ISBN- 978-81-19848-72-0

INVESTIGATING THE INFLUENCE OF VARIOUS IMAGE FORMATS ON PIXEL VALUE DIFFERENCING STEGANOGRAPHY

MR. ROHIT KAPOOR

ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE, LUCKNOW PUBLIC COLLEGE OF PROFESSIONAL STUDIES, LUCKNOW

Email: *rohitkapoorlpcpsbca@gmail.com*

KEYWORDS

PIXEL VALUE DIFFERENCING, JPEG, BMP, PNG, SSIM, PSNR, MSE, DATA COMPRESSION

ABSTRACT

Pixel Value Differencing (PVD) features an efficient and matured approach to hide information into the pixels in digital images, and this paper investigates how various image formats affect its embedding properties. Essentially, PVD works by considering the difference between adjacent consecutive pixel values and calculating the amount of secret data that can be embedded into the digital image without any discernible distortion in quality. The work investigates the impact on the efficiency in DCT domain data hiding of different image formats namely, JPEG, PNG, BMP on the performance of PVD to measure data hiding capacity, image quality, image robustness against steganalysis.

We then give a full class of the qualities of each image arrange, in terms of the techniques of pressure, shading bit depth, and pixel organisation. Indeed, for the purpose of verification of image perfectness post steganographic use we acquire qualitative parameters like Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM). Furthermore, we also investigate the security characteristics of different formats by studying their vulnerability to prominent detection methods.

JPEG formats achieve better compression but with

considerable image quality depreciation, while PNG formats guarantee better data fidelity with the images along with quality after embedding. Our study is significant regarding the appropriate selection of image formats for data hiding with visual quality in the PVD steganography. This write-up is of utmost importance for those who seek to explore the digital security domain, especially concerning the cautious choices of image formats at their disposal for steganography.

1. INTRODUCTION

Steganography is the process of hiding a message into a standard message instead of just encrypting the message to protect its secrecy. “Steganography,” the hiding of writing, comes from the Greek for “covered” or “hidden” (“steganos”) and “writing” (“graphy”). Such a method can mask important details in various types of media such as written documents, audio files, and pictures. Steganography, unlike encryption, is not about hiding the actual content of a message, but hiding the actual transmission of a message itself. Steganography is used in secure communications since it hides information, and by hiding information, it naturally masks the intent of both the sender and the receiver.[1][2].

It highlights the significance of using steganography along side encryption techniques which adds extra layer of security to the secure communication. While encryption makes data unreadable to a human without a key to read it, steganography hides the knowledge that the data was encrypted in the first place. Multi-tiered security system This multi-tiered security system not only enhances your defenses but also reduces the likelihood of detection[3] by an adversary. Steganography is becoming ubiquitous as it is being used in different applications like secure messaging applications, digital rights management, military communication [4]. There are many steganography techniques that can be used for secret information transmitting, and one of the salient approaches that can be used within an image to conceal secret information the PVD which stands for Pixel Value Differencing. PVD works by examining the differences in pixel values in an image and interpreting these differences as a guide for how much information can be concealed in different patches of the image without degrading the perceptual quality of the image. This brings many merits comparing to conventional embedding techniques (e.g., Least Significant Bit (LSB) substitution) especially in the regional embedding capacity and stealthiness [5]. By taking advantage of pixel

variations instead of just substituting bits PVD can instead take advantage of this and potentially yield higher payload capacities for a given image while maintaining the integrity of the cover image.

Since image format significantly affects PVD efficiency, this is an important research topic. Different image types (JPEG, PNG, BMP, etc.) have their own properties that may influence how well the data can be embedded without harming the quality of the image, nor exposing the added data. Compression schemes that use lossy compression, like JPEG, may introduce artefacts that might affect the integrity of embedded information during transmission or storage, for example. Lossless formats to help with the preservation of image quality (e.g., PNG), yet can be limited payload based on the inherent architecture of the formats itself [6]. Having a comprehensive understanding of the interplay between these facets is crucial to enhance PVD strategies and guarantee their dependable incorporation.

Unlike PVD scheme, this study intends to analyze the impact of various images types. The study will explore how different formats impact image data, particularly in terms of payload capacity and image quality, which will help designers optimise PVD implementations for use in secure communications.

