http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 11 (1): 9-19, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.9.19

Pixel Forefinger for Gray in Color: A Layer by Layer Stego

Siva Janakiraman, Rengarajan Amirtharajan, K. Thenmozhi and John Bosco Balaguru Rayappan
Department of Electronics and Communication Engineering,
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur-613401, India

Abstract: In the wake of cyber era, digital crime takes its shape in the schemes of modern warfare piercing existing security system without any collateral damage. The then existent cryptic army was either unable to stop the foes or had won a pyrrhic victory and thus evolved the war veteran, steganography that could withstand any destructive mechanism forced against it. Hence, in this study, three novel steganographic methods have been proposed to enhance the randomness of the mercurial data. All the three methods are implemented using the pixel indicator technology. Method one of the three uses the chosen pixel for guidance and as data channel for embedding. Method two takes a block of three pixels at a time where the first pixel acts as the steering channel while the remaining two become the data channel. Method three is further bifurcated; the first segment of this method involves the size definition within the first four pixels of the image and determination of that type of number i.e., even, prime or other. Depending on the type the channels red, blue or green are chosen as indicators, respectively. The second segment is where the size\value is checked for even parity and odd parity. Depending on its evenness or oddness the combination of data channel for embedding is arranged i.e., size is an even number with an odd parity red is the steering channel while the order of data channels are green and blue. The bifurcation and levels of selections increase the contingency of the embedment while retaining its reticence. Results confirm that the proposed methodology yield lesser error metrics while creating an efficacious channel to secure data transmission.

Key words: Data and indicator channel, information hiding, least significant substitution, pixel indicator technique, random image steganography

INTRODUCTION

Internet created a revolution in the cycle of life and has made the world a very small place with its thrilling speeds. As technology evolves, Man gets the information to his pocket on the GO. But acts of rivalry are affecting man greatly, even significantly in the case of technology. Data can be brought to the human beings pocket but wondering about the security, boggles the mind to square ONE. As a matter of fact, Man can't guarantee his own security then how could DATA! So the Data that reaches to our feet has a threat from intruders which the internet has failed drastically despite its up-gradations. Privacy of data is prioritized and a personnel or technology maintaining the privacy information is now on the deck today.

One such Upper Deck technology is Information Hiding/Steganography (Stefan and Fabin, 2000; Petitcolas *et al*., 1999; Rabah, 2004; Cheddad *et al*., 2010), where in all the needs of man are more than fulfilled with no intruders poaching on the data. The encrypted data by information hiding is secure, faster, accurate and zooming ahead into the people's lives, empowering them with unmatched speeds and latest generations.

Cryptography (Schneier, 2007) is the ancient art of writing messages by scrambling the secret data into meaningless junks and presenting them in a manner unrecognizable to eavesdroppers and not for cryptography participants. Steganography involves hiding the data to be transmitted in cover object which could be audio, video, image, text (Al-Frajat *et al*., 2010; Al-Azawi and Fadhil, 2010; Amirtharajan *et al*., 2010d; Bender *et al*., 1996, 2000; Hmood *et al*., 2010a; Shirali-Shahreza and Shirali-Shahreza, 2008) and sometimes may be the transmission itself is not noticeable to the eavesdroppers. How to combine Cryptography and Steganography effectively to offer better data security and their differences are detailed in (Zaidan *et al*., 2010) the dexterity with which data can be hidden by this technique is unparalleled and is the most efficacious one present.

In addition to the requirement of security, equally pressing demands of the steganography system are

Corresponding Author: Siva Janakiraman, Department of Electronics and Communication Engineering, SASTRA University, Thanjavur, India

imperceptibility and high data capacity known as payload (Cheddad *et al*., 2010; Hmood *et al*., 2010b). In general, a system is considered to be suitable for information hiding "when it satisfies the three requirements of information hiding magic triangle, i.e., imperceptibility, robustness and high capacity (Stefan and Fabin, 2000; Petitcolas *et al*., 1999; Rabah, 2004; Cheddad *et al*., 2010). The other side of steganography is called Steganalysis which is an art of revealing the presence of the hidden data (Fridrich *et al*., 2001; Wang and Wang, 2004; Qin *et al*., 2010). Furthermore, steganography can be classified into spatial domain and transform domain steganography.

In the spatial domain, data is hidden in the system by direct manipulation of the pixels, the most common technique being normal Least Significant Bit (LSB) substitution method through raster scan (Chan and Cheng, 2004; Thien and Lin, 2003; Wang *et al*., 2001; Zanganeh and Ibrahim, 2011) or random traversing path (Amirtharajan and Balaguru, 2009, 2010; Provos and Honeyman, 2003; Luo *et al*., 2008). In the transform domain technique, the image is first transformed using techniques like Discrete Cosine Transform (DCT) (Provos and Honeyman, 2003) or discrete wavelet transform (Thamkaiselvan *et al*., 2011) and then the coefficients are exploited for the purpose of data concealment.

