# Secure Steganography Based on GAN Image Morphing: Implementation and Analysis

DIANA-ALEXANDRA BOZEA, University of Twente, The Netherlands

Steganography is the practice of concealing hidden data under a seemingly innocuous cover object. The necessity for secure transmission of sensitive information has become critical as digital communication has grown. Image steganography techniques, in which information is hidden in a digital image, are open to a variety of attacks that can compromise the security of the hidden message. This can occur if the steganography technology utilized is not strong enough to withstand certain attacks, such as picture compression, filtering, or other image alterations. Another issue is that some steganography systems have limited capacity, which limits the amount of information that can be buried within an image. To address these concerns, image morphing has been proposed as a viable method of improving steganography security. Image morphing is a technique for transforming one image into another through introducing transition frames between them. This paper aims to do a literature research on image morphing with image steganography and develop a new algorithm, named StegoMorph, based on DWT image steganography and GAN-based image morphing, as well as testing this new implementation against certain attacks such as statistical analysis and structural analysis. It will serve as a starting point for future research in this domain as a literature review, referencing the most relevant papers on the topic as well as propose a viable solution to enhancing steganography techniques in a novel way.

Additional Key Words and Phrases: Image Steganography, Image Morphing, Steganography Security, Robustness, Generative Adversarial Network (GAN), Discrete Wavelet Transform (DWT)

## 1 INTRODUCTION AND LITERATURE REVIEW

Steganography [5] is a technique for secret communication that involves hiding messages in cover material. Because of the prominence of digital photographs in everyday life, image steganography in particular has grown in popularity. In an early paper [5] about this topic the limitations of steganography have been highlighted, mentioning the fact that even the most robust algorithms still have a chance to be broken. Image steganography techniques are classified into two main categories [17]: Spatial Domain techniques (e. g. Least Significant Bit, Pixel Value Differencing) and Transform Domain techniques (e. g. Discrete Cosine Transformation, Discrete Fourier Transform, Discrete Wavelet Transform). Image morphing [36] consists of various techniques that create seamless transitions between two or more images using generated frames. The use of image morphing methods to increase the security of steganography is one possible answer to the limitations of image steganography [39]. This is because image morphing has the potential to increase the capacity and robustness of steganography by creating intermediate images that can be used to embed secret data. It also makes it harder for attackers to detect hidden data, making it a promising approach for enhancing security. The paper written by Wolberg [36] is one of the first papers on image morphing, it's advantages and limitations at the time. The aforementioned paper focuses on Deformation Techniques (e. g. triangulation, mesh warping, texture mapping). Recently, though, the focus in image morphing has shifted from deformation techniques towards deep learning approaches. This can be seen when looking up recent papers on image morphing steganography, that most of them utilize neural networks for image morphing. Such algorithms include Convolutional Neural Networks (CNN) [23] and Generative Adversarial Networks (GAN) [25]. These networks have the ability to generate new, natural looking images. As such, an attacker would not be able to compare a potential stego-image with a cover object already available on the internet. Furthermore, the networks may generate images of various sizes, having more capacity for embedding a message. This increases the capacity of the hidden data and makes it more resistant to steganalysis attempts. Image steganalysis is the technique of identifying the presence of hidden information in digital photographs by examining their statistical features. There are numerous such techniques [9, 10, 16] and after a literature review on steganalysis we selected one tool in order to assess the proposed solution.

This project has developed a new steganography technique based on image morphing which has been tested against certain steganalysis techniques in order to conclude whether the security enhancement is substantial or if further research must be done. The proposed solution, StegoMorph, is a new direction in image steganography, due to the fact that while there are already papers on steganography using deep learning [38], there has been no research done in applying an already robust steganographic technique to generated images from neural networks. This paper specifically will contribute to research in this domain by providing an extensive literature review, as well as propose a new tested method of using image morphing for digital image steganography.

### 1.1 Concepts involved

In this section there will be brief explanations of the concepts involved in this project, such as image steganography, image morphing, Discrete Wavelet Transform steganography and Generative Adversarial Networks.

*1.1.1 Image steganography.* Steganography, like cryptography, is an important area of information security. It has been around in many forms, from messages hidden under wax on wooden tablets, to putting pins above certain letters of a seemingly harmless message [14]. With the rise of technology, steganography has also evolved to utilize digital means. Today, there are many types of steganography, based on the nature of the cover object: text steganography, video steganography, network steganography, audio steganography and image steganography [27]. This paper focuses on the last mentioned type, namely digital image steganography, in which the information is hidden within the pixels of an image. There are two subcategories

*TScIT 39, July 7, 2023, Enschede, The Netherlands*

[17] to image steganography, based on the way the information is embedded: Spatial domain techniques and Transform domain techniques. This project utilizes Transform Domain techniques, due to their already high robustness and ability to maintain the quality of the cover image [4]. Within transform domain techniques, the image is represented in terms of frequencies instead of pixel values, and by modifying the coefficients of these frequencies, the message can be hidden in a seamless manner [18].

*1.1.2 Image morphing.* Image morphing is a collection of techniques through which a seamless transition is created between two or more images. It is an important development, commonly used in animation [26] and the film industry [36]. Existing image morphing techniques can be classified into mesh-based, point-based and patch-based techniques [7]. However, with the growing popularity of neural networks, researchers have shifted their focus on deep learning approaches, with multiple implementations of image morphing using various neural networks [8, 15, 33]. We have selected GAN based image morphing, for it's ability to create natural looking images [21, 40].

*1.1.3 Discrete Wavelet Transform steganography.* Discrete Wavelet Transform (DWT) is a transformation domain technique of steganography [24]. The way this technique works [32] is by representing the spatial domain of pixel values into frequencies, converting the image into sub bands of low-pass and high-pass coefficients. There are multiple variations of this technique [32], including Haar DWT, Diamond Encoding in DWT and Redundant DWT with QR Factorization. This project in particular is using Haar DWT due to the fact that it is the most simple and widely used approach.

