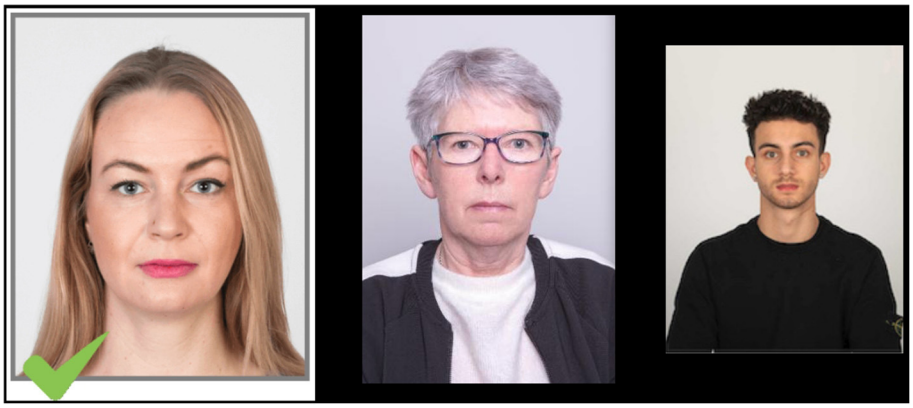

FIGURE 2
Examples of accepted images from Estonia **(Left)**, Ireland **(Middle)** and the UK **(Right)** (Get a passport photo GOV.UK, 2022; Photo Guidelines - Department of Foreign Affairs, 2022; Police and Border Guard Board, 2022).

For the sake of simplicity we will assume that no additional compression is allowed for all three enrolment processes and ignore Estonia's resolution requirement.

The third and final problem with these enrolment processes, which is also in contradiction with the no editing requirement, is the range of accepted image formats. Unlike Ireland, Estonia and the UK do not require a specific image format. Most citizens nowadays have smartphones or digital cameras capable of capturing high quality images and there are many ID face image capturing applications that will ensure captured images comply with official requirements. In the digital age this is very convenient for both citizens and authorities as it saves time and resources. The vast majority of digital cameras and smartphones will produce images of "lossy" JPEG format. In other words, devices have software that compress images internally by default. This is almost always the case for smartphones, as digital cameras usually have the option to save the image in a RAW format. A RAW format image contains the information of the camera sensor, one or three colors per pixel. To view, edit or print it, the image needs to be "interpreted" by software and converted to a different format like JPEG or PNG which is another popular format. Different software may "interpret" the RAW image differently and thus we might have different images "developed" from the same RAW image. This adds complexity and uncertainty to the whole process. For better or worse JPEG is the standard format for most image capturing capable devices nowadays. Allowing only JPEG images would simplify things from a forensics perspective.

2.1.2. Genuine scenarios

We use the term genuine to refer to an image the content of which has never been altered by computer software, except during the moment of acquisition. There are many publicly available face datasets containing images that would comply with the ICAO criteria for passport images. However, based on some test we suspected that at least three of them contain images that have been processed in some way (cropping, resaving, scaling) that is not allowed by the examined enrolment processes, which makes them unsuitable for our task. These datasets are the Utrecht face dataset, Eurecom-IST face dataset and Face Research lab London dataset (one of the authors confirmed our suspicion). To the best of our understanding the FRGC dataset contains unprocessed images (Phillips et al., 2005). To add some variability to our research and simulate real world scenarios we acquired images with a Canon DSLR camera (RAW and high quality JPEG format) and a Samsung A40 smartphone (JPEG format).

Examples of the images we used in our experiments are shown in Figure 1. The main reason we test PNG images is that the format is accepted by the UK and Estonia. Another reason is that both morphing algorithms produce PNG images (to avoid double compression) and we cannot exclude that morphs directly after their creation from these or similarly functioning software will not be submitted to the authorities. So it is important to examine the behavior of genuine PNG images in juxtaposition with morphed PNG images.

In terms of lighting conditions, pose and face proportions, and after comparing them to the acceptable images of Figure 2, we could reasonably argue that the images we acquired could be accepted in a passport application. Additionally, in terms of their technical characteristics, FRGC has 1,704 × 2,272 JPEG images with size of approximately 2 MB, the smartphone images are 3,456 × 4,608, JPEG with size of approximately 5 MB and the DSLR images are 3,456 × 5,184, approximately 5 MB, whereas the RAW images are about 30 MB after PNG conversion. Images comply with all three examined enrolment processes if we exclude Estonia's requirement for a precise resolution and the size of our PNG images, which could be easily covered with a more distant acquisition followed by cropping.

2.1.3. Morphing attack scenarios

We focused on a family of automated face morphing methodology, namely landmark and triangulation based face morphing (LM based morphing) because it has proven to be very effective and is widely accessible to the public (Ferrara et al., 2019; Venkatesh et al., 2020; Zhang et al., 2021). These algorithms have common basic steps. We use two such algorithms, one from the University of Bologna that we refer to as UBO

(Ferrara et al., 2018) and ours, which we refer to as UTW and include as supporting material. Both algorithms (or versions thereof), among others, have been used to create morphs for the two morphing attack detection benchmarks (Raja et al., 2021; Face Recognition Vendor Test (FRVT) Ongoing NIST, 2022). The basic steps of both algorithms are landmark detection, triangulation, image blending, image splicing and post-processing to make the morphs realistic. In so called splicing morphs the morphed inner face is transferred to a target image to avoid texture inconsistencies (ghost artifacts) in areas where landmarks are not extracted automatically (ears, hair, shoulders, neck, etc.). This can also happen to areas like the eyes, nostrils, lips in which detection is inaccurate to avoid visible texture inconsistencies that will easily give away the morph. These image manipulation steps will leave traces on an image which sometimes can be visualized and used as evidence of face morphing. For a comprehensive analysis of automated LM-based morphing, we refer the reader to Hildebrandt et al. (2017) and Makrushin et al. (2017).

Here we only focus on average morphs i.e., with the average geometry and texture of the two contributing images but results apply to morphs with different blending and warping factors as well. To maintain average geometry of the morphed inner face, the target image is also warped to fit the morphed inner face by both algorithms. This increases the chances of the morph matching with both contributors but it also introduces periodic noise due to the affine transformations (Kirchner and Bohme, 2008).

