

Protecting Privacy with Image Processing: How Blurring and Masking Help Keep Us Safe Online

Khairi Salem Ahmed¹ and Abdulhakim A. S. Baroud²

¹Department of Computer, College of Science, Bani Waleed University, LIBYA.

²Department of Computer, College of Science, Bani Waleed University, LIBYA.

²Corresponding author: abdulhakimbaroud@bwu.edu.ly



www.jrasb.com || Vol. 1 No. 1 (2022): April Issue

Received: 03-04-2022

Revised: 13-04-2022

Accepted: 25-04-2022

ABSTRACT

Because more people are using technological networks, it is now easier to share pictures that contain private information. PSNR, SSIM and a custom Privacy Preservation Score. Median blur, Box Blur (Average Blur), Pixelation and Masking methods to an array of facial images or license plates or background objects We measured how well they worked using we investigate the effectiveness of image obfuscation techniques such as pixelization, masking, and blurring in protecting privacy during online sharing for images. We were applied a certain range of filters, such as Gaussian blur, about identity theft, privacy and the unauthorized use of your information. In this work, Now people are worried The results show that Gaussian blur keeps things clear to the eye while also providing a good level of anonymity. Average blur, on the other hand, keeps the structural boundaries but may leave hints that help you figure out what the object is. Pixelation makes things more private by changing the size of the blocks, which is especially useful for organized elements. Masking methods give it is the highest level of confidentiality achievable because they eliminate of each identifiable knowledge. A glance at how people see images supports the idea that masking is an effective method to circulate pictures safely, regardless of whether it may not appear as good. The results show that there is no one best way to do things; instead, the choice should depend on how sensitive the information is and what the image will be used for. For social networking companies, application developers, and individuals looking to enhance digital safety, this study offers practical insights. While identification algorithms advance, it also emphasizes the requirement that more robust private measures which artificial intelligence cannot violate.

Keywords- Privacy Preservation, Image Blurring, Face Masking, Data Protection, Online Safety.

I. INTRODUCTION

The rapid growth of networking platforms as well as digital technology has made photo sharing a crucial means of communication. People often share photos to commemorate social events, showcase individual accomplishments, or connect with unfamiliar individuals online. But our growing reliance on visual media has also made privacy problems harder to solve. Pictures that are shared online may be used by individuals or robots that shouldn't have access to private information such as individuals, license plates, locations, surrounding objects, or biographical data. . AI and computer vision are getting better all the time, and even pictures that seem harmless can give away a lot of private information about

you, like who you are, where you go, and how much money you have. Because of this, online privacy is now a big concern, and we need to find good ways to protect personal information in digital pictures.

1.1 Role of Image Processing in Privacy Protection

Image processing methods are becoming a crucial component of protecting people's privacy online. Before releasing images to the public, identifiable elements may be obscured using techniques including pixelation, masking, and blurring. These techniques can alter a portion of a picture while preserving the remainder. This allows users to continue utilizing the image without exposing sensitive areas. As surveillance equipment as face identification software improve, such privacy-protecting measures are more crucial as before. Image

processing helps consumers better control their digital footprints through rendering identifying information more difficult to recognize or see. Additionally, it prevents malicious actors or unapproved technology from using their graphical data.

1.2 Problem Statement

Even though there are many ways to process images to protect privacy, it's not clear how well different blurring and masking methods work in real life, how easy they are to use, or how effective they are. Many people on social media sites use the default filters without knowing if they really protect them from new threats like deep learning-based facial recognition, automated data mining, or identity reconstruction. Also, the privacy features that are available now are very different on different platforms, and there are no standard rules for how to protect personal information in images. These gaps show that we need to look at how well blurring and masking techniques work in real life and how they help keep people safe online in a more organized way.

1.3 Objectives of the Study

The purpose of this investigation is to methodically examine how picture masking or obscuring protect personal privacy in online settings. The particular objectives are:

1. To investigate the primary image processing techniques utilized for privacy protection.
2. To determine the efficacy, decrease of clarity, and durability of detection algorithms of different blurring as well as masking strategies.
3. To evaluate the effectiveness of techniques such as region-based masking, median blur, Gaussian blur, and pixilation
4. To demonstrate the advantages and disadvantages of each approach as well as how they function in actual situations.
5. To provide advice concerning how to utilize image processing technologies that protect personal data on applications or social media.

