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 10 (10): 1896-1907, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.1896.1907

Stego on 2^n:1 Platform for Users and Embedding

[1]M. Padmaa, [1]Y. Venkataramani and [2]Rengarajan Amirtharajan
[1]Saranathan College of Engineering, India
[2]School of Electrical and Electronics, Engineering SASTRA University, India

Abstract: The study of communication security includes not just encryption but also traffic security, whose essence lies in "Information Hiding". The security of an image can be enhanced by cleverly embedding data without affecting its quality. This can be done by using information hiding techniques like steganography and cryptography. Combining steganography with cryptography becomes an essential facet for secure communication. In present study, enhanced image quality and security is obtained by consorting pixel indicator technique with PVD technique. Here, the raw data is first encrypted to get two different forms of message T1 and T2 using two distinct keys K1, K2 which is done by using encryption algorithms. As two encrypted messages can be embedded in this process, we have to first extract and then decrypt the message to retrieve the original data. The enhanced level of security is defined by the fact that even if one retrieves the message from the image it's still incomprehensible to get the original message without the two keys K1 and K2.

Key words: Information hiding, Pixel Value Differencing (PVD), Pixel Indicator (PI), steganography

INTRODUCTION

Being in the age of Electronics and Information Technology, majority of the information of large enterprises is maintained on machines in the form of digital data. This information is very sensitive and several mission-critical-applications depend upon this information (Stefan and Fabin, 2000). Any intruder who may get access to this information can not only leak the information but also tamper this information which can lead to malfunctioning of the mission-critical systems. This certainly can create havoc to the future of such organizations and nations. So, information security plays a vital role in today's info driven scenario (Amirtharajan and Balaguru, 2009).

Petitcolas *et al.* (1999), Rabah (2004) and Cheddad *et al.* (2010) elucidated steganography is a method of hiding data into another cover media in such a way that only the receiver knows the presence of secret data in the cover and retrieve it. Schneier (2007) explained various encryption methods for data security whereas steganography is a very secure method, because the intruder has no idea of presence of a secret data (Stefan and Fabin, 2000; Zaidan *et al.*, 2010). Bender *et al.* (1996) discussed various techniques of data hiding, where some of the methods have been used from long past included usage of wax to cover data engraved on wooden pieces and also use of invisible inks (Petitcolas *et al.*, 1999). So many authors highlights that (Amirtharajan *et al.*, 2010b; Hmood *et al.*, 2010a, b; Cheddad *et al.*, 2010) rather than robustness, steganography concentrates more on the payload i.e., the amount of data to be embedded. Another important aspect of steganography is the imperceptibility (Aura, 1996; Wang *et al.*, 2001; Chan and Cheng, 2004; Zanganeh and Ibrahim, 2011), i.e., the stego cover has to maintain its original quality even after the secret data is embedded into it (Bender *et al.*, 1996, 2000; Amirtharajan and Balaguru, 2009, 2010).

Though very secure, there are analytical techniques by which the presence of secret data can be found out using statistical difference between the cover and stego objects. To fight against this type of analysis (Fridrich *et al.*, 2001; Wang and Wang, 2004; Qin *et al.*, 2010), two things should be kept in mind. First, while embedding the data into the cover, avoid conspicuous parts. Secondly, the embedding efficiency has to be improved.

The image based steganography (Hmood *et al.*, 2010a; Cheddad *et al.*, 2010; Amirtharajan and Balaguru, 2009, 2010; Amirtharajan *et al.*, 2010a-c) requires an image as the media to embed the secret data into. The secret data can be embedded by modifying or changing the pixel values or by changing the intensity value of the pixel. Least Significant bits LSB (Cheddad *et al.*, 2010; Amirtharajan and Balaguru, 2009, 2010; Amirtharajan *et al.*, 2010a-c), Pixel Indicator (Gutub *et al.*, 2008; Gutub, 2010; Parvez and Gutub, 2008; Upreti *et al.*, 2010; Amirtharajan and Balaguru, 2010; Amirtharajan *et al.*, 2010a-c) and Pixel Image intensity

Corresponding Author: M. Padmaa, Saranathan College of Engineering, India

variation (Park *et al*., 2005) based are few techniques for image steganography.

The most well-known Steganographic technique in the data hiding field is least-significant-bits (LSBs) substitution (Cheddad *et al*., 2010; Amirtharajan and Balaguru, 2009, 2010; Amirtharajan *et al*., 2010a-c). This method embeds the fixed-length (maximum of 3) secret bits in the same fixed-length LSBs of pixels but it generally causes noticeable distortion(if it is more than 3). Several adaptive methods for steganography have been proposed to reduce the distortion caused by LSBs substitution (Zanganeh and Ibrahim, 2011). Chan and Cheng (2004) proposed one such method to reduce distortion called Optimal Pixel Adjustment Process [OPAP]. On the other hand the adaptive methods vary the number of embedded bits in each pixel and they possess better image quality than other methods. However, this is achieved at the cost of reduction in the embedding capacity.

A state-of-the-art survey on current digital image steganography, steganalysis methods along with some common standards and guidelines drawn from the literature are available in Cheddad *et al*. (2010). It also classifies steganography based on covers like video (Al-Frajat *et al*., 2010; Amirtharajan *et al*., 2010d), audio (Amirtharajan *et al*., 2010d), text (Shirali-Shahreza and Shirali-Shahreza, 2008; Al-Azawi and Fadhil, 2010) and image whereas another classification is based on the modification on the covers.

