International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Simulation based Performance Analysis of Histogram Shifting Method on Various Cover Images

Garima Sharma[1], Vipra Bohara[2], Laxmi Narayan Balai[3]
[1]P. G. Scholar (Electronics & Comm.), Yagyavalkya Institute of Technology, Jaipur, Rajasthan, India
[2]Assistant Professor (Electronics & Comm.), Yagyavalkya Institute of Technology, Jaipur, Rajasthan, India
[3]H.O.D. (Electronics & Comm.), Yagyavalkya Institute of Technology, Jaipur, Rajasthan, India

ABSTRACT

In this paper we have simulated and analyzed histogram shifting method on different types of cover images. Secret image which is used to hide in cover image is called payload. We have analyzed this algorithm in MATLAB simulation tool. This analysis is performed to find out the performance of this method on different types of cover images. We have analyzed this to find out how much accuracy can we get when extracting payload from cover image. We have computed peak signal to noise ratio, mean square error.

Keywords: *Steganography, Histogram, Fragile, Spatial, Reversible Data Hiding*

1. INTRODUCTION

In cutting-edge world popularity of digital image situated most of the time applications is likely one of the necessity for copyright defense with the intention to avert crook repeating and distribution of digital information. Digital illustration offers many advantages for processing and distributing image and other types of understanding. Copyright protection provides authentication redundant power in customary data just like the possession details and owner-logo within the digital media while now not compromising its sensory recreation first-class. If within the concern of any dispute, authentication data is extracted from watermarked media and possibly utilized for an authoritative proof to validate the possession, because the methodology for copyright security, digital image watermarking have recently developed because the relevant art of curiosity and a lively area of evaluation currently days. A Watermarking is including "ownership" info in multimedia approach contents to show the legitimacy.

The designated invisible watermarking is approached in this work utilizing Histogram shifting features, the cover photograph embeds the watermark or message, as part of prior artwork photograph segmentation method to extract the object of interest in message is utilized here and covert an 8 or 16 bit message information to single bit binary information. The use of watermarking process we can embed the data object. The object may be video, image or audio.

2. DIGITAL WATERMARKING

There are many advantages for processing and distributing video and different forms of understanding which are presented by digital illustration. First, digital application applications offer important creating, modifying, imparting, and adaptability in manipulating digital expertise. The flexibleness, malleability, and extensibility of software processing are lacked by analog instruments. 2nd, the digital communications network (such because the internet) permit digital knowledge to be allotted and circulate on a vast scale. On some of these networks, currently open and proprietary protocols equivalent to the arena big internet allow any consumer to quite simply and cheaply obtain, furnish, trade, and in finding digital information. Ultimately, digital understanding can be prepared, and in targeted, copied without introducing loss,

degradation, or noise. For example, a single digital video sign may produces an infinite number of perfect copies. In distinction, the addition of noise to a replica from analog signal processing is ineluctable.

In the past years, Watermarking ways are projected for these services within which the copyright info is enclosed into transmission capabilities as a way to safeguard possession. The study is now studying watermarking schemes to preserve multimedia content. Digital watermarking is a system which can serve functions. An tremendous range of watermarking theme projected to cover copyright marks and secondary data in digital snapshots, video, audio and some alternative transmission objects. A watermark can be defined by a kind of photograph or text that's the paper supplies proof of its legitimacy, nonetheless affected. Digital watermarking is companion delay of this conception within the digital World. Unique development in recent years of the online has highlighted the requirement for mechanisms to support the possession of digital media thoroughly identical copies of digital information, be it graphics, audio or text, is made and distributed handily. Even as the aforementioned benefits present substantial possibilities for creators, the potential to type best copies and the simply applying that these copies shall be disbursed conjointly facilitate misuse, non legal repetition and distribution piracy, plagiarism, and misappropriation. Content material creators and house owners are quandary related to the penalties of forbidden repeating and distribution on a big scale. This predicament isn't entirely theoretical. Fiscal loss coming up from proscribed repeating and distribution of copyrighted matter is computable to be inside the billions of dollars. Lately, long-established web software package exceptionally based on a peer-to- peer (P2P) design (similar to Kazaa, BitTorrent, eDonkey and Gnutella) has been used to share (distribute) copyrighted track, films, software, and various substances. Future P2P methods could encode the info being shared, its users, aid domain anonymity a better number of users, and be extra powerful. These advances in P2P programs will make enormous challenges for copyright enforcement. Hence, there's the best wish for ways which can continue the financial value of digital video and defend the rights of content house owners.

