International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 03 - Issue 03 || March 2018 || PP. 20-27

Compression, Encryption, Watermarking & Steganography (CEWS) Technique for Image Steganography

M V Narayana[1]
[1]*(Department of CSE, GNITC, India)*

Abstract: Now a days, the communication over distributedsystem and Internet demands strong security. The rapidly increasing in network usage and encroachment in technology becomes challenge for protecting secure information communication over a distributed system. The major techniques to satisfy security needs are Steganography and cryptography. Steganography is a process of writing hidden message. Cryptography scrambles message so that it can't be understood. In this paper a technique named as CEWS for Compression, Encryption, Digital Watermark and steganography is proposed to provide secret exchange of data. In the CEWS technique, the data is pre-processed before embedded into the cover image. The preprocessing includes compression of data to reduce its size and encryption of the compressed data to change the data's appearance. Later on, Digital watermarks the carrier image to authenticate content and to deter unauthorized use. At last, the pre-processed data embeds behind the carrier image using a Random LSB algorithm. This proposed technique is implemented in Java and strength of the CEWS technique is compared by calculating PSNR and MSE metric measures of the carrier image to the resultant image. Experimental Results obtained from this technique shows that the resultant image attained applying CEWS technique is not visually distorted, because, the value of PSNR is high and MSE is low. The experimental outcomes of CEWS technique compared to other Steganography technique demonstrates DESW technique performs better.

Keywords: Watermark, Encryption, Compress, CEWS Technique, RSA

I. INTRODUCTION

The increasing demand on distributed data communication and technology advancement needs secure communication or information transfer. Intruders always keep on seeking to get access secret information. Preventing and protecting the exchange of information over the Internet from intruders and eavesdroppers are becoming the major focus of network security professionals. Steganography is a process of writing hidden message in such a way that the intended communicating parts recognize existence of the message [1]. The target of Steganography is to avoid suspicion of transmission of hidden message [2]. Steganography and Cryptography are closely related. Cryptography is the process of altering information into an unreadable format. Only the intended parts that have a secret key decrypt the message into plain text. Intruders and eavesdroppers easily detect distorted resultant image (Stego image). Thus, any one succeeded in breaking of the Steganography system will get access to the secret information. Preprocessing the information before it gets embedded provides strong protection. There are different characteristics of Steganography techniques, such as Audio, Text and Image Steganography. In image Steganography the secret data masks behind the cover image by modifying some bits (unneeded bits) of its pixel. The common image Steganography techniques are Least Significant Bits, Masking and filtering and transformations [3]. The paper focuses on preprocessing the data before get masked. The preprocessing phase includes Compression, Encryption and Digital Watermark. Compression shrinks down the size of the data so that number of message that will embed in the same cover image increases. Compression before encryption also increases security in network communication. Encrypt the data with the help of a key alters the original data, which is not easily understandable to intruders and eavesdroppers. Digital Watermark helps owner identification, content authentication and file reconstruction. This paper organized as follows. Section II overviews some related work techniques. In section III introduces study models. Section IV presents the proposed concept of the CEWS Technique in more detail. Section V includes advantages of the proposed technique. Section VI provides experimental results of CEWS technique. Section VII concludes the paper. Section VIII includes the future directions for the related projects or research works. Last section XI includes references.

II. RELATED WORKS

In modern digital steganography technique, the data is first encrypted and subsequently masked using a special algorithm into a redundant data. Image steganography is the most familiar method, since each pixel of the color image represented by three bytes (24-bit), and trivial noise in the same color is unable to observe by human eye. JyotiGaba and Mukesh Kumar [4] suggested a technique of compression and encryption the data before masking behind the cover image. Then the modified data is masked behind 8Ith DCT coefficients of the blue components. Naitik P Kamdar and Dharmesh N. Khendhar [5] analysed by implement Least Significant Bit and DCT steganography, and value of PSNR is high, and MSE is low in LSB based Steganography as compared to DCT based steganography. SanjeevManchanda, Mayank Dave and S. B. Singh [6] have suggested random number's logic based image steganography and layout management schemes for hiding the data. According to their study the random number generator plays a great role on identification of the position to embed a bit message and then embeds it using the LSB method. When the Xi is the current bytes, then the next target byte to replace using LSB is Xi+1. Xi+1= f(Xi, Xi-1,… Xi-n+1)(mod m)= a1Xi-1+a2Xi-1+…anXi-n+1 +c) (mod m) where m, n, a, c are non-negative integers.G. Swain and S. K. Lanka [7] has presented Encryption and Steganography hybrid technique that encrypts the text message before embedding using an extended hill cipher algorithm. Afterward, the cipher text is embedded in the brightest pixel (gray value 224-255) and in the darkest pixel(gray value from 0-31) that is in the 6th, 7th and 8th pixel position. The encoding text spreads randomly throughout the image. Another technique proposed by S. Gupta et al [8] is that first data is encrypted using the RSA or Diffie Hellman algorithm. Later on, the cipher text is embedded behind carrier image using LSB algorithm.

