International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 09 | Sept - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Analysis of Data Hiding Using Digital Image Signal Processing

BAGAVATHY R[1], RAJESH R [2], AJITH KUMAR D [3]

[1,2,3] *Department of Bio Medical Engineering, Loyola Institute of Science and Technology, Tamilnadu, India.*

Abstract - Data hiding process embeds data into digital media for the purpose of security. Digital image is one of the best media to store data. It provides large capacity for hiding secret information which results into stego-image imperceptible to human vision, a novel stenographic approach based on data hiding method such as pixel-value differencing. This method provides both high embedding capacity and outstanding imperceptibility for the stego-image. In our project, different image processing techniques are described for data hiding related to pixel value differencing. Pixel Value Differencing based techniques is carried out to produce modified data hiding method. Hamming is an error correcting method which is useful to hide some information where lost bit are detected and corrected. OPAP is used to minimize embedding error thus quality of stego-image is improved without disturbing secret data. ZigZag method enhances security and quality of image. In modified method Hamming, OPAP and ZigZag methods are combined. In adaptive method image is divided into blocks and then data will be hidden. Objective of the proposed work is to increase the stego-image quality as well as increase capacity of secret data. Result analysis compared for BMP images only, with calculation of evaluation metrics i.e. MSE, PSNR and SSIM.

Key Words: Stego-image, BMP image, Hamming Method, OPAP Method, ZigZag Method, Adaptive Method.

1.INTRODUCTION

Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as “covers” or carriers to hide secret messages. After embedding a secret message into the cover- image, a so-called stego-image is obtained. It is important that the stego-image does not contain any easily detectable artifacts due to message embedding. A third party could use such artifacts as an indication that a secret message is present. Once this message detection can be reliably achieved, the steganographic tool becomes useless.

Obviously, the less information is embedded into the cover-image, the smaller the probability of introducing detectable artifacts by the embedding process. Another important factor is the choice of the cover-image. The selection is at the discretion of the person who sends the message. The sender should avoid using cover-images that would be easy to analyze for presence of secret messages. For example, one should not use computer art, charts, images with large areas of uniform color, images with only a few colors, and images with a unique semantic content, such as fonts. Although computer-generated fractal images may seem as good covers6 because of their complexity and irregularity, they are generated by strict deterministic rules that may be easily violated by message embedding.

Scans of photographs or images obtained with a digital camera contain a high number of colors and are usually recommended and considered safe for steganography. Some steganographic experts recommend grayscale images as the best cover-images. Here are essentially three types of image formats: raw, uncompressed formats (BMP, PCX), palette formats (GIF), and Lossy compressed formats (JPEG, Wavelet, JPEG2000). Only few current steganographic programs offer the capability to embed messages directly in the JPEG stream. It is a difficult problem to devise a steganographic method that would hide messages in the JPEG stream in a secure manner while keeping the capacity practical. Far more programs use the BMP, PCX, or the GIF palette-based format. The GIF format is a difficult environment for secure steganography with reasonable capacity. Also, most steganographic

techniques for GIFs implemented in current software products prioritize capacity over security and are thus relatively easy to detect. The raw formats, such as BMP, offer the highest capacity and best overall security. In this paper, we demonstrate that even 24-bit images or grayscale 8-bit images may actually be extremely poor candidates for cover-images if they were initially acquired as JPEG images and later decompressed to a loss less format. In fact, it is quite reasonable to expect that most casual users of steganographic programs will use scanned images or images from a digital camera that were originally stored in the JPEG format due to its efficiency in data storage.

All steganographic methods strive to achieve the minimal amount of distortion in order to minimize the likelihood of introducing any visible artifacts. Consequently, if the cover-image, was initially stored in the JPEG format, the act of message embedding will not erase the characteristic structure created by the JPEG compression and one can still easily determine whether or not a given image has been stored as JPEG in the past. Actually, unless the image is too small, one can reliably recover even the values of the JPEG quantization table by carefully analyzing the values of DCT coefficients in all 8□8 blocks. After message embedding, however, the cover-image will become (with a high probability) incompatible with the JPEG format in the sense that it may be possible to prove that a particular 8□8 block of pixels could not have been produced by JPEG decompression of any block of quantized coefficients. This finding provides strong evidence that the block has been modified. It is highly suspicious to find an image stored in a loss less format that bears a strong fingerprint of JPEG compression, yet is not fully compatible with any JPEG compressed image. This can be interpreted as evidence for steganography. y checking the JPEG compatibility of every block, we can potentially detect messages as short as one bit.

