Secure Data Transmission through Color Images using PHLSB Method

S. Nanda Kishor\textsuperscript{1*}, G. N. Kodanda Ramaiah\textsuperscript{2} and S. A. K. Jilani\textsuperscript{3}

\textsuperscript{1}Jain University, Bengaluru - 560069, Karnataka, India
\textsuperscript{2}Department of Electronics and Communication Engineering, KEC, Kuppam - 517425, Andhra Pradesh, India
\textsuperscript{3}Department of Electronics and Communication Engineering, MITS, Madanapalli - 517325, Andhra Pradesh, India

Abstract
Steganography is knowledge of embedding the secrete information inside the host medium. Due to less security and embedding efficiency, some steganography algorithms can be effortlessly distinguished by steganalytical detectors. A secure data embedding scheme Polynomial based Hash Least Significant Bit (PHLSB) method is developed. Polynomial equations are powerful mathematical tool. These equations were used as secret key for hiding data in the cover object. The tentative results prove that the proposed method accomplishes high embedding capacity, less perceptual transparency. The PSNR and SC of stego object have good values, almost similar to the original object.

Keywords: HLSB, Image Steganography, Polynomial Equations

1. Introduction
Internet makes individuals' lives much simpler than some time recently, they can make use of it to pay their bills, purchase their merchandise, operate essential messages between gathering at remote distances, and several different things. Without securing that important data, assailants can get them in various ways. Steganography is one of the techniques that shields and conceals important information from unapproved individuals and even without them having any inkling of the information's presence. Human Visual System (HVS) can’t perceive a trivial transform that happens in the media cover.

There are some important characteristics that each steganography system has to take into concern; they are embedding capacity, embedding efficiency and perceptual transparency. First the Steganography system should have high embedding efficiency means high-quality of stego data i.e., it work out the possibility of error when the detector is referred after embedding. Second, The perceptual transparency should be high means after hiding process the cover object occurs without loss of perceptual quality or a lesser amount of information are going to vary. Any noticeable deformation to the spectators will increase the probability of the foe suspicion and by using some staganalysis tool the secrete information can be easily detected. So the security of the steganography system is depends on perceptual transparency. The perceptual transparency is high, and then security is high. Third embedding capacity means the capacity of secrete information to be hidden inside cover object and it should be large. The fundamental building block diagram of steganography method is revealed in Figure 1.
Secure Data Transmission through Color Images using PHLSB Method

2. Literature Review

Author in\(^8\) presents a unique index of competences for steganalysis of JPEG images.

Author in\(^10\) introduced a scheme in their article dealing with DWT and DCT. In this article steganography with watermarking applied to provide wider security.

Author in\(^11\) proposed an approach to enhance the capacity by applying compression method to data before embedded, but this technique is capable for particular bmp images.

Author in\(^3\) introduced a unique Steganography approach which is made up based on LSB with extension of sequential encoding and symmetric encryption.

Author in\(^15\), came up with a unique scheme. In this scheme, information is covered in particular position of particular blocks by LSB substitution. Polynomial equation with several coordinates is applied to obtain the particular blocks and particular position for knowledge setting. Here the polynomials carry out as stego key. This scheme reduces the lower reliable LSB method. Payload to be enhanced by adopting this scheme.

3. Proposed System

The proposed system uses color image as cover object. The color image is converted into RGB color components. The information is hidden in each color component. In this proposed system, the polynomial equations used as secrecte key for hiding the information. Symmetric encryption were used for encrypt the secrecte information before embedding and after extracting process same is used in reverse order\(^16\). Hash based Least Significant Bit (HLSB) method was used for embedding process.

3.1 Polynomial Equations

Polynomial equations are high numerical tools. In maths, polynomial is a formulation comprising variables and coordinates that concerns only the efforts of summation, subduction, repetition, and non-negative integral indexes. The \(n\)th order polynomial equation is set forth in the order as

\[
ax^n + bx^{n-1} + \ldots + rx^1 + s = y
\]

Where \(a, b, r, s\) are known as coefficients and \(y\) is the value obtain for \(x\).

3.2 Symmetric Encryption

An encryption index is applied to alter the knowledge into new manner and the same is applied at retrieval of early form in backward pattern. XOR is great tool which is drawn on for encryption and decryption the knowledge.

Let take the message '01011101' and the encryption key '00011111' then the encryption message is '01010010'. At retrieval the recovered message is '01011101'.

3.3 LSB Method

One of the obvious and familiar steganography techniques is LSB approach. In this approach, the LSB section of each pel in the cover object is spelled by one part of covert data. The straightforwardness of the LSB approach permits the implanted particles to be straightforwardly identified by employing the retrieval process of the scheme. Let us deal with an 8-bit color model in which each pel is characterized by 24 bits. 3 bits can cover in each pel. For sample, consider a grid of 3 pels in image as a cover object which is taken advantage of to cover the knowledge.