III. MODEL

A. Definition

1. Cover image: it is a bitmap image intowhich a required secret message is encoded.
2. Stego Image: it is an image produced afterencoding the required information into the cover image.

B. Error analysis

a. MSE: the mean square Error is a metric usedto measure the cumulative square error of the cover and Stego image. The lower MSE signifies the lower distortion in the Stego image.
b. PSNR: Peak Signal-to-Noise Ratio is theratio between the reference signal and the distortion signal on an image, given in decibels. The higher the PSNR, the closer the distorted image is to the original. In general, a higher PSNR value should correlate to a higher quality image.

CEWS (Compressed-Crypto-Watermarked-Stego) technique unifies four practices to satisfy the increasing security demands. The first step of the algorithm is compression with the help of Huffman code. Compression shrinks down the size of the data so that the volume of message that will embed in the same cover image increases. The Compression before encryption also increases security in network communication. Later on, the compressed data encrypts with the help of RSA key. In this technique, the size of RSA key is 1024 bits so as cracking 1024 bit key size is also nearly impossible. The third step in the CEWS technique is digital watermark the cover image to prevent unauthorized use and authenticates content. Digital watermark text is a sender signature (or sender name). At last, the pre processed data embeds behind the cover image applying Random LSB algorithm. In the steganography phase, the sender and the receiver required to give the same embed key. This key employed for generating same random number in Java. Let the embedding key is N, (it is a seed to a random function in Java), and R is a generated random positive integer number. This number R divides by eight then the remainder value P is a bit place of a byte image.

A. If the P value is 0, then the message bit embeds in the Least Significant Bit of the byte image.
B. If the P value is not zero, and both the message bit and the P position bit of the image byte are same, then that particular P position bit directly considered as a message and the LSB changed to 1. Otherwise, LSB changed to zero.

The sender and the receiver should give the same embedding key. It's only at this time the Java random function generates the same random number on both sides. The algorithm for embedding text message and for extracting text message indicated below with their flow charts as depicted in Fig. 1 and Fig. 2 for the embedding and the extracting consecutively.

A. Algorithm to Embed text in imageSteps
1. Read text messages, cover image, digital watermark text and embedding key.
2. Calculate the Huffman code value of each character in the text message
3. Convert the compressed text message in binary.
4. Calculate the RSA encryption values of each binary message.
5. Convert cover image to binary.
6. Embed watermark using step 8 to 14.
7. Embed binary message through step 8 to 14.
8. For each byte message.
9. For each bit in byte massage.

```
10. Generate random number within the key as seed.
11. Mod the random number by 8.
12. If mod result is 0.
    12.1. Replace LSB byte image by bit message.
13. If mod result is n (n<8) and $n^{th}$ bit byte image is equal to bit message.
    13.1. Make LSB byte image to 1.
14. If mod result is n(n<8) and bit message is not equal to $n^{th}$ bit byte image
    14.1. Make LSB byte image to 0.
15. Write Stego image to file.
```

The output of the embedding algorithm is the stego image (image hidden text behind it). The decoding algorithm includes the reverse steps of the embedding algorithm which are stated as follows.

