International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

Efficient Approach for Steganography Using DWT and RSA Algorithm

Ambika, Rajkumar L Biradar, Vishwanath Burkpalli

Abstract: ***Steganography is the mechanism of masking (i.e. hiding) the available data in other transmission area to achieve secure and secret transmission of data. Steganography is much secured technique and can also be applied for various file formats (Ex: Image, Video, Audio, text etc.). Several steganogrphic mechanisms are available for secret data or information hiding utilizing images. Steganography is one of the best data transmission method including security and privacy and it is utilizing in so many applications. In those applications, few applications require complete secret data invisibility and some applications require a big secret message hiding. This steganogrphic technique masks the secret or private data into the cover image. Transmission of secret information securely without data loss in the communication system inspired us to develop a proposed communication system. This proposed technique mainly comprises of two sections i.e. data transmission section and data extraction section. In data transmission section, sensitive data (i.e. secret data) is pre-processed and encrypted utilizing RSA technique or algorithm mean while preprocessing of cover image is performed and knight tour technique is utilized to make path for knight. Finally encrypted sensitive (secret)information or data is embedding with cover image utilizing DWT (Discrete Wavelet Transform). Similarly in the receiver section i.e. data extraction section, data is extracted by applying inverse transformation and RSA algorithm, hence resulting in secure transmission.***

Index Terms: ***Image Steganography, Encryption, Cover Image, DWT, RSA.Stego Image,***

I. INTRODUCTION

In a recent era the communication between two systems or multiple networks is achievable due to Internet technology. The technologies which are related to internet and its applications [1-5] are increasing day by day, where as effective progress in cyberspace will directly increase amount of sensitive data utilized to send or receive over the communication network. Increase in the communication load will lead to the multiple network challenges like data integrity, data authenticity, network attack and mainly data security.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)
Ambika*, Assistant Professor, Department of CSE APPA Institute of Engineering and Technology, Kalaburagi- 585103,Karnataka, India
Dr. Rajkumar L Biradar, Professor, Electronics and Telematics Dept.G Narayanamma Institute of Tech & Science Hyderabad, India
Dr. Vishwanath Burkpalli, Professor, Department of ISE, PDA College of Engineering Kalaburagi, Karnataka, INDIA

Cryptography is one of the traditional data encryption methods, where its application is reducing gradually due to its insecure data transmission [6]. This technical challenge is overcome by utilizing data masking or hiding technology. In which confidential one media information is embedded or implanted into another media object hence confidential data is invisible to unknown person or attackers. Data security, data capacity and data clarity are
the major functional characteristics of the data masking (hiding) technique. This data embedding or data hiding method is also termed as “Steganography”. Depending on the required cover object, steganogarphy is sectored into multiple sections i.e. Image steganography, Text, Audio, Video and Protocol steganography. In image steganography, any one of the media is utilized as a transporter object for data hiding. The basic functional diagram of the simple steganography is represented in Figure 1.

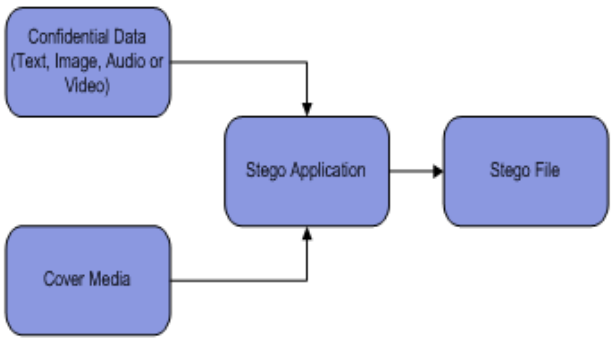


Figure 1: Steganography Module

In this proposed work effective image based information or data embedding system module is presented. To meet the efficient functional algorithm a set of research articles are studied, the referred research articles are summarized in section 2.

