Analysis of Image Hiding Process using Histogram Shifting Based Approach of Reversible Data Hiding

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
[3]H.O.D. (Electronics & Comm.), Yagyavalkya Institute of Technology, Jaipur, Rajasthan, India

ABSTRACT

In this paper we have used an algorithm for hiding secret image also called payload in different types of cover image using histogram shifting method of reversible data hiding technique. We have analyzed this algorithm in MATLAB simulation tool. In this analysis various types of cover images are used to hide secret image also called payload. Some performance parameters are computed to compare performance of all the images. Parameters are like random index, global consistency error, variation of information and peak signal to noise ratio.

Keyword: - *Payload, Random Index, Global consistency error, Histogram, Peak signal to noise ratio*

1. INTRODUCTION

In recent years copyright safety as a paramount safety is supplied in digital marketplaces. There are two watermarking process are planned and when inflected to the compressed and uncompressed video to be able to factor out the advantages and accordingly the potential helplessness inside the schemes working inside the frequency area and within the abstraction domain.

A watermark in video content is helpful in many applications to generate, as an example, services like copy direction for DVD or traitor tracing in video-on-demand frameworks. Today, video watermarking primarily broads results obtained for still pictures [1]. Thus, there are two common frame-by-frame approaches are conferred. Such straightforward adaptations have, however, led to non secure algorithms and two specific attacks are initiate to illustrate this point. Two strategies to better performance against connivance attacks such as watermark modulation and the embedding strength modulation.

A watermark could be a in sight image beaded or imprinted directly onto the digital paper or digitally further onto a picture later. It'd be name, company emblem, the company name, the copyright image or nearly one thing that marks those footage. Some are frightfully obvious whereas others unit hidden (much to the chagrin of a criminal below fire). Watermarks are used on nearly every paper supply, banknotes, passports, straightforward to shop for reams of paper, digitally created footage and pictures. We've got a bent to deploy work exploitation straightforward watermarks [2].

The use of watermarks to regurgitate the work in copies, prepare derivative works based upon the work, spread out copies or records of the work to the public by sale or other shift of ownership, display the work publicly. Essentially if we tend to took the image and wish to copyright it we will management what happens therewith image as long as we tend to own the copyright.

2. LITERATURE REVIEW

Watermarking technique has developed from stenography. Steganography is the art / science /study of communicating in a way which hides a secret message in the main information. Steganography means covered writing period. In steganography a problem of concern is information measure for the hidden message whereas robustness is of a lot of interest with the watermarking. Steganography hides messages in plain sight instead of coding the message; it's embedded in information and doesn't need secret transmission. The message is carried within the info. Steganography is thus broader than cryptography. In [3], Tanwi Biswas et al. presented a method based on compressed gray level histogram shifting which produces good quality of image with high embedding capacity. In this method range of image pixel values is compressed by computing square root of these pixel values. It is also noticed that rounded pixel values enhance the amount of peak pixel and therefore also increases the data hiding capacity efficiently. After data embedding, pixel values are squared and round values of the pixels are considered to reconstruct the image. In [4], Aulia Arham et al. proposed scheme based on difference expansion which increases embedding capacity and quality of image. Medical images have large smooth block areas. This scheme is implemented to non smooth areas images. In [5], Ali Al-Haj et al. implemented a system that joins encryption standards with watermarking methods to give security to medical images transmitted between healthcare units. This system is based on hybrid algorithm. Through this system authenticity of images can be validated either in spatial domain or in encrypted domain. Many researchers have worked on this field and still the work is going on to develop an efficient algorithm for reversible data hiding.

3. APPLICATIONS OF WATERMARKING

Digital watermarking has been widely and successfully implemented in billions of media objects across a wide range of uses. This section can present some applications of digital watermarking in each ancient and novel areas [6]-[9].

A wide vary of applications like digital watermarking are often used for:

Copyright Protection - For the security of the intellectual property, the data owner can integrated a watermark representing copyright information in the data. Integrated watermark can be used as a evidance, example in a court if someone intentionally infringed the copyrights. Source Tracking (different recipients have different watermarked content) Broadcast Monitoring (Television news often international agencies including the watermarked video)

Fingerprinting: To trace the source of illegal copies, the owner can use fingerprinting technology. In this case, the owner can embed various watermarks in the copies of the data that are supplied to various customers. Fingerprinting may be compared to embedding a serial variety that's connected with the shoppers known within the information. this permits the material possession owner to spot customers who have broken their license statement by activity the information to 3rd parties.

Copy protection: The information keep in watermark will straight management digital recording devices for copy protection functions. During this case watermark represents a copy-forbid bit and watermark detectors within the recorder verify whether or not the info offered to the recorder is also keep or not.

Broadcast monitoring: By embedding a watermark in commercial advertising, an automated monitoring system can verify whether the advertisements are broadcasted as narrowed. Broadcast monitoring can protect not only the commercials but also the precious TV products.

Data authentication: The so called fragile watermarks can be used to check the legitimacy of data. A fragile watermark point whether the data has been adjusted. Further it offers the information in which part the data are being adjusted.

