Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Enhancing Security through Steganography by using Wavelet Transformation and Encryption

Depavath Harinath[1], Mrs.B.Chithra[2],M.V.Ramana Murthy[3]
[1]Dept.of Computer Science, HRD Degree and PG College.Narayanaguda, Hyderabad,Telangana.
[2, 3] Dept. of Computer Science,OSmania University.Hyderabad,Telangana.

Abstract— The technique of standard Steganography allows the secrete information for not being perceptible to a viewer. Moreover, there is another technique that is normally used to enhance the security of the information, which is usually called Cryptography. Cryptography is also the skill and knowledge of transforming information into a series of bits that appears as arbitrary and worthless for the viewer. The encryption/decryption process have gained high recognition in broadcast of secrete information like images and those generated for the security organizations which may enclose images of tactical planning information and geographical position images. However, the amalgamation of Steganography and Cryptography that is proposed can be useful for improving the security of secrete information. This paper provides an easiness of exchanging confidential information secretly between a sender and a receiver with multimedia files like images. This paper depicts the Enhancing Security through Steganography by using Wavelet Transformation and Encryption mechanism.

Keywords— Network Security, Steganography, Wavelet Transformation, Encryption.

I. INTRODUCTION

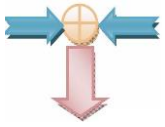
As the development of Internet technologies increases, the transmission of digital media is now-a-days convenient over the networks. But secret information broadcasting over the network suffers from severe security overhead. So, defensive of secret information for the period of transmission becomes a significant matter [1]. Though cryptography changes the message so that it cannot be understood but this can generates curiosity level of a hacker. It would be rather more sensible if the secret message is cleverly embedded in another media so that no one can guess if anything is hidden there or not [2,3]. This idea results in steganography, which is a branch of information hiding by camouflaging secret information within other information. The word steganography in Greek means "covered writing" (Greek words "stegos" meaning "cover" and "grafia" meaning "writing") [5]. The main objective of steganography is to hide a secret message inside harmless cover media in such a way that the secret message is not visible to the observer. Thus the stenography image should not diverge much from original cover image. In this generation, steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels [6, 7].

The following formula can provide a very generic description of the steganography process:

Cover Information + Secrete Information + stego key = stego Information

In this formula, the cover information is the box file in which we hide the secrete information, which may also be encrypted through special key called the stegos key. The resultant file is the stegos data which will be of the same type as the cover data [8,10]. The cover data and stegos data are typically image.


Secret Image




Cover Image of size N x N

Figure(1): The block diagram of a simple steganography system

Normally, the large amount is fixed in a cover image; the more identified artifacts would be introduced into the stegos [11]. As per many applications, the most important requirement for steganography is unidentified, which means that the stegos should be visually and statistically same to the cover image while keeping the fixed rate as high as possible. Figure 1 shows the block diagram of a simple image steganography system. The amalgamation of Steganography and Cryptography that **is** proposed can be useful for improving the security of secrete information [13,14]. The following formula can give us a effective standard way of the security Process:

Cryptography → (Hidden Data) → (Cipher Data) → Steganography → Cover Data → Stego Data

In this formula two level of security have used one is cryptography and another is used steganography. Initial our secrete data protected with strong cryptography technique and it converted into cipher data by using a secure key value this is primary level of security then after cipher data once again hidden in cover data through standard steganography technique. By using this concept proposed work in this paper has propose a new cryptography algorithm which is working with the combination of an efficient steganography technique [14].

II. LITERATURE SURVEY

In [1] a multi secure and robustness of medical image based steganography scheme is proposed. This proposed technique provides an efficient and storage security mechanism for the protection of digital medical images. In this Integer Wavelet Transform (IWT) is used to protect the MRI medical image into a single container image. The container image was taken and flip left was applied and the dummy container image was obtained. Then the patient's medical diagnosis image was taken as secret image and Arnold transform was applied and scrambled secret image was obtained. In the first case, the scrambled secret image was embedded into the dummy container image and Inverse IWT was taken to get a dummy secret image. In the second case, the container image was taken and fused with the dummy secret image and stego image was obtained. In [2] is concerned with implementing Steganography for images, with an improvement in both security and image quality. The one that is implemented here is a variation of plain LSB (Least Significant Bit) algorithm. The stegoimage quality is improved by using bit-inversion technique. In this technique, certain least significant bits of cover image are inverted after LSB steganography that co-occur with some pattern of other bits and that reduces the number of modified LSBs. Thus, less number of least significant bits of cover image is altered in comparison to plain LSB method, improving the PSNR of stego image. By storing the bit patterns for which LSBs are inverted, message image can be obtained correctly.

In [3] presented technique before embedding the secret information into an image, the secret information has been compressed using the wavelet transform technique. The obtained bits after compression are encoded using quantum gates.