*1.1.4 Generative Adversarial Networks.* Generative Adversarial Networks (GAN) are a type of architecture of neural networks. They are powerful tools used primarily in computer vision and natural text processing [6]. The network has two main components: a generator network and a discriminator network. Their goal is for the discriminator to be able to distinguish between generated images and real images, and or the generator to create images so as to fool the discriminator [35]. over time, there has been a great deal of variations in utilizing GANs for image generation. One such scope is image-to-image translation [1], in which the training dataset is divided into two domains and the goal is to morph the images from one domain into the other, while maintaining the clarity and quality of the original images [28]. There are multiple tools developed for image morphing and image generation using GAN, out of which we can name StyleGAN [15], StarGAN [8] and CycleGAN [40]. The latter has been the selected tool for this project.

### 1.2 Literature review

There has been a lot of research done in the past decades on steganography. The research can be divided into two categories: literature reviews [5, 12, 13, 31, 36] and implementations [7, 11, 19, 23, 37]. Out of these, we mainly shall focus on the papers that describe implementations of image morphing used with steganography or ideas for potential new algorithms. One such recent solution is provided by Li et al. [23], who present an innovative coverless image steganography system that uses morphing facial recognition based on convolutional neural networks (CNNs). The recommended approach uses CNN-based feature extraction and image processing methods to achieve high capacity and robustness. However, it has been found that the morphing process may result in distortion in the images, affecting the quality of the hidden message. Another solution is provided by Kadhim et al. [13], who provide a full evaluation of image steganography methods, including those that use image morphing. The survey examines several steganography methods' benefits, drawbacks, and potential future developments. The main limitation identified in this paper is that the image morphing based techniques have only been tested with a small range of images, consisting of mainly of gray-scale images. Furthermore, Kondo and Zhao [19] suggested an image morphing-based steganographic technique for hiding high-capacity and high-security data in digital photographs. Nevertheless, the main limitation with this method is its vulnerability to spatial transformations: rotations, scaling and skewing may affect the quality of the hidden information. Due to these limitations (applicability on small range of images, vulnerability to distortions), this paper aims to find a novel algorithm for digital image steganography based on image morphing.

## 2 RESEARCH QUESTIONS

The lack of concrete solutions in the field and the lack of technical implementations raise the following question:
*How can a new image steganography technique for all types of images based on image morphing be developed in order to enhance security against attacks?*
In order to be able to answer this, we shall further mention the following sub questions (SQ):
***SQ1:*** What image morphing technique is compatible to use with image steganography?
Firstly we must do a systematic literature review on the existing image morphing algorithms. In the past we could only find papers on deformation based techniques such as [2, 7, 22, 41]. However, since then the focus has changed towards deep learning based techniques [20], as the popularity of neural networks (NNs) grew. Two of the most popular NN types used in image morphing are convolutional neural networks (CNNs) and generative adversarial networks (GANs) [21, 30]. Due to the fact that research has shown that GANs have the potential to create more natural and expressive looking images [29, 34], that has been the selected image morphing technique used in this project.
Furthermore, the image steganography technique chosen for this project is the Discrete Wavelet Transform (DWT) [24] technique, due to the fact that it is an already robust algorithm that generates visually imperceptible stego-images. However, it may still be vulnerable to attacks and image transformations, thus we chose this algorithm.
***SQ2:*** What are the criteria (e. g. capacity, detectability, visual impact) that require enhancing in existing solutions of image morphing steganography?
During the literature review done for answering SQ1, it has been found that DWT has the potential to create artifacts when embedding the secret message, thus making the algorithm application detectable both through more advanced steganalysis techniques and

visually. Thus, the main criteria that we would like to enhance are visual aspect, security and robustness. Furthermore, even though it is not part of the main focus of the project, we would like to observe the impact that image morphing has on the embedding capacity of steganography.

***SQ3:*** Which steganography tools shall be used in the development process, considering the outcome of SQ1 and SQ2?

In order to answer this question, a systematic review of all the existing open source tools available for the chosen algorithms is needed. There are multiple tools available for GAN based image morphing. Amongst them we can name StyleGAN, StarGAN and CycleGAN. All of them are primarily used with facial images, using databases such as CelebA[1] or the Toronto Face Dataset (TFD)[2]. Due to its powerful and novel approach as well as the results showcased, the image morphing tool of choice is CycleGAN. Furthermore, due to its availability, wide range of images and size, we shall be working with the CelebA dataset, as it provides high quality facial images. By having facial images, the visual impact shall be easier to test.

As for the chosen tool for steganography, we will be using MATLAB[3], for its built in implementation of DWT steganography.

***SQ4:*** Which steganalysis tools shall be used for testing the robustness of the developed algorithm?

Due to the time constraint, we shall be testing the robustness and security of the proposed algorithm using statistical steganalysis.

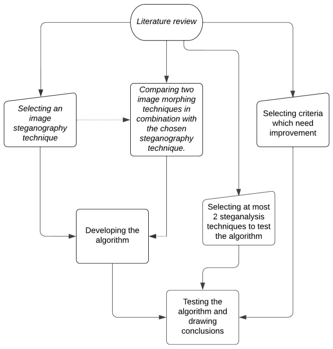
## 3 DESIGN & IMPLEMENTATION

In this section, the research process will be detailed and the proposed algorithm will be explained.

### 3.1 Methodology

In order to gather as much information as possible the databases IEEE, ScienceDirect, Wiley, Springer and Google Scholar were used, with search queries such as "image morphing", "image steganography", "steganography advancements", "image steganography security" and "image steganalysis" have been used. In order to answer the main research question, we must first answer the four sub-questions. For SQ1, we shall first have a systematic review of the already existing relevant literature on image steganography with image morphing. In this step we would like to select an image steganography technique which will be tested together with two image morphing techniques. For the reasons listed in the answer to SQ1, we have chosen Haar DWT and GAN-based image morphing. In order to answer SQ2, shall select after this step a set of criteria to be enhanced by the proposed solution as well as the type of images that the project will focus on (e. g. gray-scale, colour, image format). These criteria are based on the limitations identified in the already existing research done prior. Furthermore, in order to answer SQ3 we shall conduct another research on available open source tools for steganography that implement a certain algorithm chosen while answering SQ1. Then will follow a comparison of a selected robust steganography technique used with two different image morphing techniques, so as to find a pairing that enhances most, if not all of the chosen criteria. Lastly, in order to answer the final sub question, SQ4, there has to be done another research on available tools, this time for steganalysis techniques that assess the selected criteria from SQ2. A flowchart of the research process is in figure 1.