II. LITERATURE SURVEY

Vojtech Holub et.al [7] has presentenced an efficient approach the universal distortion based steganography module. The referred system is designed by using BOSS base version 1.01 dataset, which includes 512*512 gray scale sample images. Each image is presented with 8 bit. This data base include 10000 data sample which are captured from eight multiple cameras. In the referred steganography module the system designer considered a compressed cover

object and universal wavelet relative distortion (UNIWARD) functional parameter for steganography. The application of DCT and wavelet directional filter bank efficiently defines the co-efficient changes between stego and cover images. The referred module is implemented in three different approaches. The performances of three approaches are studied in two functional parameters i.e. embedding distortion and DCT coefficients by considering quantization error. By considering the result section the system designer concluded that the side- informed steganography presents zero data embedding distortion when DCT coefficients quantization error value is ½.Saiful Islam et.al [8] has proposed secret image embed module utilizing cover image edges. Edge based steganography mechanism is one of the emerging data embedding technique, in which based on the secrete amount of data the respective cover object edges are estimated. Weak edge part in the cover image is considered to entrench the large amount of data. The referred system is worked on BOWS2 and BOSS base version 1.01 dataset. The effective edge data has been collected by applying the canny edge detection techniques where selection of the edges for particular image payload. Threshold selection is the main functional parameter and it is utilized to classify the cover image effective edges. Depending thresholding image response a respective edges are estimated and finally the edges which has the high threshold is considered for sensitive data implanting techniques. A 2-bit LSB replacement technique is used embed the sensitive image (i.e. secret image) into a high threshold detected cover edges. The referred system performance is estimated by considering embedding rate. Equivalently S-UNIWARD and HUGO data embedding techniques are used to compare the referred system performance. Finally the conclusion the system designer summarized that the referred system presents the good steganogrphic output compared to S-UNIWARD and HUGO when data hiding rate will be lesser than 10%bpp and 5% bpp.

Hamidreza Rashidy Kanan et.al [9] has presented an image steganograpy method utilizing generic algorithm. The searching is the most the challenging task in steganography for the estimation of best place within the cover image to mask the secret data. It include the two functional step i.e. first one before embed the image data into the cover object the input data is modified to raise the system security. The modified data is implanted in to the cover image. The excellence of the stego data and effectiveness of hided data is analyzed and the system performance is measured with different image steganography mechanisms. From result analysis the referred research work concluded that designed approach presents the high data embedding power with better quality of the stego output.

Debiprasad Bandyopadhyay et.al [10] has worked on image based Chao theory steganography mechanisms. In this referred system secret data is encoded utilizing chaos theory. This data encryption before data embedding increases security level over the communication channel. For data embedding 3-3-2 LSB techniques is used. The referred system performance is analyzed by considering the stego output PSNR and extracted image PSNR. Along with PSNR and Image Fidelity (IF) estimated. Based on the data encryption technique at the result section the research work is summarized that referred system increases the security level and enhance the image value i.e. quality by improving the PSNR level. The entire functional step is conducted on JPEG image formats and it's defined that these steganography mechanisms can also be applicable to any image formats.

Table 1: Survey Table

Year	Title	Encryption	Embedding	Advantage	Performance
2014	Edge-Based Image Steganography	Masking, Canny Edge Detection	Least Significant Bit (LSB) Method	Improved Embedding Capacity	Accuracy = 51.1%
2014	Optimized Image Steganography using Discrete Wavelet Transform (DWT)	Arnold Transformation	DWT(Discrete Wavelet Transform)	Improved Security using Arnold Transformation	PSNR = 48.06, Embedding Capacity = 75%, Correlation = 0.9999
2014	A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain	Chaos Theory	C- LSB (Chaos based LSB) Insertion Technique	Improved Peak Signal to Noise Ratio (PSNR) and Image Fidelity	PSNR = 49.12, MSE = 1.00, IF = 0.99
2014	A Novel Image Steganography Scheme with High Embedding Capacity and Tunable Visual Image Quality Based on a Genetic Algorithm	-	Genetic Algorithm	Improved Embedding Capacity and image quality enhancement	PSNR = 45.13
2015	A Novel DWT Based Image Securing Method using Steganography	SSIM (Structural Similarity Index Matrix)	Discrete Wavelet Transform(DWT)	Better Data Compression before Embedding	PSNR = 55.13
2016	An Improved Method for LSB Based Color Image steganography Combined with Cryptography	RSA (Rivest, Shamir and Adleman) Algorithm	Improved LSB Color Image Steganalysis Algorithm	Higher PSNR	PSNR = 56.513