And the steganalytic method will work for virtually any steganographic or watermarking method, not just the LSB embedding! Indeed, in our experiments, we have found out that even one randomly selected pixel whose gray level has been modified by one can be detected with very high probability. For longer messages, one can even attempt to estimate the message length and its position in the image by determining which 8□8 blocks are incompatible with JPEG compression. It is even possible to analyze the image and estimate the likely candidate

for the cover-image or its blocks (the "closest" JPEG compatible image/block). This way, we may be able to identify individual pixels that have been modified. All this indicates that an extremely serious information leakage from the steganographic method can occur and thus completely compromise the steganographic channel.

2. METHODOLOGY

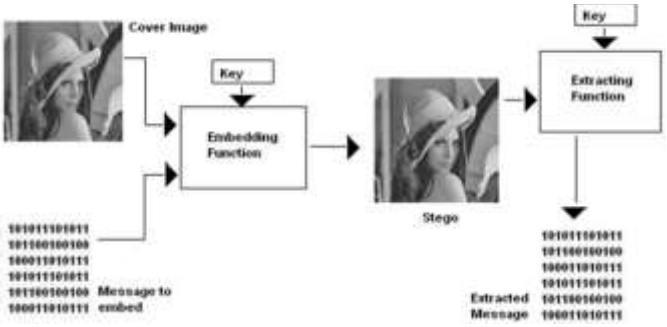

Fig – 1: Block diagram for proposed system

Steganography refers to the science of "invisible" communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an observer. Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem [1] where Alice and Bob are two inmates who wish to communicate in order to hatch an escape plan. However, all communication between them is examined by the warden, Wendy, who will put them in solitary confinement at the slightest suspicion of covert communication. Specifically, in the general model for steganography, we have Alice wishing to send a secret message to Bob. In order to do so, she " embeds" into a cover-object, to obtain the stego-object .

The stego-object is then sent through the public channel. The warden, Wendy, who is free to examine all messages exchanged between Alice and Bob, can be passive or active. A passive warden simply examines the message and tries to determine if it potentially contains a hidden message. If it appears that it does, she then takes appropriate action, else, shelets the message through without any action. An active warden, on the other hand, can alter messages deliberately,

even though she may not see any trace of a hidden message, in order to foil any secret communication that can nevertheless be occurring between Alice and Bob. The amount of change the warden is allowed to make depends on the model being used and the cover objects being employed. For example, with images, it would make sense that the warden is allowed to make changes as long as she does not alter significantly the subjective visual quality of a suspected stego-image.

It should be noted that the main goal of steganography is to communicate securely in a completely undetectable manner. That is, Wendy should not be able to distinguish in any sense between cover-objects (objects not containing any secret message) and stego-objects (objects containing a secret message). In this context, "steganalysis" refers to the body of techniques that are designed to distinguish between cover-objects and stego-objects. It should be noted that nothing might be gleaned about the contents of the secret message . When the existence of hidden message is known, revealing its content is not always necessary. Just disabling and rendering it useless will defeat the very purpose of steganography. In this paper, we present a steganalysis technique for detecting stego-images, i.e., still images containing hidden messages, using image quality metrics. Although we focus on images, the general techniques we discuss would also be applicable to audio and video media. Given the proliferation of digital images, and given the high degree of redundancy present in a digital representation of an image (despite compression), there has been an increased interest in using digital images as cover-objects for the purpose of steganography. The simplest of such techniques essentially embeds the message in a subset of the LSB (least significant bit) plane of the image, possibly after encryption [2]. It is well known that an image is generally not visually affected when its least significant bit plane is changed. Popular steganographic tools based on LSB like embedding vary in their approach for hiding information. For example Steganos and Stools use LSB embedding in the spatial domain, while Jsteg embeds in the frequency domain. Other more sophisticated techniques include the use of quantization and dithering. For a good survey of steganography techniques, the reader is referred to [2]. What is common to these techniques is that they assume a passive warden framework. That is they assume the warden Wendy will not alter the image. We collectively refer to these techniques as passive warden steganography techniques.