Medical safety: Embedded the date and the patient's name in medical images could be a useful safety measure.

Data Hiding: Watermark techniques can be used for the transmission of concealed messages. Since many governments confine the use of encryption services, people can hide their messages in other data.

In international show business, piracy of film, music and video could be a multi-billion dollar huge drawback. The digital watermarking will ease limit the unlicensed copy and spread.

4. PROPOSED WORK

In our work we have comparatively analyzed various features of cover image by hiding payload using histogram shifting method of reversible data hiding procedure. All the simulations are carried out in MATLAB simulation tool. Secret image is shown in Fig 1.

Fig 1 Secret image

Fig 2 CCTV image as cover image

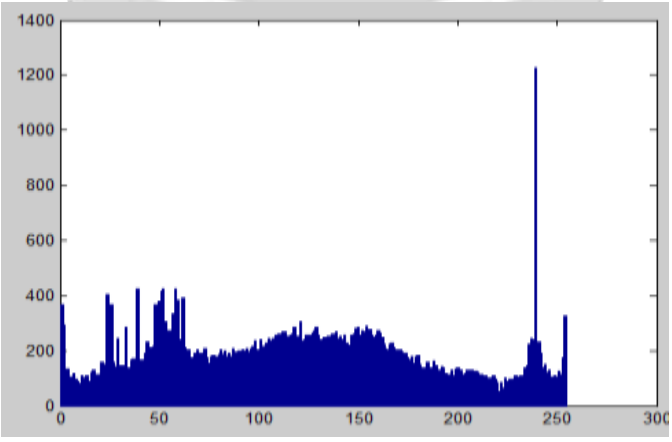

Fig 3 Histogram of CCTV image

Fig 4 Watermarked image of CCTV image

Fig 5 Medical image as cover image

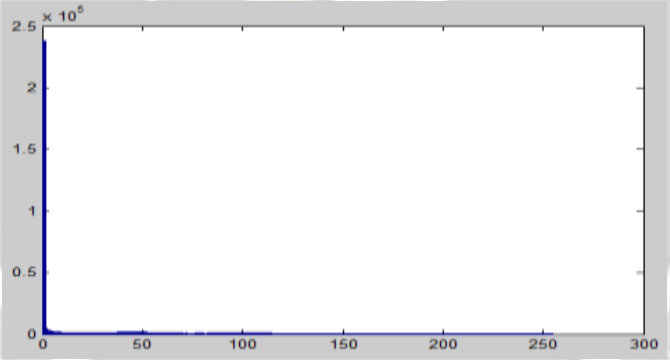

Fig 6 Histogram of medical image

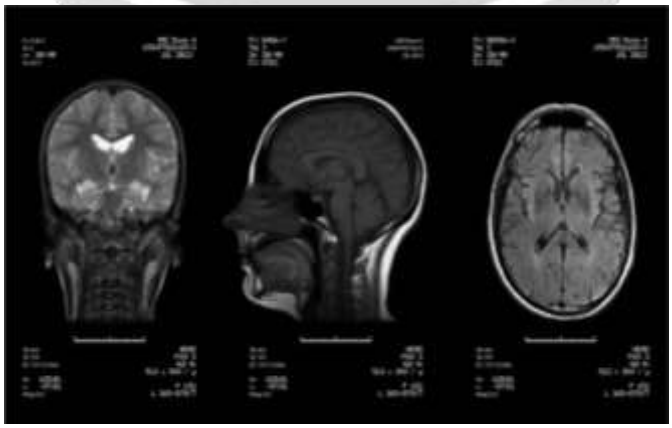

Fig 7 Watermarked medical image

5. EXPERIMENTAL RESULTS

We have considered different types of cover image to hide a secret image and computed different performance parameters which are then used to compare the performance of different images. In the below table INF means infinite value.

Table 1: Performance parameters

Image	Random Index	Global Consistency Error	Variation of Information	PSNR
CCTV-1	1	0	-3.5527	INF
CCTV-2	1	0	0	INF
Medical	0.9972	0.0048	0.0425	74.0765
Artificial	0.9931	0.4497	2.3574	48.2660
Satellite	0.9915	0.4955	2.5618	52.5752
Boat	0.9992	0.0474	0.3045	64.1469
YIT	0.9980	0.1051	0.6456	46.1283