Fig. 1. Research outline


Literature review
Selecting an image steganography technique
Comparing two image morphing techniques in combination with the chosen steganography technique.
Selecting criteria which need improvement
Developing the algorithm
Selecting at most 2 steganalysis techniques to test the algorithm
Testing the algorithm and drawing conclusions

### 3.2 Development and Design Choices

The proposed algorithm is composed of two main parts: the image morphing tool and the steganography tool. Both of these parts have been implemented in MATLAB[4].

The image morphing part consists of an implementation of the CycleGAN architecture in MATLAB. It is a deep learning algorithm that specializes in image-to-image translation. It has two main components: a generator network and a discriminator network. The generator is trained to create images, while the discriminator learns how to distinguish between the generated images and the original training dataset. The goal is for the discriminator to become very good at classifying the images and for the generator to be able to fool the other component. GAN learns how to map images from one domain to another. In this project, the network has been trained with a small part of the CelebA[5] dataset, divided into two domains: 25 images of female celebrity faces, and 25 images of male celebrity faces. The source images are all of size 178x256p. The generates images, of size 256x256p, have as a source another sample (referred to as test sample) from the same dataset, using 21 images from each category. These sizes have been considered because the CycleGAN implementation only accepts outputs of size 128x128p, 256x256p or 512x512p, and the input must be of relatively similar, but preferably the same size. The result is 42 images, corresponding to each of the images in the test sample. Due to the fact that the dataset used to train the algorithm is small and the fact that the total number of iterations of the training algorithm was only 100, the resulted images have lower visual quality. The entire CelebA dataset consists of over 65000 images, thus the chosen sample is quite small. Also, the number of epochs used in training this GAN is 1000, according to the original implementation[6], but due to time constraints and

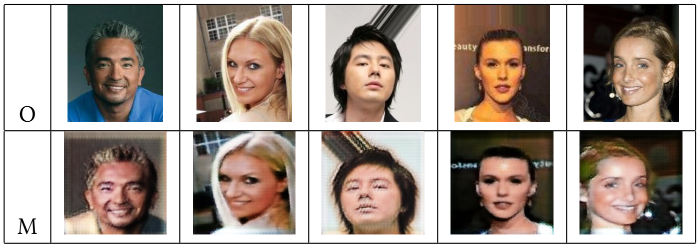
[1] https://mmlab.ie.cuhk.edu.hk/projects/CelebA.html
[2] http://www.iro.umontreal.ca/ lisa/twiki/bin/view.cgi/Public/ListDatasets
[3] https://nl.mathworks.com/products/matlab.html
[4] https://github.com/dianab613/StegoMorph.git
[5] See footnote 1
[6] https://github.com/matlab-deep-learning/Image-domain-conversion-using-CycleGAN.git

machine limitations the number has been greatly reduced. Furthermore, due to the fact that CycleGAN uses unsupervised learning, the resulting images have a clear correspondent in the original dataset. Secondly, the steganography part is a DWT implementation in MATLAB[7]. We have used the Haar wavelet [24], which is the most simple and used of the DWT variations. The cover image is divided into 4 frequency bands: LL (approximation band), LH (horizontal details band), HL (vertical details band) and HH (diagonal details band). The secret message is embedded into the LH band, due to the fact that it contains high frequencies, and the human eye is very sensitive to perceiving changes in low frequencies [32].

The algorithm works as follows: Firstly we generate the new cover images using the CycleGAN implementation. The generated images are saved and used as cover images in the DWT implementation. The resulting stego-images are then tested for performance, robustness and security.

Table 1 showcases the sample images used in the tests from the following sections. The first 5 images are the original images (first row, marked as O) from the dataset CelebA, and the other 5 are the corresponding morphed images (second row, marked as M).

Table 1. Sample images



## 4 PERFORMANCE ANALYSIS AND EXPERIMENTAL RESULTS

The stego-images resulted from the original dataset as well as the images resulted from applying StegoMorph correspondent with the sample images shown in Table 1 are shown in Tables 2 and 3. In both of the aforementioned tables, the first row (C) showcases the cover objects, and the second row (S) shows the resulting stego-images.

Table 2. Comparison between cover and stego-images of the original dataset using only DWT

Table 3. Comparison between cover and stego-images of the StegoMorph algorithm

Due to the fact that we would also like to know the Peak Signal to Noise Ratio (PSNR), the Mean Squared Error (MSE) as well as the maximum number of bytes that can be embedded into the image, the MATLAB implementation of the DWT steganalysis algorithm, we also calculate the PSNR, MSE and the maximum number of bytes that can be embedded. Table 4 showcases the results. In the algorithm column (Alg.), symbol $\alpha$ represents simple DWT, and symbol $\beta$ represents DWT used together with image morphing. The numbers 1 to 5 represent the cover images from Table 1, with 1 representing the images from the second column ( $\alpha$ 1 being the original cover image and $\beta$ 1 being the morphed cover image) and so on.