There are many LM-based morphing algorithms that we could have used, however the basic steps and thus the basic traces are similar. The main variations lie in the post-processing which might include combinations of image processing techniques to conceal traces. To avoid redundancy we selected two methods that achieve this objective differently and in our opinion are representative of possible good post-processing combinations. The post-processing steps between the two algorithms vary. UBO's algorithm uses local blurring on the boundaries of the transferred morphed face and manipulates color histograms to correct for color inconsistencies on the face, whereas ours manipulates color gradients using the Poisson image editing technique (Pérez et al., 2003) implemented by OpenCV and finally inner and outer face regions are sharpened at a different level to enhance loss of details due to primarily the image blending operation.

Additionally, both algorithms (as well as most online morphing tools) align faces based on eye positions (rotation), crop them to passport like proportions and scale them. This introduces interpolation artifacts due to rotation and scaling, additional noise throughout the whole image. Although this is not difficult to detect, it will make other traces more difficult to distinguish. In reality, this alignment may not always happen, in which case the lack of noise in the outer face region will most likely make the inner face region traces more prominent and thus easier to detect.

We only use contributing images from the same database to create the morphs. Examples of resulting morphs are shown in Figure 1.

There are many different parameters and processing steps that can affect a forensic examination of an image, especially a morphed image. It is very difficult to investigate every possible outcome. We have evaluated the following scenarios which we consider likely to be encountered in the real world:

2.1.3.1. Scenario 1

Morphs are submitted to the authorities in PNG format without any JPEG compression after their creation.

Both morphing algorithms produce a PNG image. No information is discarded after the morphs have been created as would be the case if they were saved as JPEG. Morphing traces are clearly visible in such cases. In reality, an attacker would likely compress the resulting morph with the lowest compression factor (highest quality) similar to default camera values, not only to simulate a smartphone or digital camera capture but to conceal manipulation traces. Nonetheless, we cannot exclude that an unsophisticated attacker will submit the morph directly after creating it with an online available morphing algorithm and examining such cases is useful to evaluate the characteristics of such algorithms and create targeted feature extraction and detection mechanisms.

2.1.3.2. Scenario 2

Morphs are saved in JPEG using OpenCV, compressed with QF 100 (highest quality) before being submitted to the authorities, simulating the behavior of genuine smartphone or digital camera captured images.

As mentioned above, this pipeline is more likely to be encountered in reality. A criminal with basic computer knowledge would likely be aware of the JPEG algorithm properties and use it to discard encriminating morphing traces as well as avoid JPEG ghosts.

2.1.3.3. Scenario 3

Morphs are saved in JPEG using a default Windows 10 application.

The default Windows 10 application Snip and Sketch does not offer QF options. It is a native Windows 10 application and because Windows is the most popular mainstream operating system, it is likely to be used and thus important to investigate.

2.2. Methods

The literature is rich when it comes to digital image forensics but since face morphing has resurfaced as a threat relatively late, research that focuses specifically on visualization or localization of face morphing-related traces is missing. Research has focused on general image forgery like copy-move forgery, local tampering, splicing, double JPEG compression.

Most of these approaches work with assumptions that the genuine group of images is unprocessed, and parts of the tampered group images are untampered with or unprocessed in any way. However, in case of face morphing and online passport application processes these assumptions do not hold because on the one hand ICAO allows for some processing of passport images like rotation, cropping, down sampling, white balance correction and on the other hand face morphing might involve several types of processing both locally and globally. Given the above we present some related work in the field.

Ferrara M., et al. (2012), Ferrara P., et al. (2012) exploited Color Filter Array (CFA) demosaicking artifacts to discriminate between original and forged regions in images captured by digital

cameras that use a CFA to produce 3 color channel images (color interpolation). Forged regions exhibit a different CFA pattern than original regions which can be statistically modeled. Problems arise when limited compression and "legitimate" processing is expected.

Bianchi and Piva (2012) have proposed a method for automatically detecting 8 × 8 blocks that have undergone double JPEG compression in an image by statistically modeling these artifacts, producing a double compression probability map of the image. However, the method assumes that parts of the questioned image will have a different level of compression, while in case of morphing this might not happen when both contributing images are initially uncompressed.

Similarly, Iakovidou et al. (2018) have proposed a method for detecting indicators and then producing a map of image forgery by locating grid alignment abnormalities in JPEG compressed images. This method focuses on image splicing or tampering that breaks the characteristic JPEG block grid.

Agarwal and Farid (2017) have done extensive experiments with another less known JPEG artifact. They show that the so-called JPEG dimples artifacts which are based on the choice of the DCT quantization step rounding operator can be used to detect and visualize some manipulations like content-aware fill, re-sampling, airbrushing and compositing in most examined commercial cameras and under varying post-processing operations. They also report that the method fails when two major image processing applications are used.

Mahdian and Saic (2009) detect variations in the noise levels of an image which is indicative of tampering by using wavelet decomposition and image blocks noise variance estimation. They propose a framework for dividing an investigated image into various partitions with homogenous noise levels. The method can also be used to detect traces of tampering where local noise is used to hide them.

Finally, as far as we are aware Venkatesh et al. (2019) is the only research so far that has focused on morphed images. They used a denoising convolutional neural network to denoise morphed images, create residual images by subtracting the denoised image from the morphed image and based on the residual classify an image as morphed or not. However, this approach is not an explicit image forensics approach which is what we focused on in this paper and it makes the same assumption for genuine images as mentioned in the second paragraph of this section.

2.2.1. JPEG compression error

The first method we evaluate is based on JPEG compression algorithm properties (Wallace, 1992). JPEG compression can be thought of as a Low Pass filter in the frequency domain with which the imperceptible to the human eye high frequency content of an image (minute details, edges) is discarded to save storage space. The frequency content of an image are represented by Discrete Cosine Transform (DCT) coefficients. The loss of information or main compression happens at the quantization step which involves dividing each coefficient with an integer from a quantization table (QT). High frequency coefficients are divided with larger numbers and are zeroed out by rounding. This results in efficient compression in the encoding stage which saves a significant amount of storage space. The algorithm is applied independently to small image blocks. Blocks that make up a rather homogeneous area are expected to be treated analogously by the JPEG algorithm due to their similar properties.