The pixel values corresponding to color components as follows

|   | R   | G   | B   |
|---|-----|-----|-----|
| P1 | 39  | 64  | 125 |
| P2 | 48  | 229 | 178 |
| P3 | 186 | 75  | 25  |

Binary representation of the pixels is

\[(00100111\ 01000000\ 01111101\ 00110000\ 11100101\ 10110010\ 10111010\ 01001011\ 00011001)\]
the letter A, with binary representation '10000011' is entrenched into LSB's of the pel, the consequential grid follows as

\[(00100111 01000000 01111100  \\
00110000 11101001 10110010  \\
10111011 01001011 00011001)\]

Although the letter was entrenched into the foremost 8 bits of grid, highlighted 3 bits are going to be distorted according to covered message. On average, half of the bits of image are modified to hide a covert message.

### 3.4 Hash LSB

HLSB approach is applied to characterize the location where the data should secure. Hash function determines the position of bit of pel. Equation (2) is applied to distinguish location LSB of the pel.

\[q = b \% m \quad (2)\]

where, q is bit location of pel; b depicts the pel positions and m is the quantity. If q = 0, the bit is stored in 0th position of the pixel, q = 1 means the bit is stored in 1st position of the pixel, q = 2 means the bit is stored in 2nd position of the pixel. Where 7th bit is MSB and 0th bit is LSB.

### 3.5 Proposed Methodology

In this section, the operations of data hiding by PHLSB method are expressed. The covert information is changed into double form i.e., n-bit data and the polynomial report is formed by polynomial equation for n-bit data, which acts as secret key for hiding the data into cover-image. The procedure for embedding (hiding) and extraction (de-hiding) as follows.

#### 3.5.1 Embedding Process

Let \(I\) be the original 8-bit color image as cover of size \(m \times n\) and characterized as

\[I = \left\{(i, j, k) | 0 \leq i \leq m, 0 \leq j \leq n, 0 \leq k \leq 2 \right\} \quad (3)\]

Where i stands for rows, j stands for columns and k stands for color components of color image.

**Step 1:** Select the secret information to hiding, convert it into binary form using ASCII, which is denoted by M and express as

\[M = \{m_i | 0 \leq i \leq N, m_i \in \{0,1\}\} \quad (4)\]

Where \(N\) is the no of bits in secret information,

**Step 2:** Encrypt the information using encryption key \(K\) defined as

\[K = \{k_i | 0 \leq i \leq N, k_i \in \{0,1\}\} \quad (5)\]

The ultimate secret information \(\overline{M}\) for hiding is obtain by XOR operation of \(M\) and \(K\) represented as

\[\overline{M} = \{m_i \oplus k_i \} \quad (6)\]

Where \(\oplus\) denotes XOR operation.

**Step 3:** Convert the cover image into \(m \times n \times 3\) matrix form as

\[C = \{c_{i,k} | 0 \leq i \leq mn, 0 \leq k \leq 2, c_{i,k} \in \{0,1,2, \ldots, 255\}\} \quad (7)\]

Here, cover is separated into color compents. Each layer size is \(m \times n\) and it is converted into vector form. Finally we concatenate all the vectors corresponding to color components.

**Step 4:** Generate polynomial data which acts as secret key using polynomial equation. The G order polynomial equation can express as

\[P(x) = ax^G + bx^{G-1} + \ldots + rx^1 + s \quad (8)\]

Where a, b, r and s are scalars and \(x = \frac{\overline{N}}{2^G}\). Calculate the \(P(x)\) for \(r = \frac{N}{2^G}\). If \(P(x) > mn\) means the secret information size is larger than size of image vector, then change the cover object which is suitable.

**Step 5:** For \(x\), calculate the \(P(x)\) and select the corresponding element in image vector where information to be hide

\[H = \{c_{i,k} / k + 1 | j = P(x), 0 \leq k \leq 2c_{i,k} | k \in \{0,1,2, \ldots, 255\}\} \quad (9)\]

Where \(\bar{j}\) the pixel element and \(H\) is the intensity vector representation of color components of corresponding element in image vector.

**Step 6:** Select three successive bits in ultimate secret information for hiding. Hide the information using HLSB in \(H\).

**Step 7:** Rearrange the image vector \(m \times n \times k\), Afterwards the Stego-image is defined as

\[\tilde{I} = \left\{(\tilde{x}, i, j) | 0 \leq i \leq m, 0 \leq j \leq n, 0 \leq k \leq 2 \right\} \quad (10)\]

Where \(\tilde{x}\) the pixel element and \(\tilde{I}\) is the intensity vector representation of color components of corresponding element in image vector.
3.5.2 Extracting process

In the extracting process, the concealed knowledge can be deduced without having relation to the fundamental cover-object. The following steps consist in extraction process.