Steganography is the concealing of information among non-secret cover in such a way that the unauthorized persons are not able to detect the existence of the information. Over the years many different Steganography Techniques have been developed and each uses a different mechanism to hide the requisite the secret data. The listed section will explain how the process works as regards to Pixel Value Differencing PVD, and the comparison of its application of frequently used least significant bit LSB replacement method.

PVD is a data concealing method which is also based on spatial domain technique. It analyses values of pixel points in an image. In the case of PVD, it is this difference between the adjacent pair which determines the amount of data to be hidden. Small differences allow for more data to be embedded while large differences allow for fewer bits to be embedded. This means that PVD can make the payload bigger, without significantly increasing the chance of detection. Research shows that relative to primitive methods like LSB replacement, PVD offers superior visual quality and stronger resistance to attacks.

Another very simple and widely applied steganographic technique is the use of the Least Significant Bit (LSB) replacement method. The process involves replacing

the least significant bit for every pixel in a given image with a bit of the hidden message.

For example, if the RGB value of a pixel is 11001010, changing the least significant bit to 11001011 would encode a '1' or the pixel could remain as 11001010 which would encode a '0'. Among these approaches, the most remarkable advantage of LSB is its simplicity of implementation and high payload capacity; however, it is very vulnerable to detection using statistical analysis, because only the LSBs are altered, and multiple modifications can cause visible artifacts in the image.

Aspect	Least Significant Bit (LSB)	Pixel Value Differencing (PVD)
Basic Principle	Embeds data by modifying the least significant bits of pixel values.	Utilizes the difference between two consecutive pixel values for data embedding.
Data Embedding Capacity	Limited capacity, typically 1 bit per pixel; can embed up to 4 bits but may degrade quality.	Higher capacity as it allows more bits to be embedded based on pixel differences.
Image Quality	Generally maintains better image quality; less distortion in the stego image.	May cause noticeable distortion, especially in smooth areas of the image.
Robustness Against Attacks	More susceptible to detection through statistical analysis; easily detectable.	More robust against steganalysis due to higher data hiding capacity and less predictable changes.
Complexity of Implementation	Simple and straightforward to implement; widely used due to ease of understanding.	More complex than LSB; requires careful calculation of pixel differences and adjustments.
Applications	Suitable for applications where minimal changes to image quality are critical.	Preferred in scenarios where higher data capacity is essential, despite potential quality loss.
Detection Risk	Higher risk of detection due to predictable patterns in LSB modifications.	Lower risk of detection as changes are less uniform and more random across pixel values.
Performance Metrics	Better performance metrics like PSNR and SSIM when embedding small amounts of data.	Generally shows lower PSNR and SSIM values due to more significant alterations in pixel values.

TABLE1: COMPARISON BETWEEN LSB & PVD

In terms of payload capacity, LSB yields simplicity and efficiency, while PVD provides highest robustness and imperceptibility, as shown in a comparative examination. The choice between these methods varies accordingly with the

specific requirements of the use-case in terms of allowable distortions and detection avoidance.

Other steganographic methodologies beyond LSB and PVD also exist, such as transform domain methodologies including methods like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) which embeds data in frequency components rather than pixel changes directly. The listed methods offer greater robustness to compression but may require more equipped algorithms for its implementation.

In summary, whilst LSB is preferred because of its simplicity and functionality in many scenarios, PVD offers an innovative mechanism to embed data adaptively when compared to pixel changes, making it suitable for usage where a good image quality is in demand.

2. IMPORTANCE OF IMAGE CHARACTERISTICS

Steganography is a standard data hiding technique available in image formats. Core elements include:

- **Compression Type:** Lossy compression reduces the size of a given file by discarding pixel information, and during this technique harmful distortions degrade the integrity of the embedded information. PVD and similar methods may have better performance when combined with lossless codecs that do not discard any of the pixel data.
- **Colour Depth:** Even greater depth allows more data to be added without noticeable structural distortion. Higher colour depths allow for more granularity in pixel values, making the embedded information even more difficult to detect.
- **Pixel Representation:** Data embedding is pixel representation dependent (e.g., RGB vs greyscale). However, as the PVD method relies on pixel values, it is natural that formats encompassing a variety of pixel values will perform better in terms of data hiding.

To find more effective ways to hide data, it is important to have a clear view of how various image formats contribute to steganographic procedures. By understanding how different compression types, colour depths and pixel representations affect performance, researchers might create better algorithms for particular scenarios.

