



INVERTIBLE MESSAGE HIDING USING HISTOGRAM MODIFICATION BY LabVIEW: A NEW APPROACH.

KEYWORDS

histogram, pixel, adjoining, embedding capacity, consociated

Vivek Onkarnath Rathi

Instrumentation and Control Engineering,
Vishwakarma Institute of Technology, Pune

Priyanka Shrikant Patil

Instrumentation and Control Engineering,
Vishwakarma Institute of Technology, Pune

Prof. Manisha Mhetre

Instrumentation and Control Engineering, Vishwakarma Institute of Technology, Pune

ABSTRACT *An approach in which the original image is retrieved effectively without any failure is known as reversible or lossless data hiding. It is primitively a water marking. Basically the ideology is to embed the data in a host image and reconstruct original host image along with the embedded data without any failure and distortion loss. We have implemented an algorithm based on histogram modification and put forward it in LabVIEW. The rudimental approach of this paper is to use LabVIEW tool effectively and elegantly to implement the reversible data hiding technique using the block diagram approach. In the propounded algorithm, the difference between the neighboring pixels is used to accomplish higher data hiding capacity. The algorithm uses the difference between the adjoining pixels to embed the data. The amount of data to be embedded into the image is decided by the number of pixels consociated with peak point. Observations are visualized using the image histograms of the 8 bit image i.e. grayscale image. The algorithm also works effectively for colored images considering one plane at a time.*

INTRODUCTION

Any of the data that can be rebuild and reconstructed back without any failure using several algorithms, mathematics, calculations, evaluation techniques explicitly is lossless data hiding also known as reversible data hiding. This operation embeds data message usually some cryptic information into an image in a reversible trend i.e. considering the aspect to recreating the original image. Data Hiding merges image processing along with cryptography, coding theory and human visual perception. Hiding any sensitive data inside a digital image is also called as steganography. Medical, military, authentication, fingerprinting are few applications. Copyright protection of the images i.e authentication, image integrity protection a.k.a (also known as) fraud detection, this reversibility is a crucial aspect and the most desirable characteristic, and thus considerable amount of research has been done over last so many years. The root challenge for all the known data hiding techniques is only the embedding capacity, i.e. the number of data bits one can embed. The conduct of the image defines and assesses the performance of a reversible data hiding methodology. For required embedding capacity, a good embedded/watermarked image quality can be obtained by reducing the distortion of the image obtained after embedding the data or message as much as possible. Some of the methods used so far for reversible data hiding are histogram modification, difference expansion, prediction-error expansion, integer transform, lossless compression, etc. Amid all these methods, the most widely used methods are Histogram methods. It is used widely and applied so as to prevent overflow i.e. $(255+1) 256$ and underflow i.e. $(0-1)-1$ problems. Several arithmetic operations performed on the pixel during the data embedding, the addition/subtraction of 1, could result in an overflow at edge values like 0 and 255. Because the -1 and 256 are not valid in a gray scale. Henceforth, it must be dodged cleverly. An image histogram is chiefly a graphical representation of color allocation in a digital image. It is just a plot of number of pixels against the intensity of each pixel. It gives correlation among the adjoining pixels of the image.

Not all data hiding techniques are reversible completely. There are chiefly three main categories of the reversible data hiding techniques-

1. Data compression,
2. Pixel value difference expansion
3. Histogram shifting.

The method of histogram based reversible data hiding was incorporated by Ni et al. in [1], wherein message is embedded within the histogram. In the histogram shifting methodology the peak and zero points of the histogram are changed for embedding of the message or data. In addition histogram shifting technique prevents overflow, the situation wherein the gray value exceeds overshoots 255 and underflow, the situation wherein the gray value undershoots 0. The data embedding in the original image is accomplished by repositioning the histogram of the image. This methodology produces higher data hiding capacity with very low distortion. The approach described in this paper is inspired by the Ni's Reversible Data Hiding algorithm [1]. The method of Ni uses certain histogram properties to embed data. More precisely it focuses on the peak point of the histogram, i.e., the pixels that have the most common pixel value.