Gutub *et al*. (2008) and Gutub (2010) pioneered the Pixel Indicator Technology (PIT) (Upreti *et al*., 2010) based on random color image steganography where the last two bits of the indicator plane would decide whether the remaining data channels are useful for embedment.

Amirtharajan *et al*. (2010a, b, c) have also proposed few variants using this technology. In all their aforementioned algorithms, the authors have used pixel indicator as a means to suitably find planes to embed the secret data, whose length is determined by excess 3 values of indicating pixel.

In another technique, from the same author pixel value differencing (Amirtharajan *et al*., 2010c; Park *et al*., 2005; Wu *et al*., 2005) decides the number of bits for embedment, along with pixel indicator. Another variant of the aforesaid method was employed by Amirtharajan *et al*. (2010a) where a new factor E is introduced which provides the user a flexibility to embed the secret data from a particular position in a pixel, thereby boosting the robustness of the system itself.

Padmaa *et al*. (2011) proposed a multiuser Pixel indicator method, where the 2nd number of users shares the same image to transfer the secret information in a single cover image. Kumar *et al*. (2011) proposed multiuser steganography in Orthogonal Frequency Division Multiplexing (OFDM) symbols which would be useful to embed additional information during high data rate transmission in the presence of Additive White Gaussian Noise (AWGN) channel. Furthermore Code Division Multiple Access (CDMA) based multiuser Steganographic embedding elucidate by Amirtharajan *et al*. (2011). In all the aforesaid multiuser stego methods there is a possibility of sharing a common cover object to transfer the secret.

In this study, three methods have been suggested with an aim of achieving high capacity, imperceptibility or both. These proposed methods are implemented in SCIlab for random Image steganography and the results are encouraging.

LSB substitution method revisited: The most well-known steganographic technique in the data hiding is Least Significant Bits (LSBs) substitution. This method embeds the fixed-length secret bits in the same fixed-length LSBs of pixels (Chan and Cheng, 2004; Thien and Lin, 2003).

Let C be the original cover object (Image) of M×N pixels and m be the secret data (message or image).

The stego object (Image) S could be computed as follows:

Embedding process
Stego (S)= cover – cover mod 2^k + secret data
Decoding Process
Data = stego mod 2^k
Example: if cover =160 data is 1111 decimal is 15
Then Steg = 160-160 mod 16+15 = 175
Data = 175 mod 16 = 15
Let cover = 150 data is 1111 decimal is 15
Steg = 150-150 mod 16+15 = 159
Data = 159 mod 16 = 150
160 binary is 10100000 data 15 binary 1111 simple substitution
will give 10101111 decimal is 175
Last four values are 1111.
150 binary is 10010110 data 15 binary 1111 simple substitution
will give 10011111 decimal 159
Last four values is 1111

Even though this LSB method is simple and easy to implement but it generally causes perceptible alteration in the stego Image, if the number of embedded bits for each pixel exceeds three. The other methods like adaptive LSB vary the number of embedded bits in each pixel. These methods possess better image quality in comparison with simple LSBs substitution with reduction in the embedding capacity or payload.

Optimum pixel adjustment procedure (OPAP): Chan and Cheng, (2004) elucidate Optimal Pixel Adjustment Procedure (OPAP) which reduces the deviation caused by

the LSB substitution method. In this process, the payload is embedded in a way such that the overall quality of the stego output is good and it would not affect the hidden data.

Procedure for data hiding through OPAP: Initially few least significant bits are embedded with the data.

Next step is to reduce the error, it would be carried out by properly adjusting all the remaining k+1th bits.

Let n be the number of LSB substituted in each pixel and d be the decimal equivalent of the pixel after embedding.

d_1 is the decimal value of last n bits of the pixel and d_2 be the decimal value of n bits hidden in that pixel. Then compute the following:

If $(d_1 \sim d_2) <= (2^k)/2$

Then no adjustment is made in the pixel.

Else, If $(d_1 < d_2)$
$d = d - 2^k$.

If $(d_1 > d_2)$
$d = d + 2_k$.

This adjustment would considerably reduce the error to 2^{k-1} instead of 2^k.

PIXEL INDICATOR TECHNIQUE

Pixel indicator technique, as the name implies uses the pixel value as an indicator to see whether a secret data bit is embedded or not in that pixel. As the pixel value determines the embedding process it is not sequential, thus nonlinear nature of embedding bits will improve security. In the gray scale the pixel value ranges from 0 to 255. The binary represented bits in locations specified will determine the bits to be embedded. PIT technique is followed in color image with great effect.

PIT considering same pixel as indicator and channel: This pixel indicator technique considers a single pixel of cover image as indicator and the secret information is embedded in that pixel itself. Many consideration could be possible for this pixel indicator technique, the methodology adapted in this PIT by considering the 3rd, 2nd bit of the pixel as indicator and 1st, 0th bit as channel for secret information hiding. The tabulation will depict the methodology. In this PIT methodology the maximum number of bits that could be embedded per pixel is two and the minimum is 0 bit per pixel.