1.4 Research Questions

The following research questions are examined in the study:

1. In what ways can features like disguising as well as blurring protect user privacy as we upload images to the internet?
2. Which picture editing methods keep privacy while still being easy to use?
3. How well do these methods work against modern threats like AI-powered face recognition software?
4. What kinds of problems come up when these methods are used on well-known digital platforms?

1.5 Significance of the Study

As more or more people use digital communication and AI, protecting visual privacy is no longer a choice but a necessity. Many different groups of people can use the information in this study. It teaches individuals who use social networking sites how to protect their private information in pictures. It shows how

programmers or system designers can improve privacy features. The study's findings could assist legislators in formulating regulations and legislation concerning digital privacy. The research provides significant insights into a domain that influences online safety as well as privacy freedom, particularly as individuals remain concerned about issues such as telecommunications doxxing, digital surveillance, while stolen identities.

1.6 Scope of the Study

The study focuses on image processing techniques used to protect privacy, particularly blurring and masking techniques. It doesn't talk about encryption or watermarking, but these could work well with tools that protect your privacy. The work focuses on privacy-preserving image processing methods, namely masking or blurring methods. Watermarks and encryption aren't discussed, although they could be useful with privacy-protecting technologies.

II. METHODOLOGY

2.1 Research Design

This investigation employs an exploratory research approach to assess the efficacy of blurring as well as masking methods for safeguarding confidentiality in digital images. The approach strongly emphasizes contrast between the findings obtained from implementing multiple image processing techniques to a controlled dataset or evaluating the outcomes against established criteria. There are both qualitative as well as quantitative tests. The work focuses on privacy-preserving image processing methods, namely masking or blurring methods. Watermarking and cryptography aren't discussed, although they could be useful with privacy-protecting technologies.

2.2 Dataset Description

- The collection contains several images of people, license plates, as well as additional objects which are often seen through online postings. To ensure that the photos were utilized fairly or failed to infringe on any individual's privacy, they were selected from open, free sources such as Unspeakeable and Pexels. The dataset contains:
 - 50 pictures of faces with various lighting, poses, as well as settings
 - 20 pictures with identification numbers to test concealing that works in some places
 - 15 images with different types of content that show at least one private belonging during a given moment.
- During uniform editing, every picture was downsized to a standard dimension of 640×480 pixels.

2.3 Tools and Technologies Used

Since Python offers many image analysis tools, we utilized it to build blurring or masking methods. People primarily use these tools:

- OpenCV: for using filters like median blur, Gaussian blur, pixelation, or region masking.
- NumPy: for working with numbers or arrays

- Matplotlib: to show processed outputs in a visual way. Everyone picked these tools since they are very precise, simple to use, as well as can be used more than once.

2.4 Preprocessing Steps

Before using privacy-preserving methods, the data went through a number of steps to get ready:

1. For an uninterrupted look, change the color space from BGR to RGB.
2. identifying locations, such as faces or items, which require privacy protection on their own utilizing OpenCV's Haar Cascade classifier.
3. Annotation to make sure that the areas that were found match the objects that can be seen these steps made sure that all of the techniques were used correctly and the same way on all the images.

2.5 Image Blurring Techniques

Three types of blurring techniques were chosen because they are often used to protect confidentiality.

2.5.1 Gaussian Blur

To apply Gaussian blur, the image was convolved with a Gaussian kernel. By smoothing down pixel values, this technique renders it more difficult to discern the features of a person's face. We examined the effects of varying intensity degrees on confidentiality by examining kernels dimensions such as 15×15 and 25×25 .

2.5.2 Box Blur (Average Blur)

The box blur effect takes the average of the pixel intensities in a given area. We used kernels that were either 10×10 or 20×20 . This method is easier than Gaussian blur, but it might leave behind patterns that can be seen. This is a good way to compare the quality of the picture and the strength of privacy.

