HIDING DATA BY LSB SUBSTITUTION WITH POLYNOMIAL EQUATIONS IN COLOR IMAGES

*S.NANDA KISHOR, &Dr.G.N.KODANDA RAMAIAH, +Dr.S.A.K.JILANI, &A.AMARESWAR KUMAR
*Research Scholar, JAIN UNIVERSITY, BANGALORE, INDIA.
& Dept. of Electronics and Communication Engineering, KEC, KUPPAM, A.P, INDIA.
+Dept. of Electronics and Communication Engineering, MITS, Madanapalli, A.P, INDIA.

Abstract: ***Steganography is the process of embedding the secrete information inside the host medium. Due to less security and embedding efficiency, Some steganography algorithms can be easily detected by steganalytical detectors. In this paper, a data hiding scheme is developed by LSB substitution using polynomial equations. Experimental results show that the stego-image is visually indistinguishable from the original cover-image. The obtained results also show a significant improvement with respect to a previous work.***

Keywords: ***Image Steganography, Polynomial equations, LSB, data hiding.***

I.**Introduction**

Internet makes individuals' lives much simpler than before; they can utilize it to pay their bills, purchase their merchandise, operate essential messages between gathering at far 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 suspicion of the information's presence. Human Visual System (HVS) can't perceive a slight change that happens in the media cover.

There are some important characteristics that every steganography system should take into consideration, which are embedding capacity, embedding efficiency, perceptual transparency and false alarm rate. First the Steganography system should have high embedding efficiency means good quality of stego data i.e., it measures the probability of error when the detector is applied after embedding. Second, The perceptual transparency should be high means after hiding process the cover object occurs without loss of perceptual quality or less amount of data are going to change. Any obvious distortion to the viewers will increase the probability of the attacker's 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, 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 basic block diagram of steganography process is shown in Fig1.

II. **Literature Review**

Vojtech Holub and Jessica Fridrich, proposed a paper "Low-Complexity Features for JPEG Steganalysis Using Undecimated DCT". In this paper presents a novel list of capabilities for steganalysis of JPEG pictures. Its name is DCTR on the grounds that the components are registered from clamor residuals got utilizing the 64 DCT bases[9].

Gabriel BUGÁR, Vladimír BÁNOCI, Martin BRODA, Dušan LEVICKÝ, Denis DUPÁK, in their paper "Data Hiding in Still Images Based on Blind Algorithm of Steganography", a steganography method designed that uses the properties of Haar transform coefficients. The secret message is compressed before insertion in order to enlarge the capacity of the proposed system[6].

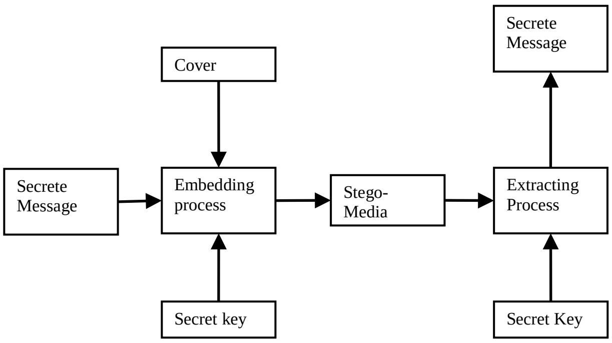


Fig 1. Basic Block diagram of Steganography

Shivani khosla and paramjeet kaur proposed a method in their paper "Secure Data Hiding Technique Using Video Steganography and Watermarking" using DWT and DCT techniques. In this paper Steganography with watermarking were used to provide more security[10].

Vipul Sharma and Sunny Kumar, proposed a technique in their paper "A New Approach to Hide Text in Images using Steganography". In this paper to increase the capacity of storage a compression algorithm were used that compressed data to be embedded but this method is efficient for only bmp images[11].

Swathi, S.A.K Jilani, proposed a novel method in his paper " Video steganography by LSB substitution using different polynomial equations". LSB insertion method is one of the oldest and easiest method of data hiding in which least significant bit of host file is used for hiding the information bit. In this method, information is embedded in specific location of specific frames by LSB substitution. Polynomial equation with different coefficients is used to get the specific frames and specific location for information embedding. Here the polynomial equation work as a stego key. This method overcomes the less secure LSB method. Pay load can also be increased by using this method[15].

