Design of Image Steganography & Symmetric Cryptography for Image hiding by using DWT

Hemant Sharma[1], Aumreesh Kumar Saxena[2], Abhigyan Tiwari[3]
[1,2,3]Dept. of CSE, SIRTS, Bhopal (M.P.) India.

ABSTRACT
The combination of encryption and invisibility of encrypted data, it unchanged the message entirely protected against data espionage. This concept can also provide an easy means to exchange imperative messages in a message. Based on this concept, we proposed a new encryption algorithm that providing confidentiality and authentication for secure data and this data is hiding behind cover image by using proposed steganography algorithm having less cover size. Another concept we used in this that is discrete wavelet transform which is applicable on large size of secretes image data to compress. PSNR and Entropy of stego image is showing the effectiveness of proposed algorithm.

Keyword: Security, Cryptography, Encryption, Decryption, Steganography, Wavelet Transform

I INTRODUCTION

The uses of digital media and transmission of the information is easiest way through network in today world just because of expansion of internet knowledge [1]. However, the transmission of secret messages through the Internet system suffers serious security expenses [2]. Therefore, the fortification of top secret messages for the period of transmission becomes an important issue. Although cryptography changes the message so that it can't be understood, this can generate the level of curiosity of a hacker [3]. It would be much more sensible if the secret message is integrated intelligently in another medium so that no one can guess if there is something hidden there or not. This thought in steganography, which is a subdivision of information that is secreted by hiding secret information inside other information [4]. The word stegano-graphy in Greek means "covered writing" (Greek words "stegos" meaning "cover" and "graffia" meaning "writing") [4]. The key objective of steganography is to hide a secret message inside harmless means of coverage in such a way that the observer can't see the secret message [5]. Therefore, the stego image should not diverge much from the original cover image. In this generation, steganography is used primarily in computers with digital data that are operators and networks are high-speed delivery channels [6]. Here figure 1 is showing that the basic structure of the steganography.

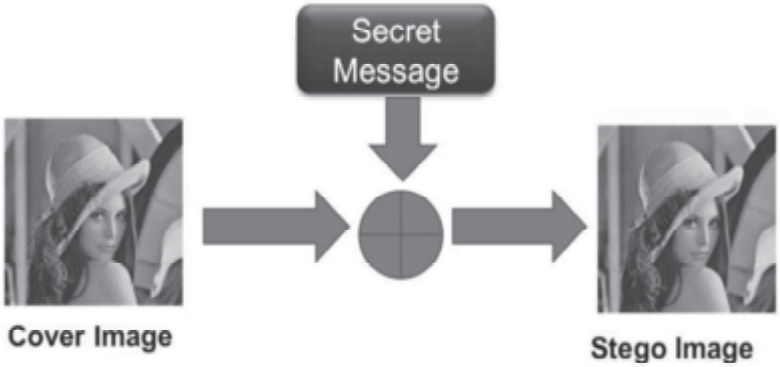


Fig. Error! No text of specified style in document.**: Block diagram of steganography system**

Cryptography and steganography are measurably two traditions of trouncing messages, they are corresponding, and they are not the same.

Organization of the paper is as follow: section-I is presetting introduction, section-II is presenting literature survey. Section-III is presenting proposed work, Section-IV is presenting results and section-V is presenting conclusion.

II LITERATURE SURVEY

A new steganography method proposed by [7] which included two methods, one is symmetric key cryptography and another is wavelet transformation. In this steganography method, secrete data is selected and if it is an image then authors apply image compression technique to reduce the size of image. Here they used lossless wavelet transformation for image compression. After that compressed image pass to the proposed symmetric cryptography to encrypt. At last proposed steganography method apply on encrypted data and authors used standard LSB mechanism.

Another image steganography approach is presented in [8] where the cover image is splitting into 2×2 non-overlapping pixel blocks. The upper-left pixel of that block embeds a certain number of bits of the secret bit stream. Whereas, the remaining pixels of the same block embed the secret data using a advancement of the 'pixel-value-differencing' (PVD) technique that considers concealing confidential message into both vertical and horizontal edges.