In [4] the proposed work presents a exclusive technique for Image steganography which is based on the Data Encryption Standard (DES) through the power of S- Box mapping & private key. The preprocessing of confidential image is passed by embedding function using two unique Sboxes. The preprocessing provides echelon of security as extraction is not likely without the acquaintance of mapping policy and private key of the function. Furthermore the proposed concept is accomplished of not just scrambling information but it also alters the intensity of the pixels which contributes to the security of the encryption.

In [5] I have analyzed that author proposes three native methods as a variation of Cipher Block Chaining (CBC) mode for image encryption/decryption by allowing for three various traversing path (Vertical, Horizontal, and Diagonal). In this one easy Raster Scan has been engaged to scramble the secrete Image called Horizontal Image Scrambling (HIS). Second Process is a variation of technique first called Vertical Image Scrambling (VIS), here traversing pathway probable top to bottom and left to Right. Process third employs diagonal traversing pathway called Diagonal Image Scrambling (DIS). At last standard Image Steganography has been adapted to mail these jumbled Images in an unremarkable manner in [6] a tutorial review of the standard steganography techniques appeared. The least-significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image with high capacity, while it is detectable by statistical analysis such as RS and Chi-square analyses. In [9] articulated an algorithm of information hiding through cryptography called as ASK algorithm. Confidential data is protected in a color full image through cryptography which shows how information can be send through a color full image without unawareness of third party users.

In [10] inattentive on the amalgamation of cryptography and steganography techniques and a technique – Metamorphic Cryptography proposed. The information is transformed into a image called cipher image through a key value, hidden into another image called cover image through steganography technique by converting it into an intermediary text and lastly transformed once yet again into an image. The complexity of cryptography does not permit many users to actually recognize the motivations and therefore accessible for enthusiastic security cryptography. Hence, in [11] described and reviewed the various research works that has done in the direction of text encryption and description in the block cipher. Furthermore, in this suggests a cryptography model in the block cipher. There are lots of security issues in data message.

III. PROPOSED ALGORITHM

Wavelet Transformation: Wavelet transformation technique is compression technique which is reduced the size of the information and its applicable for large information like image. Basically it is two type, one is lossy and another is lossless in which lossless is used when original information is required without any lossless in the information otherwise lossy transformation is used because its loss some information during un-compression [3]. With the help of such technique we can reduce the size of original information and efficiency can be increased. In this first of all input the secrete image and perform wavelet transformation compression of the image through predefined threshold value [3]. Similarly during uncompression, first load the image and perform wavelet transformation un-compression to get the original image.

Proposed Encryption Approach: Figure 2 is showing the architecture of proposed encryption technique. Here secrete information dived into its binary value and at a time 128 bits block selected to perform operation during whole process. Now selected 128 bits value divide into two sub parts of 64-64 bits as a left and right sub parts respectively. Then apply series of operation like circular shifting (left and right) followed by XOR operation between selected key value and other sub parts. Detailed steps of the proposed encryption technique are shown in section of algorithm.

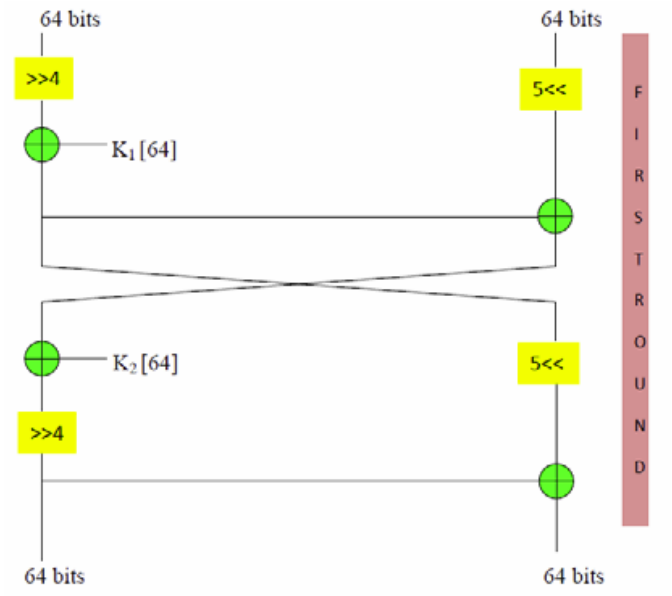


Figure 2: Architecture of Proposed Encryption

Proposed Decryption Approach: Figure 3 is showing the architecture of proposed decryption technique. Here cipher information dived into its binary value and at a time 128 bits block selected to perform operation during whole process. Now selected 128 bits value and divide into two sub parts of 64-64 bits as a left and right sub parts respectively. Then apply series of operation like circular shifting (left and right) in reverse order followed by XOR operation between selected key value and other sub parts. Detailed steps of the proposed decryption technique are shown in section of algorithm.

