Steganography Technique with Huffman Code

Nilambar Sethi, Padmaja Patel

Abstract: The growth of modern communication technologies imposes a particular means of security mechanisms in particular in case of data networks. In order to protect sensitive data while these are en route, applications call up different methods. Here we are trying to code the message by Huffman coding technique and applying the Steganography using differencing and substitution mechanisms with encryption to the original message which can give multi label security. Here we are trying to communicate in two phases such as (1) Encrypt the message by Huffman code and (2) applying the In Steganography. We divide the image into multiple blocks which are non-overlapped in nature and the block size is 3×3 pixel that will consider as matrix. For every value from the matrix can be represented in eight bit where two bit will use as least significant bit (LSB) substitution and quotient value differencing (QVD) is applied for other bits. We are trying to process in three levels: (i) Huffman tree through message is encrypted which is secret (ii) LSB substitution at lower bit planes and (iii) QVD at higher bit planes.

Keywords : *Steganography, LSB substitution, QVD, Huffman code, Encryption, Decryption.*

I. INTRODUCTION

Today the whole world is internet era. Almost all people dependents on that. Each user wants his/her data to be sent to others safe and securely when they are using internet. So we are trying encrypting the data by different techniques. The primary focus is the computer that we are identifying to send the message over network must assure no one will able to identify our primary data by decrypting by the key through which the message is enciphered. For that many security technique is applied by different source. Cryptography is one of that."Cryptography" derives from the Greek word criptus, meaning "hidden" and graphian means writing. Cryptography is the science of encrypting and decrypting information. Steganography is another technique for encryption which is originated from Greek words which literally means “cover writing”. We can consider to steganography as “invisible” communication. Steganography is also an approach of secret data exchange. It is performed by including the original data within the image, [1]. In steganography, bind the primary data into the image and numerical properties of the image can be potted [2]. Least significant bit (LSB) substitution and pixel value differencing (PVD) is one of the majority admired steganography approach in specific area [3]. properties of the image can be potted [2]. Least significant bit (LSB) substitution and pixel value differencing (PVD) is one of the majority admired steganography approach in specific area [3]. When we are considering pixel value differencing in one dimensional block like pixel 1×2, the hiding capacity is very less that can be breakable by the hikers. To advance the hiding capacity and un detect ability the block size can be enlarge and PVD practice has been extended to seven-directional PVD in [4]. Looking to the strength and softness of surrounding pixel Nilizadeh and Nilchi proposed a model where it is given the liberty to select the block size in square form [6]. The hiding technique within the image with large merging capability can be done using multiple techniques like LSB substitution and quotient value differencing (QVD) [7]. In execution point the image can break into different block of size 3 × 3 pixel and assuming it is no overlapping in nature. In every block can be consider two parts as lower bit planes and higher bit planes and LSB and QVD technique can be applied respectively. Every block should check fall off boundary problem after embedding. Here we are assuming it is not exceeding boundary. If it suffers then we can move forward towards direct 4-bit LSB substitution. Still, such FOBP cases are negligible and defeat power is improved to a larger degree. In [8] image steganography is clustered in different aspects. Considering three pixels for message emerge near the target pixel and applied PVD is another approach discussed [9]. Considering the data it considered m-bit LSB approach for primary message embedding that bit is predictable by next to three pixels with high difference value. An optimization technique which adjusts the target pixel can be introduced for better visibility and good capacity. In this study the cover image and stego image are very similar but it is applicable for very low data set. Selecting the random pixel from an image and applied LSB is discussed Madhuet al., in [10]. Their approach is looking to perk up the strength where password is incorporated by least significant bit of graphical points. It produces the random numbers and identify the area where actually data to be hide. The positive aspect of this method is its security of inject data in stego-image. In [11], authors looking specific color of the image area to inject the message using suitable technique. It changes the image into binary and labels each point using 8 way connectivity schemes for hiding data bits. Its complexity and hiding capacity fully depends on texture of image. In [12] Stego analysis is the talent of judgment the message’s existence and blockading the channel. Many techniques have been proposed by many authors but LSB is one such technique in which least significant bit of the image is replaced with data bit. In this approach raw data is encrypt before injecting it in the image

Revised Manuscript Received on July 05, 2019.

Nilambar Sethi, Department of CSE, GIET University, Gunupur, India. Email: nilambar@giet.edu

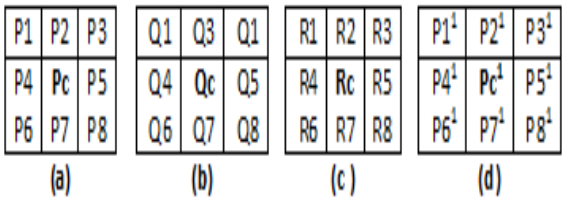
Padmaja Patel, Department of CSE, GIET University, Gunupur, India. Email: padmaja@giet.edu

which gives more security but time complexity increases some times. In [13] the locked data passing over internet is successful applying Steganography. Here high capability and defense Steganography with discrete wavelet transform (HCSSD) is proposed.