Considering a face image intended for passport use, we expect that mostly homogeneous areas like the skin area or the background will not exhibit variations or anomalies in discarded or affected content. However, a kind of morphed images may exhibit such anomalies, the level of which depends on the processing steps of the morphing algorithm that was used and the characteristics of the contributing images. We can see some of these anomalies by visualizing which areas of an image were affected unexpectedly and disproportionately by the JPEG algorithm. This is the primary motivation for using this method.

To visualize which pixels changed after an image has been compressed, we take the absolute difference of the initial image and its decompressed version and map non-zero values to 255 in RGB, although different mappings are possible (value normalization, different color space, single channel). We will refer to this absolute image difference as compression error or simply error. This method is mostly known in the literature as JPEG ghosts (Farid, 2009).

Most image editing software allow users to control the level of compression by choosing a quality factor (QF) between 1 and 100, with 100 meaning best quality and lowest compression and 1 meaning highest compression and lowest quality. In other words, the QF is a scaling factor for the QT. Depending on the software, QFs may have a different range such as 0–12 or low, medium and high. We use OpenCV (Bradski and Kaehler, 2008) which offers a QF range between 1 and 100. An important property of JPEG compression is that when a genuine image is recompressed using the same or similar parameters (QF, QT) the vast majority of its pixel values will remain the same. The DCT coefficients of each block will be divided by the same QT elements that they were multiplied with during decompression. Very few pixels will change due to rounding errors, floating point conversions and slightly different QTs. Most internal camera software will compress an image with a high QF which will lead to minimal error when we recompress the image with the highest OpenCV QF of 100.

In the first row of Figure 3, we show a bona fide JPEG image and its error for QF 100 (right). The image was captured with a commercial smartphone, and it has not been processed except with the internal camera compression. The lower the QF the higher the error, as we require the JPEG algorithm to suppress more high spatial frequencies. In the second row, we have applied sharpening to the left part of the face and recompressed (resaved) the image with QF 100. The sharpening in the natural image (left) is barely visible if at all, but it is clearly visible in the error image (right) for the same QF as above.

If we replace parts of an image with parts of another image or if we manipulate an area of an image by applying sharpening, blurring, color correction for example, we will introduce new spatial frequencies in some blocks which will result in a different (higher or lower) error compared to neighboring areas with seemingly similar texture that were not manipulated. Automated LM-based morphing involves a number of manipulations which may introduce new spatial frequencies only in some parts of the

10.3389/fcomp.2023.981933

FIGURE 3
In the first row a genuine face image **(Left)** and its compression error image for quality factor (QF) 100. In the second row the same image but slightly sharpened on the left part of the face with the corresponding compression error image. In the third row the luminance or gray level sharpened image **(Left)** and its Discrete Fourier Transform (DFT) magnitude spectrum **(Right)** and finally in the fourth row the high pass filtered magnitude spectrum **(Right)** and the reconstructed (Inverse DFT) high pass filtered image **(Left)**.

image or more in some parts of the image than in others. This knowledge is what we exploit to visualize the manipulations.

It is important to note that interpretation of error images should be done with caution. The examiner should draw conclusions only after comparing the error between homogeneous areas like skin (face, forehead, neck) and the background. Abnormal variations in seemingly homogeneous areas are a strong indication of manipulation as we will see in the results section.

2.2.2. Frequency domain filtering

The second method of visualizing morphing related traces is based on frequency domain filtering. The method has been widely used in image processing. For example, periodic background noise in medical images can be easily identified and suppressed in the frequency domain (Archibald and Gelb, 2002). The two methods are based on the same logic although the latter one can be more flexible and versatile. A single channel image is a two dimensional signal which can be decomposed in its component spatial frequencies (a weighted sum of sines and cosines in this case) by applying the Discrete Fourier Transform (DFT) (Winograd, 1976). Each spatial frequency can be represented by its magnitude and its phase in the frequency domain. The DFT returns as many spatial frequencies as there are pixels in the image in the form of complex numbers. The magnitude of a complex number, i.e. the magnitude of a particular spatial frequency, encodes how much of that particular frequency there is in the signal. We can suppress or enhance certain spatial frequencies of an image by manipulating its magnitude spectrum. This is as simple as multiplying the magnitudes with a factor. The luminance or gray level channel of the sharpened image of Figure 3 and its conjugate symmetric magnitude spectrum are shown in the third row of Figure 3.

It is common to shift the zero frequency component (DC) to the center for easier processing and more intuitive interpretation. Magnitudes of low spatial frequencies are gathered around the center and are increasing as we move toward the corners. The spectrum is shown in log scale as the prevalent low frequency magnitudes are orders of magnitude larger than high frequency magnitudes. White color corresponds to higher values.

Our aim here is to progressively filter out lower spatial frequencies in the frequency domain and then visualize what the remaining mid to high spatial frequencies correspond to in the spatial domain by applying the inverse DFT. First we convert the RGB image to YCbCr color space and apply the filters to each channel separately to capture manipulations that might be more prevalent in the luminance than the chrominance channels or vice versa. In the fourth row of Figure 3, we applied a high pass filter to the magnitude spectrum (right) and then reconstructed the filtered image (left) by applying the IDFT using the original phase spectrum. Pixel values of the reconstructed filtered image are in log scale and normalized between 0 and 1, with 0 being the highest value (reversed colors). Values below the mean are mapped to 1 (white), while values above it are mapped to 0 (black) for better visualization. Varying mapping methodologies may be implemented.

An unaware observer would probably not notice anything suspicious when looking at the sharpened image. However, the sharpening effect is clearly noticeable in the reconstructed filtered image. The remaining high frequency magnitudes correspond more to the sharpened left part of the face as sharpening enhances high spatial frequencies. In case of applying bluring on a region, the higher spatial frequencies of the region would be suppressed,

FIGURE 4
In the first row left to right, the UTW morph of FRCG (Phillips et al., 2005) images, its compression error (QF100), high pass filtered luminance channel image and high pass filtered chrominance red channel image. In the second row, the UBO morph and the corresponding results.

FIGURE 5
In the first row left to right, the UTW morph of DSLR acquired images in JPEG format, its compression error (QF100), high pass filtered luminance channel image and high pass filtered chrominance red channel image. In the second row, the UBO morph and the corresponding results.

resulting in a lighter region. The effect depends on the nature of the manipulation.