Let Pi = b7 b6 b5 b4 b3 b2 b1 b0

Here, b3 and b2 acts as indicator pixels and b1 and b0 are the channels for secret messages.

The adapted methodology is given in Table 1 and the embedding and extraction flowchart is given in Fig. 1 and 2.

PIT considering three pixels as a block (Method 2): In PIT technique considering 3 pixels as a block, the entire image is divided into blocks of three pixels each. The first pixel value acts as indicator while the successive second and third pixel acts as channel for secret information to be hidden. The corresponding embedding and extraction flowchart are detailed in Fig. 3 and 4.

Let P_i, P_{i+1} and P_{i+2} forms a block of three pixel values. Let us name those bits of these 3 pixel in a block as follows:

- $P_i = b_{23}\ b_{22}\ b_{21}\ b_{20}\ b_{19}\ b_{18}\ b_{17}\ b_{16}$
- $P_{i+1} = b_{15}\ b_{14}\ b_{13}\ b_{12}\ b_{11}\ b_{10}\ b_9\ b_8$
- $P_{i+2} = b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0$

Here, in this PIT of gray image steganography, the b_{17} and b_{16} bits acts as indicator while the following bits b_{10}, b_9, b_8, b_2, b_1 and b_0 acts as a data channel. The adapted methodology is given in Table 2.

Hence, in this case of PIT with three pixels as a block the capacity of this proposed method increased considerably. The minimum number of bits embedded in that block is four and a maximum of six bits per block is achieved. This is comparatively higher than method 1 which considers one pixel at a time. As this case of PIT considers embedding of bits more than 1, there is a chance of applying OPAP in order to reduce the error metrics values.

Pit and channel selection criteria (Method 3): In this PIT technique, the indicator and channel selections

Table 1: Function of the proposed pixel indicator choices in gray cover object (method 1)

Indicator channel 3rd and 2nd bit	Channel 1 1st bit	Channel 2 0th bit
00	No hidden data	No hidden data
01	No hidden data	Embed single bit
10	Embed single bit	No hidden data
11	Embed single bit	Embed single bit

Table 2: Function of the proposed 3 pixel block embedding (method 2)

1st pixel of block as indicator (1st and 0th bit)	2nd pixel of block as channel	3rd pixel of block as channel
00	2bits embedding	2bits embedding
01	2bits embedding	3bits embedding
10	3bits embedding	2bits embedding
11	3bits embedding	3bits embedding

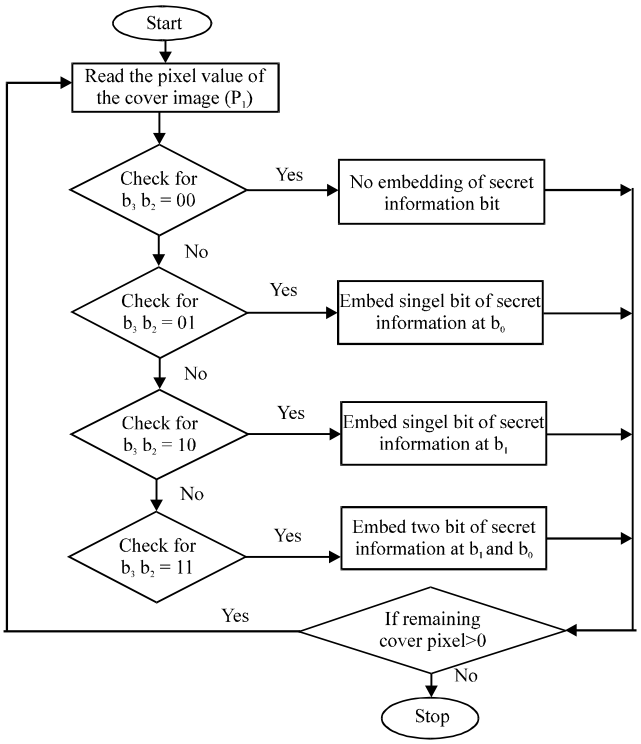


Fig. 1: Flow chart for Embedding (PIT considering same pixel as indicator and channel)

