Pixel Value Differencing Image Steganography using Secret Key

Ankita Sancheti

Abstract: ***In this paper, secure steganography is used to obtain high capacity of image for data hiding. Both color and gray scale images have been used as cover file for PVD method. Then a secret key is used to control the message embedding process. To estimate how many secret bits will be embedded into the pixel, largest difference value between the other three pixels close to the target pixel is used. This makes edge areas of image to be used for higher embedding capacity. In order to avoid the need of a copy of cover file at receiver, size of message file is also embedded in stego file. Thus only stego-image is required at receiver. Peak signal to noise ratio (PSNR) is used to measure the quality of stego images.***

Index Terms: Steganography, PVD, PSNR, Cryptography

I. INTRODUCTION

Nowadays, due to a fast growth of the modern technology, Internet has become a convenient way for data transmission. To avoid security attack, data encryption and data hiding techniques like cryptography and steganography are very popular in information transmission over internet.

Steganography is art of secret communication which hides the fact that communication is taking place. Most of today‟s steganographic systems use digital multimedia objects like audio, videos, images etc. as cover media because they are not suspicious and doesn‟t draw attention like cryptographic objects. 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.

Digital images have been used here as cover file to hide information. After embedding a secret message into the cover-image, a stego-image is obtained. It is important that the stego-image is free from any easily noticeable change due to message embedding. A third person could use such changes as an indication that a secret message is present. Once this message detection can be considerably decoded, the steganographic implementation becomes of no use.

Many steganographic methods have been developed for hiding secret information in digital images [1]-[4]. The most common method is the least significant bit or LSB method, which utilizes some least bits of pixels in the cover image to embed the hidden data. The advantages of the LSB method is ease of computation with high visual quality.

Several methods exploiting these human visual characteristics have been studied recently [6]-[9]. This proposed method improves on the Han-lingZHANG‟s PVD technique [1] by increasing capacity and security. The results have shown that our method increases the amount of secret data that can be stored in a cover image, while at the same time producing a secure stego-image. The remaining paper is organized as follows. In section 2, we present our steganographic algorithm for color and gray images. In section 3 Experimental illustrations are given. Section 4 shows comparison results. Finally, in section 5 the conclusion of the paper is given.

II. PVD STEGANOGRAPHY WITH SECRET KEY

This method is based on PVD method proposed by Han-lingZHANG, Guang-zhi GENG, Cai-qiongXiongand [4].It is modified to give a secure and high capacity steganographic system. It has advantage of high capacity as in PVD and has good security as in encrypted system.

LSB steganography method gives a very low embedding capability, which is 1 bit par byte. On other hand PVDmethod gives very good embedding capability, in between 2-4 bits par byte. This is more than 2-3 times to LSB method. By combining encryption techniques with PVD steganography a secure as well as high capacity stego system can be achieved.

While human perception is less sensitive to subtle changes in edge areas of a pixel, it is more sensitive to change in the smooth areas [1].Even when we modify last 1-2 bits of all image pixels in smooth area, it isn‟t distinguishable to human eyes.

Fig 1: (a) Lena.jpg

Fig 1: (b) Lena_00.jpg Fig 1:(c) Lena_11.jpg

Fig. 1: Lena.jpg and its transforms

Revised Manuscript received on December, 2012.

Ankita Sancheti, M.tech Scholar, Computer Science, Mewar University,Chittorgarh,India.

A standard image lena.jpg as in fig. 1(a) is modified. Last two bits of all image pixels are set to 00 in fig. 1(b) Lena_00.jpg and to 11 in fig. 1(c) Lena_11.jpg. There is no visible difference in between these images.

A. Data Hiding Procedure:

In this method capacity of each pixel is determined as in PVD method. Then password is combined with 5th bit of that pixel to achieve hiding properties of data. If password matches, data is inserted directly. Otherwise inverted data is inserted into the pixel. Thus somewhere data is inserted inverted and at other places it is hidden directly.

Without knowledge of secret key if data is extracted then it is not of any use. Other main point is that size of embedded bit is unknown without key. So with wrong key, the message can‟t reshape. For a message as image, extracted file will have some random dimensions which make it useless.