Following this logic, we expect that morphing related manipulations will change the spatial frequencies on parts of the facial area, depending of course on the used method. By filtering out the more prevalent low to mid frequencies of a facial area, we try to uncover abnormal variations in mid to high spatial frequencies in some areas relative to others. We use Gaussian filters to minimize ringing artifacts (Dogra and Bhalla, 2014) and varying sigmas and power factors for the Guassian adapting to each case. The method can also be used locally on regions of interest to avoid for example interference by noisy background. Many parameters can be tweaked and there is no "one size fits all" with this method. On the other hand, background analysis might reveal interpolation artifacts caused by affine transforms (warping) as we will see in the results section.

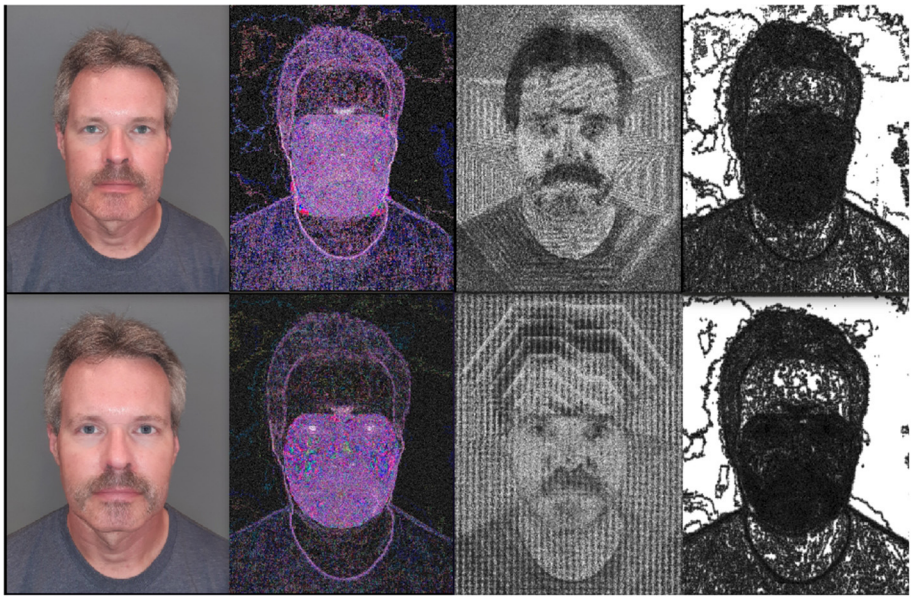

FIGURE 6
In the first row left to right, the UTW morph of smartphone acquired images in JPEG format, its compression error (QF100), high pass filtered luminance channel image and high pass filtered chrominance red channel image. In the second row, the UBO morph and the corresponding results.

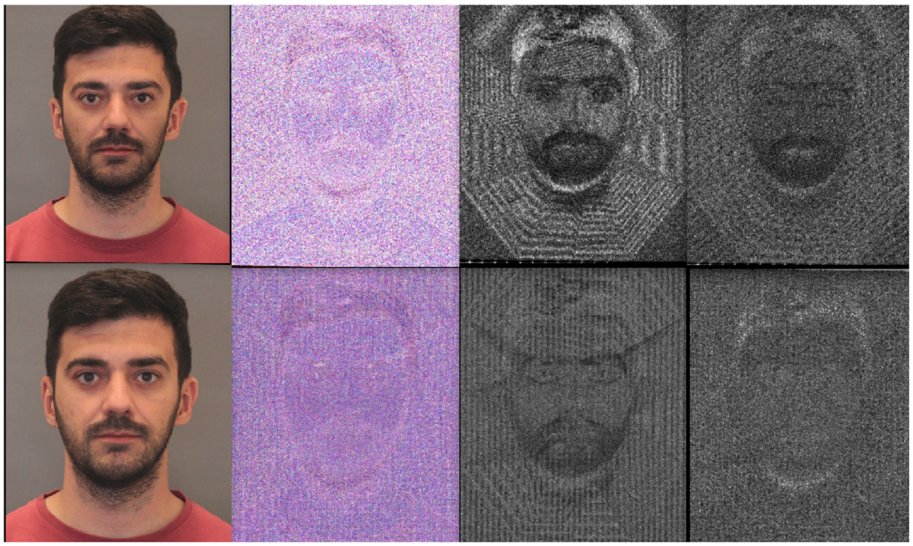

FIGURE 7
In the first row left to right, the UTW morph of DSLR acquired images in RAW format, converted to PNG with the Image Viewer Linux application, its compression error (QF100), high pass filtered Y channel image and high pass filtered chrominance red channel image. In the second row, the UBO morph and the corresponding results.

3. Results

Here we present some of our visualization results for the three scenarios and for the different types of intial images and morphing alogorithms. We will compare the behavior of morphed images with that of corresponding type genuine images to understand what would be expected in genuine cases. Unfortunately, given the limitation in the total number of figures that we can include in the manuscript, we only show the most interesting results of a limited number of cases. Nonetheless, we believe that what is presented is enough to steer research toward visualization of morphing related traces and critical analysis of passport enrolment processes. Additionally, we include all the scripts that have been used, with as much documentation as possible for the interested reader.

10.3389/fcomp.2023.981933

FIGURE 8
Genuine images acquired with a DSLR camera. The first and third rows were converted from RAW to PNG with the Image Viewer Linux application, while the second and fourth with the Snip and Sketch Windows application. From left to right the compression error (QF100), high pass filtered luminance channel image and high pass filtered chrominance red channel image.

3.1. Scenario 1

Here we are dealing with morphs in PNG format which are not JPEG compressed after creation. That means that manipulation traces are not discarded and both methods perform well. In Figure 4 as in all figures of this subsection, the morphs are in the first column, the error image for QF 100 in the second column, the reconstructed filtered image of the luminance channel in the third column and the reconstructed filtered image of the chrominance red channel in the last column. The FRGC morphs were the most challenging of all scenarios because of the increased noise and considerably lower resolution compared to images from other sources. Nonetheless, we can observe increased error around the face region and periodic artifacts in the luminance channel filtered image, evidence of manipulation. The chrominance channel does not offer convincing evidence although there is some indication of abnormal variation in frequency content in the face region.

In Figure 5, we examine morphs created with images acquired from the DSLR camera with the highest quality setting. Periodic artifacts due to the affine transformations of the triangles during the morphing process stand out both for UTW and UBO morphs. Additionally, UBO morphs exhibit a characteristic block grid caused by upscaling. The difference between the two morphing methods in the compression error can be explained by the additional sharpening of the outer face region in UTW morphs causing more error all around the image. In the chrominance red channel filtered image of the UTW morph the inner face mask appears darker (increased high spatial frequencies), caused again by sharpening.