Algorithm to Decoding text in imageSteps

```
1. Read cover image, Digital watermark text and decoding key.
2. Convert cover image in binary.
3. Extract  watermark using step 6-12.
4. If watermark text is much
5. Extract text message using step 6-12.
6. For each character in text message
7. For each bit in byte message
8. Generate random number with in decoding key as seed.
9. Mod random number by 8.
10. If mod result is 0.
    10.1. Replace bit message by LSB byte image.
11. If mod result is n (n<8 and LSB byte image is 1.
    11.1. Replace bit message by $n^{th}$ bit of byte image
12. If mod result is n(n<8) and LSB byte image
    12.1. Replace bit image by opposite value of nth bit byte image.
13. Calculate RSA value of extracted text message.
14. Calculate Huffman code value of decrypted text message.
15. Write text message to file.
```

A) Embedding algorithm flow diagrams

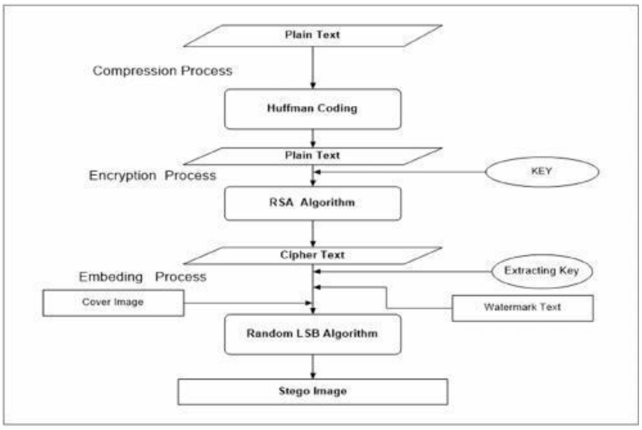


Fig.1 Embedding Flow Diagram

B) Decoding algorithm flow diagram

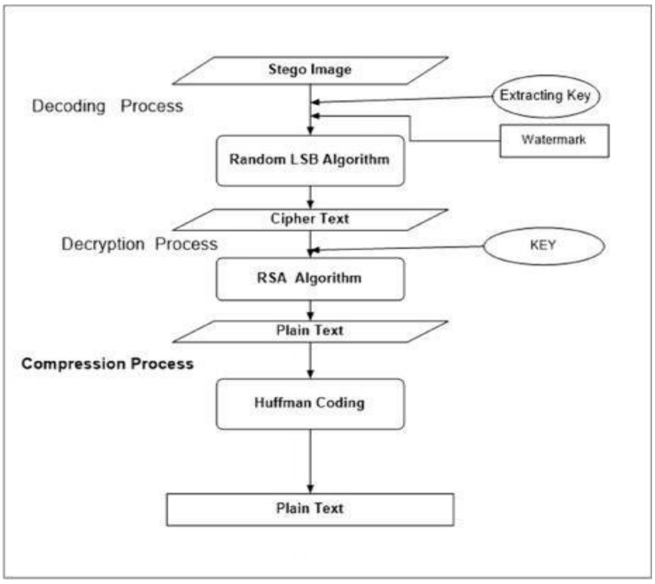


Fig.2 Extracting Flow Diagram

IV. ADVANTAGES OF CEWS TECHNIQUES

CEWS technique has various advantages. Even though, the adversary detects and decodes the secret message behind the Stego image the data have not appeared as plain text. To break 1024 bit key size is also nearly impossible. The third step of CEWS technique is digital watermark the cover image to prevent unauthorized use. Any attempts to extract a Stego image must first know the watermark text. If the text matches with the masked watermark text, then he will be further proceeding with extracting and encrypting of the data. The message embeds not only in LSB but also in any of the eight bits. Selecting the bit image to embed the message is totally randomized. Thus, it is exceedingly hard to speculate the existence of masked data behind the image.

V. EXPERIMENTAL RESULTS

The proposed steganography technique implemented and executed using Java. Various experiments have performed by utilizing several different text messages, cover pictures, watermark texts and embedding keys to check how CEWS technique performed. Both the carrier and the resultant images (Stego image) have compared on the basis of MSE and PSNR. The lower value of MSE implies lower error between the two images. The higher PNSR value signifies that the resultant image is not more distorted (lower error). The compressed message (after compressed using Huffman code) and the modified message (after altering with the help of RSA key) also displayed below for all the cases. The obtained MSE and PSNR values of the cover and the resulting image of all the cases have also displayed below in Table I. This experimental result shows that MSE value is low and PSNR value is high. Hence, the CEWS technique provides sufficiently better PSNR Value and low MSE compared to other imageSteganography. Histograms of resultant images of these experiments are displayed in Figure 3 to Figure 8.