METHOD

It is expected to construct a reversible method of data hiding with higher data embedding capacity than Ni's approach along with relatively high Peak Signal-to-Noise Ratio a.k.a PSNR. Henceforth this approach proves to be very convincing along with good results making human visual perception almost unnoticeable in regards to the image. Assume an image, basically a grayscale image I with N as the number of pixels with p_i as the i^{th} pixel of the image. In the gray scale image the pixel values are in the range of $[0, 255]$. As image is itself a 2D object, constructing a single 1D vector from the 2D matrix is the most primitive stage of the algorithm. This is accomplished by viewing image through Inverse-S Order. A histogram is created with the adjoining pixel difference values to discover the peak point a.k.a PP. It is the most frequent difference. The data to be ciphered is embedded only a bit at a time as follows.

1. The very first element of 1D vector retains its value.
2. The second and following elements of the vector calculates the difference between the prevailing pixel and the preceding pixel from the created 1D vector. It is denoted by d .
3. If d is equal to PP i.e., this identifies an embeddable pixel, then increase the difference by the correspondent bit value from the data byte from LSB to MSB i.e. add 0 or 1 to the prevailing pixel value, if the next pending bit from the message byte is 0 or 1.

4. If d_i is greater than PP , then simply increase the difference by 1, so that this value does not become a part of the embedding data pixels of the 2D image, i.e. w_i , free the $(PP + 1)$ value for embedding purposes. It makes sure that if a pixel consociated with the peak point is encountered, it implies data is embedded in it. [4]

SIMULATION USING LabVIEW

LabVIEW (Laboratory Virtual Instrument Engineering Workbench) is a basically a software tool used for multidisciplinary engineering applications. It is a platform for system design and visual programming language environment for the development of system and system applications. It is a product by National Instruments. It uses graphical programming unlike traditional C. The graphical language is named as "G". LabVIEW programs are called as Virtual Instruments, or VIs.

The most consequential and crucial aim of this paper is to use LabVIEW tool for image processing applications through different image processing algorithms and applications using LabVIEW and its IMAQ (Image Acquisition) vision toolbox. IMAQ vision toolbox proffers dynamic and complete set for digital image processing and data acquisition functions to enhance the efficiency of the projects along with reducing the effort of the programming undertaken by the users. Hence LabVIEW helps to achieve better results in shorter time duration. Therefore, the IMAQ vision toolbox utilized by LabVIEW is a very interesting and an unique tool used to and for analyzing an image in subtle details and in simplicity. The purpose of emphasizing the effectiveness and flexibility offered by LabVIEW tool is seen through this data embedding algorithm. Henceforth, presenting different proposition and strategies about digital image processing and its different applications in the field of image acquisition, image transformations such as inverse and transpose images, image handling, image processing using IMAQ vision toolbox. [5]

WHY ONLY LabVIEW?

It uses graphical programming language called G programming. It is one of its own kind along with easy to use and execute. LabVIEW is one of the most advanced tool for real time application, yet unknown to most the users and to simplify algorithms efficiently with robust methodologies using simple block diagrams.

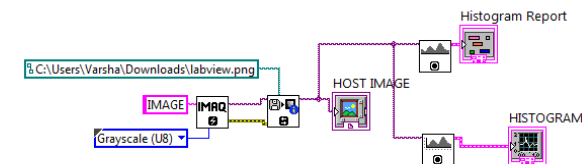


Fig 1. Block-Diagram code to display an image.

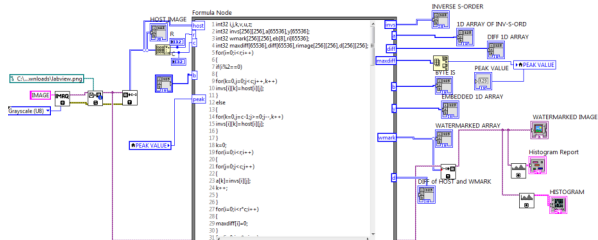


Fig 2. LabVIEW code for the proffered algorithm.