Della Baby et.al [11] presented an image steganography by utilizing Wavelet Transformation method. In which a set of color images are embedded into a color cover object. To increase the level of security and image embedding capability the considered cover object is separated into its planes i.e. RGB planes. Further by applying N-level DWT decomposition technique the given image plane is breakdown into two bands such as low and high frequency bands.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

In this research work three color images are embedded into an LL band of cover object planes. The reverse technique is performed at secret image extraction techniques. A MATLAB 2012a software tool is used implement the techniques. This referred system performance is measured in PSNR, MSE and Structural Similarity Index Matrix (SSIM). By considering the simulation performance, simulation the research work is summarized that the referred system provided higher security with better PSNR.

Xinyi Zhou et.al [12] has proposed a cryptography approach based on enhanced data embedding mechanism of LSB. In this system security level of the data is increased by encrypting the data using RSA cryptography method. A secret key utilized to embed the private data into a color object. Adding the signature and encryption technique increases the performance level. A LSB data embedding is preferred for data embedding technique. The referred system efficiency is computed utilizing PSNR parameter and in which each planes PSNR value, is analyzed. By considering stego quality, it is summarized that the implemented scheme provides best output with high security.

Hayat Al-Dmour et.al [13] implemented a XOR and edge based image steganography. The cover image sharp edges are extracted by applying the novel edge detection techniques. The data embedding in sharp edges presents best data embedding quality than smooth edges. A XOR coding is preferred for data embedding, in which three bit secret information is embedded into a four bit of edge bits in cover image. Out of that four cover bit two bits are modified to present the stego data. In this work the designer mainly concentrated on sharp edge and lesser sharp region for data embedding. System performance is measured with PSNR. MSE with different data embedding ration, considering the resulting table the research work summarized that proposed present's best imperceptibility. Table 1 presents the respective information about various data encryption and data embedding techniques carried out in literature for stegnography.

III. METHODOLOGY

Working procedure of the proposed method is represented in Figure 2 and 3. The overall system works in two sections i.e. data transmission section and Data extraction section (Receiver). Initially in the transmission section, the secret image (i.e. data) which is to be transmitting is preprocessed by resizing the input image. Security level is enhanced by utilizing RSA algorithm. Preprocessed image is encrypted by adding signature into the secret image using RSA algorithm [14-15]. In the same time, preprocessing of cover image is performed using median filter to reduce noise in the covered image. Preprocessed cover image is split into several blocks in the block generation block. Knight Tour is the mathematical method utilized to recognize the knight path inside the image. Knight Tour algorithm is applied on the generated blocks of cover image. Pixels are chosen by considering the movement of Knight Tour. Secret images are converted in to binary form based on the pixel movement. The converted binary format is embedded (hided) in the cover image utilizing DWT (Discrete Wavelet Transform). Finally binary information of the encrypted secret image is hided using DWT transform and secured stego image is produced.

The stego output is send to receiver through the network system. In the data (i.e. secret data) extraction section (Receiver section), stego image is decrypted and added security signature is extracted by utilizing Knight Tour application, inverse transformation and RSA algorithm. Secret data is extracted only if extracted signature matches with the signature which is added at the time of transmission. The explanation of each algorithm used in our system is explained in below section.

3.1 Data Encryption

Data encryption is the method of converting known form of data (readable format) into unknown form (unreadable format) by encrypting the data. Multiple data encryption and extraction methods are available. In the proposed system, RSA technique is utilized for encryption of data and signature extraction (Decryption).