Haar Discreet Wavelet Transform (HDWT) method for data hiding along with Advanced Encryption System (AES) for encrypting the data is proposed by [9]. The aims of HDWT is to reduce the difficulty occur during normal steganography while providing low image distortion and lesser detection ability. In this method, one portion of the cover image carry the details of the one-fourth of the image and rest of the portion of the cover image carry less details of the image then the cipher-text is hidden at most two LSB positions in the less detailed portion of the cover image, second LSB used if and only if the message does not fit in the first LSB

In [10] we propose a Discrete Wavelet Transform (DWT) based high capacity steganography using coefficient replacement with increased security by adapting an encryption of payload Image. The Haar and biorthogonal DWT is applied separately on cover image and Advanced Encryption Standard (AES) with modification is applied on payload to convert payload image into an encrypted image. The resulted coefficients of payload image are embedded inside the high frequency bands of cover image. The new concept of replacing HH sub band coefficients by encrypted payload is introduced to generate intermediate stego image.

In [11] another combination of cryptography and steganography is presented. Here cryptography is used to encrypt the data and then steganography conceal to encrypt data in cover image so two layer of security can be applicable on a confidential data.

Picture quality based on PSNR and uncertainty (entropy) in the produced stego image are the two parameters which is play important role to evaluate the performance of any steganography technique. In [7, 8 and 9] produced PSNR is not satisfactory and basically PSNR is giving the picture quality of original cover image and produced stego image. For example if a cover image has 100% picture quality then stego image should near about 100%. Similarly uncertainty (entropy) mean differences between original cover image pixel and produced stego image pixel. For example if a pixel of cover image has third position and same pixel has 78th position in stego image, then this is representing the uncertainty which is calculated as entropy. In [10 and 11] producing low entropy which can be increased.

III PROPOSED WORK

The proposed encryption algorithm is simple and efficient against existing algorithms. It has a key of 128-bits long which has enhancing its security. Its structure is robust against an assortment of attacks. Adding a steganography procedure increases its security, the proposed steganography is implemented in such a way that it improves the quality of cover file without changing the cover file size. Here the secrete message which is image using wavelet transform compression mechanism to compress the size of the image and this compression is not for text data. Proposed encryption applies on compress data to encode and this encoded data is concealing behind a cover image by using proposed steganography mechanism.

Fig.-2 is showing the sender side steganography architecture where secrete message 'SI' is required wavelet transformation 'WT' to compress 'COM' data if it is image. Here Lossless 'L' wavelet transformation is used. Once we completed 'WT' step if its applicable then proposed encryption 'E' encoded that data with key 'K' of 128-bits. At last steganography 'S' is applied on encoded data which is required a cover image 'CI'. Standard least significant bit (LSB) mechanism is using to implant encoded data to produce stego image 'SIm'.