Gutub *et al*. (2008) and Gutub (2010) proposed Pixel Indicator based color image steganography, where in the last two bit of the indicator plane decides, the remaining planes are data channel or not. Amirtharajan *et al*. (2010a-c) exploited Pixel indicator method by several variations. In all the proposed, the authors have taken Pixel Indicator as a base to identify suitable plane of a pixel for embedding, later how many bits are used to embed would be decided by Excess 3 value of the indicator values (Amirtharajan *et al*., 2010b). In another variation from the same author (Amirtharajan *et al*., 2010c) pixel value differencing (Park *et al*., 2005; Wu *et al*., 2005) decides the number of bits along with pixel indicator. Furthermore one more Pixel indicator method has been considered by Amirtharajan *et al*. (2010a) where in the authors proposed a method to increase the robustness by introducing a factor E as an option to select the bit position in a pixel to plant the message to be concealed.

Another classification in image steganography is methods using raster scan Chan and Cheng (2004) or random scan (Amirtharajan and Balaguru, 2009, 2010; Padmaa and Venkataramani, 2010; Provos and Honeyman, 2003; Luo *et al*., 2008). The former visits the entire pixel like regular TV scanned lines from left to right, top to bottom where the later by traversing all the pixels by pseudo random path. Aura (1996) proposed a random image steganography. Its drawback is huge time in computing the suitable target pixel for embedding. Amirtharajan and Balaguru (2009, 2010) proposed two such random traversing paths, offering random traversing LSB embedding method but fails to improve its randomness while embedding. There are papers available in literature for multiuser secret sharing using visual cryptography proposed by Naor and Shamir (1994) but it's not hiding the aspect of sharing the cryptographic share among users. No authors in the recent past have reported multi user secret sharing using pixel indictor methods.

Hence, in present study, an optimistic maiden effort has been taken to propose a method which improves the randomness while embedding, by adapting pixel indicator method for multi user and encryption prior to embedding. This makes the hacker to think more to device a method to crack the system. Later after embedding OPAP module has been put upon to improve the quality of the stego cover.

PROPOSED METHODOLOGY

In steganography, according to the Magic triangle, robustness, security and capacity are the three characteristics which are of prime importance (Stefan and Fabin, 2000). For an ideal steganographic algorithm, all the three characteristics altogether can never be satisfied. Until now, only one user could use steganographic conditions in a channel. Whereas, this study explores the possibility of having "Two Users" using this technique, where two different keys would be given to each user after symmetric encryption through DES. To improve the level of security a steganographic method "Pixel Indicator Technique" is included along with a blend of cryptography. The research done on "Two Users" can further optimize the data capacity, compared to a single user in the earlier techniques in steganography.
This methodology enables us to achieve the following:

- Flexibility of using two users in the same channel
- To increase the information hiding capacity
- To achieve high security by implementing different encryption algorithm
- To achieve randomization
- To increase the robustness of the cover image

The procedure applied here involves raw secret data from two distinct users. In the Encryption process, the

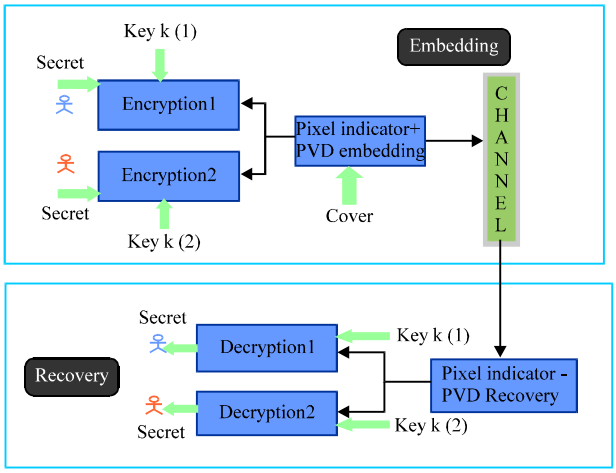

Fig. 1: Block diagram of the proposed methodology

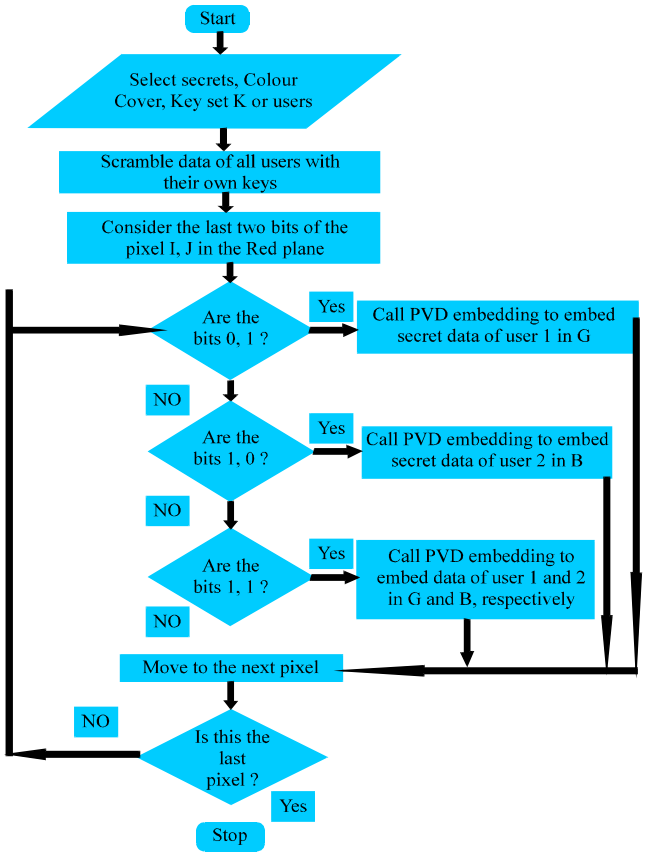

Fig. 2: Flowcharts for embedding

data T1 and T2 is encrypted using two distinct keys K1 and K2 known by the individual users, respectively using (Schneier, 2007) Symmetric Data Encryption Standard (DES) the block diagram representation of the proposed method is shown in Fig. 1 and Flowchart for Embedding and Extraction in Fig. 2 and 3. The encoded data D1 and D2 is enclosed inside a cover image using Pixel indicator method. a color image comprises of pixels having three 8