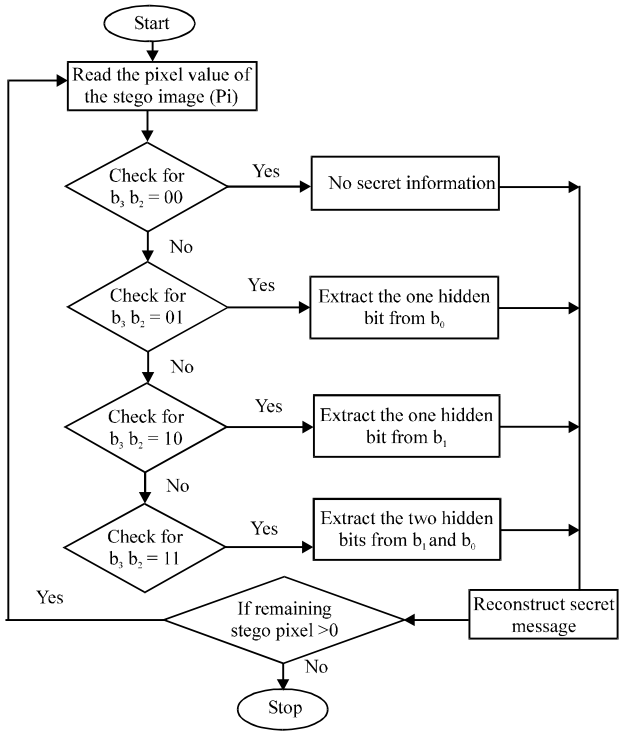


Fig. 2: Flow chart for Retrieval (PIT considering same pixel as indicator and channel)

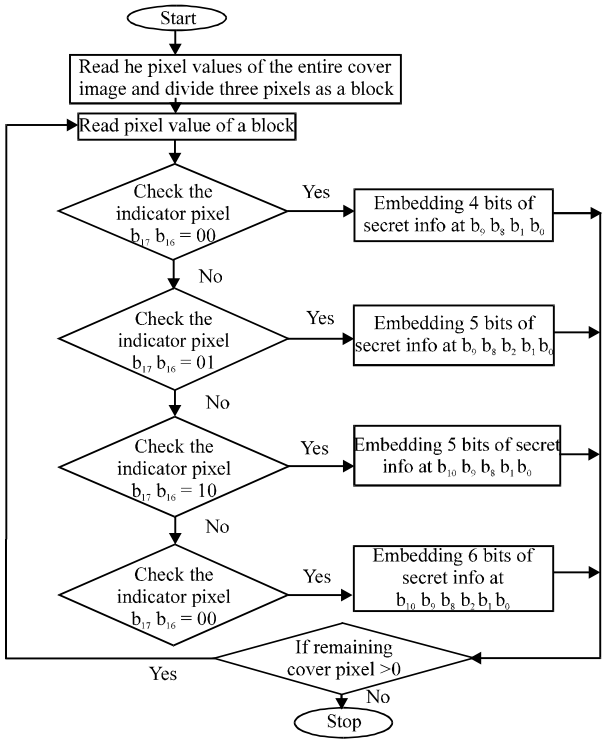


Fig. 3: Flowchart for embedding (PIT considering 3pixels as a block)

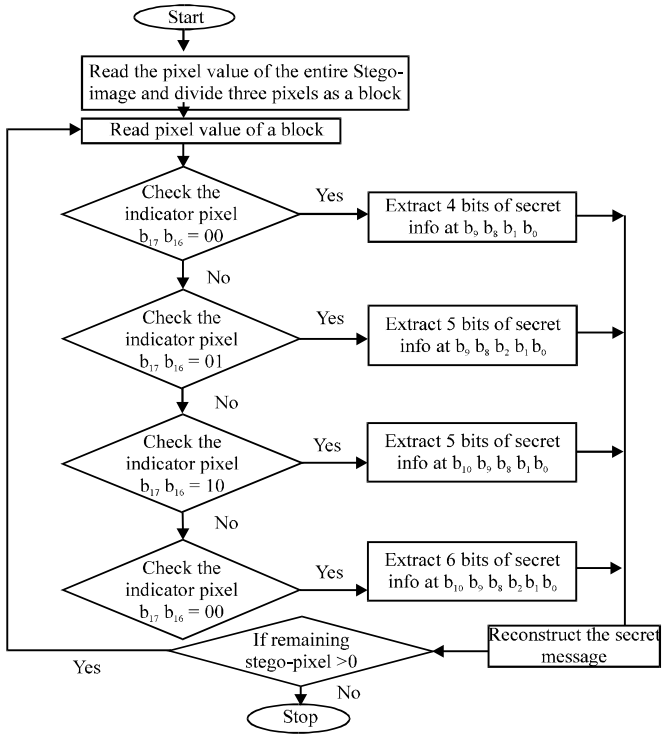


Fig. 4: Flowchart for retrieval (PIT considering 3pixels as a block)

are decided during the time of embedding. The secret information size or length decides the indicators and channels for itself. Thus the indicator and channels are not decided by the authorized person but by the nature of secret data. Hence, the idea about the channel and indicators is not given to anyone. As the secret information size decides the indicators and channels, this should also be hidden and not revealed to others. The hiding of the secret information size happens to be the LSB 2 bit insertion at the starting of the cover image pixel.