Table 4. Performance analysis

| Alg. | Img. | PSNR (dB) | MSE | Max cap. (B) |
|---|---|---|---|---|
| $\alpha$ | 1 | 58.5673 | 0.0904 | 3637 |
| $\alpha$ | 2 | 61.6710 | 0.0443 | 3637 |
| $\alpha$ | 3 | 66.8015 | 0.0136 | 3637 |
| $\alpha$ | 4 | 59.4206 | 0.0743 | 3637 |
| $\alpha$ | 5 | 59.2696 | 0.0769 | 3637 |
| $\beta$ | 1 | 73.9151 | 0.0026 | 6144 |
| $\beta$ | 2 | 71.0930 | 0.0051 | 6144 |
| $\beta$ | 3 | 68.0630 | 0.0102 | 6144 |
| $\beta$ | 4 | 66.4234 | 0.0148 | 6144 |
| $\beta$ | 5 | 68.5602 | 0.0091 | 6144 |

After analyzing the performance of the DWT algorithm implementation and the combination of DWT and GAN based image morphing, we can conclude the following points. To begin, comparing the Peak Signal-to-Noise Ratio (PSNR) [3] values of the original cover photos and matching morphing images reveals that the quality of the created stego-images is statistically greater. This means that the stego-images created by this novel approach are more accurate representations of the source cover images.

Secondly, Mean Squared Error (MSE) [13] evaluations demonstrate that it is more difficult to detect the presence of a hidden message in stego-images generated using GAN-based image morphing. The significantly reduced MSE values indicate that the changes made during the embedding process are less obvious when compared to the standard DWT implementation. This statistical aspect enhances the security and robustness of the steganographic process, making it more challenging for external parties to detect the hidden message.

[7] See footnote 3.

Furthermore, even though this was not in the scope of the project, we have found that there has been an increase in the embedding capacity of the algorithm. When compared to the traditional DWT technique, the usage of GAN-based image morphing nearly doubles the embedding capacity. Because of the increased embedding capacity, larger messages may now be put into stego-images, broadening the range of potential uses for this technology.

Lastly, the resulting morphed images have a lower visual quality than the original cover photos. While not unnatural, these images are less clear and have a slight reduction in visual clarity. This trade-off between visual quality and message imperceptibility is a common steganographic consideration. It is important to reach a compromise between visual clarity and efficient message embedding while developing steganographic algorithms.

Finally, combining DWT with GAN-based picture morphing produces promising results in terms of stego-image quality, message security, and embedding capacity. Statistical metrics such as PSNR and MSE indicate the advantages of this technique over traditional DWT implementation. Although the images produced are less clear, they are still within an acceptable range of naturalness.

Furthermore, we would also like to analyze the algorithm's robustness to image compression, as well as check the statistical qualities of the stego-image compared to the cover image. In order to do this, we have created the scripts in MATLAB.

For the compression, we test the PSNR (measured in dB) of the stego-image compared to the compressed stego-image. We shall use the same 3 images as before, with 3 different compression rates. The results have been gathered in table 5. In the same manner as table 4, symbol $\alpha$ represents simple DWT, and symbol $\beta$ represents DWT used together with image morphing.

Table 5. Compression analysis

| Algorithm | Img no. | Compression rate | | |
|---|---|---|---|---|
| | | 90 | 70 | 50 |
| $\alpha$ | 1 | 47.29 | 43.91 | 34.80 |
| $\alpha$ | 2 | 47.22 | 43.24 | 34.39 |
| $\alpha$ | 3 | 48.83 | 44.15 | 35.38 |
| $\alpha$ | 4 | 48.70 | 44.29 | 36.50 |
| $\alpha$ | 5 | 45.07 | 42.16 | 31.38 |
| $\beta$ | 1 | 49.68 | 45.07 | 37.08 |
| $\beta$ | 2 | 49.13 | 44.98 | 36.89 |
| $\beta$ | 3 | 48.76 | 44.46 | 36.10 |
| $\beta$ | 4 | 50.26 | 45.95 | 38.09 |
| $\beta$ | 5 | 49.20 | 45.19 | 36.90 |

After getting these results, we can conclude that the stego-images resulted from the morphed cover images are more resistant to compression than the stego images resulted from classical DWT, thus proving themselves to be more robust to spatial attacks.

## 5 SECURITY ANALYSIS

When generating the histograms of the morphed stego-images in order to compare them with the histograms of the respective cover images, we have found that the shapes are nearly identical. This means that the presence of a hidden message within the stego-image was imperceptible. To further prove that the difference between the morphed cover image and the stego-image, we calculated the mean value, the median, the variance and the skewness of the histogram. We would like to see how small the changes are and how sensitive the statistical analysis must be done in order to detect the presence of a hidden message. In Tables 7, 9, 11, 13, 15, 17, 19, 21, 23 and 25, the column Stego denotes of the image is a cover image (✗) or a stego-image (✓).

Table 6. Histogram comparison between 1st morphed cover and stego-image

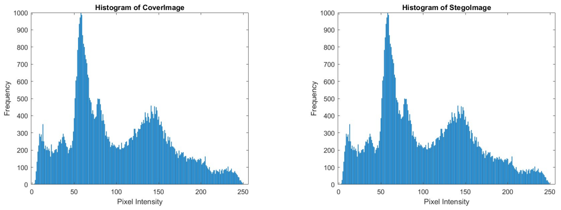


Table 7. Statistical values of morphed cover and stego-image 1

| Stego | Mean | Median | Variance | Skewness |
|---|---|---|---|---|
| ✗ | 102.1079 | 89.0000 | 3223.9498 | 0.4346 |
| ✓ | 102.1079 | 89.0000 | 3223.9498 | 0.4346 |

Table 8. Histogram comparison between 2nd morphed cover and stego-image

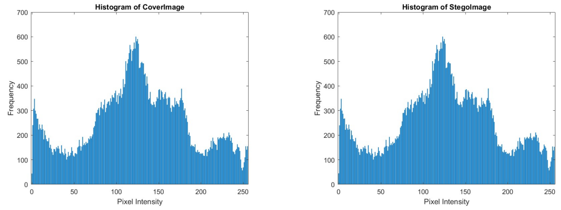


Table 9. Statistical values of morphed cover and stego-image 2

| Stego | Mean | Median | Variance | Skewness |
|---|---|---|---|---|
| ✗ | 125.2581 | 125.0000 | 3816.2453 | -0.0532 |
| ✓ | 125.2574 | 125.0000 | 3816.1123 | -0.0533 |