III. **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 secrete key for hiding the information. Symmetric encryption were used for encrypt the secrete 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.

a. **Polynomial equations**

Polynomial equations are powerful mathematical tool. In mathematics, polynomial is an expression consisting of variables and coefficients that involves only the operations of addition, subtraction, multiplication, and non-negative integer exponents.

The nth degree polynomial equation is written in the form as

$$ax^{n}+ bx^{n-1}+\ldots\ldots\ldots+rx^{1}+s=y \qquad (1)$$

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

b. **Symmetric Encryption**.

In Symmetric encryption, an encryption key is used to transform the information into other form and same is used at retrieval of original form in reverse order. XOR is powerful tool which is used for encryption and decryption the information. With the key the XOR transform the information into another form which is also binary form.

Let take the message '01011101' and the encryption key '00001111' then the encryption message is '01010010'. At retrieval the recovered message is '01011101'.

c. **LSB Method.**

One of the easy and popular steganography techniques is LSB method. In this method, the LSB position of each pixel in the cover image is substituted by one bit of secret data. The simplicity of the LSB technique allows the embedded bits to be easily detected by applying the retrieval method of the scheme. Let us consider an 8-bit color image in which each pixel is represented with 24 bits. So 3 bits can hide in each pixel. For example, let take a grid of 3 pixels in image as a cover object which is used to hide the information. 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)

When the letter A, which binary representation is '10000011' and is embedded into LSB's of the image, the resulting grid is as follows

(0010011**1** 0100000**0** 0111110**0**
0011000**0** 1110010**0** 1011001**0**
1011101**1** 0100101**1** 0001100**1**)

Although the letter was embedded into the first 8 bytes of grid, only 3 highlighted bits need to be changed according to embedding message. On average half of the bits of image are modified to hide a secret message.

d. **Proposed Methodology**

In this section, the general operations of data hiding by PHLSB method are described. The message data is converted into binary form that is n-bit secret message and the polynomial data is generated using polynomial equation for n-bit data, which is acts as secret key for hiding the data into cover-image. The procedure for Embedding (hiding) and extraction (de-hiding) as follows.

i) Embedding process

Let I be the original 8-bit color image as cover image of size m x n and represented as

$$I = \left\{x(i,j,k) \middle| \begin{smallmatrix} 0\le i\le m, 0\le j\le n, 0\le k\le 2 \\ x(i,j)\in\{0,1,2,.....255\} \end{smallmatrix}\right\} \qquad (2)$$

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

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

$$M = \{m_i | 0 \le i \le N, m_i \in \{0,1\}\} \qquad (3)$$

Where N is the no of bits in secrete information,

Step 2: Encrypt the information using encryption key K defined as

$$K = \{k_i | 0 \le i \le N, k_i \in \{0,1\}\} \qquad (4)$$

The ultimate secrete information $\widehat{M}$ for hiding is obtain by XOR operation of M and K represented as

$$\widehat{M} = \{\widehat{m}_i | \widehat{m}_i = m_i \otimes k_i\} \qquad (5)$$

Where $\otimes$ denotes XOR operation.

Step 3: Convert the cover image into mn x 3 matrix form as

$$C = \{c_{ik} | 0 \le i \le mn, 0 \le k \le 2, c_{ik} \in \{0,1,2,\dots,255\}\} \qquad (6)$$

Here, cover image is divided into color compents such as R,G,B layers. Each layer size is m x 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 secrete key using polynomial equation. The G order polynomial equation can express as

$$P(x) = ax^G + bx^{G-1} + \cdots .. + rx^1 + s \qquad (7)$$

Where a, b, r and s are scalars and $x = 1,2,\dots N/3$. Calculate the $P(x)$ for $x = N/3$. If $P(x) > mn$ means the secrete 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

$$H = \left\{c_{jk} \middle| j = P(x), 0 \le k \le 2c_{ik} \in \{0,1,2,\dots,255\right\} \qquad (8)$$

Where j is 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 secrete information for hiding. Hide the information using LSB in H.

Step 7: Rearrange the image vector m x n x k, Then the Stego- image is defined as

$$\hat{I} = \left\{\hat{x}(i,j,k) \middle| \begin{smallmatrix} 0\le i\le m, 0\le j\le n, 0\le k\le 2 \\ \hat{x}(i,j)\in\{0,1,2,.....255\} \end{smallmatrix}\right\} \qquad (9)$$

ii) Extracting process

In the extracting process, given the stego-image, the hidden information can be extracted without referring to the original cover-image. The extraction process consists of the following steps.