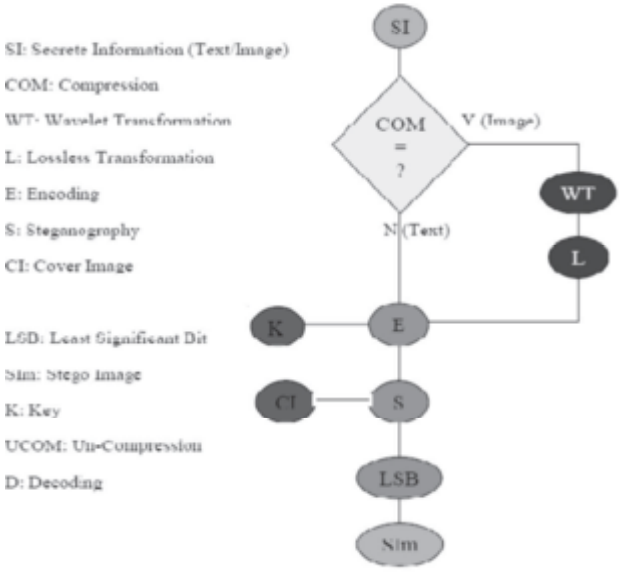


Fig. 2: Encryption of Proposed Steganography

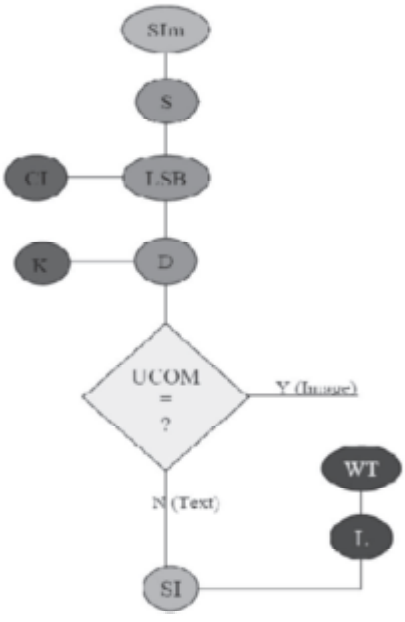


Fig. 3: Decryption of Proposed Steganography

Fig.-3 is showing the receiver end steganography architecture. Here stego image 'SIm' work with steganography 'S' which interpret 'LSB' of 'SImg'. Once we get 'LSB' of 'SImg' which is encoded by encryption mechanism pass to propose decryption 'D' mechanism to decode and rest of the value make cover image 'CI'. Key 'K' is used in decoding, once we decode the data, we apply wavelet compression 'WT' mechanism to uncompress 'UN-COM' data to get secrete image 'SI' if data is text then no need of 'WT'

(a) 'Wavelet-Transform' Method - Lossy and Lossless are two wavelet compressions method are available [12] where lossless compression provide the facility to get original image from compressed image, but this is not possible with lossy compression because its support to the partial reconstruction of the original image. As we know that wavelet transformation is the facts which is required few space to store compressed data, due to this mechanism large image can be easily transferred from one place to another [13].

(i) Steps In 'Wavelet-Compression'

- Initially select secrete image
- Apply 'Wavelet-Decomposition' on the secrete image,
- At last 'compress' through fixed 'Threshold'.

(b) Proposed 'Encryption/Decryption' Architecture- Fig.-4 is presenting the encryption architecture. Initially 128-bits of secrete message interpreted which is splitting in two part each one is 64-bits and each part of secrete message performing circular shifting operation in sequential manner. XOR operation is performing with key which is also split in two parts of 64-bits to get cipher message.

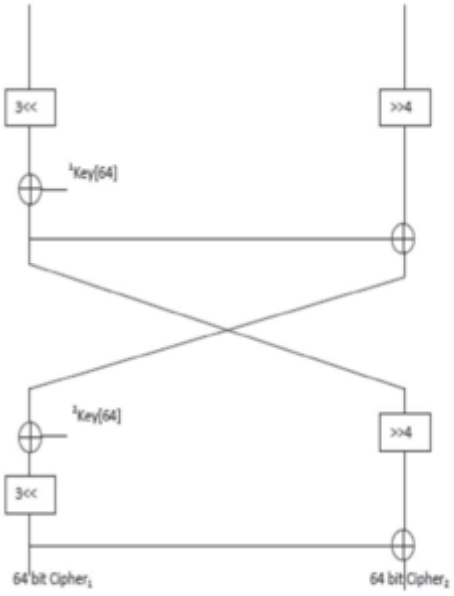


Fig. Error! No text of specified style in

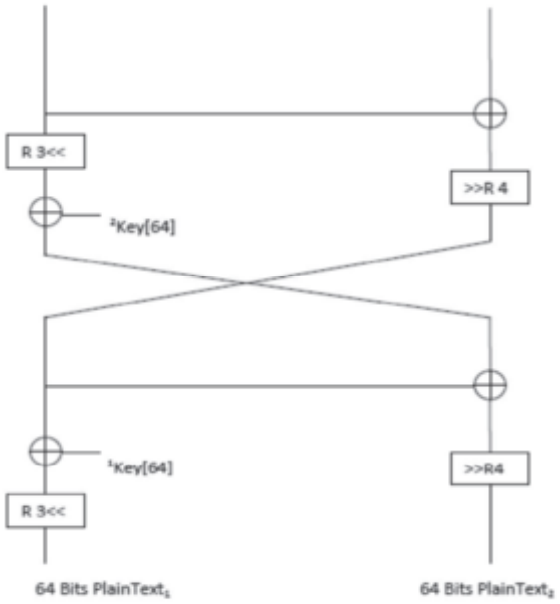


Fig. 5: Proposed Decryption Architecture

Fig.-5 is presenting the architecture of proposed decryption. Initially 128-bits cipher data is splitting in two part 64-bits each, and each part of cipher data performing circular shifting operation in sequential manner and XOR operation is performing with key to get original secrete message.