Visualization of traces is most effective in morphs created with smartphone acquired images as can be seen in Figure 6. Internal default JPEG compression appears to be higher in the smartphone than in the DSLR, discarding more high frequency noise and detail and making the morphing related traces more prominent. Here the

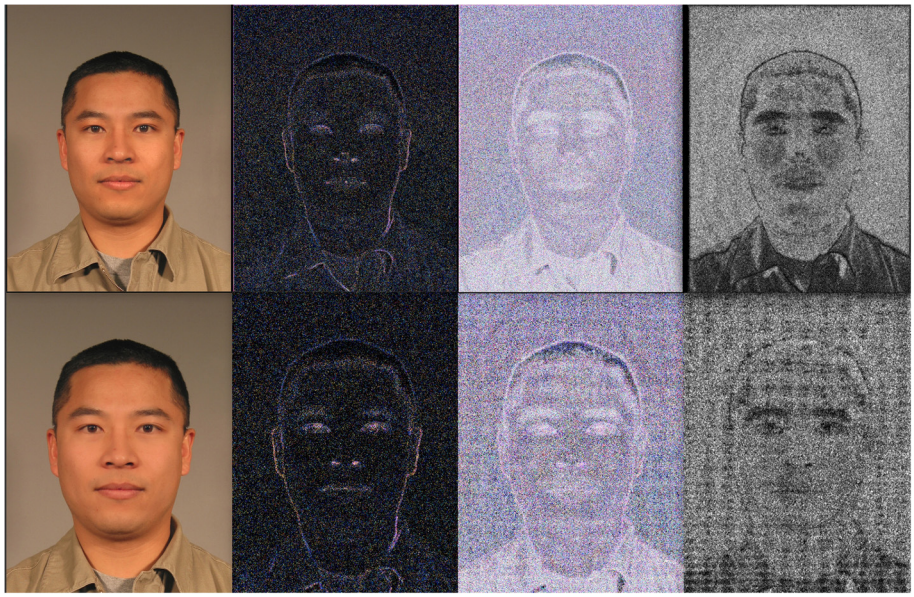

FIGURE 9
In the first row left to right, the UTW morph of FRCG (Phillips et al., 2005) images, the compression error for QF100 and QF 95, and the high pass filtered luminance channel image. In the second row, the UBO morph and the corresponding results.

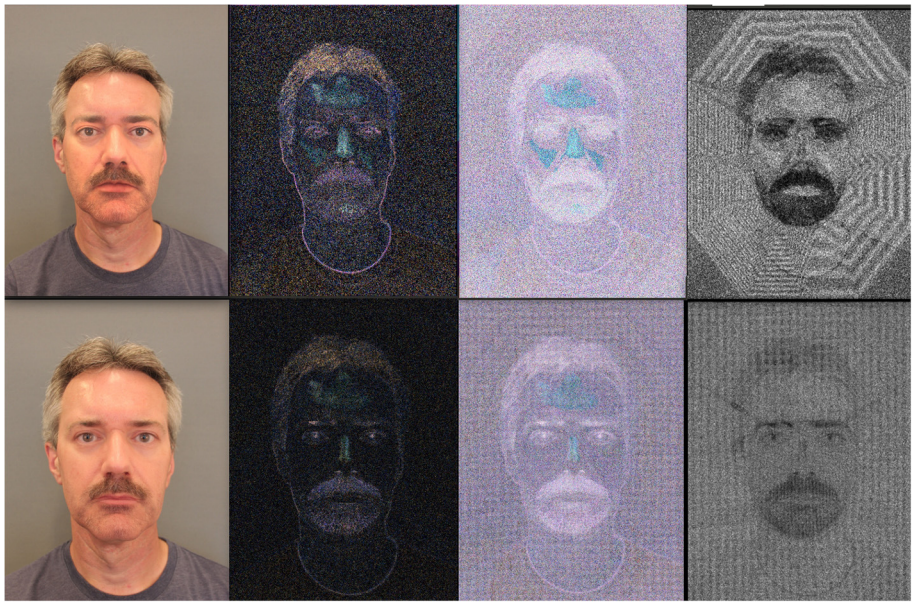

FIGURE 10
In the first row left to right, the UTW morph of DSLR acquired images in JPEG format, the compression error for QF100 and QF 95, and the high pass filtered luminance channel image. In the second row, the UBO morph and the corresponding results.

chrominance red channel high pass filtered image clearly shows the presence of high frequency content in the inner face. This is due to the color corrections which do not necessarily translate to high spatial frequencies in the luminance channel.

In Figure 7, we examine morphs created with images that were converted from RAW to PNG format with the Linux Image Viewer application. The error images (second column) do not reveal variations in the face region due to overall increased high frequency content (no JPEG compression). However, they do have some affine transformation traces, especially in the full-size images. These are clearly visible in the luminance channel high filtered images and less so in the chrominance red channel.

Finally, in Figure 8, we can see what we can expect to observe in genuine PNG images. In the first and second row we show the same image converted to PNG with Image Viewer Linux application and Snip and Sketch Windows application respectively.

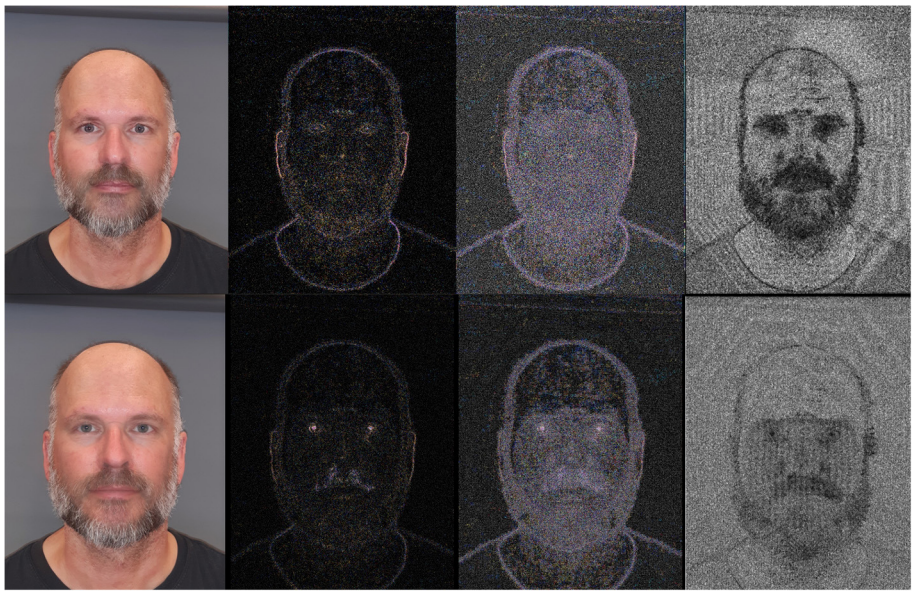

FIGURE 11
In the first row left to right, the UTW morph of smartphone acquired images in JPEG format, the compression error for QF100 and QF 98, and the high pass filtered luminance channel image. In the second row, the UBO morph and the corresponding results.