2.5.3 Median Blur

In median blur, each pixel is replaced by the median value of the pixels around it. It works well to reduce noise while keeping the edges. We tried out filters 11 and 21. This way, some of the picture stays clear while small details on the face are hidden.

2.6 Masking and Pixelation Techniques

2.6.1 Pixelation

To pixelate something, you lower the resolution of the area you found and then bring it back up to its original size. This makes it look blocky. Different downscale factors, such as $4 \times$, $8 \times$, and $12 \times$, were used to figure out how serious privacy was.

2.6.2 Region-Based Masking

A black or distorted patch was put over the recognized face or plate when solid-color masking was used. We tried out two different versions:

- A solid black mask for the most privacy
- Mask that is blurry we tried these methods to see how full obstruction compares to partial detail reduction:
- Blurred Mask with a longer Gaussian kernel.

2.7 Metrics for Evaluation

To assess the effectiveness of each technique, a combination of qualitative and quantitative evaluation metrics was utilized:

2.7.1 Peak Signal-to-Noise Ratio (PSNR)

PSNR tells you exactly how worse an image looks after you use a privacy filter. Larger changes that might be seen by smaller PSNR evaluations often mean that confidentiality is better safeguarded.

2.7.2 Structural Similarity Index (SSIM)

SSIM checks how similar the altered image is to the original image. Lower SSIM values mean more distortion and less recognizability, which is important for privacy reasons.

2.7.3 Privacy Preservation Score

We came up with a custom score based on how distorted the area was and how well facial recognition tools could find it. We found this out by running processed images through an open-source face detection model. A lower rate of identification meant better privacy protection.

2.7.4 Human Perception Test (Qualitative)

A few individuals examined the specimens in order to determine if they continued to locate the secret location. This helped check if the picture was still easy to see after it was processed.

III. IMAGE PROCESSING TECHNIQUES FOR PRIVACY PROTECTION

3.1 Overview of Privacy-Preserving Filters

Privacy-preserving filters are special ways to change images so that they don't show identifiable details but still show the overall context of the image. These filters protect people from being seen without their permission, having their personal information used without their permission, and automated surveillance systems. These methods let individuals share photos with others without giving away personal information by only changing certain parts of the image, like faces, license plates, and various other confidential things. The kind of filter they selects will depend on how much safety, usefulness, as well as aesthetic that individual want through the picture.

3.2 Facial Blurring and Identity Obfuscation

One of the most common ways to protect your data is to blur your face, especially on news and social media sites. To make it harder to see and recognize, an optical mask is put on some parts of the face. As an, people frequently resort to movement blur, median blur, as well as Gaussian blur. Such approaches change the arrangement of the pixels and make facial features less consistent, which makes it less likely that people and AI-based face recognition systems will be able to identify someone. Visual distortion keeps the picture intact, but it has to be strong enough to keep computers from figuring out what's hidden.

3.3 Object-Specific Masking

The objective of object-specific masking is to hide parts of a picture that could give away private information. Common targets are things like residence

numbers, license plates, brand names, or documentation that can be seen in the background. People frequently apply solid shapes like polygons, circles, or squares to cover up the area they would like to hide. On the other hand, hiding offers the most privacy by taking away all information from the hidden area. On the other hand, blurring keeps some of the initial layout. This approach works best when just a little of information that is easy to see could put protection at risk, like in court documents or images of automobiles.

3.4 Pixelation and Resolution Reduction

One way to keep secret information safe is to make some parts of an image appear pixelated by lowering the pixel density. Pixelation takes small groups of pixels as well as puts them all together to make larger squares. This renders the region less detailed, though one can continue to tell which it is. Pixelation is a common way to protect people's identities in TV shows, online videos, and educational materials. Pixelation can still give advanced artificial intelligence enough information to determine out who an individual is, but it's not as clear as concealed. Therefore, choosing the appropriate pixel limit dimension is crucial to protecting personal privacy.