Conventional passive warden steganography techniques like LSB embedding are not useful in the presence of an active warden as the warden can simply randomize the LSB plane to thwart communication. In order to deal with an active warden Alice must embed her message in a robust manner. That is, Bob should be able to accurately recover the secret message despite operations like LSB randomizing, compression, filtering, and rotation by small degrees, etc. performed by the active warden Wendy. Indeed, the problem of embedding messages in a robust manner has been the subject of intense research in the image processing community, albeit for applications other than steganography, under the name of robust digital watermarking A robust digital watermark is an imperceptible signal added to digital content that can be later detected or extracted n order to make some assertion about the content. For example, the presence of her watermark can be used by Alice to assert ownership of the content. Recent years have seen an increasing interest in digital watermarking with many different applications, ranging from copyright protection and digital rights management, to secret communication. Essentially robust digital watermarks provide a means of image-based steganography in the presence of an active warden since modifications made by the warden will not affect the embedded watermark as long as the visual appearance of the image is not significantly degraded. However, despite this obvious and commonly observed connection to steganography, there has been very little effort aimed at analyzing or evaluating the effectiveness of common robust watermarking techniques for steganographic applications. Instead, most work has focused on analyzing or evaluating the watermarking algorithms for their robustness against various kinds of attacks that try to remove or destroy them. However, if robust digital watermarks are to be used in active warden steganography applications, detection of their presence by an unauthorized agent defeats their very purpose. Even in applications that do not require hidden communication, but only robustness, we note that it would be desirable to first detect the possible presence of a watermark before trying to remove or manipulate it. This means that a given signal would have to be first analyzed for the presence of a watermark. In this project, we develop steganalysis techniques both for conventional LSB-like embedding used in the context of

a passive warden model and for watermarking which can be used to embed secret messages in the context of an active warden. In order to distinguish between these two models, we will be using the terms watermark and message when the embedded signal is in the context of an active warden and a passive

warden, respectively. Furthermore, we simply use the terms marking or embedding when the context of discussion is general to include both active and passive warden steganography.
The techniques we present are novel and to the best of our knowledge, the first attempt at designing general purpose tools for steganalysis. General detection techniques as applied to steganography have not been devised and methods beyond visual inspection and specific statistical tests for individual techniques like LSB embedding are not present in the literature. Since too many images have to be inspected visually to sense hidden messages, the development of a technique to automate the detection process will be very valuable to the steganalyst. Our approach is based on the fact that hiding information in digital media requires alterations of the signal properties that introduce some form of degradation, no matter how small. These degradations can act as signatures that could be used to reveal the existence of a hidden message. For example, in the context of digital watermarking, the general underlying idea is to create a watermarked signal that is perceptually identical but statistically different from the host signal. A decoder uses this statistical difference in order to detect the watermark. However, the very same statistical difference that is created could potentially be exploited to determine if a given image is watermarked or not. In this paper, we show that addition of a watermark or message leaves unique artifacts, which can be detected using Image Quality Measures (IQM).

3. RESULT AND DISCUSSION

Four standard BMP color images of size 600 x 480 pixels and secret data upto 200 KB are taken to implement the above process. The effectiveness of the stego process is verified with different metrics such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Method (SSIM). Higher the values of PSNR, better the image quality. SSIM value falls in the interval [1, 0]. The value 1 means that the two images are exactly the same and 0 means they are totally unrelated.

The results obtained for Mean Square Error (MSE) increases with increase in the size of data embedded in the image. The results show that value of MSE increased in Hamming, OPAP, Zig-Zag and thus in Modified because it is combined hamming, OPAP and Zig-Zag method. Adaptive method gives less MSE than other methods.