Many existing pixel value difference gives hiding capacity near about 4.55 bit per byte which is more than 55% of original size of the image. This article producing near about same hiding capacity with more security as data is coded by the coding technique Huffman code. This coding technique we can be considered as secrete key and that is also be injected to the image.

II. Related Works

Swain [7] proposed a hiding technique where the image is divided into different block which are not overlapping and consist of 3× 3 pixels. One Primary block has been given away in Fig. 1 a. Merge technique is described in details.



Fig(1)a. Primary Block, b. Quotient Block, c. Reminder Block and d. Stego Block

Initially from the original block is converting to higher bit-plane block by implementing quotient division on every pixel by Eq. (1); this block is shown in Fig. 1b. Again the LSB block can be constructed by applying residue division to all using Eq. (2); this block is appears in Fig. 1c

$Q_i = P_i / 4$ for all i=1 to 8

and $Q_c = p_c / 4$ (1)

$R_i = P_i \%4$ For all i=1 to 8

and $R_c = p_c \%4$ (2)

For example 7/3=2 and 7%3=1 which indicate the quotient and reminder respectively.

Again suppose the two LSBs of Pc are b_2b_1. Rc is the decimal equivalent of b_2b_1. Rc is converted to R_c^1 after substituting b_2 in place of $b_1$and a bit from binary data stream in b_2. Likewise, for i = 1 to 8, two binary bits can be considered from binary data stream and that can be converted to decimal which can renamed as R_i^1 in the Stego block. From the quotients there are eight pairs. Those are (Q_c, Q_i), where i=1 to 8. Eight difference values can be evaluated from Eq. (3).

$$d_i = Q_i - Q_c \quad (3)$$

Now using the range Table 1 from[7] absolute difference values $|d_i|$, for i = 1 to 8 falls into range r_j (for $1 \le j \le 4$) whose lower bound is L j i and hiding capability is $n_{j\,i}$.

Now For i = 1 to 8. $n_{j\,i}$ is data bits are taken and converted to decimal one b_i . Finally the new values d_i can be evaluated by Eq (4)

$$d_{ci}^1 = L_{ji} + b_i \text{ if } d_i \ge o$$
$$\text{or } d_{ci}^1 = -L_{ji} - b_i \text{ if } d_i \le o \quad (4)$$

Then calculating the value mi= d_i^1 - d_i for all 8 points. Doing this eight quotient pair (Q_c, Q_i) can be merged into the eight pair by the Eq(5).

$(Q_{ci}^1, Q_i) =$

(Qc-$\lfloor \frac{mi}{2}, \rfloor$, Qi + $\lceil \frac{mi}{2} \rceil$) when d_i is even

And

(Qc –m i/2 , Qi+$\lfloor \frac{mi}{2}, \rfloor$) when d_i is odd. (5)

After merging the pixel Q_c we can eight new values in different pair which can be unified to a single value from eq (6)

$$Qc = (\sum_{i-1}^{8} Q_{ci}^1) / 8 \quad (6)$$

As each Q_{ci}^1 has changed to Q_c^1 , at the same time $Q_i^1 = Q_i^1 + (Q_c^1 - Q_{ci}^1)$ for all eight points also be changed. Finally the stego pixel for all eight points can be calculated by (7)

$$P_c^1 = Q_c^1 \times 4 + R_c^1, P_i^1 = Q_i^1 \times 4 + R_i^1 \quad (7)$$

During this if any of Q_i^1 exceed the boundary [0, 63] from the table -1 then the whole block can be undo and 4 bit LSB can be applied.

Range Table

Range	r1=[0, 7]	r2=[8, 15]	r3=[16, 31]	r4=[32, 63]
Capacity n,j	3	3	4	5

III. Proposed QAV Huffman Code Technique

The image is separated into 3× 3 pixels block that are not overlapping in nature as in the fig-1.The injection procedure can be describe as follow.

Step 1: From the plaintext identified the number of different types of character and its frequency.

Step 2 create an array and store it as symmetric key.

Example: the word "GOOD"

3	*G*	*O*	*O*	*D*	*1*	*2*	*1*

First position indicate number of different types of character which

is 3 and next 3 position indication that the actual character and next three position indicating their frequency.

Step 3: Encrypt the original message into Huffman code. From the above example the code for G=0, code for O=10 and code for D=11. Where our plan text GOOD will be 0101011

Step 4: convert the symmetric key to 8-bit form and append with encrypted code done by Huffman code and append parity bit 0 if it is not divisible by 2.

Example for the above data will be 00000011 1000111 1001001 0101011

After adding the parity bit 00000011 1000111 1001001 01010110

Step5: Apply eight directional QVD techniques.