3.5 Edge Preservation vs. Privacy Trade-Off

Striking the right balance between hiding details and keeping boundaries or other information that helps maintain matters in context is among of the most challenging aspects of the processing of images that protects privacy. Median blur and other methods may assist hide key characteristics without making the picture look worse by keeping the outer edges sharp. Never the less retaining too much crucial data may make security more problematic because particular algorithms may use outside signals to find people and things. Black box masking along with other severe techniques, on the other hand, decrease the picture's quality while maintaining all the details private. When picking a method, you need to think about how much structure the image needs for its purpose and how much privacy requires to be kept.

IV. RESULTS

4.1 Performance of Blurring Techniques

We observed distinct variations in how well the Gaussian, median, and box blur methods hid sensitive human facial features when we examined them. Gaussian blur made the distortion look the smoothest as well as made the picture the hardest to recognize. Median blur was good at getting rid of smaller details, but it kept some of the edges of the face, which made it a little less private overall. Box blur did the worst of the three, leaving behind structural patterns that modern recognition algorithms continued to understand. Quantitative metrics corroborated that Gaussian blur offered superior privacy protection, evidenced by diminished SSIM values and decreased visual clarity.

Table 1. Performance Metrics of Blurring Techniques

Technique	PSNR Score	SSIM Value	Privacy Score (0–10)
Gaussian Blur	21.4 dB	0.42	9.2
Median Blur	23.8 dB	0.51	8.1
Box Blur	27.3 dB	0.62	6.7

4.2 Effectiveness of Masking and Pixelation Methods

Among all the methods tested, masking methods offered the best privacy protection. Black box masking completely hid the information, giving it a perfect privacy score. Pixelation worked, but it worked better on some block sizes than others. Smaller pixel blocks kept too much structural information, which made it easier to put things back together. On the other hand, bigger blocks made things less visible and better for privacy. Shape-based masking worked okay, but it wasn't as good as rectangular black masking because it didn't cover everything completely.

Table 2. Evaluation of Masking and Pixelation Techniques

Technique	Clarity Reduction	SSIM Value	Privacy Score (0–10)
Black Box Masking	100%	0	10
Pixelation (Small)	60%	0.48	7.4
Pixelation (Large)	85%	0.33	8.8
Shape-Based Masking	90%	0.27	9.1

4.3 Comparative Summary Across All Techniques

We looked at different methods to see which ones work best for different types of sensitive information, such as faces, license plates, and background details. For facial areas where context is important, blurring worked well. For sensitive numbers or text, such as license plates, masking performed better. Pixelation was a good choice because it made things less clear but still let some shapes be seen. The results indicate that no single method is universally superior; the choice is dependent upon the specific type of detail that needs safeguarding.

Table 3. Best Technique for Each Sensitive Region

Sensitive Information	Most Effective Technique	Reason
Human Faces	Gaussian Blur	High obscurity with preserved context
License Plates	Black Box Masking	Complete concealment required
Background Objects	Median Blur	Removes detail while preserving edges
Text on Documents	Large Pixelation	Breaks text structure effectively

4.4 User Perception and Visual Assessment

A qualitative evaluation was conducted to ascertain how human observers perceived the privacy level of each processed image. People said that images that were just a bit blurry looked the most real, yet individuals also said that a little bit of blurring still made it possible to tell what they were. Some people liked pixelated images better because they looked better, but others thought they were too distracting. People said that masking techniques were the best for privacy but the worst for how they looked. The perception results were very close to the numbers overall.

Table 4. User Feedback on Visual Quality and Privacy

Technique	Visual Quality Rating (0–10)	Perceived Privacy (0–10)
Gaussian Blur	8.5	9
Median Blur	7.8	8.2
Pixelation	6.9	8.5
Black Box Masking	5.1	10

V. DISCUSSION

The results of the investigation indicate that various image processing techniques safeguard privacy to varying extents, each possessing distinct advantages and disadvantages. Blurring methods, specifically Gaussian blur, worked well to make small things or facial features less clear without disrupting the entire image too much. It was clear that there became additionally a lot of conceptual understanding needed to get decent SSIM measurements, nevertheless though the imagery was very unreliable. This indicates that advanced AI methods might be able to put the picture back together in some way. But masking methods offer the most anonymity, as shown by their very low SSIM assessments or highest privacy ratings. The Pixelation impact did an excellent job of hiding details while still keeping the context. All of the tried ways true techniques make things safer, however the best one will regarding on the level of security it ought to be as well as the level of details you are sending.