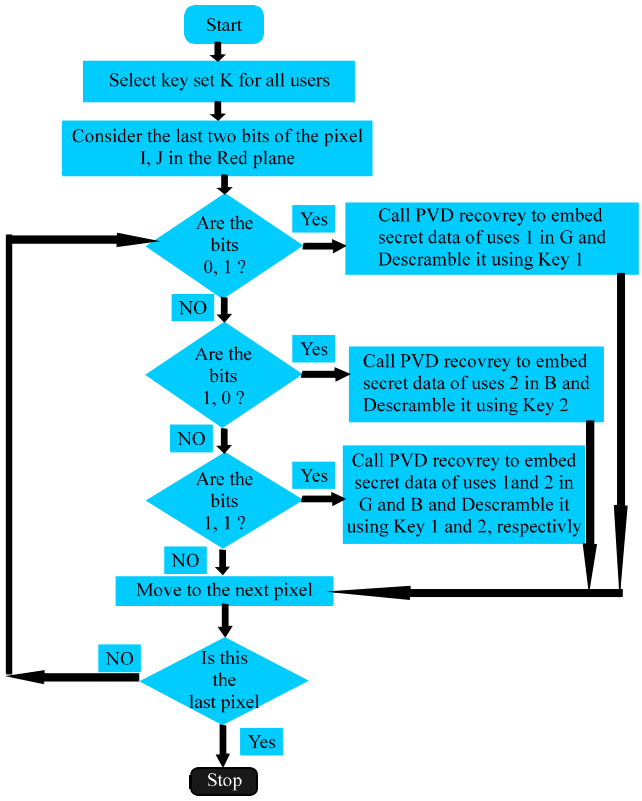

Fig. 3: Flowcharts for extraction

Table 1: Function of the proposed two user pixel indicator method

Indicator channel	Data channel I	Data channel II
00	No Hidden Data	No Hidden Data
01	No Hidden Data	User I Data
10	User II Data	No Hidden Data
11	User I Data	User II Data

bit channels RED, GREEN, BLUE in each pixel. In pixel indicator method, one of the three channels is selected as an indicator channel, whereas the remaining two channels are used to embed the encoded data. Depending on the last two bits of the indicator channel data to be embedded in the other two channels is conferred. In this scenario, there are four possibilities to be considered are shown in Table 1. If the last two bits,

- 00-None of the channels are used for embedding
- 01-K bit embedding of D1 derived from PVD (user 1) is done in BLUE channel
- 10-K bit embedding of D2 derived from PVD (user 2) is done in GREEN channel
- 11-K bit embedding of D2 and D1 derived from PVD is done in both GREEN and BLUE channels simultaneously

The randomization is increased by using Pixel value differencing technique (Park *et al*., 2005) as the method itself decides as to how many bits are to be embedded in the respective channels. Also, the imperceptibility and robustness of the system can be achieved here by hiding the secret data with more randomization.

During retrieving, the data should be first extracted from the channel i.e., the image and then original data is decrypted by using the same algorithm which is used during the encryption. This retrieving process can be done only if the individual opponents know their respective keys k1 and k2 and hence it makes the process more secure are as shown in the Fig. 1. As mentioned above the security of the process is enhanced since the user has to extract and then decrypt the message to get the required data.

Mathematical model for 2 user, pixel indicator: Two flavors of secret data:

- Secret data of User 1 (m 1)
- Secret data of User 2 (m 2)

3 Planes:

Cover image is split into 3 planes R, G and B.
Message data (secret) to be embedded
Variable k bit length for each pixel derived from PVD
k = log2D where D =Max (neighbors) - Min (neighbors)
mu (I, j) , where I = row identifier
j = Pixel inside a row
where 1<=u<=2

Embedding procedure: Let the cover image be C with Mc×Nc pixels.

Let 'k' be the number of LSBs derived from PVD to be replaced in cover pixels.

Let each secret message be a matrix Mu, where each element of Mu is made up of k bits. Then we can denote the message to be embedded in the ith row, jth pixel as mu (I, j).

Let the stego image also be split into 3 planes Rs, Gs and Bs corresponding to R, G and B planes of cover image.

Let the indicator I (I, j) be defined for each pixel as the last two bits of R (I, j),

I (I, j) = R (I, j) mod 4

Stego image's planes can be denoted as:

- Rs (I, j) = R (I, j) for all I and j
- Gs (I, j) = G (I, j)-G (I, j) mod2k+ m1 (I, j), if I(I, j) = 1 or I (I, j) = 3
- G (I, j) , if I (I, j) = 0 or 2
- Bs (I, j) = B (I, j)-B (I, j) mod2k+ m2 (I, j), if I (I, j) = 2 or I (I, j) = 3
- B (I, j) , if I (I, j) = 0 or 1

Retrieval procedure: Let the indicator I (I, j) be defined for each pixel as the last two bits of Rs (I, j),

I(i,j) = R(i,j) mod 4

The messages mu (I, j) can be extracted from pixels in stego image as:

- m1 (I, j) = Gs (I, j) mod 2k , where I (I, j) = 1 or 3
- m2 (I, j) = Bs (I, j) mod 2k , where I (I, j) = 2 or 3

THE PROPOSED METHOD ALGORITHMS

Case-1: Two users PVD with Tri-Colour random image steganography

Embedding Algorithm method 1:

- **Inputs:** Secret Data (D), Cover Image (C), Key Set (K) for 2 users.
- **Output:** Stego image (S) with secret data embedded in it.