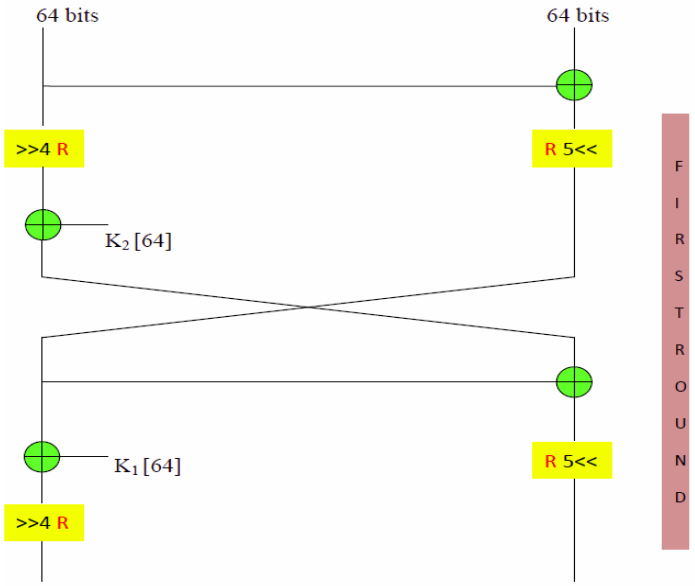


Figure 3: Architecture of Proposed Decryption

Algorithm Step: Proposed encryption/decryption algorithms Step are defining in next section.

Algorithm of Proposed Encryption

1. For b = 1to N bits
2. Input Confidential Information at a time
   b→ 128 bits

3. Input Key Value
   K⟶128 bits
4. Divide b and K into two sub parts
   b = b/2⟶ (b1, b2)
   K = K/2⟶ (K1, K2)
5. Perform Shifting on b1, b2
   b1 = Right_Circular_Shift_4 (b1)
   b2 = Left_Circular_Shift_5 (b2)
6. Perform XOR between b1 & K1
   b1 = b1 K1⊕
7. Perform XOR between b1 & b2
   b2 = b1 b2⊕
8. Interchange Value of b1, b2
   b2 = b1 ⟶ b2
   b1 = b2 ⟶ b1
9. Perform XOR between b1 & K2
   b1 = b1 K2⊕
10. Perform Shifting on b1, b2
    b1 = Right_Circular_Shift_4 (b1)
    b2 = Left_Circular_Shift_5 (b2)
11. Perform XOR between b1 & b2
    b2 = b1 b2⊕
12. End Loop
13. Exit

Proposed Decryption Algorithm

1. For C = 1to N bits
2. Input Cipher Information at a time
   C⟶ 128 bits
3. Input Key Value
   K⟶ 128 bits
4. Divide b and K into two sub parts
   C = C/2⟶ (C1, C2)
   K = K/2⟶ (K1, K2)
5. Perform XOR between C1 & C2
   C2 = C1 C2⊕
6. Perform Shifting on C1, Cb2
   C1 = Right_Circular_Shift_4 (C1)
   C2 = Left_Circular_Shift_5 (C2)
7. Perform XOR between C1 & K2
   C1 = C1 K2⊕
8. Interchange Value of C1,C2
   C2 = C1 ⟶C2
   C1 = C2 ⟶ C1
9. Perform XOR between C1 & C2
   C2 = C1 C2⊕
10. Perform XOR between C1 & K1
    C1 = C1 K1⊕
11. Perform Shifting on C1, C2
    C1 = Rev_Right_Circular_Shift_4 (C1)
    C2 = Rev_Left_Circular_Shift_5 (C2)

12. Combine C1 and C2 to get 128 bits C as a cipher value
    C = C1◎C2
13. Replace C (Cipher value) into b as Original value
    b = C
14. End Loop
15. Exit

Random Number Generation Technique: Blum Blum Shub generator is the pseudo random number generator. By using this random numbers are generated. The formula has shown below [3, 6],

$$Xi+1=(X/\text{mod } n)$$

Where, Xi is the seed, and n be the range.

The pseudo random bit generator is used for generating random numbers in cryptography. Seed, two large prime numbers, and the range is the inputs for the pseudo random bit generators [3]. The mathematical formulae has shown below,

$$Xi+1= (PXi+Q) \text{ mod } n$$

Where P,Q are two large prime numbers, Xi is the seed, n be the range.

Steganography Algorithm Steps:- Steganography algorithm steps at sender/Receiving end is in next section.