3. REVERSIBLE DATA HIDING

Hiding data inevitably destroys the host image even though the distortion introduced by hiding is imperceptible to the human visual system. However, there are some sensitive images where any embedding distortion made to the image is intolerable, such as military images, medical images or artwork preservation. For example, even slight changes are not accepted in medical images due to a potential risk of a physician giving a wrong explanation of the image. Hence, reversible data hiding techniques give a solution to the problem of how to embed a large message in digital images in a lossless manner so that the image can be completely restored to its original state before the embedding occurred. Procedure of reversible data hiding is shown in Fig 1.

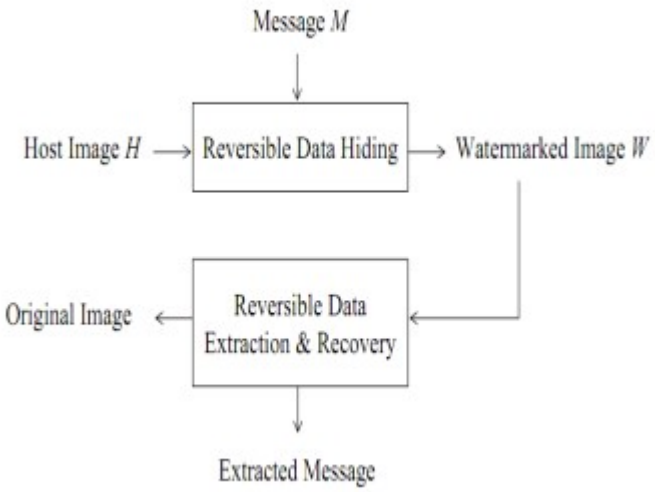

Fig-1: Reversible data hiding process

In this process the sender embeds the message M to a host image H in a lossless manner so that after the message is extracted from the watermarked image, the exact copy of the original image is obtained. reversible data hiding technique can be used as a fragile invertible authentication watermarking that embeds an authentication code in a digital image in a reversible way. Only when the embedded authentication code matches the extracted message, the image is deemed authentic.

4. HISTOGRAM SHIFTING

The histogram modification technique involves generating histogram and finding the peak point and the zero point and shifting histogram bins to embed message bits. For a given host image, we first generate its histogram and find a peak point and a zero point. A peak point corresponds to the grayscale value which the maximum number of pixels in the given image assumes. On the contrary, a zero point corresponds to the grayscale value which no pixel in

the given image assumes. Fig 2 shows a histogram of an image.

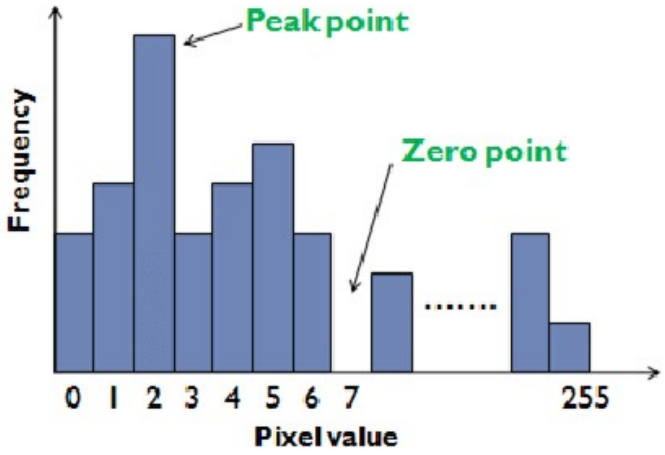

Fig-2: Histogram of image

In the above image peak point is at 2 and the zero point is at 7. Let P be the value of peak point and Z be the value of zero point. The range of the histogram, [P+1, Z-1], is shifted to the right-hand side by 1 to leave the zero point at P+1 as shown in Fig 3.

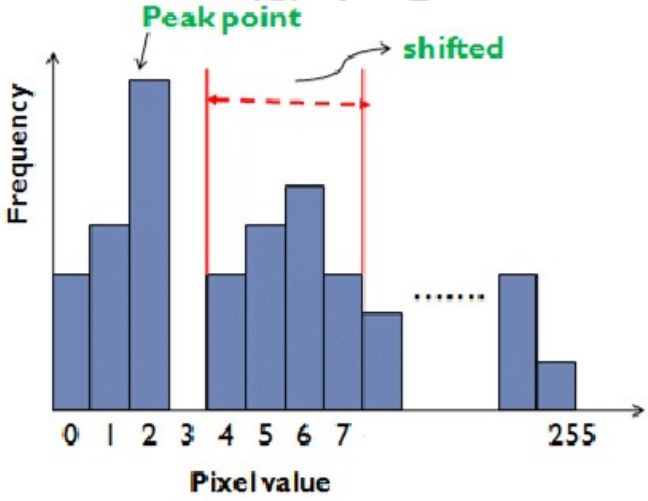

Fig-3: Shifting a range of histogram

Once a pixel with value P is encountered, if the message bit is "1," increase the pixel value by 1. Otherwise, no modification is needed. We note that the number of message bits that can be embedded into an image equals to the number of pixels which are associated with the peak point.