1 Convert the Secret Data (D) into binary format
2 Split the cover image C into Red, Green and Blue Planes.(R, G and B respectively)
3 For each pixel in R, do the following
  3.1 Let b[0] = LSB of the current pixel in R
  3.2 Let b[1] = Next LSB of the current pixel in R
  3.3 If b = 00 then
Go to next pixel.
  Else if b = 01 then
    Scramble data of User 1 with Key K [1].
    Call PVD Embedding to embed secret data of User 1 in current pixel of G.
  Else if b=10 then
    Scramble data of User 2 with Key K[2].
    Call PVD Embedding to embed secret data of User 2 in current pixel of B.
Else
  Scramble data of User 1 and 2 using Keys K[1] and K[2], respectively.
  Call PVD Embedding to embed secret data of Users 1 and 2 in current pixel of G and B, respectively.
3.4. If all secret data is embedded, then
Go to 4 step
4 Store the resulting image as Stego Image (S) after applying OPAP.

Recovery algorithm method 1:

- **Input:** Stego Image (S), Key Set K for 2 users
- **Output:** Secret Data (D)

1 Split the stego image S into Red, Green and Blue Planes. (R, G and B, respectively)
2 For each pixel in R, do the following:
  2.1 Let b[0] = LSB of the current pixel in R
  2.2 Let b[1] = Next LSB of the current pixel in R
  2.3 If b = 00 then
Go to next pixel.
  Else if b=01 then
Call PVD Recovery to recover secret data of User 1 from current pixel of G.
  De-Scramble data of User 1 with Key K [1].
  Else if b = 10 then
  Call PVD Recovery to recover secret data of User 2 from current pixel of B.
  De-Scramble data of User 2 with Key K [2].
  Else
  Call PVD Recovery to recovery secret data of Users 1 and 2 from current pixel of both
  G and B.
  De-Scramble data of Users 1 and 2 with Keys K [1] and K [2], respectively.
3 Store the resulting recovered data as Secret Data (D)

Case-2: Two user PVD with Custom-indicator-plane Tri-colour random image steganography

Embedding Algorithm method 2:

- **Inputs:** Secret Data (D), Cover Image (C), Indicator-plane IndeI), Key Set K for 2 users.
- **Output:** Stego image (S) with secret data embedded in it.

1 Convert the Secret Data (D) into binary format.
2 Split the cover image C into Red, Green and Blue Planes.(R,G and B respectively)
3 If I = 1 then,
  P [1] = R, P [2] = G, P [3] = B
  Else if I = 2, then
  P [1] = G, P [2] = R, P [3] = B
  Else if I = 3, then
  P [1] = B, P [2]=R, P [3] = G

4 For each pixel in P[1], do the following:
4.1 Let b [0] = LSB of the current pixel in P [1]
4.2 Let b [1] = Next LSB of the current pixel in P [1]
4.3 If b = 00 then
Go to next pixel.
Else if b = 01 then
Scramble data of User 1 with Key K [1].
Call PVD Embedding to embed secret data of User 1 in current pixel of P [2].
Else if b = 10 then
Scramble data of User 2 with Key K [2].
Call PVD Embedding to embed secret data of User 2 in current pixel of P[3].
Else
Scramble data of Users 1 and 2 using Keys K [1] and K [2], respectively.
Call PVD Embedding to embed secret data of Users 1 and 2 in current pixel of P[2] and P [3], respectively.
4.4 If all secret data is embedded, then
Go to next step-5
5 Store the resulting image as Stego Image (S) after applying OPAP.

Recovery algorithm method 2:

- **Input:** Stego Image (S), Indicator-plane index (I), Key Set K for 2 users.
- **Output:** Secret Data (D)

1 Split the stego image S into Red, Green and Blue Planes. (R, G and B, respectively)
2 If I = 1 then,
P[1] = R, P [2] = G, P [3] = B
Else if I = 2, then
P [1] = G, P [2] = R, P [3] = B
Else if I = 3, then
P [1] = B, P [2] = R, P [3] = G
3 For each pixel in P [1], do the following:
3.1 Let b [0] = LSB of the current pixel in P [1]
3.2 Let b [1] = Next LSB of the current pixel in P [1]
3.3 If b = 00 then
Go to next pixel.
Else if b=01 then
Call PVD Recovery to recover secret data of User 1 from current pixel of P [2].
De-Scramble data of User 1 with Key K [1].
Else if b = 10 then
Call PVD Recovery to recover secret data of User 2 from current pixel of P [3].
De-Scramble data of User 2 with Key K [2].
Else
Call PVD Recovery to recovery secret data of Users 1 and 2 from current pixel of both P [2] and P [3].
De-Scramble data of Users 1 and 2 with Keys K [1] and K [2], respectively.
4 Store the resulting data as Secret Data (D).

Case-3: Two user PVD with Cyclic-indicator-plane Tri-colour random image steganography

Embedding Algorithm method 3:

- **Inputs:** Secret Data (D), Cover Image (C), Key set K for 2 users.
- **Output:** Stego image (S) with secret data embedded in it.