Step 1: Convert the Stego image $\hat{I}$ into mn x 3 matrix form as

$$\hat{C} = \{\hat{c}_{ik} | 0 \le i \le mn, 0 \le k \le 2, \hat{c}_{ik} \in \{0,1,2,\dots,255\}\} \qquad (10)$$

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 secrete information using LSB extraction. The ultimate secrete information is

$$\widehat{M} = \{\widehat{m}_i | 0 \le i \le N\} \qquad (11)$$

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

$$K = \{k_i | 0 \le i \le N, k_i \in \{0,1\}\} \qquad (12)$$

Step 6: The secret information after decryption is obtain by XOR operation of $\widehat{M}$ and K and expressed as

$$M = \{m_i | m_i = \widehat{m}_i \otimes k_i\} \qquad (13)$$

IV. 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 measure the error between cover and stego image and defined as

$$MSE = \frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}(F_{m.n} - F'_{m,n})^2 \qquad (14)$$

Peak signal to noise Ratio (PSNR) : The PSNR is also used for quality measurement. PSNR is inversely to MSE. The MSE represents the cumulative squared error between the compressed and the original image, whereas *PSNR* represents a measure of the peak error.

$$PSNR = 10\ \log_{10}\left(\frac{max^2}{MSE}\right)\ dB \qquad (15)$$

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

$$SC = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N}(F'_{m,n})^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}(F_{m.n})^2} \qquad (16)$$

[a,b
c,d]

Fig 2. Cover Images : (a) Lena (b) F16 (c) Baboon (d) Forest (e) Peppers (f) Flower.

In the experiments, different types of color images with size of 512 x 512 are used as the cover images and six of them are shown in Fig. 2. Fig. 3 shows the stego-images corresponding to the six cover images in Fig 2 obtained by proposed scheme.

From Fig. 3 we can notice that there are no perceptual distorting occurred by proposed method. The Human Visual System (HVS) cannot identified the difference between cover and Stego images.

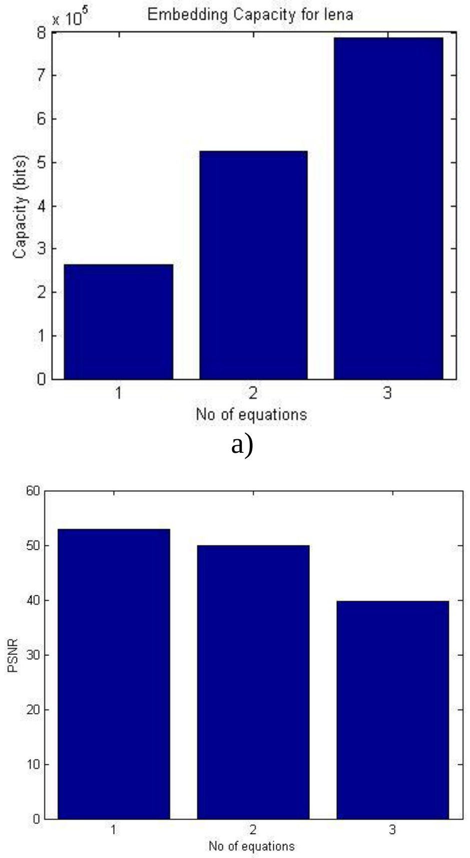
[a,b
c,d]

Fig. 3: Stego Images : (a) Lena (b) F16 (c) Baboon (d) Forest (e) Peppers (f) Flower.

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	1.0

Table. 2: Capacity, PSNr and SC for Different order and No. Of equations used.

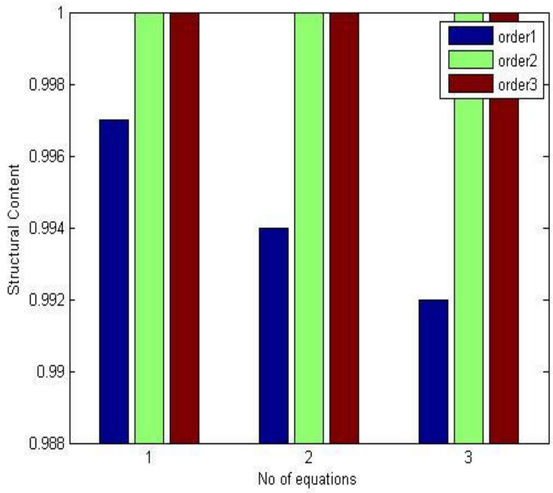
Here, by taking different orders of polynomial equations and no of equations are analyzed by capacity, PSNR and SC. By the analysis, Order increases, the capacity of hiding data were decreases and PSNR, SC increases. The number of Polynomial equations used increases i.e two equations were taken for hiding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



a)

b)

Fig. 5: Comparison of different equation a) Capacity b) PSNR.