Steganography Algorithm Steps at Sender Side:-

1. Input Cover Image
   C_Img = C_Img→Image
2. Input Confidential Information b_Info
3. For b_info = 1 to N
4. b_Info = b_Info→128bits at a time
5. Read binary value of confidential information and cover image
   Bin_Val_b_Info = Binary_Reader (b_Info)
   Bin_Val-C_Img = Binary_Reader (C_img)
6. Read LSB from Cover Image
   LSB_C_Img = LSB_Reader (C-Image)
7. Replace LSB_C_Img from Bin_Val_b_Info
   LSB_C_Img = Bin_Val_b_Info
8. End Loop
9. Exit

Reverse Steganography Algorithm Steps at Receiver Side:-

1. Input Stego Image
   S_Img = S_Img Image
2. Loop for S_Img = 1 to N
3. Read Binary value of Stego Image
   Bin_S_Img = Binary_Read (S_Img)
4. Read LSB from Bin_S_Img
   LSB_Bin_S_Img = LSB_Reader (Bin_S_Img)
5. Embedded all LSB_Bin_S_Img in as confidential information
   B_Info = Embedded_LSB (LSB_Bin_S_Img)
6. End Loop
7. Exit

IV. PERFORMANCE ANALYSIS

This section presents the Evaluated results through Existing as well as proposed technique by using selected performance parameters analysis. Analysis is done on Peek Signal to Noise Ratio

(PSNR) analysis, Entropy analysis, Correlation analysis and Key Space Analysis. Proposed system is design in MAT LAB programming language. There are two type of information (Text and Image) has selected for Performance of the proposed system. During evaluation proposed system has run on number of several size of text and image information and captured overall performance on selected parameters like PSNR, Entropy, and Correlation. Here results is based on selected cover Images which is follow

(1) Img1.jpg

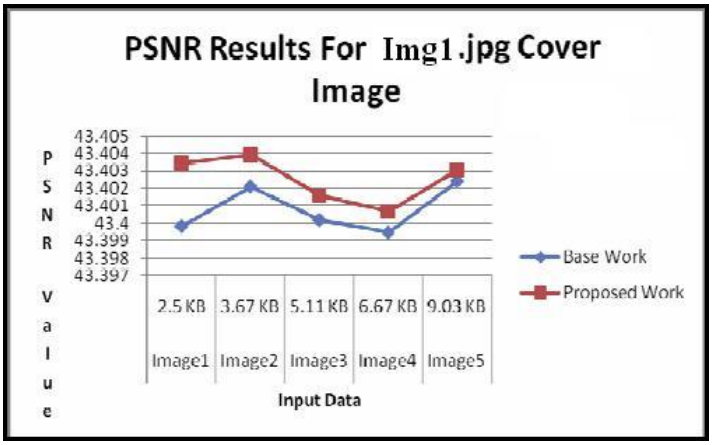
(2) Img2.jpg

(3) Cover.jpg

Peek Signal to Noise Ratio (PSNR) Analysis: PSNR is defined as assume that N is the total number of pixels in the input or output image, MSE (Mean Squared Error) is evaluated as [2,3 ,4]

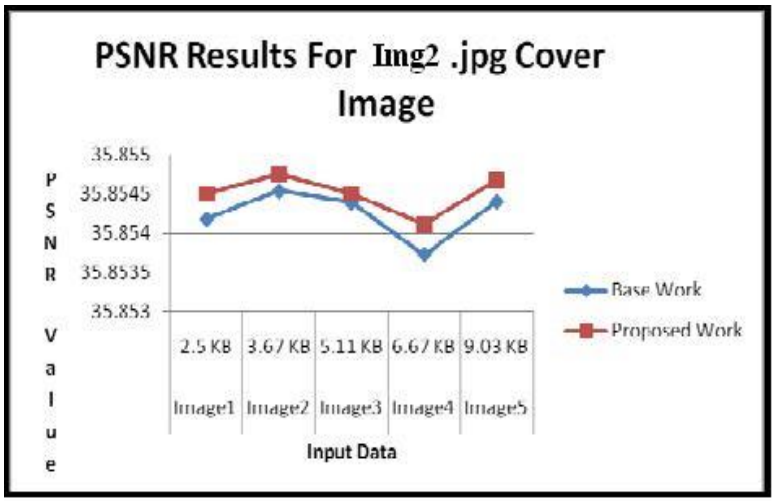
$$\text{MSE} = \frac{\sum_i \sum_j |x(i,j) - y(i,j)|^2}{N} \qquad PSNR = 10log_{10}\frac{(L-1)^2}{MSE}$$

L is the number of discrete gray levels The value of PSNR should be greater for the better of the output image quality.