Table 10. Histogram comparison between 3rd morphed cover and stego-image

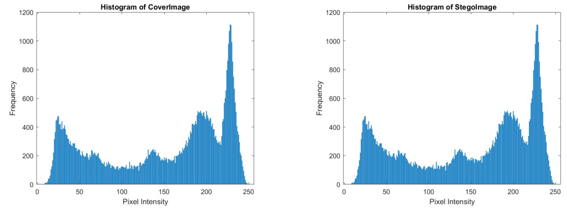


Table 11. Statistical values of morphed cover and stego-image 3

| Stego | Mean | Median | Variance | Skewness |
|---|---|---|---|---|
| ✗ | 148.9072 | 175.0000 | 5404.0006 | -0.4787 |
| ✓ | 148.9072 | 175.0000 | 5404.0006 | -0.4787 |

Table 12. Histogram comparison between 4th morphed cover and stego-image

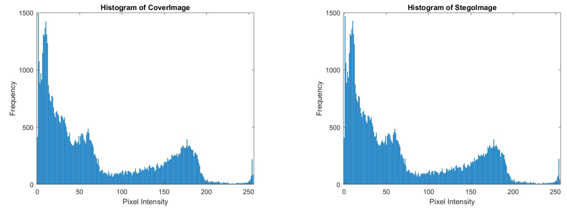


Table 13. Statistical values of morphed cover and stego-image 4

| Stego | Mean | Median | Variance | Skewness |
|---|---|---|---|---|
| ✗ | 69.9515 | 44.0000 | 4340.0797 | 0.8158 |
| ✓ | 69.9503 | 44.0000 | 4338.1745 | 0.8151 |

Table 14. Histogram comparison between 5th morphed cover and stego-image

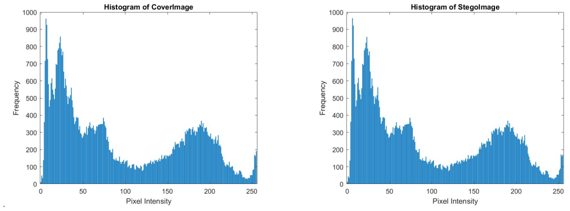


Table 15. Statistical values of morphed cover and stego-image 5

| Stego | Mean | Median | Variance | Skewness |
|---|---|---|---|---|
| ✗ | 95.5070 | 71.0000 | 5485.1919 | 0.4417 |
| ✓ | 95.5051 | 71.0000 | 5484.2009 | 0.4414 |

Table 16. Histogram comparison between 1st original cover and stego-image

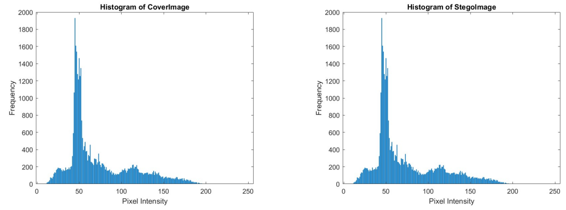


Table 17. Statistical values of original cover and stego-image 1

| Stego | Mean | Median | Variance | Skewness |
|---|---|---|---|---|
| ✗ | 73.0160 | 55.0000 | 1495.2555 | 1.0839 |
| ✓ | 73.0155 | 55.0000 | 1495.2387 | 1.0840 |

Table 18. Histogram comparison between 2nd original cover and stego-image

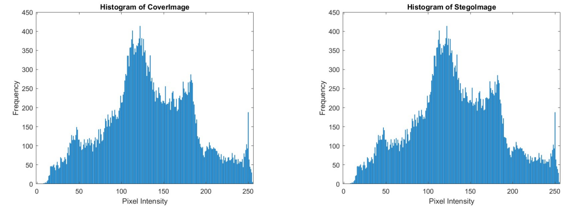


Table 19. Statistical values of original cover and stego-image 2

| Stego | Mean | Median | Variance | Skewness |
|---|---|---|---|---|
| ✗ | 132.5482 | 129.0000 | 2724.9940 | 0.0791 |
| ✓ | 132.5487 | 129.0000 | 2725.0250 | 0.0790 |

Table 20. Histogram comparison between 3rd original cover and stego-image

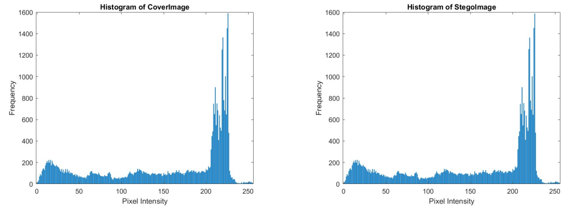


Table 21. Statistical values of original cover and stego-image 3

| Stego | Mean | Median | Variance | Skewness |
|---|---|---|---|---|
| ✗ | 154.3514 | 191.0000 | 5698.0546 | -0.7246 |
| ✓ | 154.3521 | 191.0000 | 5698.0744 | -0.7246 |

Table 22. Histogram comparison between 4th original cover and stego-image

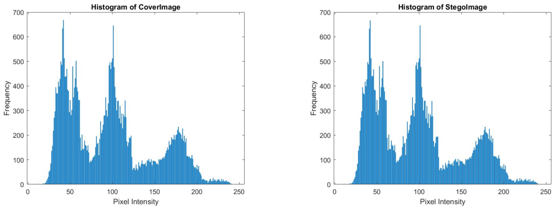


Table 23. Statistical values of original cover and stego-image 4

| Stego | Mean | Median | Variance | Skewness |
|---|---|---|---|---|
| ✗ | 97.6282 | 95.0000 | 2618.4367 | 0.5553 |
| ✓ | 97.6296 | 95.0000 | 2618.4644 | 0.5555 |