The data embedding process is as following:

1) Read cover image and create RGB matrixes. For gray scale image create gray matrix.
2) Insert secret key and convert it into bit stream.
3) Determine gray level variation near target pixel and thus determine capacity of that pixel say „n‟.
4) XOR 5th bit of cover pixel with one bit of secret key.
5) If password matches, „n‟ bits of message data are embedded in cover pixel.
6) Otherwise data is inverted before embedding.
7) Steps 3-6 are repeated till whole data is embedded.
8) Then Size of message file is embedded into last 100 bytes using same procedure.
9) Data is written in form of image file to obtain stego-image.

Data embedding Capacity:

Capacity of a pixel can be determined as follow [1]:

1. First row and column of cover image are not used for insertion. Target pixel is selected starting from position (2,2).
2. Find gray level G of a pixel at position P for left, upper and left upper positions to the target pixel P_X.
5. Data embedding capacity is restricted to 4; over this, cover image quality may degrade.

In smooth areas where variation in color is negligible, two bits are inserted. In edge area this can go to 2-4 bits in a byte.

For a RGB image this process is applied independently

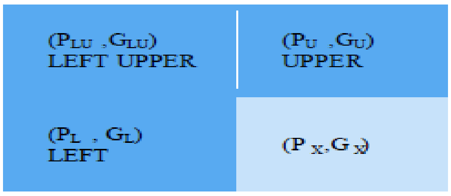


Fig 2: Target and its neighboring pixels.

3. Now difference of maximum and minimum gray level is determined as[1]

   Gmax = Max(GL, GU, GLU);
   Gmin = Min(GL, GU, GLU); Difference d = Gmax – Gmin;
4. Embedding capacity „n‟ is calculated as:

   n = 4 ; d >15
   = $\log_2(d)$; 3 <d<16

on each color matrix. Variation in gray level is more significant than colors, so capacity of gray scale image is higher than RGB image for same size.

B. Data Extraction Process:

For reconstruction of message file two things are required. First is all embedded data and second is the size of file.

Data is protected with password but it is not same as combining cryptography and steganography. In that case data is first encrypted and then embedded. Here data is embedded and encrypted simultaneously. Thus even if someone is able to collect all embedded data, he need cover file to reconstruct it. So any modification in image will make it unrecoverable.

Extraction of data can be done as follow:

1. Open stego file and convert it in RGB matrixes.
2. Enter password and convert it into 1D bit stream.
3. Extract last 100 bytes of stego image to get message file sizes.
4. Calculate capacity of stego pixels (as in data hiding process).
5. Now extract last „n‟ bits of stego pixel as message data.
6. XOR 5th bit of stego image with secret key.
7. If key matches insert data to message bit stream directly, else invert data first and then insert to bit stream.
8. Repeat steps 4-7 till full size of message data is obtained.
9. Now reshape message data and write to the file.

Experimental results are demonstrated using some standard RGB and Gray level images of dimension 255x255.Message file is a standard image of dimension 80x80.

Figure 2: Message image (Baboon_80.jpg 80x80) Secret key or password

was taken same as the cover file name, i.e. Secret key or password was taken same as the cover file name, i.e.