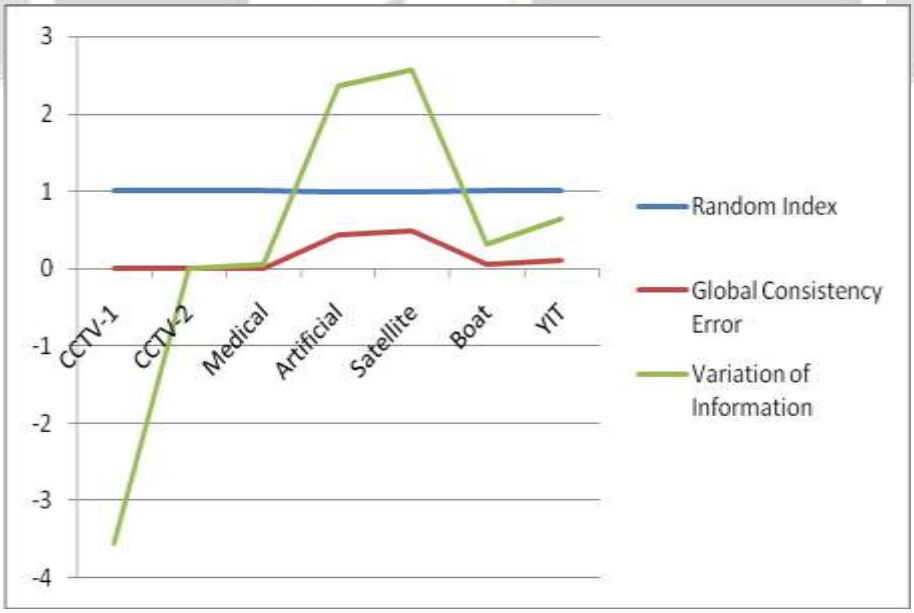

Fig 8 Comparison graph

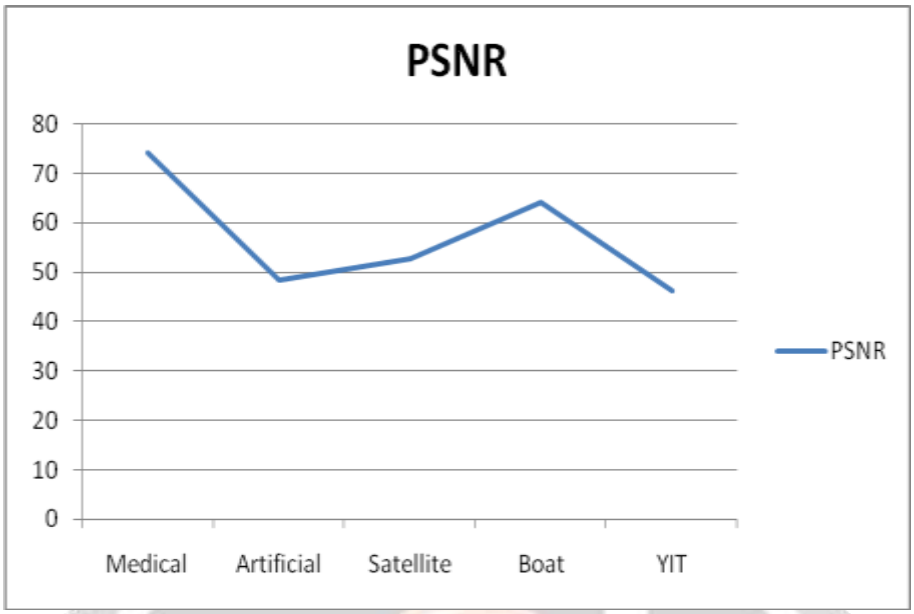

Fig 9 PSNR comparison

6. CONCLUSIONS

We have successfully performed analysis of hiding secret image in different types of cover image. We have obtained infinite PSNR for CCTV image which shows that we get a very good quality image after payload is embedded. All the simulations have been carried out in MATLAB simulation tool. After CCTV image we have obtained maximum PSNR (74.0765) for medical image. We have also compared all the images according to different parameters such as random index, global consistency error, variation of information and peak signal to noise ratio.

7. REFERENCES

[1] J. Lee et al, A survey of watermarking techniques applied to multimedia, IEEE International Symposium on Industrial Electronics, vol. 1,pp. 272-277, 2001.

[2] F. Hartung and M. Kutter,: 'Multimedia watermarking techniques', Proceedings of the IEEE, vol. 87, no. 7, July 1999.

[3] Tanwi Biswas, Md. Mehedi Hasan and Tanoy Debnath, "A New Method of Reversible Data Hiding Based on Compressed Gray Level Histogram Shifting", IEEE, 2016.

[4] Aulia Arham, Hanung Adi Nugroho and Teguh Bharata Adji, "Combination Schemes Reversible Data Hiding for Medical Images", International Conference on Science and Technology-Computer, IEEE, 2016.

[5] Ali Al-Haj, Hiba Abdel-Nabi, "Digital Image Security Based on Data Hiding and Cryptography", IEEE, 2017.

[6] Coatrieux, G., "Relevance of watermarking in medical imaging", Information Technology Applications in Biomedicine, 2000. Proceedings. 2000 IEEE EMBS International Conference.

[7] Nikos Komninos and Tassos Dimitriou, "Protecting Biometric Templates with Image Watermarking Techniques", Vol.4642, Springer Berlin Heidelberg.

[8] Sanghyun Joo, Youngho Suh, Jaeho Shin, and Hisakazu Kikuchi, "A New Robust Watermark Embedding into Wavelet DC Components", vol. 24, no. 5, Oct. 2002, pp. 401-404 in ETRI journal.

[9] Y.-C. Tseng and H.-K. Pan. Secure and invisible data hiding in 2-color images. 20th Annual Joint Conference of the IEEE Computer and Communications Societies, 2:887–896, 2001.