Table 24. Histogram comparison between 5th original cover and stego-image

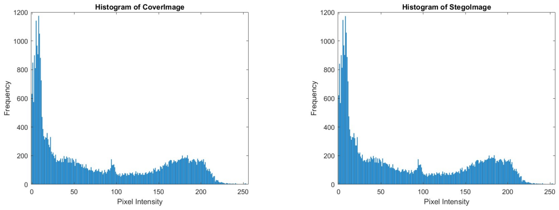


Table 25. Statistical values of original cover and stego-image 5

| Stego | Mean | Median | Variance | Skewness |
|---|---|---|---|---|
| ✗ | 78.5679 | 51.0000 | 5280.6124 | 0.5230 |
| ✓ | 78.5581 | 51.0000 | 5282.1398 | 0.5229 |

According to the Tables above, we can observe that with a sensitivity of 4 decimals is sometimes not enough to distinguish the difference between the morphed cover image and the morphed stego-image. These cases are shown in Tables 7 and 11 However, for all stego-images resulted from classic DWT, the difference is noticeable, as shown in Tables 17 to 25. We can also see the difference in the histogram comparison of the original dataset cover images with their respective cover images, in Tables 16, 18, 20, 22 and 24. We can see a difference in the distribution of the high frequencies, where the message has been hidden.

In all cases though the value difference between the means of a cover image and the respective stego-image is quite small. Thus, we can safely assume that the algorithm is secure against statistical steganalysis.

We can also see the original cover images have the same peak values as the corresponding morphed images, but do not necessarily follow the same curvature. Thus, we can tell that the original image has been used as input in the morphing process, but we cannot assume the fact that it is a stego-image.

### 5.1 Research outcome

After finishing this project, we have a new algorithm for image steganography based on GAN image morphing, that has been tested with steganalysis on the criteria selected in the research process. The proposed solution has proven to improve not only security of the image steganography algorithm, but also robustness and embedding capacity.

Furthermore, this paper will be beneficial for future research by providing areas which have not been covered in already existing literature as well as having a list of features that have the potential to be enhanced. It also contains references to the most relevant papers on the topic of image morphing used with image steganography for a further literature review.

## 6 CONCLUSIONS AND FUTURE WORK

To sum up, this paper has proposed a new algorithm based on CycleGAN image morphing and Haar DWT image steganography. It has been proven that this new solution enhances DWT's security against statistical attacks, embedding capacity and relative image quality when compared to the cover image used. The scope of this project was not only to create a new algorithm, but also to do a literature review and showcase the areas of research that have not been touched yet. This paper may serve as a reference for future researchers in the domain, in order to perhaps use the proposed solution for a more advanced algorithm or as a point of comparison. There have been some limitations to the project as well, which may be a starting point for future research or a potential continuation of this project. To begin with, the network for the CycleGAN has not been trained sufficiently, resulting in low visual quality images. Had there been available more time, the network could have been trained with a larger dataset, with more epochs, instead of only 100. Furthermore, for the steganalysis part, it would have been more appropriate to use a special tool that could test the detectability of the stego-images. However, due to time constraints again, it was not possible to train another network for deep learning steganalysis, and the commercially available tools found have not been compatible with DWT steganography. As such, in the future it would be ideal to test the security of the algorithm against other kinds of attacks. Another point for future advancements may include generating images of various sizes in order to test the flexibility of this algorithm.

## REFERENCES

[1] Alankrita Aggarwal, Mamta Mittal, and Gopi Battineni. 2021. Generative adversarial network: An overview of theory and applications. *International Journal of Information Management Data Insights* 1, 1 (April 2021), 100004. https://doi.org/10.1016/j.jjimei.2020.100004

[2] Marc Alexa. 2002. Recent Advances in Mesh Morphing. *Computer Graphics Forum* 21, 2 (2002), 173–198. https://doi.org/10.1111/1467-8659.00575 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/1467-8659.00575.

[3] Alaa A. Jabbar Altaay, Shahrin Bin Sahib, and Mazdak Zamani. 2012. An Introduction to Image Steganography Techniques. In *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*. 122–126. https://doi.org/10.1109/ACSAT.2012.25

[4] Farah Qasim Ahmed Alyousuf, Roshidi Din, and Alaa Jabbar Qasim. 2020. Analysis review on spatial and transform domain technique in digital steganography. *Bulletin of Electrical Engineering and Informatics* 9, 2 (April 2020), 573–581. https://doi.org/10.11591/eei.v9i2.2068 Number: 2.

[5] R.J. Anderson and F.A.P. Petitcolas. 1998. On the limits of steganography. *IEEE Journal on Selected Areas in Communications* 16, 4 (May 1998), 474–481. https:

//doi.org/10.1109/49.668971 Conference Name: IEEE Journal on Selected Areas in Communications.

[6] Zhipeng Cai, Zuobin Xiong, Honghui Xu, Peng Wang, Wei Li, and Yi Pan. 2022. Generative Adversarial Networks: A Survey Toward Private and Secure Applications. *Comput. Surveys* 54, 6 (July 2022), 1–38. https://doi.org/10.1145/3459992

[7] Jiaxu Chen, Long Zhang, Baoen Liu, Xiaoxu Li, and Zhongfu Ye. 2017. Image morphing using deformation and patch-based synthesis. In *2017 2nd International Conference on Image, Vision and Computing (ICIVC)*. 376–380. https://doi.org/10.1109/ICIVC.2017.7984581

[8] Yunjey Choi, Youngjung Uh, Jaejoo Yoo, and Jung-Woo Ha. 2020. StarGAN v2: Diverse Image Synthesis for Multiple Domains. 8188–8197. https://openaccess.thecvf.com/content_CVPR_2020/html/Choi_StarGAN_v2_Diverse_Image_Synthesis_for_Multiple_Domains_CVPR_2020_paper.html

[9] Numrena Farooq and Arvind Selwal. 2023. Image steganalysis using deep learning: a systematic review and open research challenges. *Journal of Ambient Intelligence and Humanized Computing* (March 2023). https://doi.org/10.1007/s12652-023-04591-z

[10] Huayong Ge, Mingsheng Huang, and Qian Wang. 2011. Steganography and steganalysis based on digital image. In *2011 4th International Congress on Image and Signal Processing*, Vol. 1. 252–255. https://doi.org/10.1109/CISP.2011.6099953