= 2 ; d < 4

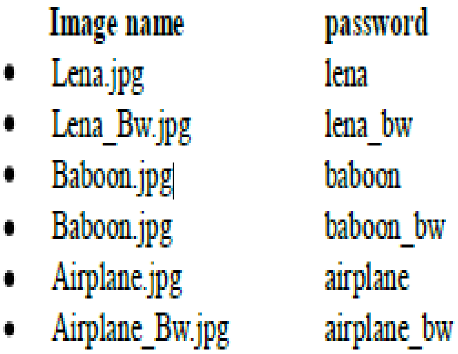
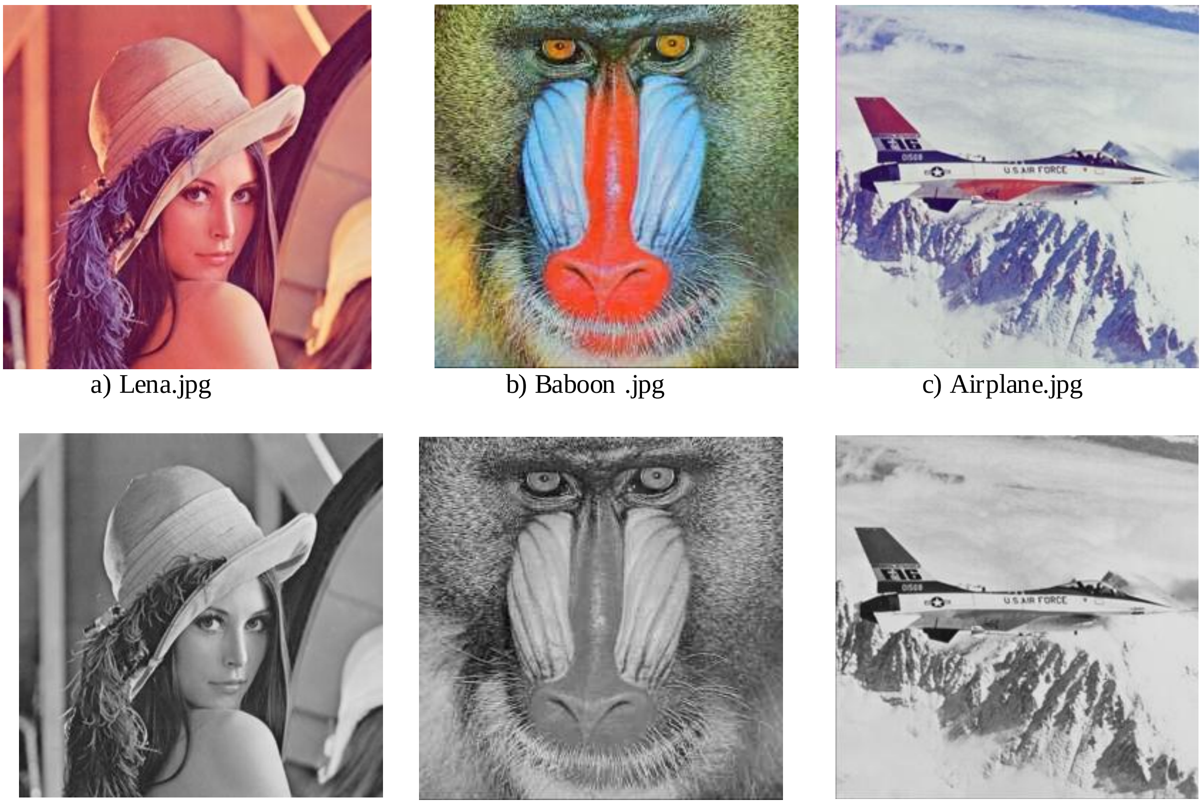


Image name	password
• Lena.jpg	lena
• Lena_Bw.jpg	lena_bw
• Baboon.jpg|	baboon
• Baboon.jpg	baboon_bw
• Airplane.jpg	airplane
• Airplane_Bw.jpg	airplane_bw

Both RGB and gray images are used for cover image. Color images have 256x256x3(196,608) bytes space while gray images have 256x256(65,536) bytes space for data embedding. Cover images are shown in figure 3.