CASE I)
Plain text:
http://www.orbit-computer-solutions.com/Switches.php
Watermark text: negaselomon
*Embed Key***:**3434
*Compressed text***:**
4Àa|Ã¸ð.Ã{ÄF ž,Ýä-Ã- Á —*ƒ*#Ÿ°Ù:Â£rÔÂºOEôàÿ¿*ƒ*
Compressed Text (in bits):
(0011010000011101000100011100000000011101011000010111110011000011101110001111000000010111 01
10000110111101100011100101000001100010001000110100111101000001011011101000110001110010000 0
01101101011011100000111010110111000001100101111000001100100011100111111011000011011001001 11
01011000010101000110111001011010100110000101011101000000001010011110100010111110100111000 0
0111111111011111110000011)

Encrypted Text: †poí¦Ë¶û¹»m²Í"Ú°i¹×ßëG7yk%ž: áþþã -eçv3[Æ 2@“…
.‘ÆßjÉ’^îÃ€»Ï˜ÿ†zô¾YöQ0›'kåÄB6, çQor×
Ú2¼ÈÇÇæÝŽ©x:J+ôÍé!æ0Ž,$`~ÓŸÔy:#·aæWÌ¡Î˜&P}Éî”!>¿å%;GÖŒ†èòEÎŸ,[NÛ®(ÒÙ¢A.ÄŒÂ³¿wÌå}˜•\C
Öm†±ôâ¹~ŸYæÐiÕÕuRä¨~ãÞO(†-dK.§º×z²Â^z9e*uq]7@L\^½ ´ÿßÆþ

