DATA HIDING USING HPSNR TECHNIQUE IN VISUAL IOT SECURITY

R. Karthika,
Department of Computer Science, Muthayammal College Of Arts & Science, Rasipuram(Tk),Namakkal (Dt), 637 408. Affiliated by Periyar University, Salem, Tamil Nadu, College Code: 123. E-Mail: karthikar1195@yahoo.com

Mr. P. Subramaniam, *M.S(IT&M)., M.Phil.,[Ph.D].,*
Assistant Professor, Department of Computer Science, Muthayammal College of Arts & Science, Rasipuram(Tk),Namakkal (Dt), 637 408. Affiliated by Periyar University, Salem, Tamil Nadu, College Code: 123. E-Mail: subramaniam78@gmail.com.

Abstract

Data is the today's gold. Securing the data over the internet plays an important role. Visual Internet of things is one that collects huge volume of visual information over the internet. One of the methods to secure the data is to hide the information using various techniques and transferring the secured data. In this paper, a technique called HPSNR (Human-Visual Peak Signal-To-Noise Ratio) is used. It generates high quality images on inverse half-toning. It uses least mean square (LMS) algorithm to find the relationship between neighbouring positions of the image. With this technique, probabilistic values of all possible grayscale pixel values can be obtained using Bayesian theorem. The image is compressed and transmitted over the internet and at the receiver's end the image is reproduced. The data obtained from the sensors are accumulated, pre-processed and then the data is hidden and transferred over the internet. It is evident that HPSNR is best suited with data hiding in images.

Keywords: ***Visual Internet of Things, HPSNR, inverse half-toning, LMS, Bayesian theorem, sensors, grayscale pixel, data hiding.***

I. INTRODUCTION

Visual Internet of Things is a IOT which collects the data from the cloud or internet .In this technique the data can be transmitted using any devise such as mobiles, laptops etc. This technique is mainly used to exchange the information using the image or video .Some time doing such things we may face problems like, there can be a loss in the quality of images. Our system is based on a novel technique where by using it. We can assure the quality of image to the higher level. We are going to use a novel stenography in our IOT.

Steganography is mainly done to hiding file, message, image, or video within another file, message, image, or video. In Steganography, electronic communications may include encoding information that encodes data within the transport layer, such as the document

layer, image file, program, or protocol. Media files are suitable for steganographic data transfer due to their large size. For example, the sender can start from a harmless image file and adjust the color of each hundred pixels to match a character in the alphabet. This change is so subtle that it is unlikely to notice the change it does not seek. This method may seem simple and easy, but it is poor compression for JPEG images. Replacing least significant bit (LSP) is the most common information masking technique, but in our approach we will use HPSNR with LPS (low mean quadrature error).

II. LITERATURE SURVEY

There are many Steganographic techniques for image file has been created in the past which are as follows:

A. Spatial Domain Technique

There are several versions of spatial Steganography, all of which directly convert a few bits of image pixel values into masking data. Least significant Bit (LSP) is one of the simplest techniques, which hides a secret message in LSPs without apparent distortion of pixel values. Changes in the LSP value are not visible to the human eye. Message bits can be included simply or randomly. LSP, matrix modulation, some spatial domain techniques.

B. Masking and Filtering

Masking and filtering is an information masking technique that can be used in gray scale films. Hiding and filtering is similar to placing watermarks on a printed image. These techniques include information in the most important areas of the noise level. Watermarking techniques are integrated with the image and can be used without fear of damaging the image due to loss compression.

C. Transform Domain Technique

The frequency field message is inserted into the converted transactions, giving it the ability to hide additional information and give greater strength against documents. Transform Domain Embedding - Multiple mechanisms can be called recommended embedding technologies, as many of these powerful imaging systems today work in the field of conversion. The parts of the image that are exposed less. Some metamorphic field technologies do not rely on image format, which may be more than lossless design changes.
Domain conversion methods of different types:

1. Unique Fourier transform technology (TFT).
2. Unique DCT technology.
3. Unique bandwidth transfer technology (DWT).

III. EXISTING METHODOLOGY

PSNR is an improved version of BTC, preserves absolute moments rather than standard moments, in this technique digitized image is divided into blocks of n x n pixels. Each block

is quantized in such a way that each resulting block has the same sample mean and the same sample first absolute central moment of each original block.