The length of the secret message is embedded in the 2 LSB bit positions of Green and Blue channels of first four pixels. In this present method, It is assumed that 16 bits space is enough to specify the size of the secret information. Then leaving those first four pixels, embedding the secret message is carried on the data channel based on the selected indicator's bit values. The adapted methodology is given in Table 3 and the work flow has been detailed in Fig. 5 and 6.

Thus, first level of selection considers the numerical nature of the length of secret information (N). Based on N to be even, prime or other, the indicator is selected from the three color combinations. The binary nature of the secret information decides the second level selection of channel order from the remaining pair.

The selection of indicator and channel alone varies here, while the embedding methodology remains the same as the first technique of PIT described earlier as of Table 1. If the indicator LSB bit value is one, then corresponding channel will carry 2 bits of secret information. Thus, in this case also, maximum of 4 bits per pixel and a minimum of 0 bit can be achieved. Capacity for this case is not increased but the security level is better compared to fixed indicator PIT.

RESULTS AND DISCUSSION

For all the three methods, Baboon or Parrot 256×256 pixel gray and color image has been taken as cover images and city top view of size 91×91, 117×117 and 129×129 pixels are considered as secret images. To evaluate the performance of the proposed system MSE, PSNR and BER have been computed for all the three methods.

Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE): The PSNR is calculated using the equation:

$$PSNR = 10\log_{10}\left(\frac{I_{max}^2}{MSE}\right)dB \quad (1)$$

where, I_{max} is the intensity value of each pixel which is equal to 255 for 8 bit gray scale images.

The MSE is calculated by using the Eq. 2 given below:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{i,j} - Y_{i,j}\right)^2 \quad (2)$$

where, M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image $X_{i,j}$ represents the pixels in the original cover image and $Y_{i,j}$ represents the pixels of the stego-image.

Bit Error Rate (BER) and bit error: BER evaluates the actual number of bit positions which are replaced in the stego image in comparison with cover image. It has to be computed to estimate exactly how many bits of the original cover image (Ic) are being affected by stego process. The BER for the Stego image (Is) is the percentage of bits that have errors relative to the total number of bits considered in Ic.

Let I_{cbin} and I_{sbin} are the binary representations of the cover image and stego cover then, the total number of bit errors:

$$T_e = \sum_{i=1}^{n}\left|I_{cbin} - I_{sbin}\right|$$

and the bit error rate:

$$\frac{T_e}{T_n}$$

T_n is the total number of bits considered for the gray image of size M×N pixels. T_n will be M×N×8.

Table 3: Functions of PIT and channel selection criteria (method 3)

		II level selection of channels for secret data embedding			
		Parity of secret data length (N)			
	I level	Odd parity		Even parity	
Length of secret data (N)	Selection of channel indicator	Ch1	Ch2	Ch1	Ch2
Even	Red	Green	Blue	Blue	Green
Prime	Blue	Red	Green	Green	Red
Else	Green	Red	Blue	Blue	Red

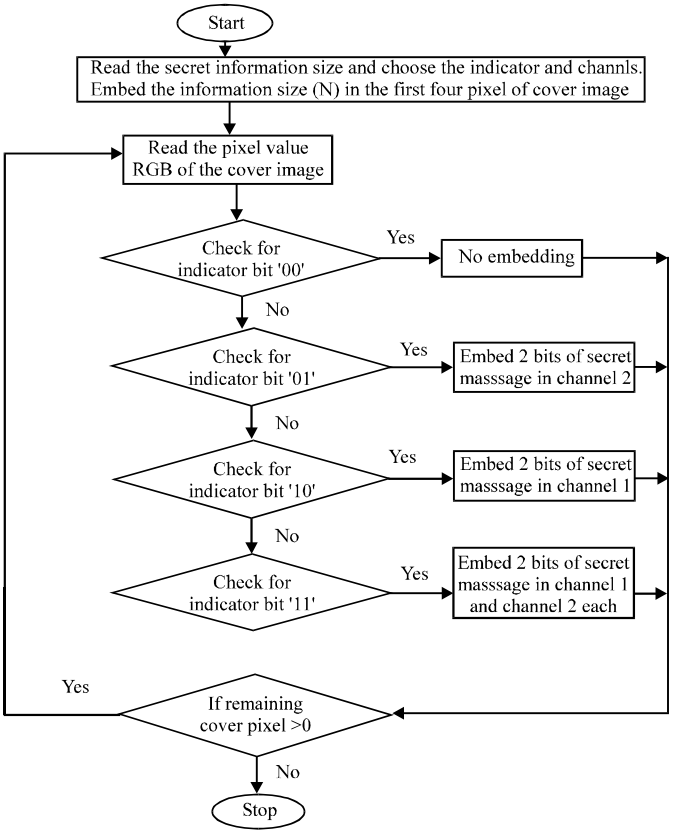


Fig. 5: Flowchart for embedding (PIT with indicator and channel selection criteria)