A. RSA Algorithm

RSA is more utilized in data secure system. RSA is nothing but Ron Rivest, Shamir and Adleman. These are the researchers who publically described RSA technique (1977). From that time, this technique is implemented in the generally utilized Internet electronic communications encryption program. It is utilized in Secure Sockets Layer (SSL) implementations of the Microsoft Explorer web browsing program and Netscape Navigator. It is used also for credit card transactions in the SET (Secure Electronic Transactions) by VISA and Master card. RSA technique is only the one implementation for the most familiar public key cryptography implementation.

Distinctive encryption mechanisms utilize mathematical operation to convert a message (defined as sequence of numbers) into an unreadable text format. In this proposed system we are utilizing RSA technique to encrypt the information to achieve security, from this only authorized person can access the data. In the encryption formula of RSA, the S is multiply by e times itself and then using modulus r the product is divided by modulus r, remaining remainder is considered as cipher text A:

$$A = S^e \bmod r \qquad (1)$$

In the operation of decryption section, another exponent d is utilized to convert back to the original (i.e. plain) text format from the Cipher format:

$$S = A^d \bmod r \qquad (2)$$

The modulus r = Composite number, created by product of two prime numbers i.e. u and v:

$$r = u * v \qquad (3)$$

and also, $\varphi(r)$ is called as Euler's Phi-Function and it is compute by the below mentioned equation:

$$\varphi(r) = (u-1)(v-1) \qquad (4)$$

The encryption e exponent is selected such that:

$$gcd\left(e, \varphi(r)\right) = 1 \text{ , where } 1 < e < \varphi(r) \qquad (5)$$

The d is the decryption exponent is computed by resolving the below formula:

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

$$e.d = 1 mod \varphi(r) or\ d = e^{-1}\ mod\ \varphi(r) \qquad (6)$$

Where $0 \leq d \leq r$, Hence the public encryption key is $\{e, r\}$ and the private decryption key is $\{d, r\}$. Therefore, the RSA technique is breakdown into three stages:

1. Key Generation

To encrypt secret date there must be significance to add a key. This is done by key generation. The step involved in key generation is presented in below key generation algorithm steps in *Algorithm 1*.

2. Encryption

The method of converting original clear data into cipher data is known as encryption. Further encryption steps are presented in below section:

Step.1. Sender should provide or transmit the Encryption-Key (r, e) to the receiver.

Step.2. By utilizing an agreed upon reversible protocol, data is mapped to an integer and it is called as padding scheme.

Step.3. Data is encrypted, then resulting cipher data A is computed using Eq. (1).

Algorithm 1: Key Generation Algorithm

1. *Consider two different prime numbers u and v. The u and v integer is selected at random for security purpose. The selected integer should have same bit length.*
2. *Calculate r by using Eq. (3).*
3. *Calculate Euler's Phi-function, $\varphi(r)$ using Eq. (4).*
4. *Select an integer e as per the Eq. (5). Now e is considered as Encryption-Key exponent.*
5. *Compute d using Eq. (6).*
6. *d is kept as decryption Key component, hence $d * e = 1\ mod\ \varphi(r)$.*
7. *The encryption-Key consists of modulus r and the encryption exponent e i.e. (e, r).*
8. *The Decryption-Key consists of modulus r and the decryption exponent d i.e. (d, r).*

3.2 Processing of Cover Image

Cover Image is the image which is used to hide the sensitive (i.e. secret) data into it. Processing of cover image is a very important task in the proposed technique. Initially, cover image is pre-processed using median filter in order to remove noise or artifacts in the cover image. Later pre-processed image is divided into blocks. This block generation is achieved by using knight tour algorithm.