MSE = (1/(x*y))*sum(sum((m-n).^2)) **(eq 1.1)**

PSNR=0*log(max(max(m)))/((MSE)^0.5) **(e.q 1.2)**

Legend:

m - the matrix data of our original image

n - the matrix data of our degraded image in question

m -the numbers of rows of pixels of the images

y - the number of columns of pixels of the image

MAX is the maximum signal value that exists in our original image.

A. PSNR Algorithm:

Step 1: Dividing the image into small non overlapping blocks of size 4 x 4 pixels.

Step 2: Calculate the statistical moments and σ of the block using the equations 1, 2.

Step 3: Creating the bit-plane with 0's and 1's.

Step 4: send or store the bit-plane, x and σ.

Step 5: Do again the steps 2 through 4 for all the blocks of the input image.

B. Merits of PSNR:

- It requires extra memory.
- Maintaining edges.
- Adaptive bit-allocating optional

C. Demerits of PSNR:

- Huge bit-rate when compared to technique such as DCT, VQ, etc…
- Sometimes it Block appearance of image at the time of reconstructing image in some cases.
- torn edges

IV. PROPOSED METHODOLOGY

In the proposed system we are going to use HPSNR technique since it generate a high quality image on inverse half-toning. Inverse half-toning is the process of reconstructing high-quality continuous-tone images from the halftone version. In our approach we are using the LMS, it will help us in finding pixel value and from that value we can extract the grayscale value of the pixel using the Bayesian theorem . After doing this the image is compressed and transmitted in the cloud so that the other person and access the data .in our approach we are assuring that quality of the image remain in tacked.

In our comparison we have also embed data into smooth blocks, and the proposed method is used to embed data into complex blocks. In addition to comparing the payload (i.e., data capacity in units of bits), this work adopts two image quality measures to fairly evaluate the

performance of each method. The first quality measure is called Human visual based Peak Signal-to-Noise Ratio (HPSNR), The HPSNR can be expressed as follows:

$$\mathrm{HPSNR} = 10 \times \log \left(\frac{P \times Q \times 255^2}{\sum_{P,Q} \left[\sum_{m,n} q_{m,n} \left(g_{i+m,j+n} - h_{i+m,j+n} \right) \right]^2} \right) (\mathrm{dB}), \quad (1.3)$$

P, Q indicates the image size, q indicates the HVS low-pass filter; g,i,j and hi,j indicate the pixels.

In our approach we get a better result in calculating the HPSNR. The HPSNR block computes the signal-to-noise ratio, in decibels, between two images. This ratio of difference is used as a quality measurement between the original and a compressed image. The higher the HPSNR, the better the quality of the compressed, or reconstructed image. The Least mean-square error (LMS) and HPSNR are used to compare image compression quality. The LMS represents the cumulative squared error between the distorted image and the original image, whereas HPSNR represents a measure of the peak error. The lower the value of LMS, the lower the error. Our technique show a better result that the existing one. This is the flow of our image compression.

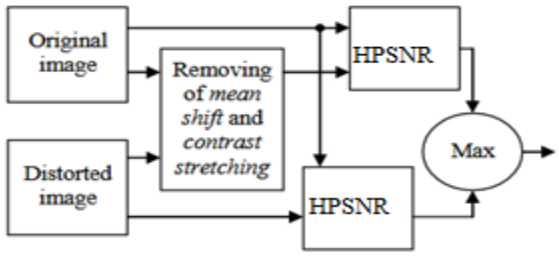

Fig 4.1 comparing the original and input image.