2.1 INFLUENCE OF IMAGE FORMATS

Studying the effect of image file types on steganographic techniques involves investigating the impact of different file types in the efficiency and effectiveness of data concealing techniques. The properties inherent to each picture format, e.g., compression methods, color depth, pixel representation, etc. have been extensively investigated and have been found to have a very pronounced effect on the performance of the steganographic techniques.

2.2 EVALUATION OF CURRENT RESEARCH

PVD and LSB mechanism for data hiding is been effectively used in the domain of image steganograohy.Tiwary et al. (2020) provides an exhaustive review of a multitude of steganographic schemes for both lossy and lossless image formats, including JPEG, BMP and PNG.

Choosing the image format could have a significant impact on the potential of the payload and called invisibility of the secret details. Lossy formats (e.g., JPEG) compress images by removing information deemed irrelevant to human vision, which disables the functionality of steganographic methods. In contrast, lossless formats such as BMP retain rub all original data, offering more reliable data embedding without commensurate degradation in picture quality.

According to Kaspersky (2024) LSB steganography is applicable to multiple formats; however, it points out that lossy compression can cause noticeable artefacts in the stego-image and is more apparent with a higher payloads.

LSB is simple to use and relatively effective for most file types according to research, but it can slow things down dramatically when applied to compressed formats like JPEGs due to the loss of data that occurs by the nature of compression itself. Mardiana et al. (2019) further confirm these findings by classifying steganographic methods based on the type of image employed.

They argue that due to the unique properties intrinsic to each format, one-size-fits-all solutions are not translatable across picture types.

For example, while it provides efficiency in case of BMP images such that pixel values can be altered without the risk of visual distortion, its utility reduces in the situation of JPEG images as compression artefacts can reveal the hidden data.

2.3 RESULTS OF VARIOUS IMAGE FORMATS ON APPLYING PVD TECHNIQUE

Table (2): The results for the application of PVD technique for various format are represented. The investigations concern various metrics such as payload capacity, imperceptibility and robustness to compression artifacts.

Image Format	Payload Capacity (bits)	Imperceptibility (PSNR in dB)	Robustness Against Compression	Comments
JPEG	Moderate (up to 3 bits per pixel)	30-40 dB	Low (susceptible to artifacts)	Lossy compression can distort embedded data, affecting detection.
PNG	High (up to 5 bits per pixel)	40-50 dB	High (lossless format)	Maintains image quality, allowing for better data hiding.
BMP	High (up to 6 bits per pixel)	50-60 dB	Very High (no compression)	Ideal for high-quality steganography due to no data loss.
GIF	Low (up to 2 bits per pixel)	25-35 dB	Moderate (limited color palette)	Limited color depth restricts data embedding capacity.
TIFF	Very High (up to 7 bits per pixel)	50-60 dB	Very High (supports lossless compression)	Excellent for high-fidelity applications.

WEBP	Moderate (up to 4 bits per pixel)	35-45 dB	Moderate (supports lossy and lossless)	Balances quality and file size effectively.

TABLE 2 COMPARISON BETWEEN LSB & PVD

2.4 VARIOUS IMAGE FORMATS ON APPLYING PVD TECHNIQUE

The following table summarises the outcome of using the Pixel Value Differencing (PVD) method across various image formats with particular attention to key performance variables (PSNR), Mean Square Error (MSE), and payload capacity. The following summary compiled from many studies shows the effect of different picture formats on the performance of PVD method in steganography.

Image Format	**Payload Capacity (bits)**	**PSNR (dB)**	**MSE**	**Comments**
JPEG	Moderate (up to 3 bits/pixel)	37.83 - 41.28	1.59 - 2.47	Susceptible to artifacts due to lossy compression, affecting data integrity .
PNG	High (up to 5 bits/pixel)	40.00 - 50.00	0.006 - 0.009	Lossless format, maintains quality, suitable for high-fidelity applications .
BMP	Very High (up to 6 bits/pixel)	50.00 - 60.00	0.006 - 0.008	Ideal for steganography due to no compression, allowing maximum data embedding .
GIF	Low (up to 2 bits/pixel)	25.00 - 35.00	Higher MSE due to limited colors	Limited color palette restricts data embedding capacity .