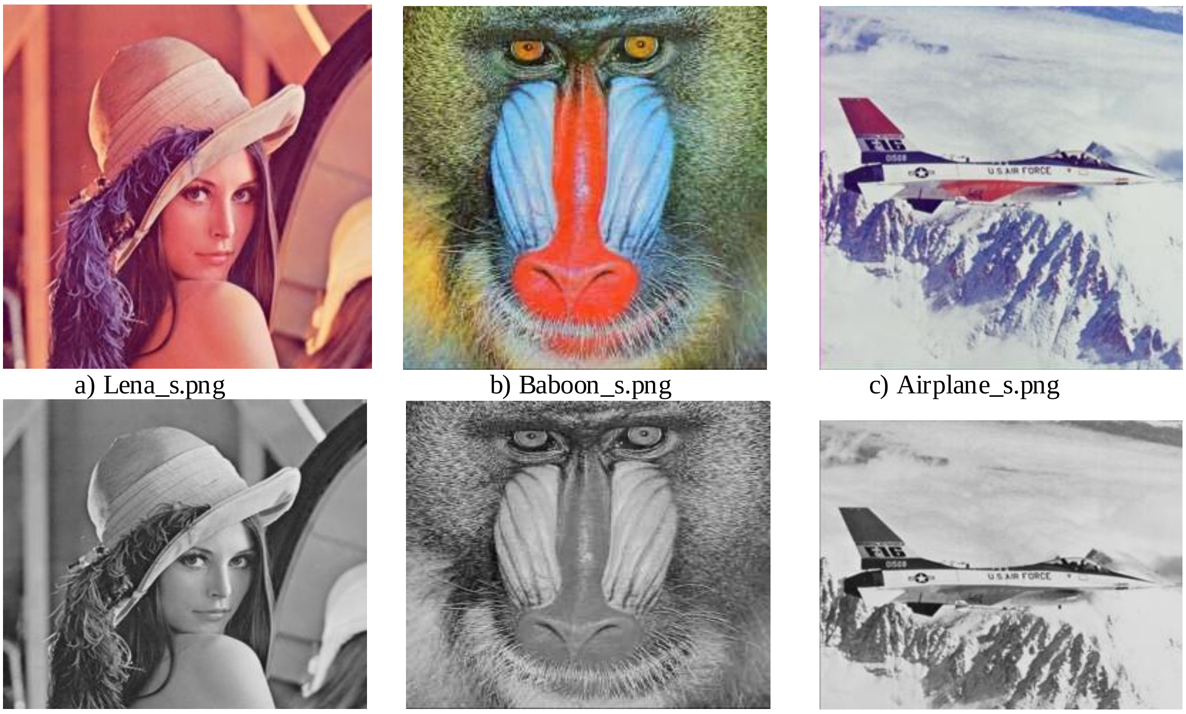


a) Lena.jpg b) Baboon .jpg c) Airplane.jpg

d) Lena_Bw.jpg e) Baboon_Bw.jpg f) Airplane_Bw.jpg

Figure 4: Original Cover images (256x256)

Stego image is obtained by adding message file to cover file. Password is used to encrypt the process. As jpg/jpeg is a compressed file format some data may get corrupt while writing stego file, so stego images are saved with PNG extension. If jpg files are to be used then while writing the file, lossless compression should be used. Stego images corresponding to cover images are as shown in fig. 5. They look similar and are imperceptible to human eyes.



a) Lena_s.png b) Baboon_s.png c) Airplane_s.png

d) Lena_Bw_s.png e) Baboon_Bw_s.png f)
Airplane_Bw_s.png

Fig. 5: Stego images

Images Recovered With Wrong Password When data is extracted from these stego file, it recovers
the message file as in Fig 3 only if correct password is provided. If secret key or password provided is wrong then it recovers some irrelevant images as shown in Fig. 6.

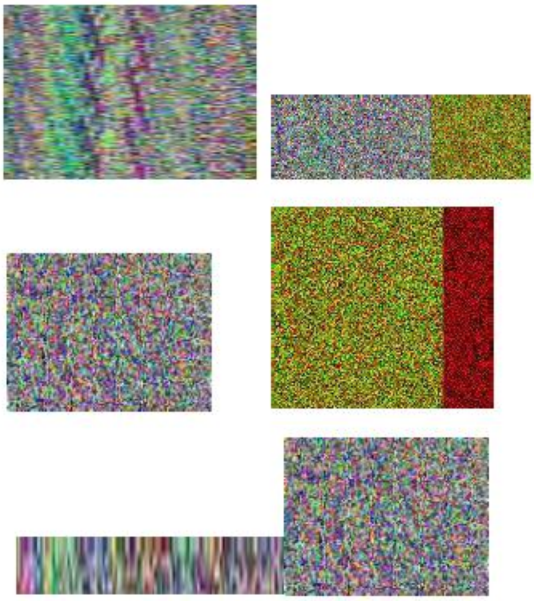


Fig. 6: Images recovered with wrong password

IV. COMPARISON RESULT

We can say by seeing results of above three methods that cover image and stego images look alike. We can‟t differentiate them on visual basis. But all of them are having some differences. So to distinguish there quality wrt cover image PSNR is used.