Step 1: Convert the Stego image \( \tilde{I} \) into \( mn \times 3 \) matrix form as

\[
\tilde{c} = \{c_{ik} | 0 \leq i \leq mn, 0 \leq k \leq 2, c_{ik} \in \{0,1,2,...,255\} \}
\] (11)

Step 2: Generate polynomial data \( P(x) \)

Step 3: For \( x \), calculate the \( P(x) \) and select the corresponding element in image vector where information is hidden.

Step 4: Extract the three successive bits of ultimate secret information using HLSB extraction. The ultimate secret information is

\[ \tilde{M} = \{m_i | 0 \leq i \leq N \} \] (12)

Step 5: Decrypt the information using encryption key \( K \) defined as

\[ K = \{k_i | 0 \leq i \leq N, k_i \in \{0,1\} \} \] (13)

Step 6: The secret information after decryption is obtained by XOR operation of \( \tilde{M} \) and \( K \) and expressed as

\[ M = \{m_i \oplus k_i \} \] (14)

4. Experimental Results and Analysis

To analyze the stego image a simple statistic error metrics such as Mean square Error (MSE), Peak signal to noise Ratio (PSNR), and Structural Content (SC) methods are taken.

Let us consider \( F_{m,n} \) is the cover image and \( F'_{m,n} \) is the Stego image then

Mean Square Error (MSE): The MSE is the simplest and most widely used method for quality measurement. It measures the error between images and defined as

\[
MSE = \frac{1}{MN} \sum_{m=1}^{M} \sum_{n=1}^{N} (F_{m,n} - F'_{m,n})^2
\] (15)

Peak signal to noise Ratio (PSNR): The PSNR is also used for quality measurement. PSNR is inverse to MSE.

\[
PSNR = 10 \log_{10} \left( \frac{\text{max}^2}{\text{MSE}} \right) \text{dB}
\] (16)

Structural Content (SC): The Structural content estimates the similarities of the structure of two images. SC varies between 0 to 1. If SC is equal to 1 means both images are similar and defined as

\[
SC = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} (F'_{m,n})^2}{\sum_{m=1}^{M} \sum_{n=1}^{N} (F_{m,n})^2}
\] (17)

Figure 2. Cover images. (a) Lena. (b) F16. (c) Baboon. (d) Forest. (e) Peppers. (f) Flower.
In this experimentation, various samples of pigments with size of 512 x 512 are taken as the cover object and some of them are illustrated in Figure 2. Figure 3 shows the stego-images obtained by proposed scheme corresponding to the six cover images in Figure 2.

From Figure 3 we can notice that there are no perceptual distorting occurred by PHLSB method. The Human Visual System (HVS) cannot recognize the discrepancy among cover and Stego images.

The obtained results compared with existing methods Wu et al’s Method\(^1\), H. Yung Method\(^2\) with respect to Embedding Capacity and PSNR for Lena Image. The proposed method obtained high embedding capacity and better PSNR than existing methods.

### Table 1. Comparison of results

| Method              | Capacity | PSNR |
|---------------------|----------|------|
| Wu et al’s Method\(^1\) | 757000   | 38.22|
| H. Yung Method\(^2\)  | 757332   | 39.31|
| Proposed Method (PHLSB) | 786320   | 39.68|

The comparison of results of Wu et al’s Method\(^1\), H. Yung Method\(^2\) and proposed method listed in Table 1 with respect to capacity and PSNR.

Figure 4. Comparison of results. (a) Capacity. (b) PSNR.

Figure 4 shows the graphical illustration of comparison of results. Here, by taking different orders of polynomial equations and no of equations are analyzed by capacity, PSNR and SC. By the analysis, Order increases, the capacity of hiding data were decreases and PSNR, SC increases. The number of Polynomial equations used increases i.e., two equations were taken for hiding process then the capacity increases almost twice than single equation with slight changes in PSNR and SC. Similarly
three equations were taken for hiding process the capacity increases almost thrice.