V.ALGORITHM STEPS

In this we are going to discuss the text embedding and Text extraction steps

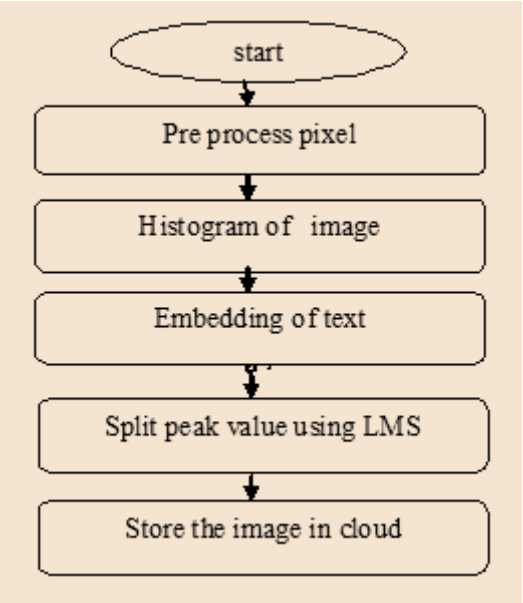

Fig 5.1 flow of Text Embedding

The extraction and recovery process include the following steps:

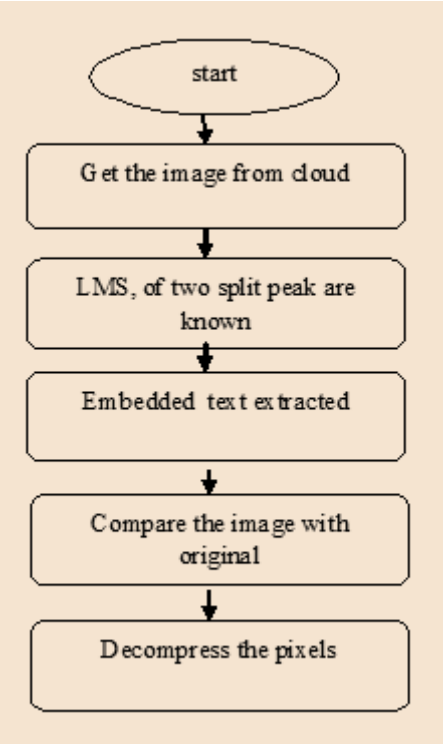

Fig 5.2 flow of Text extraction

VI. EXPERIMENTS AND RESULTS

In this paper, the experiment is done with java and Windows 7. The computer has Intel CPU 1.8 GHz and 2GB RAM. The HPSNR and payload are used to evaluate the quality of the stego image after embedding.

$$\mathrm{LMS} = K\sum_{i=1}^{I-7}\sum_{j=1}^{J-7}\sum_{m=1}^{8}\sum_{n=1}^{8}((X[m,n]_{ij} - X[m,n]_{ij}^{e})T_c[m,n])^2$$

Where LMS is the mean squared error between cover image (I) and stego image (J). m and n are the row size and column of cover image. Thereafter HPSNR value is calculated using formula .

Comparison between Shahryari and Masaebi and the proposed method in terms of HPSNR using clock (128x128) as the secret image

		Method		
	Image	Shahryari method	Masaebi method	Proposed method
HPSNR	Baboon	43.12	51.09	52.66
	Lena	43.69	51.67	53.28
	Airplane	40.84	48.53	51.35

Table 1.1 table of performance evaluation

The way of shahryari and masaebia are compared with the proposed method in this paper. The size of image is 512x512 and secret image is 128x128. They are both 8-bit grayscale images.

From the table, it can be concluded that the quality of the stego image with the proposed algorithm is much better than others. The maximum embedding capacity for LMS substitution in proposed method is 25%. Though text hiding capacity is low, visual quality of the stego image is high. The embedding capacity can be increased by increasing the number of Text bits embedded in contour let coefficients.

It also can be shown in Figure that the stego image in proposed approach is the closest to the original cover image in three methods.

Stego image with HPSNR is 53.28db, and extracted image with HPSNR is 46.47db.
Stego image with HPSNR is 51.72db, and extracted image with HPSNR is 45.83db.
Stego image with HPSNR is 52.66db, and extracted image with HPSNR is 46.28db.