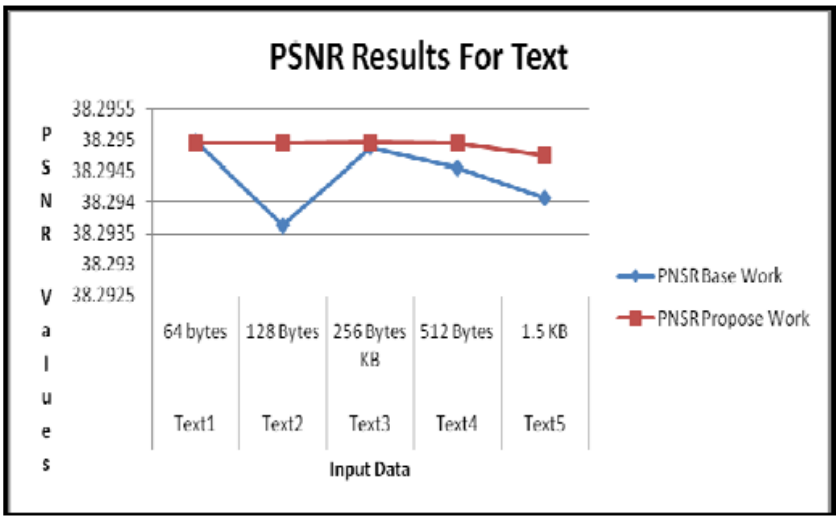
Graph 1: PSNR Graphical Analysis On Image Secrete Information when Cover image is Img1.jpg

Graph 1 shows that in our base work the PSNR value for image information when the cover image is lena.jpg and the secrete image is of 2.5KB is near to 43.399 whereas in our proposed work the value increases to 43.403459 which is good.



Graph 2: PSNR Graphical Analysis On Image Secrete Information when Cover image is Img2.jpg

Graph 2 shows that in our base work the PSNR value for image information when the cover image is monalesa.jpg and the secrete image is of 2.5KB is near to 35.854177 whereas in our proposed work the value increases to 35.8545 which is good.



Graph 3: PSNR Graphical Analysis of Text Secrete Information

Graph 3 shows that in our base work the PSNR value for text information where a text of 512 bytes is 38.294545 whereas in our proposed work the value increases to 38.29495 which is good.

Entropy Analysis: Entropy defined as follows [12,13].

$$H_e = -\sum_{k=0}^{G-1} P(k) \log_2 (P(k))$$

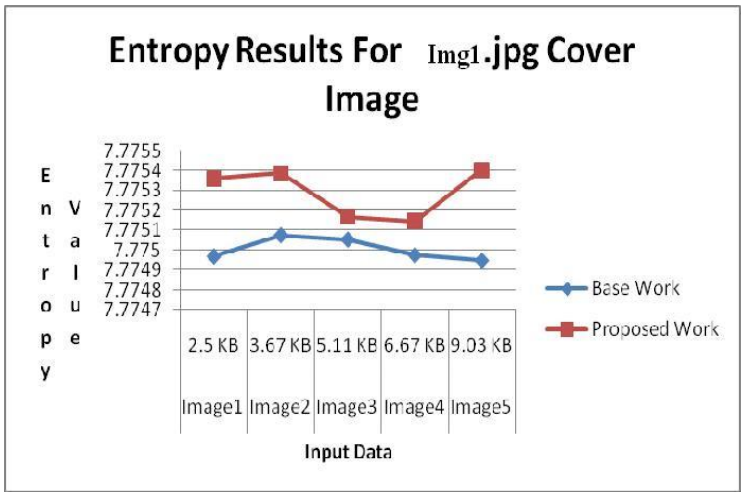
Where:

He: entropy.

G: gray value of input image (0... 255).

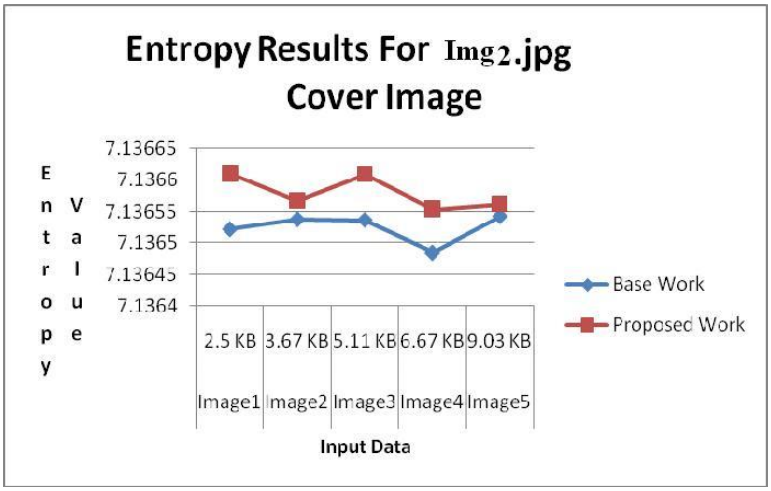
P(k): is the probability of the occurrence of symbol *k*.

The Entropy is a used to measure the richness of the details in the output image.