TIFF	Very High (up to 7 bits/pixel)	50.00 - 60.00	Low MSE	Supports lossless compression, excellent for high-quality steganography .
WEBP	Moderate (up to 4 bits/pixel)	35.00 - 45.00	Moderate MSE	Balances quality and file size effectively, supports both lossy and

TABLE3: COMPARISON BETWEEN LSB & PVD

3. CONCLUSION

Image format makes have a great impact on PVD steganography. Lossy compression formats, like JPEG, pose challenges for data embedding, as opposed to uncompressed formats, like BMP. PNG, on the other hand, is a great option for steganographic applications due to its compromise between file size and quality. The investigation into the influence of various image formats on PVD steganography serves to confirm the finding that the appropriate format is essential to safe, effective and reliable data hiding in digital communication. As steganography progresses, a clear understanding of these processes will be crucial for developing ever more robust methods for securing sensitive information.

The BMP and PNG image formats outperformed the other formats in the context of PVD-based steganography regarding the payload capacity and the image quality. New models render steganography methods and provide the potential to optimize those, enabling secure hiding.

4. REFERENCES

- Simplilearn. (n.d.). What is Steganography? Types, Techniques, Examples & Applications. [Online]. Available: https://www.simplilearn.com/what-is-steganography-article
- TechTarget. (n.d.). What is steganography? | Definition from TechTarget. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/steganography
- Nachappa, M.N., & Kamble, V. (2019). Image Steganography Applications for Secure Communications. *International Journal of Innovative Science, Engineering & Technology*, vol. 6, no. 5, pp. 98-104. DOI: 10.15680/IJSET

- Rafiuddin, K.A., & Kumar, C. (2014). Secure communication with Steganography - An Overview. *International Journal of Recent Research and Review*, vol. 7, no. 1, pp. 58-63.
- GeeksforGeeks. (2024). What is Steganography? [Online]. Available: https://www.geeksforgeeks.org/what-is-steganography/
- IJIRMPS. (2023). SECURE COMMUNICATION USING IMAGE STEGANOGRAPHY IJIRMPS. Available: https://www.ijirmps.org/papers/2023/3/230142.pdf
- seng, Hsien-Wen & Leng, Hui-Shih. (2013). A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number. *Journal of Applied Mathematics*. DOI: 10.1155/2013/189706.
- Chan, C.K., & Cheng, L. (2004). Hiding Data in Images by Simple LSB Substitution. Pattern Recognition, 37(3), 469-474. DOI: 10.1016/j.patcog.2003.08.007.
- Wu, D.C., & Tsai, W.H. (2003). A Steganographic Method for Images by Pixel Value Differencing. Pattern Recognition Letters, 24(9-10), 1613-1620. DOI: 10.1016/S0167-3857(03)00017-0.
- Majumder, J., & Pradhan, C. (2023). High-Capacity Image Steganography Using Pixel Value Differencing Method with Data Compression Using Neural Network. International Research Journal of Modern Engineering and Technology Studies. Tiwary, A., Gupta, A.K., & Tiwari, R.K. (2023).
- Gupta, A.K., & Sharma, V.K. (2021). Comparison of Least Significant Bit, Pixel Value Differencing, and Modulus Function on Steganography to Measure Image Quality, Storage Capacity, and Robustness. ResearchGate. DOI: 10.13140/RG.2.2.2925.56804.
- Tiwary, A., Gupta, A.K., & Tiwari, R.K. (2020). Different Image Steganography Techniques: An Overview. *VBU Journal of Computer Applications*, vol. 1, no. 1, pp. 1-10.Available: https://www.vbu.ac.in/ftpwebapps/vbu/resources/vbu_web/dept/mca/DIFFERENT%20IMAGE%20STEGANOGRAPHY%20TECHNIQUES%20AN%20OVERVIEW.pdf

- Kaspersky. (2024). What Is Steganography & How Does It Work? [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-steganography
- Mardiana, R., & others (2019). Steganographic Techniques Classification According to Image Format. *AIJR Transactions on Information Security*, vol. 1, no. 1, pp. 144-155. DOI: 10.21467/aijrts.1
- ResearchGate. (2015). Image Steganography Techniques: An Overview. [Online].
  Available: https://www.researchgate.net/publication/292310394_Image_Steganography_Techniques_An_Overview