PROPOSED ALGORITHM

Assume the pixel value of the i^{th} pixel of an image as p_i , the embedded/watermarked value as w_i , the difference between the current and preceding pixel as $d_i = |p_i - p_{i-1}|$ and the bit to be embedded as b from a given message byte, then the rules mentioned above can be summarized in the following

A. Encoding

1. Read the original grayscale image in Inverse-S Order.

2. Compute the difference d_i between the prevailing pixel p_i & preceding pixel p_{i-1} by using:

$$d_i = p_i, \text{ if } I = 0$$

$$d_i = |p_{(i-1)} - p_i|, \text{ otherwise}$$

3. Determine the peak point a.k.a PP from the pixel differences i.e. the most frequent difference.

4. Change each pixel by 1 unit if the difference computed is greater than the peak point i.e. $d_i > PP$, using the following equation:

$$w_i = p_i, \text{ if } i=0 \text{ or } d_i < PP$$

$$w_i = p_{(i-1)}, \text{ if } d_i > PP \text{ and } x_i \geq x_{(i-1)}$$

$$w_i = p_{(i-1)}, \text{ if } d_i > PP \text{ and } x_i < x_{(i-1)}$$

where w_i is the watermarked value of pixel P_i i.e. original image along with data bits embedded into the image.

5. Qualify the pixel p_i agreeing to the message bit $b[0,1]$ if $d_i = PP$, to form a watermarked/embedded image

$$w_i = p_i + b, \text{ iff } p_i \geq p_{(i-1)} \text{ and } d_i = PP$$

$$w_i = p_i - b, \text{ iff } p_i < p_{(i-1)} \text{ and } d_i = PP$$

where b is a data bit to be embedded, b is either 0 or 1.

B. Decoding

1. Read the watermarked/data embedded image in the same Inverse S-Order at the receiving end to extract and decipher the embedded data.

2. The data bit b can be extracted by: $b = 0$, iff $PP = I w_i - p_{i-1}$, $b = 1$, iff $PP + 1 = I w_i - p_{i-1}$

3. The pixel values p_i of the original image can be obtained back as follows:

$$p_i = w_i + 1, \text{ iff } w_i < p_{(i-1)} \text{ and } I w_i - p_{(i-1)} I > PP$$

$$p_i = w_i - 1, \text{ iff } w_i > p_{(i-1)} \text{ and } I w_i - p_{(i-1)} I > PP$$

$$p_i = w_i, \text{ otherwise.}$$

Thus by using these pixel values p_i we can rebuild the original greyscale image. Overall, this methodology uses only one peak point for embedding the data message. One must use multiple peak points so that the embedding capacity can be increased in a complex system. [4]

EXPERIMENTAL RESULTS

From the graphic illustrations given below it can be seen that the proffered methodology is used and simulated effectively through LabVIEW. It well defines the data hiding i.e. watermarking concept along with the elegance of the algorithm used. Histogram only gives the clear idea about the subtle differences between the original and watermarked image through the observation of the spikes and troughs. This methodology and algorithm was applied to variety of images like Lena, Fruits, Barbara to check its universality and effectiveness in LabVIEW environment. The images used for testing and analysis were all grayscale images. It was a success.

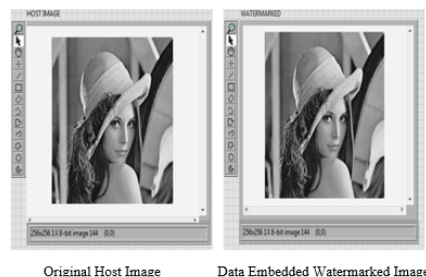


Fig 3. Original and Watermarked Images

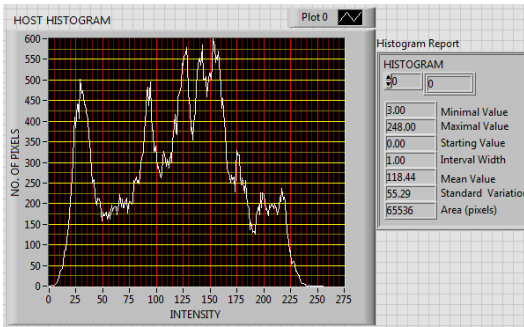


Fig 4. Original (host) Histogram (Image-Lena)