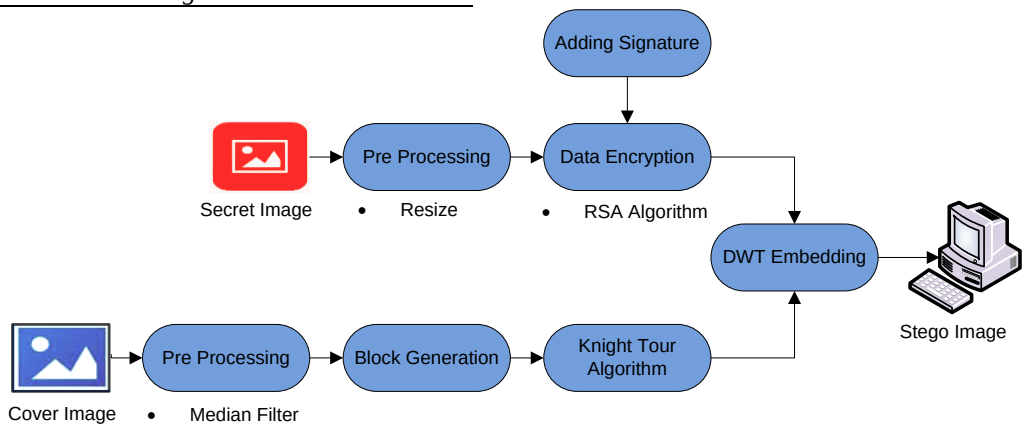


Figure 2: Secure Data Transmission Block Diagram

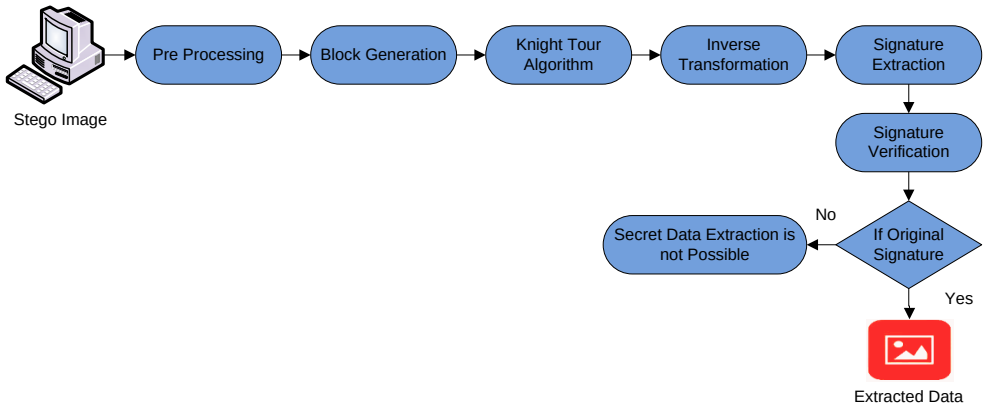


Figure 3: Data Extraction Block Diagram

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

A. Median filter

In the proposed work, median filtering is utilized to pre-process the cover image. The median filtering is one of the nonlinear filtering methods, which is utilized to remove artifacts and noise from the signal or image. Reducing of noise in an image is a pre-processing action to progress the outcome of the further processing. Median filtering is popularly utilized technique for removing of noise in an image with protection of edges. Particularly median filtering is very effective and efficient at reduction of pepper and salt type of noises. This filter works on pixel by pixel movement in an image. It moves with in the image by changing the pixel by pixel and replaces each pixel value with neighboring pixels of median value. Median value is computed by considering the sorting of all the pixel ideals or values in the numerical form and replacing the pixel with the central pixel value. In the median filter each pixel is replace by considering the median value without considering the averages pixels in the neighborhood and the mathematical equation of the median filter for the removal of noise by preserving edges is represented in Eq. (7):

$$x[n,m] = median\{y[j,k], (j,k) \in z\} \quad (7)$$

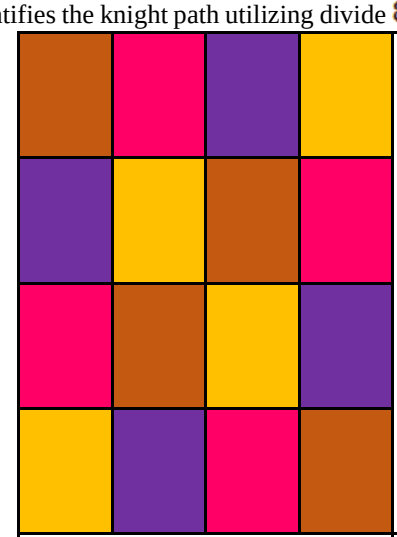
z = user defined neighborhood pixels.