(i) Algorithm of 'Proposed Encryption'

- Loop on Input Message 1to N
- Select secret message in terms of bits
  bits→ 128-bits
- Select Key
  K→ 128-bits
- Split bits and K
  bits = bits/2→ (^{1}bits, ^{2}bits)
  K = K/2→ (^{1}Key, ^{2}Key)

- Perform Shifting on 1bits, 2bits
  ^{1}bits= Left_Circular_Shift_3 (^{1}bits)
  ^{2}bits= Right_Circular_Shift_4 (^{2}bits)
- Perform XOR between 1bits & 1Key
  ^{1}bits = ^{1}bits $\bigoplus$ ^{1}Key
- Perform XOR between 1bits, 2bits
  ^{2}bits = ^{1}bits $\bigoplus$ ^{2}bits
- Interchange Value of 1bits, 2bits
  ^{2}bits = b_1 → ^{2}bits
  ^{1}bits = ^{2}bits → ^{1}bits
- Perform XOR between 1bits & 2Key
  ^{1}bits = ^{1}bits $\bigoplus$ ^{2}Key
- Perform Shifting on b1, b2
  ^{1}bits = Left_Circular_Shift_3 (^{1}bits)
  ^{2}bits= Right_Circular_Shift_4 (^{2}bits)
- Perform XOR between 1bits & 2bits
  ^{2}bits = ^{1}bits $\bigoplus$ ^{2}bits
- Loop End
- End

(ii) Algorithm Of 'Proposed Decryption'

- Loop on Cipher message (Cipher_bits) 1to N
- Select Cipher Message
  Cipher_bits → 128-bits
- Select Key
  Key→ 128-bits
- Split Cipher_bits and K
  Cipher_bits = Cipher_bits /2→ (Cipher_bits1, Cipher_bits2)
  Key = Key/2→ (1Key, 2Key)
- Perform XOR between Cipher_bits1 & Cipher_bits2
  Cipher_bits2 = Cipher_bits1 $\bigoplus$ Cipher_bits2
- Perform Shifting on Cipher_bits1, Cipher_bits2
  Cipher_bits1 = Left_Circular_Shift_3 (Cipher_bits1)
  Cipher_bits2 = Right_Circular_Shift_4 (Cipher_bits2)
- Perform XOR between Cipher_bits1 & 2Key
  Cipher_bits1 = Cipher_bits1 $\bigoplus$ 2Key
- Interchange Value of Cipher_bits1, Cipher_bits2
  Cipher_bits2 = Cipher_bits1→ Cipher_bits2
  Cipher_bits1 = Cipher_bits2→ Cipher_bits1
- Perform XOR between Cipher_bits1 & Cipher_bits2
  Cipher_bit2 = Cipher_bits1 $\bigoplus$ Cipher_bits2
- Perform XOR between Cipher_bits1 & 1Key
  Cipher_bits1 = Cipher_bits1 $\bigoplus$ 1Key
- Perform Shifting on Cipher_bits1, Cipher_bits2
  Cipher_bits1 = Rev_left_Circular_Shift_3 (Cipher_bits1)
  Cipher_bits2 = Rev_Right_Circular_Shift_4 (Cipher_bits2)
- Combine Cipher_bits1 and Cipher_bits2 to get 12- bits Cipher_bits as a cipher
  Cipher_bits = Cipher_bits1 $\bigcirc$ Cipher_bitsC2
- Replace Cipher_bits (Cipher value) into Plain_Text as Original value
  Plain_Text = Cipher_bits
- End Loop
- Exit

(c) Steganography Algorithm - Proposed Encryption/Decryption algorithm provide high security but still intruders can try to crack the keys, to strengthen the proposed architecture, the encryption/decryption algorithm is combined with steganography algorithm. Here proposed an efficient steganography algorithm which is the extension of LSB method. Steps of proposed steganography algorithm are as follow:

(iii) Sender End Algorithm

- Start
- Select Cover Image as (CImage)
  CImage = Image→ CImage
- Select Secrete Message as Binary_MSG
- Loop Binary_MSG 1 to N
- Binary_MSG = Binary_MSG →128-bits
- Interpret binaries of secret message as Binary_MSG and CImage
  Binary_Value_ Binary_MSG = BReader (Binary_MSG)
  Binary_Value_CImage = BReader (CImage)
- Interpret 'LSB' of CImage
  LSB_CImage = LSBReader (CImage)
- Substitute LSBCImage from Binary_Value_ Binary_MSG
  LSB_CImage = Binary_Value_ Binary_MSG
- Loop End
- End

(d) Receiver End Steganography

- Select Stego Image as SImage
  SImage = Image→SImage
- Loop SImage 1 to N
- Interpret Binaries of SImage
- Binary_SImage = Binary_Read (SImage)
- Interpret LSB of Binary_SImage
  LSB_Binary_SImage = LSB_Reader (Binary_SImage)
- Implanted LSB_Binary_SImage as secret message
  Binary_MSG = Implanted_LSB (LSB_Binary_SImage)
- Loop End
- End

IV RESULTS

Hear results are showing the competence of the proposed concept that is based on selected performance attribute. For a concept it is imperative to be proficient and secure. Performance of an algorithm is evaluated on the bases of selected parameters and here proposed system has chosen one performance parameters that is execution time for encryption/decryption algorithm and measurement used parameters are Entropy, Correlation and Peek Signal to Noise Ratio (PSNR) for steganography algorithm [14]. Desktop device has been used to compute experimental outcome. Configuration of desktop device is following (See Table 1)

Table 1
Configuration

S. No.	Processor	Memory(Primary)	Platform	Software Application
1	Intel Core i3 2.67 Ghz,	2 GB of RAM	Window-7 Home Basic SP1	Dot Net 2008

(a) Time Examination - It is essential for any technique that it should be time competent. Encryption and Decryption process is used for secrecy, but this secrecy is applied numerous times on real time information, if the encryption and decryption progression is not time proficient than it can't be used for actual time broadcast. The execution time is deliberate the instance that an encryption/decryption algorithm takes to construct a plain text to cipher text and cipher text from a plaintext respectively [15]. Experimental outcome of the proposed encryption/decryption algorithm is presents in Table 2.

Table-2
Assessment of Time of Encryption/Decryption in millisecond of Proposed-Algorithm with AES on different Size of File

Size of File in KB	Methods	
	Time of execution in Millisecond	
	Proposed-Algorithm	AES
5	0.140	0.201
10	0.597	0.681
20	2.252	3.038

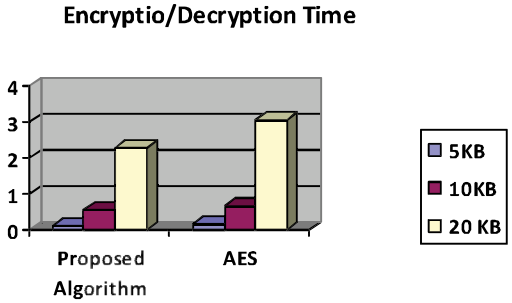
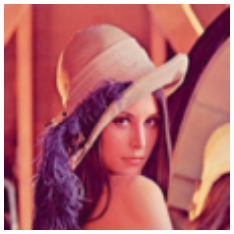


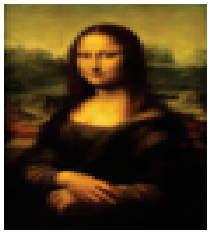
Fig. 6: Encryption/Decryption time of the proposed encryption/decryption algorithm

It is clearly seen from the Table 2 that proposed encryption/decryption algorithm is time efficient. Hence it is suitable for real time data transmission. A graphical representation for the encryption/decryption time is shown in Figure 6. From Figure 2, it is clearly seen that proposed encryption/dercyption time is much lesser than the other existing encryption algorithm. It shows the efficiency of proposed encryption algorithms. It proves that proposed encryption algorithm can be suitable real time communication.

(a) PSNR and Entropy Examination -This work has proposed its own steganography technique. Therefore it is important to ensure its effectiveness. To ensure the effectiveness of proposed steganography algorithm, I have evaluated two parameters that are entropy and PSNR [16]. Proposed algorithm run numerous time on various size of secrete image file shown in table 3 with two cover image shown in figure 7 and measure the performance.