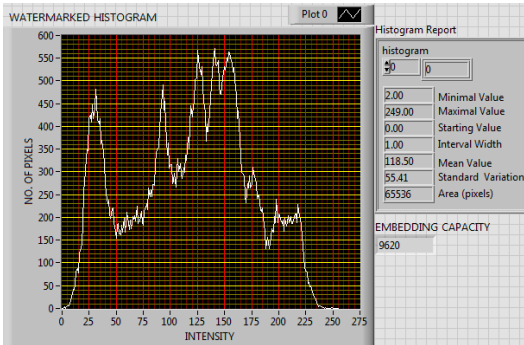


Fig 5. Watermark/Embedded Histogram (Image-Lena)

CALCULATION AND ANALYSIS

The effectiveness and application of the proposed methodology is effectively evaluated on images Lena, Fruits and Barbara. These are all gray scale images.

1. Embedding Capacity is the total number of the pixels associated with peak point a.k.a PP. It is expressed in terms of bits, i.e. number of pixels that can be used for data embedding
2. Bitrate is the ratio of the embedding capacity to the total number of the pixels in an image.
3. Peak Signal To Noise Ratio (PSNR) is defined as the ratio between the maximum possible power of the signal and power of the noise affecting the fidelity of the signal.

$$PSNR = 10 * \log_{10}((255)^2 / MSE)$$

where, Mean Square Error (MSE) is:

$$= (1/M * N) * \sum_{k=0}^{M-1} \sum_{l=0}^{N-1} (p(i,j) - w(i,j))^2$$

Here, p(i,j) is ⁱth coordinate of the original image.
w(i,j) is ⁱth coordinate of the watermarked image.

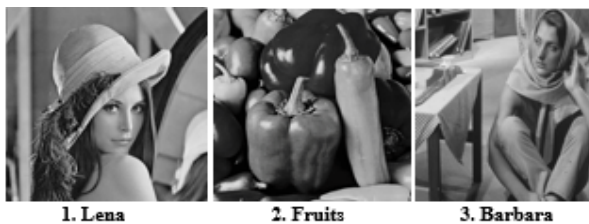


Fig 6. Images used in the algorithm execution

Table No. 01

Sr. no.	Image	Embedding Capacity	Bitrate (bpp)	PSNR (dB)
1.	Lena	9620	0.1467	48.66
2.	Fruit	33664	0.2709	48.43
3.	Barbara	31361	0.1196	48.55

CONCLUSIONS

1. A robust technique of reversible lossless data hiding using histogram modification is implemented seeing the difference between adjoining pixels.
2. Extraction and deciphering of the data message is only possible with the knowledge of the peak point i.e. the key to decipher the message.
3. LabVIEW tool and its IMAQ vision toolbox is evaluated.
4. The proffered algorithm and methodology gives higher PSNR values.
5. Algorithm work perfectly fine without any image distortion as compared to most of the algorithms extant.
6. All the experiments were simulated using LabVIEW. IMAQ vision toolbox provides basis for image processing and analysis techniques with most effective and easiest approach.

REFERENCES

1. Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., Vol. 16, pp. 354–362, Mar. 2006.
2. Seung-Won Jung, Le Thanh Ha, and Sung-Jea Ko, "A New Histogram Modification Based Reversible Data Hiding Algorithm Considering the Human Visual System" IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 2, FEBRUARY 2011.
3. Ruben Posada-Gomez, Oscar Osvaldo Sandoval-Gonzalez, Albino Martinez Sibaja, Otniel Portillo-Rodriguez and Giner Alor-Hernandez, "Digital Image Processing Using LabVIEW" Instituto Tecnológico de Orizaba, Departamento de Postgrado e Investigacion, Mexico.
4. Rajkumar Ramaswamy and Vasuki Arumugam, "Lossless Data Hiding Based On Histogram Modification", The international Arab Journal of Information Technology, Vol. 9, No. 5, September 2012.
5. <http://www.ni.com/labview/>, 18/12/2016, 14:00