Table 2. Capacity, PSNr and SC for different order and no of equations used

| No. of Eqn | Order | Capacity (Bits) | PSNR | SC |
|------------|-------|----------------|------|----|
| 1          | 1     | 262112         | 52.9 | 0.997 |
| 1          | 2     | 880            | 77.6 | 1.0  |
| 1          | 3     | 90             | 87.5 | 1.0  |
| 2          | 1     | 524224         | 49.89| 0.994 |
| 2          | 2     | 1760           | 74.6 | 1.0  |
| 2          | 3     | 170            | 84.7 | 1.0  |
| 3          | 1     | 786336         | 39.68| 0.991 |
| 3          | 2     | 2640           | 72   | 1.0  |
| 3          | 3     | 270            | 82   |      |

The analysis of work is here obtained in terms of Embedding Capacity, PSNR and Structural Content (SC) with different Order and Number of Equations used for Image (Lena) with size 512 x 512. In this work, three different equations with order 3 were taken and PSNR, embedding capacity and SC are listed in Table 2. Figure 5 illustrates the Comparison of different equation of PHLSB method in Embedding capacity and PSNR Figure 6 shows the analysis results under Structural Content with varying order and no of equations and different polynomial equations.

5. Conclusion

In this paper PHLSB method has been realized well for steganography. In this paper a a novel approach of protecting data have been developed with less Perceptual transparency, high secure and more efficient. Result analysis of the PHLSB technique have been estimated and examined with opening techniques which have resulted a good MSE and PSNR. The Structural Content also have good results which explains statistical undetectable. Different polynomial equations with changing order of proposed method were analyzed. The result shows that the PHLSB method achieves higher embedding capacity.

6. Acknowledgements

This work was applied for patent to Patent Office, Intellectual Property India, Chennai with application number 201641018458 and it is in process.
I express my heartfelt thanks and great sense of thankfulness to my guides for the technical guidance and encouragement. I would also like to thank the Kuppam Engineering College R&D Cell for providing all facilities in carrying out the work.

7. References

1. Mstafa RJ, Elleithy KM. A highly secure video steganography using Hamming code. IEEE Long Island Systems, Applications and Technology Conference (LISAT); 2014. p. 1–6.

2. Liu B, Yang C, Liu F, Sun Y. Secure steganography in compressed video bitstreams. IEEE 3rd International Conference on Availability, Reliability and Security ARES 08; 2008. p. 1382–87.

3. Yadav P, Sharma S, Mishra N. A secure video steganography with encryption based on LSB technique. IEEE International Conference on Computational Intelligence and Computing Research (CICIC); 2013. p. 1–5.

4. Idbeaa TF, Samad SA, Husain H. Comparative analysis of steganographic algorithms within compressed video domain. IEEE International Conference on Signal Processing and Communication Systems (ICSPCS); 2014. p. 1–7.

5. Yun C, Zhang H, Zhao X, Yu H. Covert communication by compressed videos exploiting the uncertainty of motion estimation. IEEE Communications Letters. 2015 Feb; 19(2):203–6.

6. Bugár G, Bánoci V, Broda M, Levický D, Dupák D. Data hiding in still images based on blind algorithm of steganography. IEEE International Conference on Radioelektronika (RADIOELEKTRONIKA); 2014. p. 1–4.

7. Patel K, Rora KK, Singh K, Verma S. Lazy wavelet transform based steganography in video. IEEE International Conference on Communication Systems and Network Technologies; 2013. p. 497–500.

8. Yang H, Sun G, Sun X. A high capacity image data hiding scheme using adaptive LSB substitution. Radio Engineering. 2009 Dec; 18(4).

9. Holub V, Fridrich J. Low-complexity features for JPEG steganalysis using undecimated DCT. IEEE Transactions on Information Forensics and Security. 2015 Feb; 10(2):219–28.

10. Shivani K, Paramjeet K. Secure data hiding technique using video steganography and watermarking. International Journal of Computer Applications. 2014 Jun; 95(20).

11. Sharma V, Kumar S. A new approach to hide text in images using steganography. International Journal of Advanced Research in Computer Science and Software Engineering. 2013 Apr; 3(4).

12. Kumar A, Sharma R. A secure image steganography based on RSA algorithm and hash-LSB Technique. International Journal of Advanced Research in Computer Science and Software Engineering. 2013 Apr; 3(7).

13. Wu, H-C, Wu N-I, Tsai C-S, Hwang M-S. Image steganographic scheme based on pixel-value differencing and LSB replacement method. IEEE Proceedings-Vision, Image and Signal Processing. 2005; 152(5):611–5.

14. Provos N, Honeyman P. Hide and seek: An introduction to steganography. IEEE Security and Privacy. 2003; 32–44.

15. Swathi A, Jilani SAK. Video steganography by LSB substitution using different polynomial equations. International Journal of Computational Engineering Research. 2012 Sep; 2(5).

16. Xu C, Ping X, Zhang T. Steganography in compressed video stream. Proceeding of the 1st International Conference on Innovative Computing, Information and Control (ICICIC’06); 2006.

17. Wang Y, Izquierdo E. High-capacity data hiding in MPEG-2 compressed video. 9th International Workshop on Systems, Signals and Image Processing; UK. 2002.