(a) "Lena.jpg"



(b) "Monalesa.jpg"

Fig. 7: Cover-Images

(b) Peek-Signal to Noise-Ratio (PSNR) - For PSNR calculation we need MSE (Mean Squared Error) and PSNR equation which are as follow:[17]

$$MSE = \frac{\sum_i \sum_j |x(i,j) - y(i,j)|^2}{\cdot\cdot}$$

$$PSNR = 10log_{10}\frac{(L-1)^2}{MSE}$$

Table 3
PSNR Evaluation of Proposed Steganography Algorithm on Cover Image Lena.jpg

Input		PNSR	
Secrete Image	**Size in KB**	**Proposed Algorithm**	**Existing[7]**
Image1	1.85	44.38	43.41
Image2	2.72	44.41	43.42
Image3	3.68	44.41	43.42
Image4	4.36	45.40	43.50
Image5	9.35	45.41	43.51

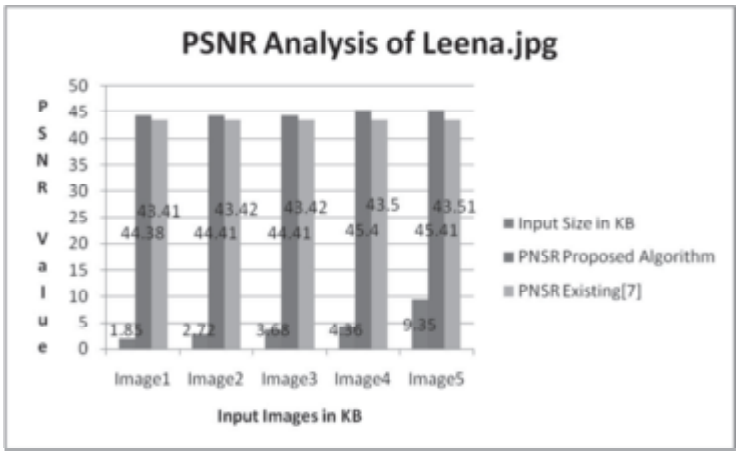


Fig. 8: PSNR analysis of Proposed Steganography Algorithm on Cover Image Lena.jpg

Table 4
PSNR analysis of Proposed Steganography Algorithm on Cover Image Monalesa.jpg

Input		PNSR	
Secrete Image	**Size**	**Proposed Algorithm**	**Existing [7]**
Image1	1.85	44.38	43.41
Image2	2.72	44.41	43.42
Image3	3.68	44.41	43.42
Image4	4.36	45.40	43.50
Image5	9.35	45.41	43.51

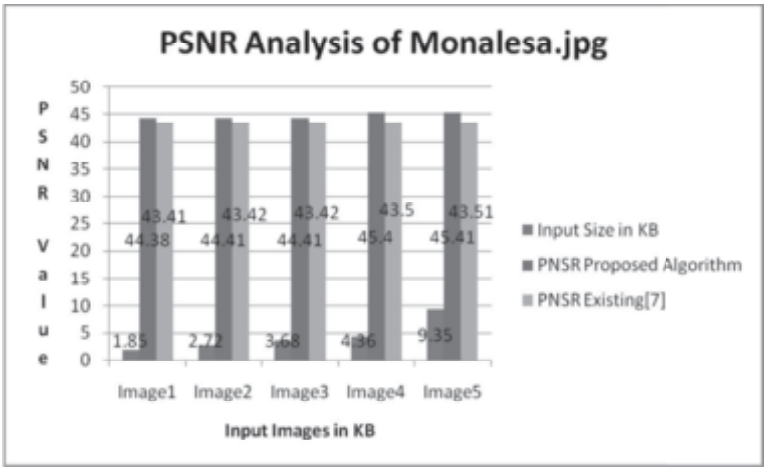


Fig. 9: PSNR analysis of Proposed Steganography Algorithm on Cover Image Monalesa.jpg

(c) Entropy Analysis

Entropy defined as follows [17].

$$H_e = -\sum_{k=0} P(k) \log_2 (P(k))$$

Table 5 and 6 is showing the Entropy performances between proposed and exiting concept over text and image of various size.