Fig, 6: Comparison with respect to SC.

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.

Fig. 5 shows the Comparison of different equation of proposed method in terms of Embedding capacity and PSNR Fig. 6 shows the analysis results under Structural Content with varying order and no of equations and different polynomial equations.

V. **Conclusion**

In this paper Polynomial based LSB method has been implemented successfully for steganography. In this paper a new way of hiding data have been developed with less Perceptual transparency, high secure and more efficient. Result analysis of the proposed technique have been evaluated and compared with exiting 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 proposed method achieves higher embedding capacity.

Acknowledgements

I express my sincere thanks and deep sense of gratitude to my guides for the technical advice, encouragement and constructive criticism. I would also like to thank the Kuppam Engineering College R&D Cell for providing all facilities in carrying out the work.

References

[1] *Mstafa, R.J., Elleithy, K.M, “*A highly secure video steganography using Hamming code*”,* IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2014, pp. 1 – 6.

[2] *Bin Liu, Fenlin Liu, Chunfang Yang and Yifeng Sun*, “Secure Steganography in Compressed Video Bitstreams”, IEEE Third International Conference on Availability, Reliability and Security, 2008. ARES 08, pp 1382 – 1387.

[3] Encryption Based on LSB Technique”, IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2013, pp 1-5.

[4] *Tarik Faraj Idbeaa, Salina Abdul Samad, Hafizah Husain*, “Comparative Analysis of Steganographic Algorithms Within Compressed Video Domain”, IEEE International Conference on Signal Processing and Communication Systems (ICSPCS), 2014, pp 1–7.

[5] *Yun Cao, Hong Zhang, Xianfeng Zhao and Haibo Yu*, “Covert Communication by Compressed Videos Exploiting the Uncertainty of Motion Estimation”, IEEE COMMUNICATIONS LETTERS, VOL. 19, NO. 2, FEBRUARY 2015. Pp 203-206.

[6] *Gabriel BUGÁR, Vladimír BÁNOCI, Martin BRODA, Dušan*

LEVICKÝ, Denis DUPÁK, "Data Hiding in Still Images Based on Blind Algorithm of Steganography", IEEE International Conference on Radioelektronika (RADIOELEKTRONIKA), 2014, pp 1–4.

[7] *Khushman Patel, Kul Kauwid Rora, Kamini Singh, Shekhar Verma*, "Lazy Wavelet Transform Based Steganography in Video", IEEE International Conference on Communication Systems and Network Technologies, 2013, pp 497-500.

[8] *H.YANG, X. SUN, G. SUN,* " a High Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Radio Engineering, Vol. 18, No. 4, December 2009.

[9] *Vojtˇech Holub and Jessica Fridrich*, "Low-Complexity Features for JPEG Steganalysis Using Undecimated DCT", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 2, FEBRUARY 2015, pp 219-228.

[10] *Shivani khosla and paramjeet kaur*, *"*Secure Data Hiding Technique Using Video Steganography and Watermarking*"*, International journal of computer applications, Volume 95, No.20,June 2014.

[11] *Vipul Sharma and Sunny Kumar, "*A New Approach to Hide Text in Images using Steganography*"*, International journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue.4, April 2013.

[12] *Anil Kumar and Rohini Sharma, "*A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique*",* International journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue.7, April 2013.

[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 Procedings-Vision, Image and Signal Processing, 2005, vol. 152, no. 5, P.611-615.

[14] *N.Provos, P.Honeyman* " Hide and Seek : An Introduction to Steganography", IEEE Security and Privacy,pp32-44. 2003.

[15] *A.Swathi and Dr.S.A.K Jilani, "*Video Steganography by LSB Substitution Using Different Polynomial Equations*",* International Journal of Computational Engineering Research, Vol.2, Issue 5, September 2012.

[16] *Changyong Xu, Xijian Ping and Tao Zhang, "* Steganography in compressed video stream*",* Proceeding of the first international conference on Innovative Computing, Information and Control (ICICIC'06), 2006.

[17] *Y. Wang, E. Izquierdo,* "High-Capacity Data Hiding in MPEG-2 Compressed Video", 9th International Workshop on Systems,Signals and Image Processing, UK, 2002.