[11] Tian Guanglai, Chi-Cheng Chen, Sun Gengxin, and Bin Sheng. 2020. Research on Face Image Morphing Based on Automatic Feature Detection. In *2020 IEEE 2nd Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS)*. 172–174. https://doi.org/10.1109/ECBIOS50299.2020.9203749

[12] Adnan Gutub and Faiza Al-Shaarani. 2020. Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons. *Arabian Journal for Science and Engineering* 45, 4 (April 2020), 2631–2644. https://doi.org/10.1007/s13369-020-04413-w

[13] Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial, and Brendan Halloran. 2019. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing* 335 (March 2019), 299–326. https://doi.org/10.1016/j.neucom.2018.06.075

[14] David Kahn. 1996. The history of steganography. In *Information Hiding (Lecture Notes in Computer Science)*, Ross Anderson (Ed.). Springer, Berlin, Heidelberg, 1–5. https://doi.org/10.1007/3-540-61996-8_27

[15] Tero Karras, Samuli Laine, and Timo Aila. 2019. A Style-Based Generator Architecture for Generative Adversarial Networks. https://doi.org/10.48550/arXiv.1812.04948 arXiv:1812.04948 [cs, stat].

[16] Manveer Kaur and Gagandeep Kaur. 2014. Review of Various Steganalysis Techniques. 5 (2014).

[17] Sumeet Kaur, Savina Bansal, and R. K. Bansal. 2014. Steganography and classification of image steganography techniques. In *2014 International Conference on Computing for Sustainable Global Development (INDIACom)*. 870–875. https://doi.org/10.1109/IndiaCom.2014.6828087

[18] Iqra Khalid, Muhammad Naeem, Asim Shahzad, Imran Muhammad, Muhammad Khan, Ahsan Zeeshan, Muhammad Zubair, Muhammad Tahir, Sibt Asshad, and Hassan Ul. 2021. A Comprehensive Analysis Of Image Steganography And Its Techniques. *Webology* 18 (Oct. 2021), 2523–2532.

[19] Satoshi Kondo and Qiangfu Zhao. 2006. A Novel Steganographic Technique Based on Image Morphing. In *Ubiquitous Intelligence and Computing (Lecture Notes in Computer Science)*, Jianhua Ma, Hai Jin, Laurence T. Yang, and Jeffrey J.-P. Tsai (Eds.). Springer, Berlin, Heidelberg, 806–815. https://doi.org/10.1007/11833529_82

[20] Vijay Kumar, Sahil Sharma, Chandan Kumar, and Aditya Kumar Sahu. 2023. Latest Trends in Deep Learning Techniques for Image Steganography. *International Journal of Digital Crime and Forensics (IJDCF)* 15, 1 (Jan. 2023), 1–14. https://doi.org/10.4018/IJDCF.318666 Publisher: IGI Global.

[21] P. G. Kuppusamy, K. C. Ramya, S. Sheebha Rani, M. Sivaram, and Vigneswaran Dhasarathan. 2020. A Novel Approach Based on Modified Cycle Generative Adversarial Networks for Image Steganography. *Scalable Computing: Practice and Experience* 21, 1 (March 2020), 63–72. https://doi.org/10.12694/scpe.v21i1.1613 Number: 1.

[22] Seung-Yong Lee, Kyung-Yong Chwa, James Hahn, and Sung Yong Shin. 1996. Image Morphing Using Deformation Techniques. *The Journal of Visualization and Computer Animation* 7, 1 (1996), 3–23. https://doi.org/10.1002/(SICI)1099-1778(199601)7:1<3::AID-VIS131>3.0.CO;2-U _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/%28SICI%291099-1778%28199601%297%3A1%3C3%3A%3AAID-VIS131%3E3.0.CO%3B2-U.

[23] Yung-Hui Li, Ching-Chun Chang, Guo-Dong Su, Kai-Lin Yang, Muhammad Saqlain Aslam, and Yanjun Liu. 2022. Coverless image steganography using morphed face recognition based on convolutional neural network. *EURASIP Journal on Wireless Communications and Networking* 2022, 1 (March 2022), 28. https://doi.org/10.1186/s13638-022-02107-5

[24] Pratap Chandra Mandal, Imon Mukherjee, Goutam Paul, and B. N. Chatterji. 2022. Digital image steganography: A literature survey. *Information Sciences* 609 (Sept. 2022), 1451–1488. https://doi.org/10.1016/j.ins.2022.07.120

[25] Hiroshi Naito and Qiangfu Zhao. 2019. A New Steganography Method Based on Generative Adversarial Networks. In *2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST)*. 1–6. https://doi.org/10.1109/ICAwST.2019.8923579 ISSN: 2325-5994.

[26] Frederic Pighin, Joel Auslander, Dani Lischinski, David H Salesin, and Richard Szeliski. [n. d.]. Realistic Facial Animation Using Image-Based 3D Morphing. ([n. d.]).

[27] Praveen. 2023. A Guide to Steganography: Meaning, Types, Tools, & Techniques. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-steganography-guide-meaning-types-tools/

[28] Elad Richardson, Yuval Alaluf, Or Patashnik, Yotam Nitzan, Yaniv Azar, Stav Shapiro, and Daniel Cohen-Or. 2021. Encoding in Style: A StyleGAN Encoder for Image-to-Image Translation. 2287–2296. https://openaccess.thecvf.com/content/CVPR2021/html/Richardson_Encoding_in_Style_A_StyleGAN_Encoder_for_Image-to-Image_Translation_CVPR_2021_paper.html

[29] Eklavya Sarkar, Pavel Korshunov, Laurent Colbois, and Sébastien Marcel. 2022. Are GAN-based morphs threatening face recognition?. In *ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2959–2963. https://doi.org/10.1109/ICASSP43922.2022.9746477 ISSN: 2379-190X.