Table Error! No text of specified style in document.

Entropy analysis of Proposed Steganography Algorithm on Cover Image Lena.jpg

Input		Entropy	
Secrete Image	**Size**	**Proposed Algorithm**	**Existing[7]**
Image1	1.85	0.621	0.6138
Image2	2.72	0.622	0.6212
Image3	3.68	0.624	0.6352
Image4	4.36	0.632	0.6447
Image5	9.35	0.634	0.6447

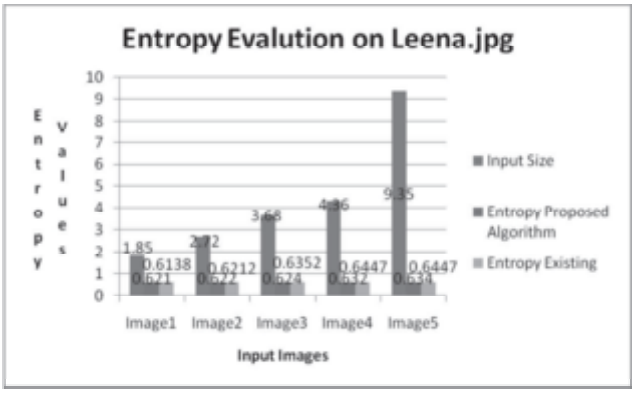


Fig. 10: Entropy analysis of Proposed Steganography Algorithm on Cover Image Lena.jpg

Table 6

Entropy analysis of Proposed Steganography Algorithm on Cover Image Monalesa.jpg

Input		Entropy	
Secrete Image	**Size**	**Proposed Algorithm**	**Existing[7]**
Image1	1.85	0.621	0.6138
Image2	2.72	0.622	0.6212
Image3	3.68	0.624	0.6352
Image4	4.36	0.632	0.6447
Image5	9.35	0.634	0.6447

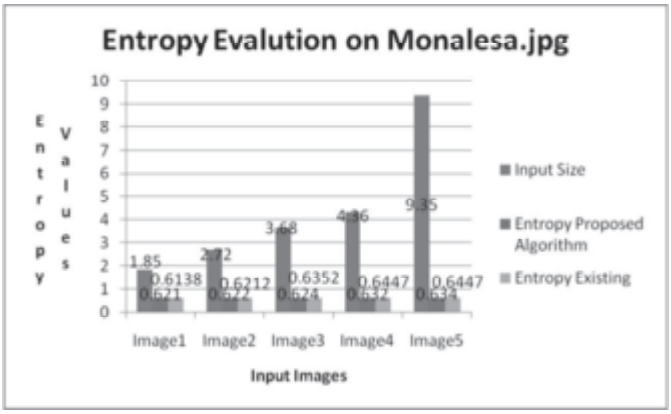


Fig. 11: Entropy analysis of Proposed Steganography Algorithm on Cover Image Monalesa.jpg

(d) Results Discussion- Calculated results are shown in table 3 to 6 for PSNR, and Entropy parameters on various image data as an input data and monalesa.jpg and Leena.jpg both are selected as cover image. Table 3 and figure 8 shown "PSNR" results 43.41 for image1 over lena.jpg cover image with existing algorithm and "PSNR" results 44.38 with proposed algorithm which is good as compare existing. Similarly table 4 and figure 9 is producing 43.41 "PSNR" with existing algorithm and 44.38 with proposed algorithm. For both results it is very clear the proposed algorithm having good results of PSNR as compare exiting. Table 5 and figure 10 showed Entropy 0.644 for image1 over lena.jpg cover image with existing algorithm and 0.634 with proposed algorithm. Similarly table 6 and figure 11 is shown entropy 0.644 with existing algorithm and 0.634 with proposed algorithm. Entropy results clearly shown that proposed algorithm is producing superior results as compare existing. Proposed security system considers the key size as a measure to evaluate the performance of the proposed concept. The obtainable experimental outcome shows the superiority of the proposed technique over other technique in terms of the processing execution time, entropy and PSNR.