1 Convert the Secret Data (D) into binary format
2 Split the cover image C into Red, Green and Blue Planes. (R, G and B, respectively)
3 Let index I = 1.
4 For each pixel in P[1], do the following:
4.1 If (I mod 3) =1 then,
I [I] = 1
Else if (I mod 3) = 2 then,
I [I] = 2
Else
I [I] = 3
4.2 Set I=I+1
5 For each pixel in P [1], do the following:
5.1 If I [j] = 1 then,
P [1] = R [I], P [2] = G [I], P [3] = B [I]
Else if I [j] = 2, then
P [1] = G [I], P [2] = R [I], P [3] = B [I]
Else if I [j] = 3, then
P[1]=B[i], P[2]=R[i], P[3]=G[i]
5.2 Let b [0] = LSB of P [1]
5.3 Let b [1] = Next LSB of P [1]
5.4 If b = 00 then
Go to next pixel.
Else if b = 01 then
Scramble data of User 1 with Key K [1].
Call PVD Embedding to embed secret data of User 1 in current pixel of P [2].
Else if b = 10 then
Scramble data of User 2 with Key K[2].
Call PVD Embedding to embed secret data of User 2 in current pixel of P [3].
Else
Scramble data of User 1 and 2 using Keys K [1] and K [2], respectively.
Call PVD Embedding to embed secret data of Users 1 and 2 in current pixel of P [2] and P [3], respectively.
5.5 If all secret data is embedded, then
Go to next step
Else
j = j+1
6 Store the resulting image as Stego Image (S) after applying OPAP.

Recovery Algorithm method 3:

- **Input:** Stego Image (S), Key set K for 2 users.
- **Output:** Secret Data (D)

1 Split the stego image S into Red, Green and Blue Planes. (R, G and B, respectively)
2 Let index I = 1
3 Let index j = 0
4 For each pixel in P [1], do the following:
4.1 If (I mod 3) =1 then,
I[i]=1
Else if (I mod 3)=2 then,
I[i]=2
Else
I[i]=3
4.2 Set I=I+1
5 For each pixel in P[1], do the following:
5.1 If I [j] = 1 then,
P [1] = R [I], P [2] =G [I], P [3] = B [I]
Else if I [j] = 2, then
P [1] = G [I], P [2] = R [I], P [3] = B [I]
Else if I [j] = 3, then
P [1] = B [I], P [2] = R [I], P [3] = G [I]
5.2 Let b [0] = LSB of P [1]
5.3 Let b [1] = Next LSB of P [1]

5.4 If b = 00 then
Go to next pixel.
Else if b = 01 then
Call PVD Recovery to recover secret data of User 1 from current pixel of P [2].
De-Scramble data of User 1 with Key K [1].
Else if b = 10 then
Call PVD Recovery to recover secret data of User 2 from current pixel of P [3].
De-Scramble data of User 2 with Key K [2].
Else
Call PVD Recovery to recovery secret data of Users 1 and 2 from current pixel of both P [2] and P [3].
De-Scramble data of Users 1 and 2 with Keys K [1] and K [2], respectively.

6 Store the resulting data as Secret Data (D)

RESULTS AND DISCUSSION

In this present implementation, Lena, Baboon, Gandhi and Big Temple Tanjore 256×256×3 color digital images have been taken as cover images, as shown in Fig. 4. The effectiveness of the stego process proposed has been studied by calculating MSE and PSNR for all the three methodologies, for all the three RGB planes and for all the four cover images. They are tabulated in Table 2, 3 and 4.

The PSNR is calculated using the equation;

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

where, Imax 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 Xi, j represents the pixels in the original image and Yi, j, represents the pixels of the stego-image.

The proposed methodology offers no clue to the intruders, because the secret message is evenly distributed in the entire channel and significantly improves the hiding capacity. If any one of the color plane had been considered as an indicator channel then characteristics of indicator channel would always be the same with the cover statistics therefore, may give a clue to the intruders.

In method 1 Red channel is selected as default indicator, then the Green is data channel 1 and the Blue is the data channel 2 i.e., the sequence is RGB. The following are observed from Table 2, there is no deviation in RED channel (MSE = 0, hence PSNR 8) value. It may be a clue to the intruders but the remaining data channel PSNR values are well above 40 dB so there is no visual degradation in stego covers. The best suitable cover for high embedding capacity is baboon (241375 bits with PSNR 40.062 dB). The corresponding stego cover results are given in Fig. 5

The stego cover results are given in Fig. 6. In method 2 the indicators are selected based on user choice: Assume Green is selected, then the Blue is channel 1 and the Red is the channel 2 i.e., the sequence is GBR. Table 3 depicts the similar trend of method 1. In this present experimental simulation, the chosen indicator is GREEN channel so the MSE = 0 and PSNR 8. The remaining two data channel PSNR value is higher than 40 dB but it has similar problem like method 1 giving a clue for the sneakers.

Table 2: Estimation parameters of the proposed embedding method I

	Channel I Red		Channel II Green		Channel III Blue		BPP(Bits Per Pixel)			
Cover image	MSE	PSNR	MSE	PSNR	MSE	PSNR	R	G	B	Maximum embedding capacity
Lena	0	∞	2.020	45.077	1.5869	46.125	0	1.102	1.0436	140607
Baboon	0	∞	6.273	40.156	6.4106	40.062	0	1.8325	1.8506	241375
Temple	0	∞	2.671	43.864	2.5092	44.136	0	1.173	1.1702	153584
Gandhi	0	∞	1.980	45.165	1.9007	45.342	0	1.03	1.0445	135943