5.1 Comparison of Techniques Based on Evaluation Metrics

Examples of quantitative measurements that show how the methods operate in various ways include the privacy preservation score, PSNR, and SSIM. Given how smooth they seemed, the blurring techniques' higher PSNR values indicate that they produced considerable distortion. The SSIM values were a little higher because median blur did a better job of keeping boundaries than Gaussian blur. Pixelation made the picture less detailed, which led to lower PSNR as well as SSIM scores. This made it easier to hide places with structure, like license plates. During SSIM, masking strategies got the lowest score possible, which meant that they got rid of all of the

data. They always got the highest score for protecting privacy. These results show that masking is the safest way to do it, but it is also the most visually intrusive. In contrast, the effects of blurring as well as pixelation vary based on the context.

5.2 Practical Implications for Real-World Applications

Journalists, multimedia creators, users of social networking sites, as well as businesses that work with visual data should pay attention to the research's findings. If confidentiality isn't equally essential as how the picture looks, blurring methods are great for exchanging pictures with relatives and friends. Pixelation is a good way to hide things like license plates in backgrounds that need to keep their shape. Disguising should be the norm for protecting very private information, like legal papers, exclusive reports, and government data, even though it may seem sudden. These findings indicate that a uniform approach to privacy is inadvisable. You should choose the best approach to your needs instead.

5.3 Challenges in Balancing Privacy and Image Utility

This survey says that finding the right balance between privacy as well as effectiveness is the biggest problem. Sometimes, masking and other privacy-preserving methods make images less useful by taking away information that gives them meaning. If researcher use methods like Gaussian blur and others that keep the quality of the picture, AI-based systems might be capable of to find an individual with enough information. It is harder to pick a strategy because new developments in machine learning could make traditional obfuscation less effective. Such issues demonstrate how important flexible as well as hybrid procedures are, like dynamic blurring, incorporated masking-blurring techniques, or confidential sharing approaches which protect security as well usability.

5.4 Limitations of the Study

While the study yielded significant results, it is imperative to recognize its limitations. The dataset was of moderate size and, despite careful selection, may not encompass the complete diversity of real-world images. The evaluation metrics, although frequently utilized in research, do not capture all aspects of privacy, especially regarding sophisticated AI adversaries. Additionally, the user perception analysis involved a limited participant pool, which may impact the generalizability of subjective assessments. Future research ought to employ additional information sets, incorporate competitive testing against deep learning models, as well as obtain input to a broader population.

5.5 Directions for Future Research

Prospective studies should concentrate on advanced privacy-preserving techniques such as adaptive blurring, dynamic distortion, as well as adversarial noise injection, all designed to mislead AI detection systems. Knowing that deep learning could be used to instinctively identify vulnerable regions makes confidentiality assessment more accurate or consistent. Comparative studies employing authentic social media compression

methods may elucidate the impact of platform-specific procedures on protecting privacy. Long-term research should also look at standard privacy rules that tell people who make digital content the safest ways to share visuals.

VI. CONCLUSION

This study investigated the extent to which diverse techniques for image processing, including pixelation, masking, as well as blurring, safeguard individuals' privacy in the digital realm. The results show that most of the techniques can be used to hide confidential data, but their effectiveness depends on the approach used as well the level of privacy needed. Blurred procedures, especially Gaussian blur, are organic methods to hide attributes that can be identified yet retain conceptual information that advanced AI systems might be able to recognize. Pixelation is a good way to do things, like license plates, but it only works well if the blocks are the right size. Masking was the safest method because it completely removed any identifiable information, which meant that there was no chance of reconstruction, even though it made things look different. In general, the results show that there is no one best way to do things; instead, the choice of technique should be based on how the image will be used, how sensitive the information is, and how much privacy and visual usefulness are needed. In order to make privacy protection stronger, we need better processing tools, more aware users, and ongoing research which keeps up with new technologies and threats in digital spaces.