V CONCLUSION

The earlier presented techniques are time consuming. So it is required to develop a fast encryption technique. In this research work, a new selective steganography technique based on a combination between LSB image hiding, and a proposed encryption method is introduced. Another image compression concept is used for image data. Here lossless wavelet transformation image compression is used along with proposed encryption and steganography. Presented outcome of the proposed method proved that proposed encryption is time efficient as compare exiting, and proposed steganography is more safe and having low deformation of the cover image. Proposed method can be applicable on any type of network because of its simplicity and portability. The proposed encryption gives remarkable execution time as compare AES for large size of data files. PSNR of stego image show that proposed steganography is batter then earlier presented technique. There are very less differences between original cover image and setgo image. In future proposed method will include all type of multimedia data file like audio, vedio and many more.

REFERENCES

[1] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption "2010 IEEE International Conference on Electronics and Information Engineering (ICEIE 2010) Pages(s): V1-141-V1-145, Japan 2010

[2] Ashwak M. AL-Abiachi, Faudziah Ahmad and Ku Ruhana "A Competitive Study of Cryptography Techniques over Block Cipher" UKSim 13th IEEE International Conference on Modelling and Simulation Pages(s):415-419 UK 2011

[3] N. Akhtar, ; P. Johri, ; S Khan, "Enhancing the Security and Quality of LSB Based Image Steganography" 5th International Conference on Computational Intelligence and Communication Networks (CICN), Page(s): 385 – 390 India 2013,

[4] R.P Kumar, V. Hemanth, M "Securing Information Using Sterganoraphy" International Conference on Circuits, Power and Computing Technologies (ICCPCT), Page(s): 1197 – 1200 India 2013,

[5] G Prabakaran, R. Bhavani, P.S. Rajeswari, "Multi secure and robustness for medical image based steganography scheme" International Conference on Circuits, Power and Computing Technologies (ICCPCT), Page(s): 1188 – 1193, India 2013,

[6] ZHANG Yun-peng, ZHAI Zheng-jun, LIU Wei, NIE Xuan, CAO Shui-ping, DAI Wei-di "Digital Image Encryption Algorithm Based on Chaos and Improved DES" "Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics Page(s): 474-479, USA – 2009

[7] Aumreesh Kumar Saxena , Dr. Sitesh Kmar, Dr. Piyush Shukla " Design and Development of Image Security Technique by Using Cryptography and Steganography: A Combine Approach" I.J. Image, Graphics and Signal Processing, 2018, 4, 13-21 DOI: 10.5815/ijigsp.2018.04.02

[8] Mohamed M. Fouad Enhancing the imperceptibility of image steganography for information hiding Federated Conference on Computer Science and Information Systems (FedCSIS) Pg No 545-548 2017 Czech Republic

[9] Essam H. Hpussein, Mona A.S. Ali & Aboul Ella Hassanien An Image Steganography Algorithm using Haar Discrete wavelet Transform with Advanced Encryption System Federated Conference on Computer Science and Information Systems (FedCSIS) Pg No. 641-644 2016 Poland

[10] Ravi S P and Dhanalakshmi L "DWT and Modified AES based Secure Image Steganography on ARM A8 Processor" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 4 Issue 05, May-2015

[11] E. Yuva Kumar, P. Padmaja E. Yuva Kumar "RSA Based Secured Image Steganography Using DWT Approach" Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 8(Version 1), August 2014, pp.01-04

[12] Ismael Abdul Sattar; Methaq Talib Gaata "Image steganography technique based on adaptive random key generator with suitable cover selection" Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Page(s):208-212 Iraq-2017

[13] Aumreesh Kumar Saxena, Dr. Sitesh Kumar Sinha and Dr. Piyush Shukla "Design and Development of Symmetric Cipher for Text Data" in SPRINGER, International Conference on Recent Advancement in Computer Page no.- May 2017 Bhopal India.

[14] Jaeyoung Kim; Hanhoon Park; Jong-Il Park "Image steganography based on block matching in DWT domain" IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Page(s):1 – 4, Italy2017

[15] Aumreesh Kumar Saxena, Dr. Sitesh Sinha and Dr. Piyush Shukla "Design and Development of Image Security Technique by Using Cryptography and Steganography: A Combine Approach" I.J. Image, Graphics and Signal Processing, 2018, Vol. 4, Page 13-21 ISSN: 2074-9082