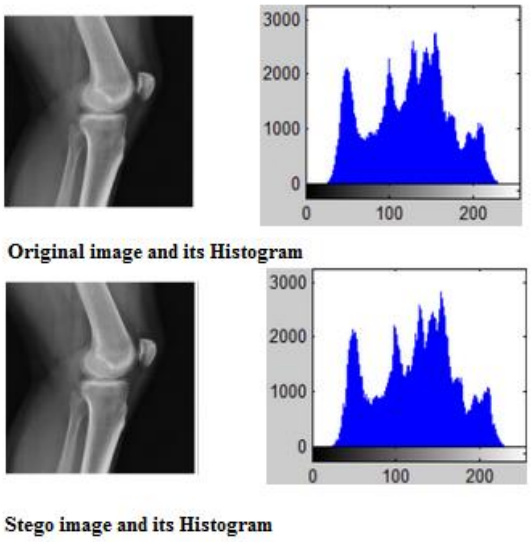

Fig 6.1 Histogram of original and stego image

Each image displays cover image, secret text, stego image, retrieved image and their histograms with proposed method. It also shows that retrieved image is very much same with original secret image.

VII. CONCLUSION

Steganography is an effective way to hide sensitive information. In this paper we have used the HPSNR Technique and LMS Technique on images to obtain secure stego-image. We have also shows that HPSNR value of our encoding is higher than PSNR of LSB encoding. Our results indicate that the LMS insertion using random key is better than simple LSB in-sertion in case of lossless compression. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected also with the personal key. So, it is not possible to damage the data by unauthorized personnel. The algorithm is usage for 8 bit image of the same size of cover and secret text, so it is easy to be implementing in both grayscale and color image. This paper focuses on the approach like increasing the security of the message and increasing HPSNR and reducing the distortion rate .By using this approach we can assure more security for the image which we stego. So we automatically get the advantage of storing the data in the cloud. Since the cloud is considered as less secure because of its nature i.e. since the storage of the data is outside our supervision the maintenance of the data becomes more critical. By using our approach we can assure more reliable cloud network, whereby we can assure more security to the users data stored in the cloud.

REFERENCES

1. *R.Anderson and F. Petitcolas, "On the limits of steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.*

2. Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganog- raphy," IEEE computer society,2003.

3. K B Raja, Venugopal K R and L M Patnaik, "A Secure Stegonographic Al-gorithm using LSB, DCT and Image Compression on Raw Images",Technical Re- port, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering,Bangalore University, December 2004.

4. An overview of image steganography by T. Morkel , J.H.P. Elo_, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Depart- ment of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

5. Johnson, N.F. Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

6. "Detecting LSB Steganography in Color and Gray-Scale Images" Jessica Fridrich, Miroslav Goljan, and Rui Du State University of New York, Binghamton.

7. Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, "Hiding data in images by opti- mal moderately signi_cant-bit replacement" IEE Electron. Lett. 36 (25) (2000)20692070.

8. Hiding data in images by simple LSB substitution by Chi-Kwong Chan, L.M.Cheng Department of Computer Engineering and Information Technology, CityUniversity of Hong Kong, Hong Kong Received 17 May 2002.

9. "A Tutorial Review on Steganography" by Samir K Bandyopadhyay, Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das, Heritage Institute of Technology.

10. International Journal of Computer Science Engineering Technology (IJC-SET) "Modern Steganographic technique: A Survey" by Pratap Chandra Mandal Asst. Prof., Department of Computer Application B.P.Poddar Institute of Man-agement Technology .

11. International Journal of Advanced Research in Engineering and Applied Sciences" Analytical Relation & Comparison Of Psnr And Ssim On Babbon Image And Human Eye Perception Using Matlab" A survey by Megha Goyal, Yashpal Lather, Vivek Lather.

AUTHORS PROFILE

R. Karthika, Department of Computer Science, Muthayammal College Of Arts & Science, Rasipuram(Tk),Namakkal (Dt), 637 408. Affiliated by Periyar University, Salem, Tamil Nadu, College Code: 123.

Mr. P. Subramaniam, M.S(IT&M)., M.Phil.,[Ph.D].,
Assistant Professor, Department of Computer Science, Muthayammal College of Arts & Science, Rasipuram(Tk),Namakkal (Dt), 637 408. Affiliated by Periyar University, Salem, Tamil Nadu, College Code: 123.