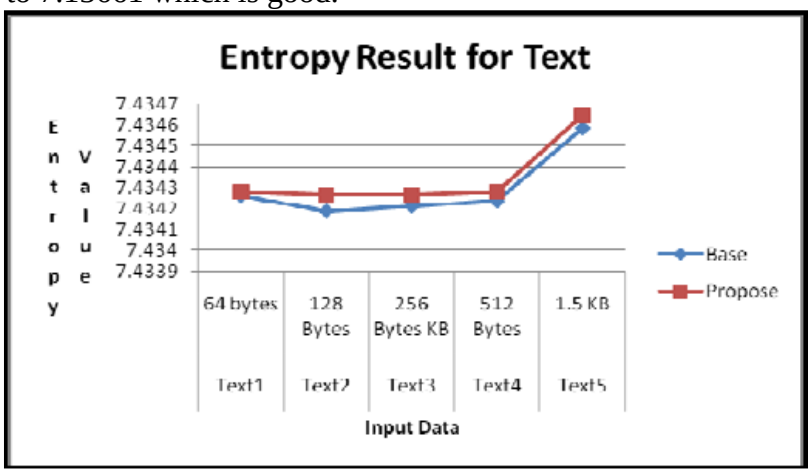
Graph4: Entropy Graphical Analysis when Cover Image is Img1.jpg On Image Secrete Information

Graph 4 shows that in our base work the Entropy value for image information when the cover image is lena.jpg and the secrete image is of 2.5KB is near to 7.774969 whereas in our proposed work the value increases to 7.775359 which is good.



Graph5: Entropy Graphical Analysis when Cover Image is Img2.jpg On Image Secrete Information

Graph 5 shows that in our base work the Entropy value for image information when the cover image is monalisa.jpg and the secrete image is of 2.5KB is near to 7.136521 whereas in our proposed work the value increases to 7.13661 which is good.



Graph 6: Entropy Graphical Analysis of Text Secrete Information

Graph 6 shows that in our base work the Entropy value for text information where a text of 512 bytes is 7.434237 whereas in our proposed work the value increases to 7.434279 which is good.

Correlation Analysis: In addition to the histogram analysis, we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image/cipher image respectively. Firstly, we randomly select 2000 pairs of two adjacent pixels from an image. Then, we calculate their correlation coefficient using the following two formulas [14]:

$$cov(x, y) = E(x - E(x))(y - E(y)),$$

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

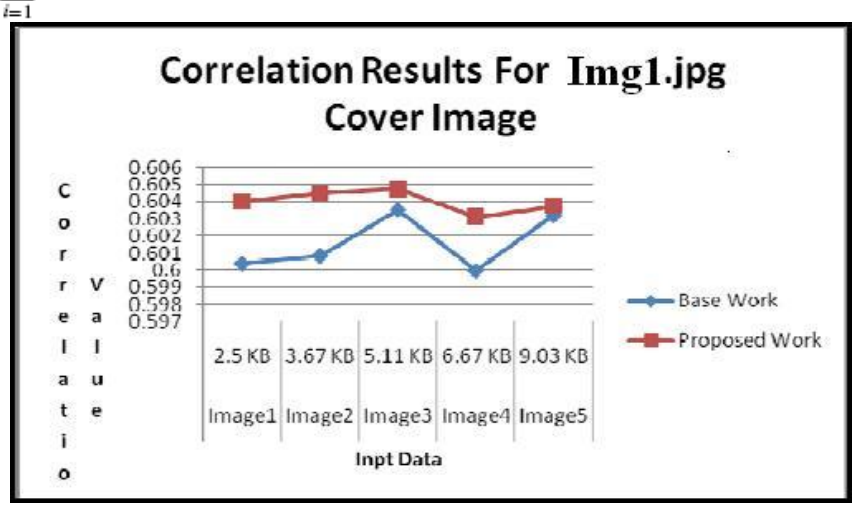
Where and are the values of two adjacent pixels in the image.

In numerical computations, the following discrete formulas were used [14]:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

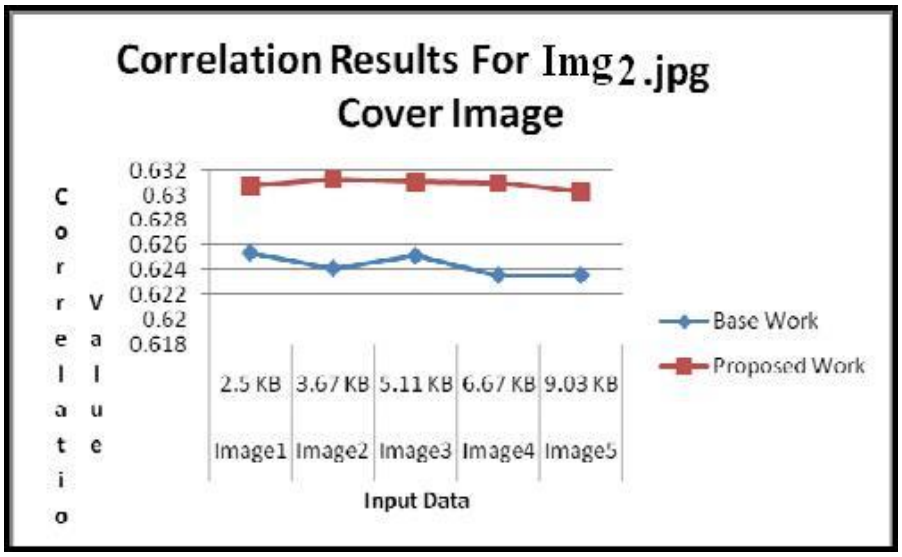
$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2,$$