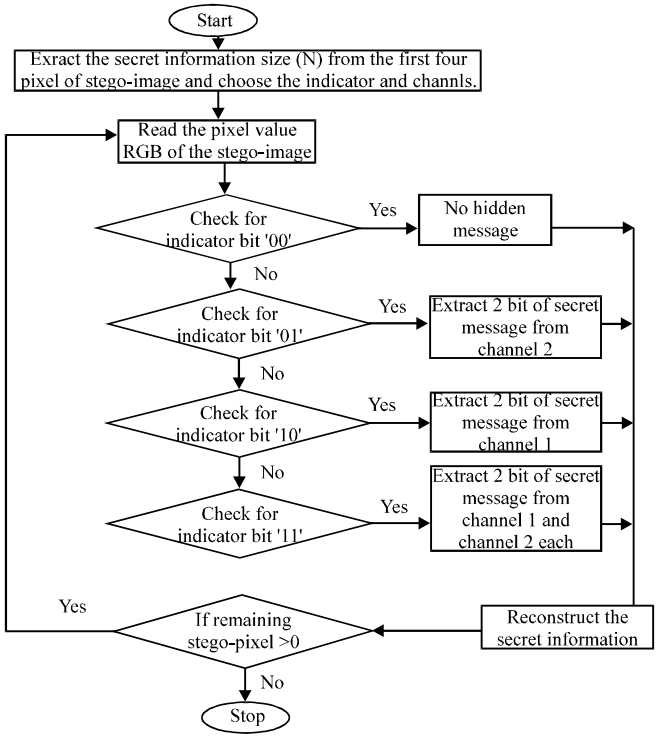
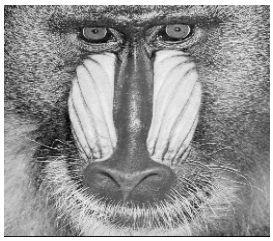


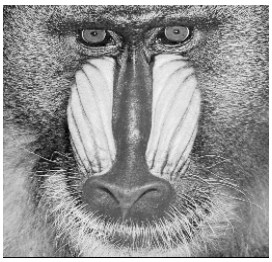
Fig. 6: Flowchart for retrieval (PIT with indicator and channel selection criteria)



Baboon_cover.png (256×256)

Secret (91×91)

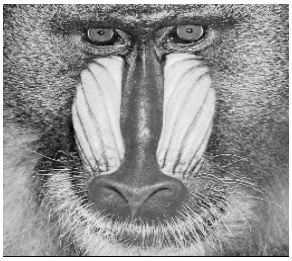
Fig. 7a: Baboon cover image and city secret Image



PIT 1_stego.png (256×256)

Extracted Secret(91×91)

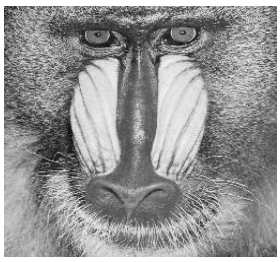
Fig. 7b: Baboon stego Image and recovered city secret Image



Baboon_cover.png (256×256)

Secret (117×117)

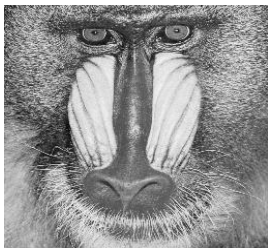
Fig. 8a: Baboon cover Image and city secret Image



PIT 3_stego.png (256×256)

Extracted secret (117×117)

Fig. 8b: Baboon Stego Image and Extracted city secret Image through simple LSB



PIT3_stego_opap.png (256×256)

Extracted Secret_ opap (117×117)

Fig. 8c: Baboon stego image with OPAP and extracted secret image through OPAP.

Table 4: Error metrics of the proposed method 1

Capacity	MSE	PSNR	BER
12.57%	1.2972	47.0009	0.0871

Table 5: Error metrics of the proposed method 2 with payload

Method	Capacity	MSE	PSNR	BER
Without OPAP	20.8%	4.7213	41.3902	0.1681
With OPAP	20.8%	2.3275	44.4618	0.1247

Method 1

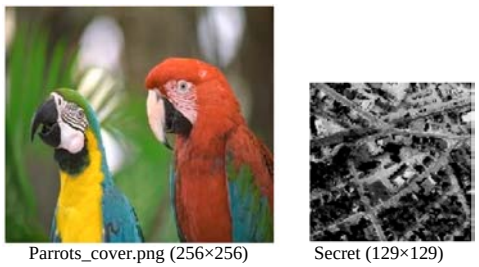
Results of PIT considering 1 pixel at a time: To evaluate the performance of the proposed method 1, Baboon cover image of size 256×256 pixels gray image and City secret gray image of size 91×91 pixels has been considered and the resultant stego image and extracted secret image are shown in Fig. 7a and b, respectively. The proposed method tested for full embedding capacity (Expected capacity is 12.5%, since k = 1 bit embedding) and the results are tabulated in Table 4. The obtained PSNR value is 47 dB with BER 0.087. It is also observed that there is slight improvement in the capacity with compromised reduction in PSNR due to random embedding.