PSNR or peak signal to noise ratio is a measure to the image quality. It compares mean square error (MSE) of stego image with peak signal modification. MSE is the easiest way to calculate PSNR.MSE can be calculated as [2],

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as

$$PSNR = 10.\log_{10}\left({MAx_i^2}/_{MSE}\right)$$

Second important term required to compare these methods is payload capacity. Method that can achieve higher payload capacity is better. Third term is security. A more secured system is required to keep the data private. A trade off b/w these three terms is required while selecting a steganographic system.

Capacity and PSNR comparison for LSB [2], PVD [1] and proposed method has been shown in table 1.

Table 1

Cover image	LSB		PVD		Proposed method	
	capacity	PSNR (dB)	Capacity	PSNR (dB)	capacity	PSNR (dB)
Lena.jpg	196608	53.7618	262197	48.5099	391135	46.5925
Baboon.jpg	196608	53.7558	355040	44.6292	464904	44.8689
Airplane.jpg	196608	52.7869	274774	47.8387	407147	46.8673
Lena_Bw.jpg	65536	53.1003	87428	47.8027	133398	46.2598
Baboon_Bw.jpg	65536	53.9023	117394	44.1239	154286	43.5354
Airplane_Bw.jpg	65536	52.3844	93566	47.9023	138359	47.0590

V. CONCLUSION

In this paper we have compared capacity and PSNR of various color and gray images for different techniques of image steganography. The proposed method gives better results regarding security and capacity. It also avoids abrupt changes in the image during data embedding procedure. This method achieves higher
embedding capacity, imperceptibility than LSB steganography. Also with increase in capacity it gives much security than PVD method. The embedded confidential information can be obtained properly from the stego-image without the assistance of the host-image. So receiver doesn‟t need to have original cover image. It is very difficult for the unauthorized users to identify and recover the changes in stego image.

References

[1] Han-ling∗ZHANG , Guang-zhi GENG , Cai-qiong Xiong. (Nov 2009) "Image Steganography using Pixel-Value Differencing." Second International Symposium on Electronic Commerce and Security, 2009. 109-112

[2] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain. (Dec 2011), "A New Approach for LSB Based Image Steganography using Secret Key." 14th International Conference on Computer and Information Technology (ICCIT 2011).

[3] Chang, C.C.,Tseng, H.-W., A steganographic method for digitalimages using side match, Pattern Recognition Lett.25, 2004:1431-1437

[4] J. K. Mandal and Debashis Das. David C. Wyld, (2012) "Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow.": CCSEA, SEA, CLOUD, DKMP, CS & IT 05, IT-CSCP 2012. 93–102

[5] T Mrkel., JHP Eloff and MS Olivier, An Overview of Image Steganography, in Proceedings of the fifth annual Information Security South Africa Conference (2005)

[6] József LENTI. “Steganographic Methods.” PERIODICA Polytechnica SER. EL. ENG. VOL. 44, NO. 3–4, PP. 249–258 (2000)

[7] H.-C Wu, N.-I Wu, C.-S Tsai, M.-S Hwang. Image steganographic scheme based on pixel-value differencing and LSB replacement methods.IEE proc.-Vis. Image Signal Process, Vol.152, No.5, Oct 2005:611-615

[8] Adnan M.Alattar , Reversible Watermark using the Difference Expansion of a Generalized Integer Transform.IEEE Transactions on Image Processing, Aug.2004,13(8): 1147-1156

[9] Chan,C.K.,Cheng,L.M., Hiding data in images by simple LSB substitution, Pattern Recognition 37, 2004. 469-474

Ankita Sancheti received in December 2009 her B.E in Information Technology from University of Rajasthan. Currently she is an M.tech Student at the Faculty of Computer Science at the Mewar University, Chittorgarh, India. Her current research interest is focused on Image Steganography.