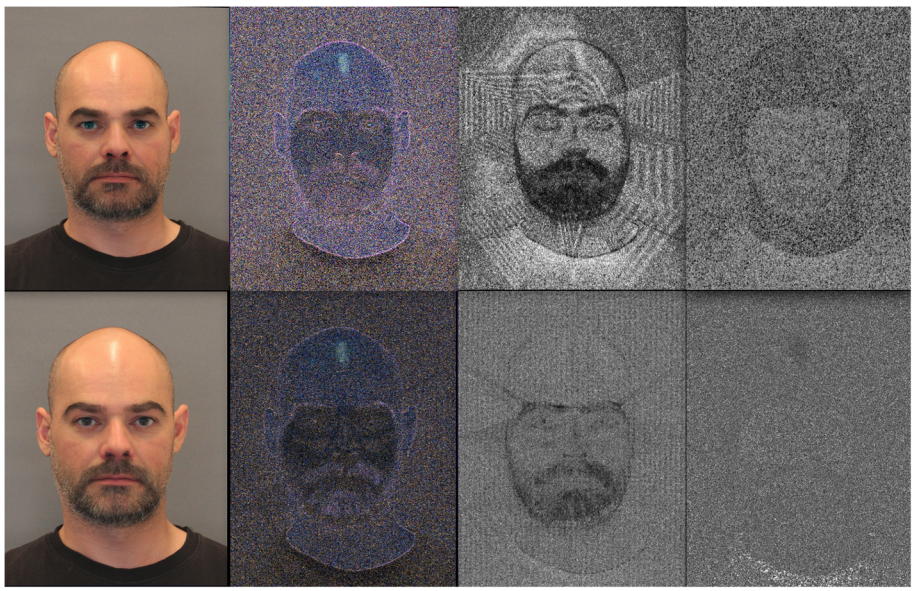

FIGURE 12
In the first row left to right, the UTW morph of DSLR acquired images in RAW format converted to PNG using Linux Image Viewer application, the compression error for QF100, high pass filtered luminance channel image and high pass filtered chrominance red channel image. In the second row, the UBO morph and the corresponding results.

Similarly, the third row image is from the Linux app and the fourth row image from the Windows app. We observe some difference between the "interpretations" of the RAW images from the two applications as mentioned in Section 2.2.1. We do not observe any indication of affine transformation traces. Regarding the compression error, second column in the second row, we observe a face mask like structure that could be wrongfully attributed to morphing. It is important to state that careful interpretation is necessary as well as the use of diverse forensics tools to avoid false positives.

FIGURE 13
Genuine images in JPEG format. FRGC (Phillips et al., 2005) image in the first row, DSLR acquired image in the second and smartphone acquired in the third. From left to right the compression error (QF100), high pass filtered luminance channel image and high pass filtered chrominance red channel image.

3.2. Scenario 2

In this scenario morphed images in PNG format are saved as JPEG using OpenCV's highest quality factor, QF 100, not only to simulate the compression error behavior of unprocessed genuine JPEG images (besides the internal camera compression), but also to avoid the appearance of the very distinct JPEG ghost for a lower QF as we will see in Section 3.3.

For most cases, the first few error images are similar to those of genuine images. However, for a lower QF in most cases we can observe the artifacts described in the previous section. The exception was most FRGC images with either morphing method, which did not exhibit any traces as seen in the first row, second and third columns in Figure 9. Even though compression was the lowest possible, morphing traces were discarded. However, in the majority of the FRGC cases traces remain visible in the luminance channel filtered images.

In Figure 10, as in the case above, we are unable to see a suspicious error variation in the face region. Nonetheless, affine transformation traces indicative of LM based morphing are clearly visible with one or both methods for certain configurations for all tested images.

Unlike the FRGC and most of the DSLR high quality JPEG images, morphs acquired with a smartphone (Figure 11) and morphs acquired with the DSLR in RAW format and then converted to PNG (Figure 12) posed no problem for either visualization method.

Finally, in Figure 13, we show results for genuine images from FRGC, acquired with a DSLR camera in high quality JPEG and acquired with a smartphone. We can observe that seemingly homogeneous areas have mostly similar responses unlike to what we observed with the morphed images.

3.3. Scenario 3

In this scenario we are resaving the morphed images with a native Windows image editing application. In countries with exclusively JPEG image format requirements like Ireland's, a criminal might use an operating system's native image editing application to convert the morphed PNG image that might have been produced by an online available morphing tool, to JPEG format with the default QF value. We chose to use a native Windows application since it is the most popular mainstream system.

In these cases, most traces we saw previously will be discarded during the compression. However, they exhibit a very distinct compression error pattern. The lowest error will appear for a QF other than QF 100. This depends on the default QF and QT parameters of the used application, which usually is either 95 or 90 (in OpenCV scale). This pattern is very different from that of a genuine image and is present in all morphs that have undergone this process. As already explained in the compression error section, when an image is recompressed using the same or similar parameters (QF, QT) the vast majority of its pixel values will remain the same. The DCT coefficients of each block will be divided by the same QT elements that they were multiplied with during decompression. Very few pixels will change due to rounding errors, floating point conversions and slightly different QTs. In Figure 14, we show the compression error of morphed images (first

FIGURE 14
From left to right natural images and their compression error for QF 100, 99, 90 and 89 with morphed images in the first and second rows and genuine images in the third and fourth rows.

and second rows) and bona fide images (third and fourth rows) for QFs 100, 95, 90 and 89. It turns out that the parameters of the default QF of the Windows application are very similar with OpenCV's QF 90 parameters.