REFERENCES

- [1] Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2017). *Deep learning with differential privacy*. Proceedings of the 2016 ACM SIGSAC Conference, 308–318.
- [2] Andrejczuk, E., & Wiliamowski, M. (2018). *Face blurring techniques in privacy protection for visual data*. Journal of Applied Computer Science, 26(1), 45–53.
- [3] Bashir, M., & Haque, M. (2018). *Image obfuscation for privacy protection using pixelation and blurring*. International Journal of Advanced Computer Science, 9(4), 112–118.
- [4] Borji, A. (2019). *Pros and cons of GAN evaluation measures*. Computer Vision and Image Understanding, 179, 41–65.
- [5] Brkic, K., Sikiric, I., & Linden, L. (2017). *Privacy-aware face recognition using blurring and low-resolution mapping*. Pattern Recognition Letters, 95, 29–35.
- [6] Chen, X., Sun, L., & Mitra, K. (2019). *Protecting identity in images using adversarial perturbations*. IEEE Transactions on Image Processing, 28(10), 5212–5224.
- [7] Choi, J., & Medioni, G. (2018). *3D face de-identification*. IEEE CVPR Workshops, 147–155.
- [8] Fan, X., & Wang, J. (2020). *A comprehensive survey of image and video privacy protection*. ACM Computing Surveys, 52(4), 1–36.
- [9] Gafni, O., Wolf, L., & Taigman, Y. (2019). *De-identification using GANs*. IEEE ICCV, 3917–3925.
- [10] Gross, R., Sweeney, L., de la Torre, F., & Baker, S. (2018). *Face de-identification*. International Journal of Computer Vision, 126(3), 343–365.
- [11] Hasan, M., & Khan, S. (2020). *Privacy-preserving image transformation using deep neural networks*. IEEE Access, 8, 18122–18135.
- [12] Hernandez, J., & Park, W. (2017). *Automated face masking for privacy protection*. Journal of Visual Communication and Image Representation, 48, 36–50.
- [13] Hukkinen, J., & Kinnunen, T. (2019). *Impact of blurring on facial recognition accuracy*. IEEE Transactions on Information Forensics and Security, 14(3), 673–684.
- [14] Jain, P., & Sahu, A. (2020). *Pixelation vs. blurring: A comparative approach to privacy preservation*. International Journal of Image Processing, 14(2), 88–95.
- [15] Li, Y., Lyu, S., & Su, C. (2018). *Image privacy protection through adaptive blurring*. IEEE CVPR Workshops, 123–131.
- [16] Liu, J., & Chen, Z. (2021). *Survey on facial de-identification*. ACM Transactions on Multimedia Computing, 17(3), 45–68.
- [17] Oh, S., & Kim, J. (2019). *License plate anonymization using hybrid blurring techniques*. Journal of Information Security and Applications, 47, 72–81.
- [18] Qian, Y., Zhang, J., & Gong, S. (2018). *Deep learning-based face de-identification*. IEEE Transactions on Information Forensics and Security, 13(2), 356–370.
- [19] Ribaric, S., Ariyaeinia, A., & Pavesic, N. (2018). *De-identification for privacy protection in multimedia content*. Signal Processing: Image Communication, 65, 24–35.
- [20] Sarkar, P., & Chaudhuri, S. (2021). *Regional image masking using automated detection*. Image and Vision Computing, 108, 104–114.
- [21] Shao, L., & Li, J. (2020). *Privacy-aware image sharing using selective blurring*. Multimedia Tools and Applications, 79(43), 32911–32927.
- [22] Wang, Y., & Gupta, A. (2017). *Face recognition resistance using obfuscation techniques*. Pattern Recognition, 67, 341–351.
- [23] Wu, Z., & Hu, J. (2019). *Performance analysis of blurring filters for privacy preservation*. Journal of Imaging Science, 13(2), 77–85.

[24] Zhang, T., & He, X. (2021). *Deep obfuscation networks for identity protection*. IEEE Transactions on Multimedia, 23, 2235–2247.

[25] Zhou, B., & Zhu, W. (2020). *Masking and redaction in visual privacy protection*. IEEE Access, 8, 160223–160235.