PSNR is inversely proportional to MSE. Our results show that, Hamming, Zig-Zag and Adaptive methods of data hiding methods gives consistently high PSNR. Hence we have obtained

Fig – 2: High image quality because PSNR is high

Fig – 3: Proportional to image quality

4. CONCLUSION

Our project provides large capacity for hiding secret information which results into stego- image imperceptible to human vision and a novel stenographic. This method provides both high embedding capacity and outstanding imperceptibility for the stego-image. In our project Pixel Value Differencing based techniques is uised to produce modified data hiding method. Hamming is an error correcting method which is useful to hide some information where lost bit are detected and corrected. OPAP minimized the embedding error thus quality of stego-image is improved without disturbing secret data. ZigZag method enhances security and quality of image. In modified method Hamming, OPAP and ZigZag methods are combined. Adaptive method image is divided into blocks and then data are hidden. Thus we increased the stego-image quality as well as capacity of secret data. Result analysis compared for BMP images only, with calculation of evaluation metrics i.e. MSE, PSNR and SSIM is shown.

REFERENCES

[1] Masoud Afrakhteh, Subariah Ibrahim “Adaptive steganography scheme Using More Surrounding Pixels”, International Conference On Computer Design And Applications (ICCDA 2010), Vol.1, V1225-V1229
[2] Wu,Tsai, ”A steganographic method for images by pixel-value differencing” ,Volume 24, Issues 9-10, June 2003, pages 1613-1626
[3] A. E. Mustafa, A.M.F. ElGamal, M.E. ElAlmi, Ahmed.BD, “A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit”, Issue No. 21, April. 2011
[4] H.C.Wu, Tsai, Hwang, “Image steganographic scheme based on pixel-value differencing and LSB replacement methods”, IEE Procvis. Image signal process, vol. 152, no.5, October 2005, 611-615
[5]Han-ling ZHANG, Guang-zhi GENG, Cai-qiong Xing, 2009.“Image Steganography using Pixel-Value Differencing”, IEEE DOI 10.1109/ISECS.2009.139), 109–112.
[6] Chi-Kwong Chan, L.M. Cheng, “Hiding data in images by simple LSB substitution”,Pattern Recognition Society. Published by Elsevier Ltd. All rights reserved.doi:10.1016/j.patcog.2003.08.007.
[7] R. Amirtharajan, R. Akila, P. Deepikachowdavarapu,” A Comparative Analysis of Image Steganography”, International Journal of Computer Applications (0975 – 8887), Volume 2 – No.3, May 2010
[8] Chung - Ming Wang , Nan-I Wu , Chwei - Shyong Tsai, Min-Shiang Hwang,”A high quality

steganographic method with pixel-value differencingandmodulus

[9] H.B. Kekre, Archana Athawale, Pallavi N. Halarnkar, "Performance Evaluation of Pixel Value Differencing and Kekre's Modified Algorithm for Information Hiding in Images", International Conference on Advances in Computing, Communication and Control (ICAC3'09)

[10]Dr H.B Kekre, Ms Pallavi Halarnkar, Kahkashan Ansari, Parakh Jindal, Yash Chaturvedi," Information hiding with increased capacity using KMLA+PVD approach", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.2, April 2012

[11]A.L.Khade. B.G.Hogde, V B Gaikwad. "Secret Communication via Image Hiding In Image by Pixel Value Differencing", ICWET', February 2010, 437-438.

[12]M.Padmaa,Dr.Y.Venkataramani,"ZIG-ZAG PVD – A Nontraditional Approach", International Journal of Computer Applications (0975 – 8887),Volume 5– No.7, August 2010

[13]J. K. Mandal 1 and Debashis Das," Steganography Using Adaptive Pixel Value Differencing(APVD) of Gray Images Through Exclusion of Overflow/Underflow", The second International Conference on Computer Science, engineering and applications (CCSEA-2012) , May 2012

[14]J. K. Mandal and Debashis Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain", International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012, 83-93