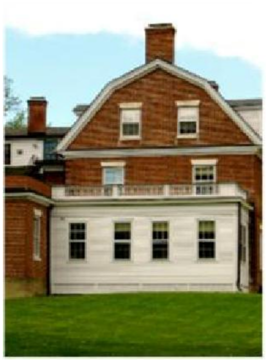


Fig. 3. Brick-house.png

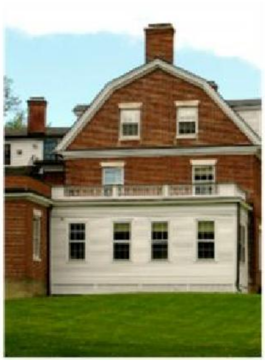


Fig. 4. Brick-houseStego.png

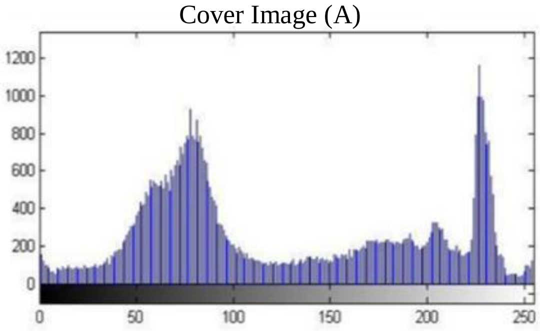


Fig. 5. Histogram of Brick-house.png

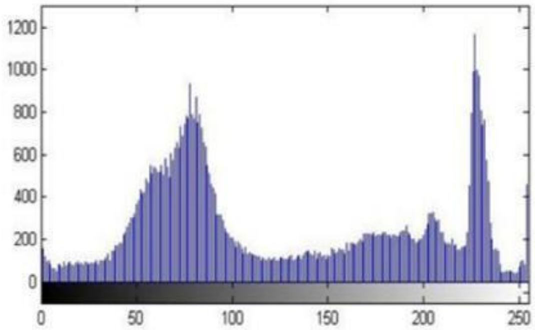


Fig. 6. Histogram ofBrick-houseStego.png

CASE II)
Plain text: Everybody says mistake is the first step to success.
Watermark text: zehabesha *Embed Key*: 4567
CompressedTex:
"†Xä-qŠÑ’ èÃæàÛãK¡ø×ñïFŒ†3<«k!K®‡\kE³€ Compressed Text (in bits)
(00100010100111011000011001011000111001000000111100111000110001010000110111101000110010010100000010000001100001110011101000110000111110011011100000110110111110001101001011000000111010000111111000110101110000101111110001111011110100011010001100100001100011001100111100101010110110101100100001000000111000011000100101110101110100001110101110000000110001101011010001011011001100001011100)
EncryptedText:
§ð´}W#R&B øÍ¨h¾Ó™<³œAœµ¿M<äÖÃbßÆ ô˜ÂM¾È@›cÈg(³gî%â9ý \de
ªálWÅÖøôøð‘}˜³ØËP³ÛgäK6R¼ðÇ¾üÃ»zŠá
aŽE?ò^gŒûh2ºËÇ+V)Qìÿ1!Jö4ïxèê‹.xRCèfÌÑP`jkF•¤àþe/…dz¶_’§è®Ý¬ÓF/

óHÚðb<EØrŠÿýŸîô`<¨Æ@Ã7©Qé<´ÍU+ US'/À‹ -fGÙ…]-ˆèBŒ…ÂÃ:ÅŠaºDhM

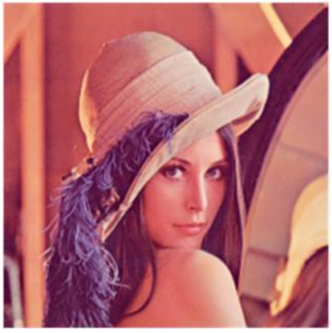


Fig. 7. lena.png

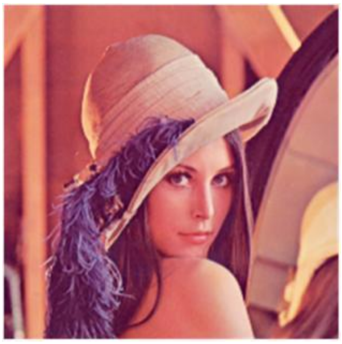
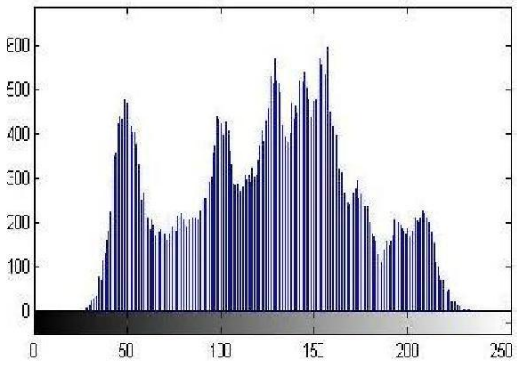


Fig. 8. lenaStego.png

Cover Image B
Fig. 9. Histogram of lena.png



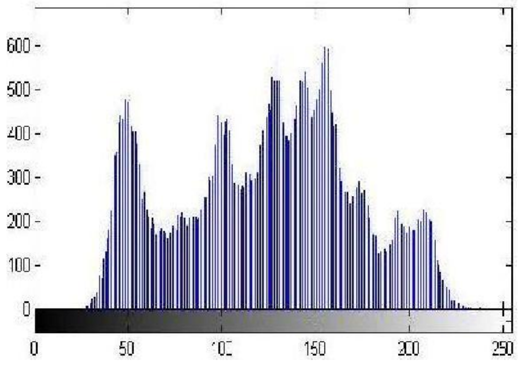


Fig. 10. Histogram of enaStego.png

CASE III)

Plain Text: http://computernetworkingnotes.com/cisco/ccna-study-guide/.
Watermark text: zeabisenya Embed Key: 9854
CompressedText:
4Àa|Ã7ñ´áÔƒ)Ü¼Žèz5ÐÓ¹ã8qÍ,æB=xwÖ|aÀ[•õÆD5ÝoS
Compressed Text (in bits)
(001101000001110100010001110000000001110101100001011111001100001100011000001101111111100011 011010011100001110101001000001100101001000111001001000011011100101111001000111011101000011 110100011010111010000110100111011100100011001111000110011100001110001110011011000001011100 110000101110100001000111101011110000111011110101100111110001100001110000000101101110010101 11111010111000110010001001000111100110101110111010110111101010011000111 0)