In all examined morphs that were created with smartphone acquired images and most of the morphs that were created with RAW to PNG images, we were still able to observe affine transformations related traces as shown in Figure 15. In contrast, this was not the case for the vast majority of the FRGC and DSLR high quality JPEG morphs.

4. Discussion

We have investigated the effectiveness of two well-known image forensics methods to visualize manipulation traces created by a family of automated landmark-based morphing algorithms. Such morphing algorithms are available online and given the security risk of face morphing, it is important to investigate mitigation strategies, detection methodologies but also methodologies to visualize morphing related manipulations that can be used as hard evidence in a forensic context. The latter has not received much attention, if at all. Besides the forensic value, visualization will help create feature extraction strategies targeting specific morphing algorithms.

The task of visualizing morphing related traces is already very complicated, thus we refrained from including mathematical formulas and concepts that are well understood in the community or are easily verified and instead focused on visualization and interpretation.

We focused on existing online passport applications and showed that the selected image forensics methods can be successfully applied to visualize traces created by State-of-the-Art morphing algorithms under three likely scenarios of morphing attacks. Nonetheless, there are many parameters that need to be taken into account to have a holistic picture, such as enrollment process requirements, possible morphing steps including pre and post-processing, contributing image characteristics, possible counter-forensics, morphing contributors' similarity among other things. For these reasons, we suggested certain amendments to the examined online passport application which will remove their ambiguity and decrease the complexity and uncertainty of the visualization task.

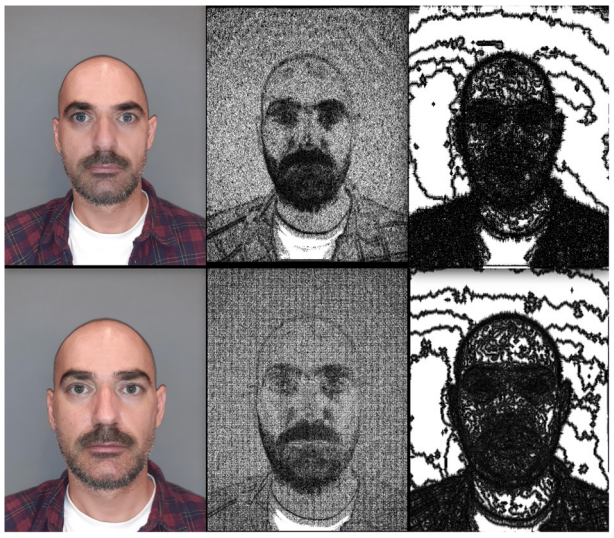

FIGURE 15
In the first row left to right, the UTW morph of smartphone acquired images, the high pass filtered luminance channel image and high pass filtered chrominance red channel image. In the second row, the UBO morph and the corresponding results.

Additionally, we recommend the implementation of an image quality assessment mechanism in online passport application processes. Image quality affects image forensics methodologies. A standard quality requirement would greatly increase the accuracy of such methods. Investment in ICAO compliant self-acquisition smartphone applications is also necessary, as the image background and the lighting conditions affect results. Thus, careful and experienced interpretation from multiple experts of any forensics-based investigation is paramount.

From an authorities' perspective, a couple of actions are expected to mitigate the risk of morphing. Namely, a record with the characteristic responses to forensic tools of online available morphing algorithms should be established and/or morphing software developers (especially for software of proprietary nature) should be requested to implement some kind of morphing persistent steganography.

In future research, we intend to extend our dataset, investigate bandpass filters in the frequency domain and try to isolate specific manipulations, investigate more morphing methodologies (GANs) and additional image forensics methods like color gradients.

Last but not least, the problem of facing morphing is an arms race. Both sides will continue to improve, criminals will find a way to avoid detection by concealing traces and once researchers become aware they will adjust detection mechanisms.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary material, further inquiries can be directed to the corresponding author.

Ethics statement

Written informed consent was obtained from the individual(s) for the publication of any potentially identifiable images or data included in this article.

Author contributions

IB is responsible for conception, execution, and manuscript preparation. LS has been responsible for the direct supervision. RV has been responsible for the indirect supervision. All authors contributed to the article and approved the submitted version.

Funding

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 883356.

Acknowledgments

Special thanks to Chris Zeinstra and Nicola Strisciuglio for their contribution.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

Supplementary material

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fcomp.2023.981933/full#supplementary-material

References

Agarwal, S., and Farid, H. (2017). "Photo forensics from JPEG dimples," in *2017 IEEE Workshop on Information Forensics and Security (WIFS)* (Rennes: IEEE), 1–6. doi: 10.1109/WIFS.2017.8267641

Archibald, R., and Gelb, A. (2002). A method to reduce the Gibbs ringing artifact in MRI scans while keeping tissue boundary integrity. *IEEE Trans. Med. Imaging.* 21, 305–319. doi: 10.1109/TMI.2002.1000255

Batskos, I., Wit, F. F., Spreeuwers, L. J., and Veldhuis, R. J. (2021). Preventing face morphing attacks by using legacy face images. *IET biom.* 10, 430–440. doi: 10.1049/bme2.12047

Bianchi, T., and Piva, A. (2012). Image forgery localization via block-grained analysis of JPEG artifacts. *IEEE Trans.Inform.Forensic Secur.* 7, 1003–1017. doi: 10.1109/TIFS.2012.2187516

Bradski, G., and Kaehler, A. (2008). *Learning OpenCV: Computer vision with the OpenCV library*. O'Reilly Media, Inc.

Dogra, A., and Bhalla, P. (2014). Image sharpening by gaussian and butterworth high pass filter. *Biomed. Pharmacol. J.* 7, 707–713. doi: 10.13005/bpj/545

Face Recognition Vendor Test (FRVT) Ongoing NIST (2022). Available online at: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing (accessed June 29, 2022).