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y - E(y_i)),$$



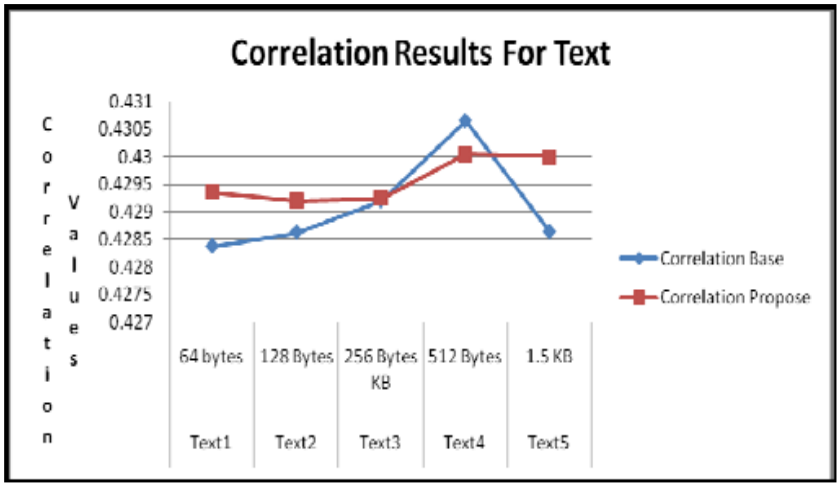
Graph 7: Correlation Graphical Analysis when Cover Image is Img1.jpg On Image Secrete Information

Graph 7 shows that in our base work the Correlation value for image information when the cover image is lena.jpg and the secrete image is of 2.5KB is near to 0.600414 whereas in our proposed work the value increases to 0.604007 which is good.



Graph 8: Correlation Graphical Analysis when Cover Image is Img2.jpg on Image Secrete Information

Graph 8 shows that in our base work the Correlation value for image information when the cover image is monalesa.jpg and the secrete image is of 2.5KB is near to 0.625315 whereas in our proposed work the value increases to 0.63076 which is good.



Graph 9: Correlation Graphical Analysis of Text Secrete Information

Graph 6 shows that in our base work the Correlation value for text information where a text of 128 bytes is 0.428633 whereas in our proposed work the value increases to 0.429209 which is good.

Key Space Analysis: Key space size is the total number of bits in a key that can be used in the encryption. For a secure image encryption, the key space should be large enough to make brute force attacks infeasible [10]. The proposed cipher has 128 bits length of the secret key. An image cipher with such a long key length is sufficient for reliable practical use.

Result Summary: Calculated results are shown in tables and Graphs 1 to 9 for PSNR, Entropy and Correlation parameters on text and image data as an input data or secret information and cover.jpg, Img1.jpg and Img2.jpg as a cover image. Graph 1 is showing "PSNR" value for image information when the cover image Img1.jpg where and secrete image of 2.5.KB having 43.403459 "PSNR" with proposed work which is good. Similar value for Img2.jpg image see graph 2 is showing 35.8545 "PSNR" with proposed work which is also good. Like that graph 3 is showing "PSNR" for text information where a text of 512 Bytes having 38.29495 "PSNR" with proposed work which is also

good. Graph 4 is showing Entropy value for image information when the cover image Img1.jpg where secret image of 2.5 KB showing 7.775359 "Entropy" with proposed work which is good. Similar value for Img2.jpg image see graph 5 is showing 7.13661 "Entropy" with proposed work which is also good. Like that graph 6 is showing "Entropy" for text information where a text of 512 Bytes having 7.415377 "Entropy" with proposed work which is also good. Graph 7 is showing Correlation value for Img1.jpg cover image where secret image of 3.67 KB having 0.604477 "Correlation" with proposed work which is good. Similarly graph 8 is showing Correlation value for Img2.jpg cover image where secret image of 3.67 KB having 0.631254 "Correlation" with proposed work which is good. Like that graph 9 is showing "Correlation" for text information where a text of 256 Bytes having 0.429243 "Correlation" with proposed work which is also good. At last Key space analysis is showing the security of the proposed technique which is also far-far batter then base work.