Taking the original image block as in fig 2.a and data block 10111100001010011000 1010 1100 001 00 11101110 and applying the QVD technique we get the Stego image Fig 2 (d).

130	132	130		32	33	32		2	0	2		125	147	138			
128	128	130		32	32	32		0	**0**	2		124	127	133			
131	129	128		32	32	32		3	1	0		137	144	151			
(a)				(b)				(c)				(d)					

Reminder

Step 6: Apply the extraction QVD process.

Considering the Stego-pixel block which is mentioned in Fig. 1(d). Considering the seed pixel which is central pixel, Pc check the least significant bit (LSB), if we found it is 0, then in this block 4-bit LSB changeover can be applied during embedding. Otherwise it found 1, then 2-bit LSB substitution and QVD approach was applied during the process.

Extract the second LSB from Pc1 for i=1 to 8. Append this 17 bit to take out the binary date stream. Two LSB from P_i^1 can be take out by calculating $R_i^1 = P_i^1 \bmod 4$ and converting R_i^1 to two binary bit. Further calculating the quotient $Q_i^1 = P_i^1 / 4$ and $Q_c^1 = P_c^1 \%4$, then eight difference value by $d_i^1 = Q_c^1 - Q_i^1$ at the end b_i^1 the extracted value in decimal from b_i^1 can be calculated as $b_i^1 = d_i^1 - L_{ji}$ for i= 1to 8 and converted to n_{ji} binary data bits and which are merged to extracted binary data stream.

Step 7: Decode the Huffman code using symmetric key which is Huffman tree and neglect the append bit. Here the first 8 bit indicate the number of character n and next n× 8 bit indicate different types character and next n× 8 bit indicate the frequency. Finally using these data we have to decode the code which is original message injected in image.

IV. CONCLUSION

Here we proposes a data hiding approach using3× 3 non overlapping pixel block within an image by encrypting the original data by Huffman code and embedding LSB substitution and quotient value differencing. Although the LSB substitution and quotient value differencing is successfully tested the security factor can be increased here by coding the data. After executing all above steps on plain text the strength of encryption message is very secure. The result of, MSE, PSNR and Compression Ratio for encryption of images are highly acceptable in this work.

References

1. Cheddad, A.; Condell, J.; Curran, K.; Kevitt, P.M.: Digital image steganography: survey and analysis of current methods. Signal Pro-cess. 90, 727–752 (2010)
2. Martin, A.; Sapiro, G.; Seroussi, G.: Is image steganography natu-ral? IEEE Trans. Image Process. 14(12), 2040–2050 (2005)
3. Fridrich, J.; Goljian, M.; Du, R.: Detecting LSB Steganography in color and gray-scale images. Mag. IEEE Multimed. Secur. 8(4), 22–28 (2001)
4. Pradhan, A.: Sekhar, K.R.; Swain: G.: Digital image steganography based on seven way pixel value differencing. Indian J. Sci. Technol. 9(37), 1–11 (2016)
5. Jung, K.H.: Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane. J. Real Time Image Pro-cess. 14(1), 127–136 (2018)
6. Nilizadeh, A.F.: Nilchi, A.R.: Block texture pattern detection based on smoothness and complexity of neighborhood pixels. Int. J. Image Graph. Signal Process. 5, 1–9 (2014)
7. Gandharba Swain: Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution. Arabian Journal for science and Engineering online 16 -6-2018
8. E Lin, E Delp, A Review of Data Hiding in Digital Images. Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS'99), Savannah, Georgia, April 25-28, (1999).
9. H. Zhang, G. Geng and C. Xiong: "Image Steganography Using Pixel-Value Differencing", Electronic Commerce and Security, ISECS '09. Second International Symposium on (2009) May.
10. V. MadhuViswanatham and J. Manikonda,: "A Novel Technique for Embedding Data in Spatial Domain", International Journal on Computer Science and Engineering, IJCSE, vol. 2, (2010).
11. H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, France, (2007).
12. N. Johnson and S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer, pp. 26-34, February (1998).
13. H. S. Majunatha Reddy and K.B.Raja, (2009) High
14. capacity and security steganography using discrete wavelet transform. International Journal of Computer Science and Security. pp. 462-472.

AUTHORS PROFILE

Dr. Nilambar sethi is working as Associate professor in Dept of Computer science at GIET University, Gunupur, Odisha. He did his Ph.D from Berhamput

University. He has 7 publications in national and international journals. He is the member of IE, CSI, and ISTE. His Research area is network security and soft computing.

Mrs. Padmaja Patel is working as Assistant professor in Dept of Computer science at GIET University, Gunupur, Odisha. She did her M.Tech form GIET Gunupur. She has 4 publications in national and international journals. She is the member of IE, CSI, and ISTE. Her Research area is network security and Block chain.