[30] Clemens Seibold, Wojciech Samek, Anna Hilsmann, and Peter Eisert. 2018. Accurate and Robust Neural Networks for Security Related Applications Exampled by Face Morphing Attacks. http://arxiv.org/abs/1806.04265 arXiv:1806.04265 [cs].

[31] Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, and Ahmed Bouridane. 2021. Image Steganography: A Review of the Recent Advances. *IEEE Access* 9 (2021), 23409–23423. https://doi.org/10.1109/ACCESS.2021.3053998 Conference Name: IEEE Access.

[32] Nishant Madhukar Surse and Preetida Vinayakray-Jani. 2017. A comparative study on recent image steganography techniques based on DWT. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. 1308–1314. https://doi.org/10.1109/WiSPNET.2017.8299975

[33] Junya Ueda and Katsunori Okajima. 2019. Face morphing using average face for subtle expression recognition. In *2019 11th International Symposium on Image and Signal Processing and Analysis (ISPA)*. 187–192. https://doi.org/10.1109/ISPA.2019.8868931 ISSN: 1849-2266.

[34] Sushma Venkatesh, Haoyu Zhang, Raghavendra Ramachandra, Kiran Raja, Naser Damer, and Christoph Busch. 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. https://doi.org/10.1109/IWBF49977.2020.9107970

[35] Zhengwei Wang, Qi She, and Tomás E. Ward. 2022. Generative Adversarial Networks in Computer Vision: A Survey and Taxonomy. *Comput. Surveys* 54, 2 (March 2022), 1–38. https://doi.org/10.1145/3439723

[36] G. Wolberg. 1996. Recent advances in image morphing. In *Proceedings of CG International '96*. 64–71. https://doi.org/10.1109/CGI.1996.511788

[37] Srushti S Yadahalli, Shambhavi Rege, and Reena Sonkusare. 2020. Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques. In *2020 5th International Conference on Communication and Electronics Systems (ICCES)*. 1325–1330. https://doi.org/10.1109/ICCES48766.2020.9137887

[38] Chaoning Zhang, Chenguo Lin, Philipp Benz, Kejiang Chen, Weiming Zhang, and In So Kweon. 2021. A Brief Survey on Deep Learning Based Data Hiding. https://doi.org/10.48550/arXiv.2103.01607 Publication Title: arXiv e-prints ADS Bibcode: 2021arXiv210301607Z.

[39] Qiangfu Zhao and Tosiyasu L. Kunii. 2013. Steganography based on image morphing. In *2013 International Joint Conference on Awareness Science and Technology & Ubi-Media Computing (iCAST 2013 & UMEDIA 2013)*. 157–163. https://doi.org/10.1109/ICAwST.2013.6765426

[40] Jun-Yan Zhu, Taesung Park, Phillip Isola, and Alexei A. Efros. 2020. Unpaired Image-to-Image Translation using Cycle-Consistent Adversarial Networks. https://doi.org/10.48550/arXiv.1703.10593 arXiv:1703.10593 [cs].

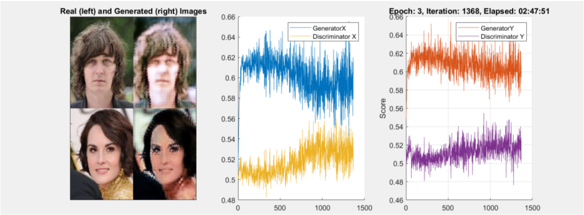
[41] Bhushan Zope and Soniya Zope. 2017. A Survey of Morphing Techniques. *International Journal of Advanced engineering, Management and Science* 3 (Jan. 2017), 81–87. https://doi.org/10.24001/ijaems.3.2.15

## A APPENDIX

In this section there are included a selection of snapshots from the actual tools used in this project.

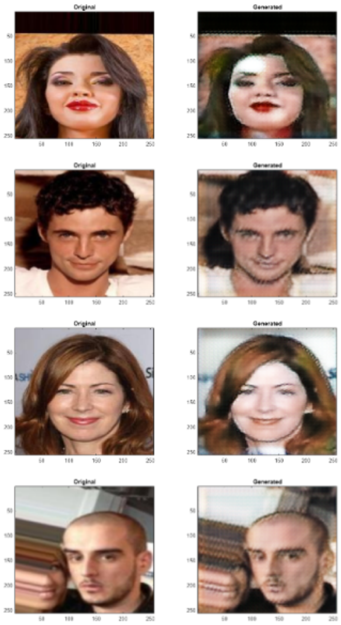
### A.1 Appendix A.1

Snapshot of the training of the CycleGAN implementation. The machine used has been a laptop with Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz 1.99 GHz Processor with 8.00 GB RAM. The total time taken for the network to train was approximately 6 hours.



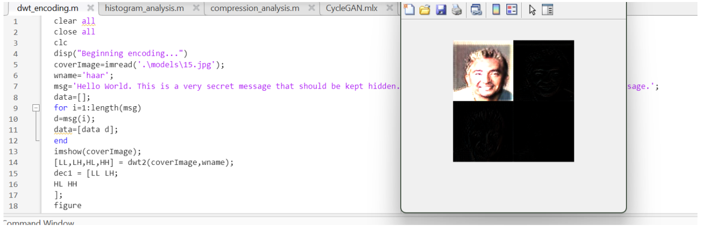
## A.2 Appendix A.2

Snapshot of a few generated images from the GAN, excluding the ones sampled in this paper.



## A.3 Appendix A.3

Snapshot of the message embedding process, with the cover image split into the 4 frequency bands discussed in section 3.2, according to DWT architecture.



```
clear all
close all
clc
disp("Beginning encoding...")
coverImage=imread('.\models\15.jpg');
wname='haar';
msg='Hello World. This is a very secret message that should be kept hidden.                    sage.';
data=[];
for i=1:length(msg)
d=msg(i);
data=[data d];
end
imshow(coverImage);
[LL,LH,HL,HH] = dwt2(coverImage,wname);
dec1 = [LL LH;
HL HH
];
figure
```