V. CONCLUSION

Generally large amount of information insertion through least significant bits (LSB) technique of steganography is not an easy task. Due to this problem an image compression technique included in the proposed concept so the proposed concept used a wavelet transforms image compression technique which is lossless technique. With this technique large amount of information like image can be reduced and easily inserted through LSB technique. So overall proposed concept is initially confidential information if an image then it worked with compression technique then the compressed image worked with proposed encryption technique followed by steganography technique, or if confidential information is text then it worked directly with proposed encryption and followed by steganography technique. It already known that compression technique is only used for image and through LSB is the batter then other techniques, due to the reduction of noise distortion. Proposed concept is providing two layer of security with the combination of cryptography and steganography technique due to this higher security aspect automatically included in this.

VI. ACKNOWLEDGMENT

I (Depavath Harinath) would like to gratefully and sincerely thank my parents - father D.Chatur Naik and mother D.Ghammi Bai and I convey my thanks to Prof. M. V. Ramana Murthy, Chairman Computer science, Head Dept. Of Mathematics , Osmania University, Hyderabad, India, without whose unsustained support, I could not have completed this paper.

REFERENCES

1] 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), Publication Year: 2013 , Page(s): 1188 –1193

[2] 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), Publication Year: 2013 , Page(s): 385 – 390

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

[4] M.K Ramaiya. ; N.Hemrajani, ; , A.K Saxena. "Security improvisation in image steganography using DES" IEEE 3rd International on Advance Computing Conference (IACC), Publication Year: 2013 , Page(s): 1094 - 1099

[5] Rengarajan Amirtharajan\ Anushiadevi .R2, Meena .y2, Kalpana. y2 and John Bosco Balaguru "Seeable Visual But Not Sure of It" IEEE- International Conference On Advances In Engineering, Science And Management (ICAESM - 2012) March 30, 31, 2012

[6] L.Jani Anbarasi and S.Kannan "Secured Secret Color Image Sharing With Steganography" IEEE 2012

[7] G.Karthigai Seivi, Leon Mariadhasan, K. L.Shunmuganathan "Steganography Using Edge Adaptive Image" IEEE International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012.

[8] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar "An Image Steganography Technique using Xbox Mapping" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[9] RigDas and Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding" IEEE 2012

[10] Abhishek Gupta, Sandeep Mahapatra and, Karanveer Singh " Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm" 2011 IEEE .
[11] Thomas Leontin Philjon. and Venkateshvara Rao. Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011
[12] 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, 2011.
[13] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) 102-108
[14] Danah boyd and Alice Marwick "Social Steganography: Privacy in Networked Publics" ICA 2011
[15] Depavath Harinath, "Net Neutrality- A Concept of Open Internet" in *International Journal of Science and Research*(IJSR),Vol.4, Issue7,July 2015.
[16] Depavath Harinath, "Corpus of Internet Standards-The Standards for Communication" in *International Journal of Advanced Research in Computer Science* (IJARCS), vol.5, No. 3, March-April 2014.
[17] Depavath Harinath, "Fast Rerouting Algorithms for Routing Protocols in IP Networks" in International Journal of Modern Trends in Engineering and Research (IJMTER), vol.2, Issue7,July 2015
[18] Depavath Harinath et. al., "Cryptographic Methods and Performance Analysis of Data Encryption Algorithms in Network Security" in *International Journal of Advanced Research in Computer Science and Software Engineering* (IJARCSSE) ,Vol.5, Issue7, July 2015.

AUTHOR 'S PROFILE:

Depavath Harinath, received the Bachelor of Science degree in computerscience from New Noble Degree college, Affiliated to Osmania University, Hyderabad, Telangana, India in 2008 and received Master of Computer Applications degree from Sreenidhi Institute of Science and Technology, an autonomous institution approved by UGC. Affiliated to JNTU, Hyderabad, Telangana., India in 2012. Now working as Lecturer in Computer Science in HRD Degree and PG college, Affiliated to Osmania University, Narayanaguda, Hyderabad, Telangana, India. Having three years of experience in teaching and already published eight manuscripts in different international journals. Research fields includes Computer Networks and Network Security.

Mrs. B.Chithra, Asst.Professor in department of mathematics and computerscience, Osmania University, Hyderabad. She has Worked as Associate Professor (dept. of Computer Science) at St.Ann's college for women, for about fifteen years and published a paper in one of the reputed International Journals. Research interest includes Network Security.

Prof.M. V. Ramana Murthy, Professor in department of mathematics and computerscience, Osmania University, since 1985. Obtained Phd degree from Osmania University in 1985 and visited many a countries across the globe in various capacities and participated in many academic programs. Research fields includes computational plasma, Artificial Neural Networks, and Network securities.