Table 3: Estimation parameters of the proposed embedding method 2

	Channel I Red		Channel II Green		Channel III Blue		BPP(Bits Per Pixel)			
Cover image	MSE	PSNR	MSE	PSNR	MSE	PSNR	R	G	B	Maximum embedding capacity
Lena	1.942	45.2483	0	∞	1.5847	46.1313	1.063	0	1.0426	137997
Baboon	5.9813	40.3628	0	∞	6.5108	39.9945	1.8203	0	1.8517	240647
Temple	2.7779	43.6937	0	∞	2.5378	44.0862	1.1998	0	1.1757	155681
Gandhi	1.9835	45.2561	0	∞	1.8273	45.5126	1.0091	0	1.0114	132412

Table 4: Estimation parameters of the proposed embedding method 3

Cover image	Channel I Red MSE	Channel I Red PSNR	Channel II Green MSE	Channel II Green PSNR	Channel III Blue MSE	Channel III Blue PSNR	BPP(Bits Per Pixel) R	BPP(Bits Per Pixel) G	BPP(Bits Per Pixel) B	Maximum embedding capacity
Lena	1.227	47.24	1.3641	46.782	1.02	48.045	0.702	0.724	0.688	138549
Baboon	4.065	42.04	4.002	42.108	4.2847	41.812	1.212	1.211	1.228	239262
Gandhi	1.348	46.83	1.2901	47.025	1.2478	47.169	0.670	0.681	0.6776	132945
Temple	1.853	45.45	1.766	45.662	1.632	46.003	0.801	0.771	0.7798	154409

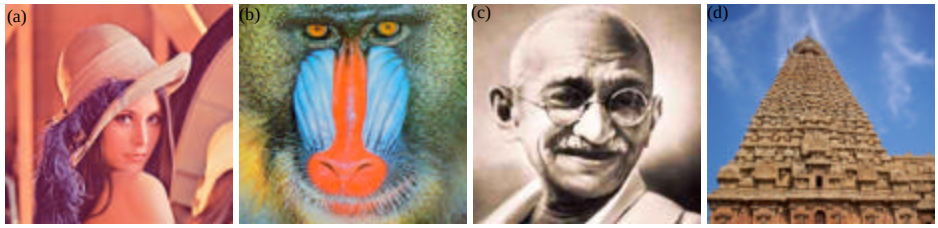

Fig. 4: Cover images (a) Lena, (b) Baboon, (c) Gandhi and (d) Temple

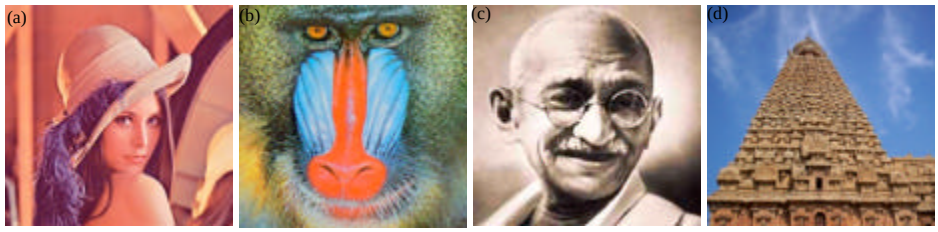

Fig. 5: Stego images method 1 (a) Lena, (b) Baboon, (c) Gandhi and (d) Temple

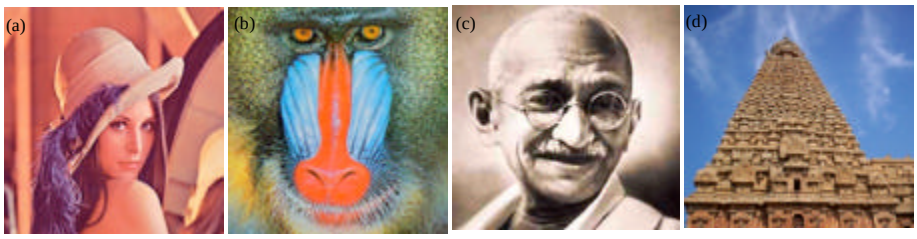

Fig. 6: Stego images method 2 green plane as indicator (a) Lena, (b) Baboon, (c) Gandhi and (d) Temple

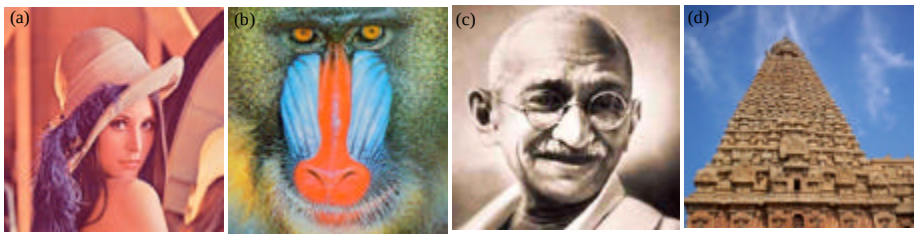

Fig. 7: Stego images method 3 Cyclic indicator (a) Lena, (b) Baboon, (c) Gandhi and (d) Temple