Encrypted Text:
˜RE¿š7\ÙrxJÌzƒåùxì ÿ=fH”¥¸UNÒmÐ^‹]3Ó9"Sš*0Zþ• Ó’ægR"ökó¥‹æ1œ€åcX_¹J0\Ï»ÂôÚÓZir@Z[ÍJ¡†¢÷ã¤ê[}ùÞlçä®CYávÇ«„9áÑôÿèàf=¥ÞÍ(îCãŸ¤GÞ\/·xjs„YG|ò:ê ¶,Ž×ð`šüŽ°‹£c&c¢uêKûIË ù:˜Ì°D,/ËÆ²ÌíÏnP•äÎû)»&»Œ³Ö0^h -½âß÷ÿÏÊ¶3Vªf:3úþsÁaáìlöBþö

Fig. 11.Peppers.png

Fig. 12. pepperStego.png

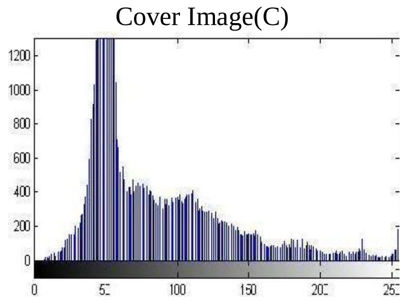


Fig. 13. Histogram of Peppers.png

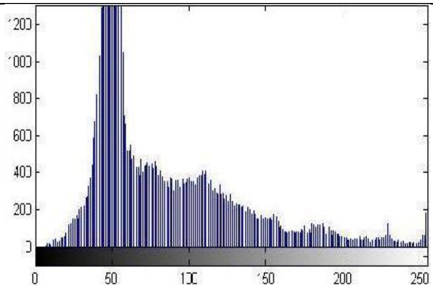


Fig. 14. Histogram of pepperStego.png

All the experimental results of the above three cases are summarized in table-I and table-II. In table-I, the original text (bits) and Huffman code column presents the number of bits before compression and after compression. Compress rate is the ratio of the number of bits before compression by the number of bits after compression. The PSNR and MSE values of the above three cases presented in table-II. The R, G and B column represents Red, Green and Blue components of the image.

VI. CONCLUSION

In the future, researches and project works may continue to change the technique by preprocessing the data in a different approach. A different lossless text compression algorithm or cryptography algorithm may use to make the technique more robust and resistant to attacks. In this technique, the data embeds randomly at any bit's place. Data can embed based on rule based technique. So, the sort of message bits will embed on the basis of value of the pixel. Steganalysis tools are not implemented in this paper so that future projects can work on implementation of Steganalysis to such system.

REFERENCES

[1]. Naghamhamid,Abidyahya and R.badlishahahmad and osamahM.AlQershi, image steganography technique an overview" International Journal of computer science and scientific(IJCSS)-volume 6-issue 3- 2012.

[2]. JyotiGaba, Mukesh Kumar," Implementation of Steganography Using CES Technique" Proc. of the 2013 IEEE Second Int. Co. onImage Information Processing (ICIIP-2013).

[3]. Shailender Gupta, AnkurGoyal and Bharat Bhushan ," Information Cryptography ,"I.J.Modern Education and Comp.Sc.- vol. 6, Jun. 2012.

[4]. JyotiGaba and DrMukeshkumar Sharma," A Review Based Study of Hybrid Security Schemes Based on Compression, Encryption and Steganography," Int.J. Of Engineering Trends and Technology (IJETT) – Volume 4 Issue 7- July 2013.

[5]. Naitik P Kamdar and DharmeshN.khandhar," Implementation of Steganography Using LSB& DCT that Minimizes PSNR & MSE." Int. Journal of Futuristic Science Engineering and Technology-Vol 1 Issue 2- February 2013.

[6]. SanjeevManchanda, Mayank Dave and S. B. Singh," Customized and Secure Image Steganography Through Random Numbers Logic." Proc.ISSN (Online)- Volume 1 -Issue1-31-06-2007.

[7]. G. Swain and S. K. Lenka, "A Hybrid Approach to Steganography Embedding at Darkest and Brightest Pixels," in IEEE Proc. Int. Conf. on Communication and Computational Intelligence, 2010.

[8]. S. Gupta et al., "Information Hiding Using Least Significant Bit Steganography and Cryptography," I. J. Modern Educ. and Comp. Sci., vol. 6, Jun. 2012.