Method 2

Results of PIT considering 3 pixels as a block: To evaluate the performance of the proposed method 2, Same Baboon cover image of size 256×256 pixels gray image and City secret gray image of size 91×91 pixels has been considered and the resultant stego image, modified stego image with OPAP and extracted secret image are shown in Fig. 8a-c, respectively. The proposed method tested for fully embedding capacity and the results are tabulated in Table 5. The obtained capacity is 20.8%, PSNR value is 41.3 dB without OPAP and there is a huge improvement in PSNR 44.46 dB.

Method 3

PIT with indicator and channel selection criteria: Parrots color cover image of size 256×256×3 pixels and secret gray

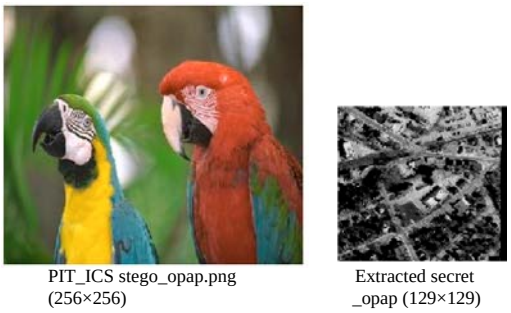


Parrots_cover.png (256×256) Secret (129×129)

Fig. 9a: Parrots cover image and secret image

PIT_ICS stego.png (256×256) Extracted secret (129×129)

Fig. 9b: Parrots stego image and extracted secret image through simple LSB



PIT_ICS stego_opap.png (256×256) Extracted secret _opap (129×129)

Fig. 9c: Parrot Stego Image with OPAP and Extracted Secret Image through OPAP

Table 6: Error metrics with and without OPAP

Method	Capacity	MSE	PSNR	BER
Without OPAP	8.26%	0.8720	48.7258	0.0531
With OPAP	8.26%	0.5043	51.1041	0.0415

image of size 129×129 pixels has been considered to evaluate the performance of the proposed method 3. Resultant stego image and extracted secret image along with cover are shown in Fig. 9 a and b, respectively. The proposed method tested for fully embedding capacity and the results are tabulated in Table 6. The obtained PSNR value is 48.72 dB with BER 0.057. It is also observed that there is a significant improvement in the PSNR with OPAP of 51.1 dB.

Security analysis:

- First the indicator can be selected in three ways (Prime, Even or Else)
- Then the channel is allotted in two ways (Odd or Even parity)
- The probability that two channels are selected is 2/3 (RG, GB, RB)
- Bits are embedded in a channel based on the indicator value
- The probability that at least two bits are embedded is 3/4 (00-no bits, 01, 10, 11-at least two bits)
- Then the embedding channel is selected in two ways
- So total complexity is 3*2*1/(2/3)*1/(3/4)*2=24
- If secret data scrambled with DES, the total complexity increases to $2^{64}\times24$

The MSE is around 0.5 and the corresponding PSNR is 51.1 dB for method 3, PSNR of 44.46 dB for method 2 and PSNR of 47 dB for method 1 which is comparable with Chan and Cheng (2004) and Amirtharajan *et al*. (2010 a- c). the other LSB based substitution are not considered (Amirtharajan and Balaguru, 2009, 2010) because they are uniform k bit embedding and their complexity are less in comparison with this proposed method. In Comparison with (Amirtharajan *et al*., 2010a, b, c) these methods has better complexity of $2^{64}\times24$

CONCLUSION AND FUTURE WORK

This study is for enhancing the information security using the hiding technique (Steganography). The degradation of the cover images with improvement in capacity is common almost in all techniques. But this variation is handled with great care such that it is not visually perceptible to human eye. This variation could be further reduced using OPAP methodology which was discussed and this benefit was utilized at most in all implemented techniques. These three techniques provides considerably better security were discussed and the two optimal techniques, one for gray scale and another for color image steganography was recommended based on several aspects of level of security, capacity and error metrics values.

The common limitation that was faced in these techniques was loss of hidden bits which could be recovered. The information security was mainly put forth as many data communication happens through Internet. In this global village of networks, there is a high possibility of cracking the sent information. If sent stego-

image got damaged during transmission or scrambling of the secret information by attackers will cause permanent loss of the secret information. Simple compression of the stego-image is also of no use, since the secret messages are hidden in the LSB positions of cover image. This compression will modify the LSB bits and once a stego-image is compressed then there is no chance of retrieval.

The future scope of this study lies in eliminating the limitation of loss of secret message in stego-image. This could be achieved by check methodologies like parity bit checking, Integrity checking of the secret message etc. For improving the security of each technique, cryptography could be combined with the steganography.

REFERENCES

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Amirtharajan, R. Rayappan and J.B. Balaguru, 2011. Covered CDMA multi-user writing on spatially divided image. Proceedings of the Wireless ViTAE Conference, Feb. 28-March 3, IEEE, Chennai, India, pp: 1-5.