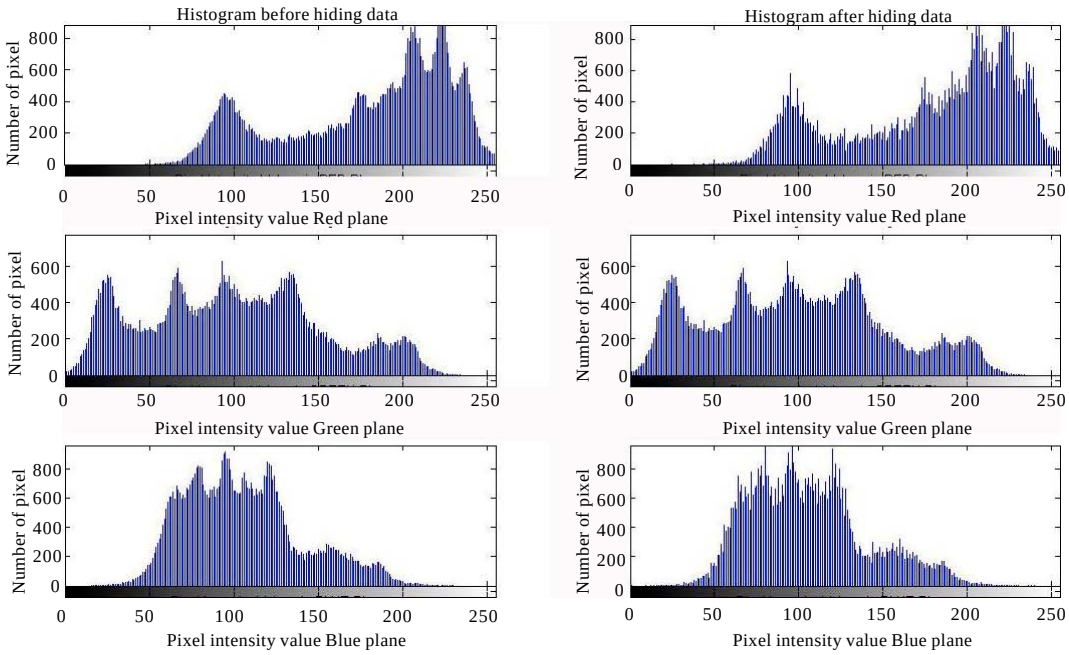

Fig. 8: Histograms for the proposed embedding method-1 Lena in all the three planes

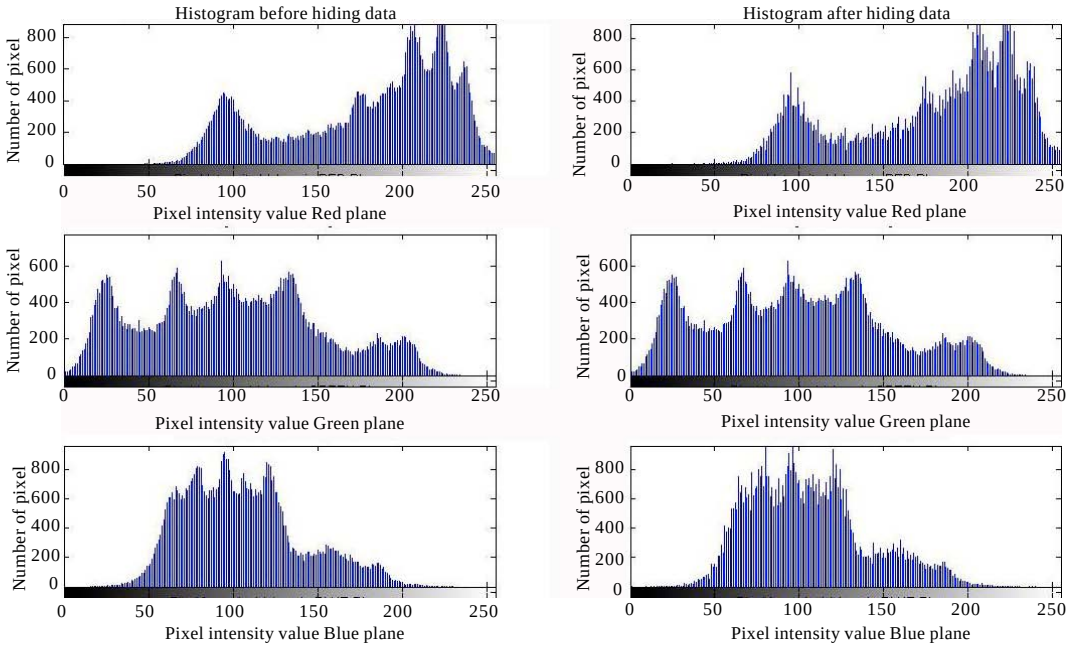

Fig. 9: Histograms for the proposed embedding method-2 Lena, in all the three planes

The stego cover results are given in Fig. 7. In method 3 the indicators are selected in sequence, In the case of first pixel indicator selection is the Red channel, then the Green is channel 1 and the Blue is the channel 2 i.e., the sequence is RGB. In the second pixel if we select, Green as the indicator, then Red is channel 1 and Blue is channel 2 i.e., the sequence is GRB. If in third pixel Blue is the indicator, then Red is channel 1 and Green is channel 2. In