Farid, H. (2009). Exposing digital forgeries from JPEG ghosts. *IEEE Trans. Inform. Forensic Secur.* 4, 154–160. doi: 10.1109/TIFS.2008.2012215

Ferrara, M., Franco, A., Maio, D., and Maltoni, D. (2012). Face image conformance to ISO/ICAO standards in machine readable travel documents. *IEEE Trans. Inform. Forensic Secur.* 7, 1204–1213. doi: 10.1109/TIFS.2012.2198643

Ferrara, M., Franco, A., and Maltoni, D. (2014). The magic passport. in *IEEE International Joint Conference on Biometrics* (Clearwater, FL, USA: IEEE) p. 1–7. doi: 10.1109/BTAS.2014.6996240

Ferrara, M., Franco, A., and Maltoni, D. (2018). Face demorphing. *IEEE Trans. Inform. Forensic Secur.* 13, 1008–1017. doi: 10.1109/TIFS.2017.2777340

Ferrara, M., Franco, A., and Maltoni, D. (2019). "Decoupling texture blending and shape warping in face morphing," in *Lecture Notes in Informatics (Darmstadt, Germany).*

Ferrara, P., Bianchi, T., De Rosa, A., and Piva, A. (2012). Image forgery localization via fine-grained analysis of CFA artifacts. *IEEE Trans. Inform. Forensic Secur.* 7, 1566–1577. doi: 10.1109/TIFS.2012.2202227

Get a passport photo GOV.UK. (2022). Available online at: https://www.gov.uk/photos-for-passports (accessed June 29, 2022).

Hancock, P. J. B. (2000). Evolving faces from principal components. *Behav. Res. Methods, Instrum. Compu.* 32, 327–333. doi: 10.3758/BF03207802

Hildebrandt, M., Neubert, T., Makrushin, A., and Dittmann, J. (2017). "Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps," in *2017 5th International Workshop on Biometrics and Forensics (IWBF)* (Coventry, United Kingdom: IEEE) p. 1–6. doi: 10.1109/IWBF.2017.7935087

Iakovidou, C., Zampoglou, M., Papadopoulos, S., and Kompatsiaris, Y. (2018). Content-aware detection of JPEG grid inconsistencies for intuitive image forensics. *J. Vis. Commun. Image Represent.* 54, 155–170. doi: 10.1016/j.jvcir.2018.05.011

Kirchner, M., and Bohme, R. (2008). Hiding traces of resampling in digital images. *IEEE Trans. Inform. Forensic Secur.* 3, 582–592. doi: 10.1109/TIFS.2008.2008214

Mahdian, B., and Saic, S. (2009). Using noise inconsistencies for blind image forensics. *Image Vis. Comput.* 27, 1497–1503. doi: 10.1016/j.imavis.2009.02.001

Makrushin, A., Neubert, T., and Dittmann, J. (2017). "Automatic Generation and Detection of Visually Faultless Facial Morphs," in *Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications* (Porto, Portugal: SCITEPRESS - Science and Technology Publications) p. 39–50. doi: 10.5220/0006131100390050

Pérez, P., Gangnet, M., and Blake, A. (2003). Poisson image editing. in *ACM SIGGRAPH 2003 Papers on - SIGGRAPH'03* (San Diego, California: ACM Press) p. 313. doi: 10.1145/1201775.882269

Phillips, P. J., Flynn, P. J., Scruggs, T., Bowyer, K. W., Chang, J., Hoffman, K., et al. (2005). Overview of the Face Recognition Grand Challenge. in *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)* (San Diego, CA, USA: IEEE) p. 947–954. doi: 10.1109/CVPR.2005.268

Photo Guidelines - Department of Foreign Affairs. (2022). Available online at: https://www.dfa.ie/passports/photo-guidelines/#digitalphotos (accessed June 29, 2022).

Police and Border Guard Board (2022). *Requirement and instructions for the document photo*. Available online at: https://www.politsei.ee/en/requirement-and-instructions-for-the-document-photo (accessed June 29, 2022).

Raja, K., Ferrara, M., Franco, A., Spreeuwers, L., Batskos, I., de Wit, F., et al. (2021). Morphing attack detection-database, evaluation platform, and benchmarking. *IEEE Trans. Inform. Forensic Secur.* 16, 4336–4351. doi: 10.1109/TIFS.2020.3035252

Scherhag, U., Nautsch, A., Rathgeb, C., Gomez-Barrero, M., Veldhuis, R. N. J., Spreeuwers, L., et al. (2017a). "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting," in *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)* (Darmstadt, Germany: IEEE) p. 1–7. doi: 10.23919/BIOSIG.2017.8053499

Scherhag, U., Raghavendra, R., Raja, K. B., Gomez-Barrero, M., Rathgeb, C., and Busch, C. (2017b). "On the vulnerability of face recognition systems towards morphed face attacks," in *2017 5th International Workshop on Biometrics and Forensics (IWBF)* (Coventry, United Kingdom: IEEE) p. 1–6. doi: 10.1109/IWBF.2017.7935088

Steyvers, M. (1999). Morphing techniques for manipulating face images. *Behav. Res. Methods, Instr. Comp.* 31, 359–369. doi: 10.3758/BF03207733

Tiddeman, B., Burt, M., and Perrett, D. (2001). Prototyping and transforming facial textures for perception research. *IEEE Comp. Graphics Appl.* 21, 42–50. doi: 10.1109/38.946630

Venkatesh, S., Ramachandra, R., Raja, K., Spreeuwers, L., Veldhuis, R., and Busch, C. (2019). "Morphed face detection based on deep color residual noise," in *2019 Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, (Istanbul: IEEE), 1–6. doi: 10.1109/IPTA.2019.8936088

Venkatesh, S., Zhang, H., Ramachandra, R., Raja, K., Damer, N., and Busch, C. (2020). "Can GAN generated morphs threaten face recognition systems equally as landmark based morphs? - Vulnerability and Detection," in *2020 8th International Workshop on Biometrics and Forensics (IWBF)*, 1–6. doi: 10.1109/IWBF49977.2020.9107970

Wallace, G. K. (1992). The JPEG still picture compression standard. *IEEE Trans. Consumer Electron.* 38, xviii–xxxiv. doi: 10.1109/30.125072

Winograd, S. (1976). On computing the discrete fourier transform. *Proc. Natl. Acad. Sci. U.S.A.* 73, 1005–1006. doi: 10.1073/pnas.73.4.1005

Zhang, H., Venkatesh, S., Ramachandra, R., Raja, K., Damer, N., and Busch, C. (2021). MIPGAN-generating strong and high quality morphing attacks using identity prior driven GAN. *IEEE Trans. Biom. Behav. Identity Sci.* 3, 365–383. doi: 10.1109/TBIOM.2021.3072349