Amirtharajan, R. and R.J.B. Balaguru, 2009. Tri-layer stego for enhanced security-a keyless random approach. Proceedings of the IEEE International Conference on Internet Multimedia Services Architecture and Applications, Dec. 9-11, Bangalore, India, pp: 1-6.

Amirtharajan, R. and R.J.B. Balaguru, 2010. Constructive role of SFC and RGB fusion versus destructive intrusion. Int. J. Comput. Appl., 1: 30-36.

Amirtharajan, R., D. Adharsh, V. Vignesh and J.B.B. Rayappan, 2010a. PVD blend with pixel indicator-OPAP composite for high fidelity steganography. Int. J. Comput. Appl., 7: 31-37.

Amirtharajan, R., G. Aishwarya, M. Rameshbabu and J.B.B. Rayappan, 2010b. Optimum pixel and bit location for colour image stego-a distortion resistant approach. Int. J. Comput. Appl., 10: 17-24.

Amirtharajan, R., S.K. Behera, M.A. Swarup, K.M. Ashfaaq and J.B.B. Rayappan, 2010c. Colour guided colour image steganography. Universal J. Comput. Sci. Eng. Technol., 1: 16-23.

Amirtharajan, R., K. Nathella and J. Harish, 2010d. Info hide: A cluster cover approach. Int. J. Comput. Applic., 3: 11-18.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.

Bender, W., W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb, 2000. Applications for data hiding. IBM Syst. J., 39: 547-568.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. J. Pattern Recognit. Soc., 37: 469-474.

Cheddad, A., J. Condell, K. Curran and P. McKevitt, 2010. Review: Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Fridrich, J., M. Goljan and R. Du, 2001. Detecting LSB steganography in color and gray-scale images. Multimedia IEEE, 8: 22-28.

Gutub, A., M. Ankeer, M. Abu-Ghalioun, A. Shaheen and A. Alvi, 2008. Pixel indicator high capacity technique for RGB image based steganography. Proceedings of the 5th IEEE International Workshop on Signal Processing and its Applications, March 18-20, Sharjah, UAE.

Gutub, A.A.A., 2010. Pixel indicator technique for RGB image steganography. J. Emerging Technol. Web Intell., 2: 56-64.

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010a. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, 2010b. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Kumar, P.P.P., R. Amirtharajan, K. Thenmozhi, Rayappan and J.B. Balaguru, 2011. Steg-OFDM blend for highly secure multi-user communication. Proceedings of the 2nd International Conference on Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Feb. 28-March 3, IEEE, Chennai, India, pp: 1-5.

Luo, G., X. Sun and L. Xiang, 2008. Multi-blogs steganographic algorithm based on directed hamiltonian path selection. Inform. Technol. J., 7: 450-457.

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on 2^n: 1 platform for users and embedding. Inform. Technol. J.,

Park, Y.R., H.H. Kang, S.U. Shin and K.R. Kwon, 2005. An image steganography using pixel characteristics. Comput. Intell. Secur., 3802: 581-588.

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.

Provos, N. and P. Honeyman, 2003. Hide and seek: An introduction to steganography. IEEE Secur. Privacy, 1: 32-44.

Qin, J., X. Xiang and M.X. Wang, 2010. A review on detection of LSB matching steganography. Inf. Technol. J., 9: 1725-1738.

Rabah, K., 2004. Steganography: The art of hiding data. Inform. Technol. J., 3: 245-269.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., Wiley, India.

Shirali-Shahreza, M. and S. Shirali-Shahreza, 2008. High capacity persian/arabic text steganography. J. Applied Sci., 8: 4173-4179.

Stefan, K. and A. Fabin, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, London, UK.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2011. Wave (let) decide choosy pixel embedding for stego. Proceedings of the International Conference on Computer, Communication and Electrical Technology, March 18-19, India, pp: 157-162.

Thien, C.C. and J.C. Lin, 2003. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modules function. Pattern Recog., 36: 2875-2881.

Upreti, K., K. Verma and A. Sahoo, 2010. Variable bits secure system for color images. Proceedings of the 2nd International Conference on Advances in Computing, Control and Telecommunication Technologies, Dec. 2-3, IEEE, Jakarta, India, pp: 105-107.

Wang, H. and S. Wang, 2004. Cyber warfare: Steganography vs. steganalysis. Commun. ACM, 47: 76-82.

Wang, R., C. Lin and J.C. Lin, 2001. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognit., 34: 671-683.

Wu, H.C., N.I. Wu, C.S. Tsai and M.S. Hwang, 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. Proc. IEEE Vision Image Signal, 152: 611-615.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zanganeh, O. and S. Ibrahim, 2011. Adaptive image steganography based on optimal embedding and robust against chi-square attack. Inform. Technol. J., 10: 1285-1294.