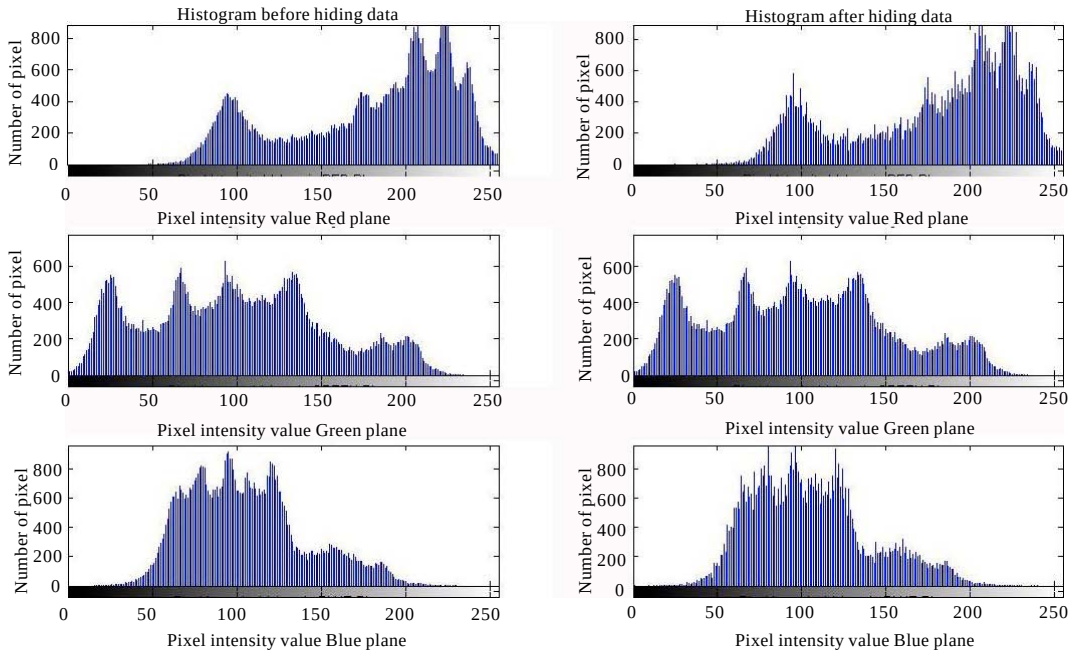

Fig. 10: Histograms for the proposed embedding method-3 Lena, in all the three planes

this case, the problem with earlier two methods is taken care of and the errors are evenly distributed. From these Table 1, 2 and 3, it has been observed that, Baboon has highest embedding capacity where Gandhi has the low embedding and high imperceptibility.

The comparative histograms (X - axis: Pixel Intensity values and Y-Axis: total number of pixels) of all the three methods, for Lena stego and cover images of RED, GREEN and BLUE planes are shown in Fig. 8, 9 and 10.

Figure 8 confirm the argument, there is no change in pixel intensity values in RED plane (Indicator channel) where is a slight change in other two data channel.

By carefully analyzing the histogram of method 2 shown in Fig. 9, there is no variation in the GREEN plane (Indicator channel) but there is some minor changes are noticeable in other two channel.

As explained in the results Fig. 10 confirms that the errors are evenly distributed in all the planes. So, this is thin difference between cover and stego histograms.

The proposed method has the following advantages. Each participant can apply one cover image to share multiple secret messages among the other participants.

Secondly, each bit plane of the cover image can share two secrets with two different participants. This indicates an economical utilization of bit planes, implying that a small number of bit planes may keep a great number of secrets to be shared. Thirdly, the camouflage ability keeps the quality of the stego-images visually acceptable. According to the property of the LSB substitution method, the stego-images will be close to the originals so that distortions between images are perceptually undetectable. The process of embedding secret data based on indicator-plane increases the embedding entropy considerably. The Pixel Value Differencing process performs intelligent embedding thereby optimally preserving the quality of the stego-image. The Optimal Pixel Adjustment Process decreases the Mean Square Error (MSE) thus making the stego image indistinguishable with the cover.

Security analysis: DES is used to randomize the user data with their known secret key of size 56 bits with a block of 64 bits. So number of combinations may be 264.

Then number of bits embedded in a pixel depends on a factor n = log2 (d) d may vary between 0 and 255 and n may vary from 1 to 7. So number of bits embedded in a pixel will vary from 1 to 7. n can be anything between 1 to 7. So, there are 7 possibilities.

Hence, complexity increases by a factor 264×7 without considering the Pixel Indicator methodologies.

Assuming 25% on each cases like 00, 01, 10 and 11 which decides the embedding capacity.

Since two users can use the same channel, we can consider complexity for first user. first user can embed data if two bits of indicator channel (red) is 01 or 11 (10 or 11). we are assuming 25% probability for 00, 01, 10, 11.

The probability that last 2 bits in a pixel of red plane to be 01 or 11 is 0.5. If the last two pixels are 01 or 11, then first user can embed in any one of the two planes.

So total complexity for first user is 2^64*7*0.5*2.

For two users total complexity will be is 2^64*7*0.5*2*2.

If possible pixels can be chosen randomly and increases the complexity.

In addition, if the secret information is encrypted before embedding with AES or Triple DES then the complexity level to extract the secret information will be high.

CONCLUSION

The process of embedding secret data based on indicator plane increases the embedding entropy considerably. The pixel indicator method used here performs intelligent embedding there by optimally preserving the quality of the stego image. The above proposed method provides the flexibility of two users using the same channel for transmission of secret data. The Optimal pixel Adjustment process decreases the mean square error thus making stego image indistinguishable with the cover. Thus the proposed method is an amalgam of above mentioned three methods which incorporates reduction of detectability and increase of entropy at the same time. The future work on this trend is to further increase the randomness by adopting random scan while embedding and to increase the number of shared user on the same covert channel.

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. 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, 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., K. Nathella and J. Harish, 2010c. Info hide: a cluster cover approach. Int. J. Comput. Applic., 3: 11-18.

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

Aura, T., 1996. Practical invisibility in digital communication. Inf. Hiding, 1174: 265-278.

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, U.A.E.

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.

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

Naor, M. and A. Shamir, 1994. Visual cryptography. Adv. Cryptol., 950: 1-12.

Padmaa, M. and Y. Venkataramani, 2010. ZIG-ZAG PVD-a nontraditional approach. Int. J. Comput. Appl., 5: 5-10.

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.

Parvez, M.T. and A.A.A. Gutub, 2008. RGB intensity based variable-bits image steganography. Proceedings of the IEEE Asia-Pacific Services Computing Conference, Dec. 9-12, Yilan, pp: 1322-1327.

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. Privac., 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. Inf. 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.

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 Xplore, Jakarta, 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 Recognition, 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. IEE Proc. 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.