5. EXPERIMENTAL RESULTS

In the proposed research we have considered various types of cover images. Secret image (payload) is shown in Fig 4. Histogram of cover image is calculated by MATLAB tool. Fig.5 represents a cover image and Fig. 6 represents histogram of that image. Fig. 7 represents watermarked image.

Fig4: Secret image

Fig-5: CCTV 1 image as cover image

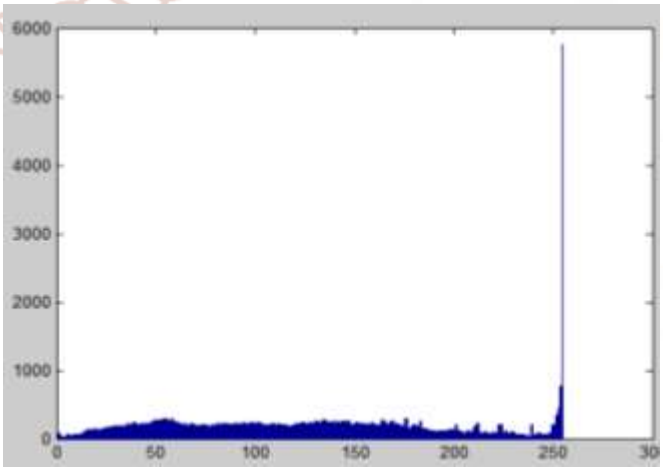

Fig-6: Histogram of cover image

Fig. 7 Watermarked image

Similarly we have taken other images also as cover image and performed data hiding process on each image. Other cover images are shown below:

Fig. 8 CCTV 2 image

Fig. 9 YIT image

This is the process of hiding secret image in cover image at transmitter side and extracting secret image from cover image at receiver side. In this case we have taken all the parameters correct. We have calculated some parameters also which are shown in table below.

Table 1: Resultant parameters

Image	Random Index	Global Consistency Error	Variation of Information	PSNR
CCTV1	1	0	-3.5527	INFINITE
CCTV2	1	0	0	INFINITE
YIT	0.9980	0.1051	0.6456	46.1283

6. CONCLUSION

This research frames a embedding model that can embed or hide a secret image into a cover image using histogram shifting method of reversible data hiding. The message examined in this research work is a binarized class of image that is embedded into a gray cover image. The proposed method of watermarking obtains a satisfactory level of watermarking.

In future we will implement this technique on different types of cover image and different types of secret image (payload) to examine the different features such as embedding capacity, signal to noise ratio etc.

REFERENCES

1. Abraham, V. K. 2002. The International Conference on Commercial Floriculture, Summary Report, 11-12 August, Bangalore.
2. Yeo and M.M. Yeung,: 'Analysis and synthesis for new digital video application,' icip, International Conference on Image Processing(ICIP97),vol. 1,pp.1,1997.
3. M. Natarajan, G. Makhdumi1,: 'Safeguarding the Digital Contents: Digital Watermarking,' DESIDOC Journal of Library & Information Technology,vol.29,May 2009,pp. 29-35.
4. C.I. Podilchuk, E.J. Delp,: 'Digital watermarking: algorithms and applications,' Signal Processing Magazine, vol. 18,pp. 33-46, IEEE, July 2001.
5. G. Doerr, J.L. Dugelay,: 'Security Pitfalls of Frame-by-Frame Approaches to Video Watermarking,' Signal Processing, IEEE Transactions, vol. 52,pp. 2955-2964, 2004.

6. M. K. Thakur, V. Saxena, J.P.Gupta,: 'A Performance Analysis of Objective Video Quality Metrics for Digital Video Watermarking,' Computer Science and Information Technology (ICCSIT),2010, 3rd IEEE International Conference, vol. 4,pp. 12-17,2010.
7. S. Voloshynovskiy, S. Pereira, T. Pun,: ' Watermark attacks,' Erlangen Watermarking Workshop 99, October 1999.
8. G. Langelaar, I. Setyawan, and R. Lagendijk,: ' Watermarking Digital Image and Video Data: A State of - Art Overview,' IEEE Signal Processing Magazine, vol.,pp. 20-46, Sep. 2000.
9. F. Hartung and B. Girod ,: ' Watermarking of uncompressed and compressed video,' Signal Processing, 1998,vol. 66, no. 3,pp. 283-301.