$[n,m]$ = Centered location coordinates in an image

$[j,k]$ = Size of the pixels

3.3 Knight Tour Algorithm

Knight tour algorithm is applied to pre-processed cover image and it generates the blocks of an image. Knight Tour technique is a self designed mathematical method developed to create a secret bit streams sequence. The input image (example cover image or stego image) is dividing into $8 * 8$ sized blocks. Inside the input image, knight tour technique identifies the knight path utilizing divide $8 * 8$ sized blocks.



1. Brown: -Left Diamond
2. Pink : -Left Square
3. Yellow: -Right Diamond
4. Purple : -Right Square

Figure 4: (a) $4 * 4$ Blocks of Pixel (b) Pixel Name Plates

In the four different forms, divided $8 * 8$ sized blocks are grouped such as Left Square, Right Square and Right Diamond, Left Diamond. The major rule of this Knight Tour technique is shift a one square inside as chessboard or each group image. Similarly after get done of a one square, same procedure is followed for remaining squares. The diagrammatic Knight Tour representation of single $4 * 4$ sized block is presented in Figure 4. The stages involved in the Knight Tour technique are presented in below steps,

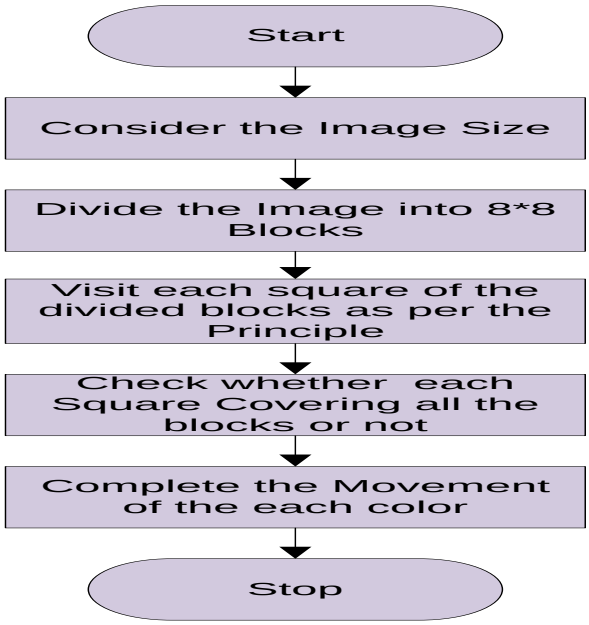


Figure 5: Functional Steps of Knight Tour Algorithm

3.4 Discrete Wavelet Transform (DWT)

In the proposed system Discrete Wavelet Transform [16-17] is utilized to embed (i.e. hide) the secret image inside the cover image for secure data transmission. The Discrete Wavelet Transform which can recognize fractions of cover image where secret information could be efficiently hidden. DWT divides data into its low frequency and high frequency parts. The high frequency part of the signal have information regarding the edge components, whereas the low frequency part have the majority of the signal details of the image which is again split into higher and lower frequency components. For all plane of disintegration in two dimensional functions, first DWT is executed in the vertical path followed by horizontal path. One of the most accepted cover objects utilized for steganography is an image. Cover images may be gray scale images or color images. Color images have large space for information hiding and color image steganography is well-liked than gray scale image steganography. Color images can be illustrated in different formats such as RGB (Red Green Blue), HSV (Hue, Saturation, and Value), YUV, YIQ and YCbCr (Luminance, Chrominance) etc. Color picture steganography can be completed in several color space fields. When the wavelet transform is utilized to a color picture, the transformation coefficients are attained for all the three paths in the equivalent illustration.

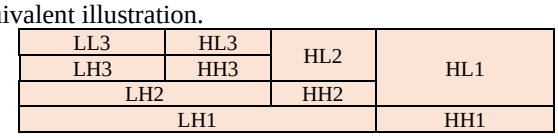


Figure 6: DWT based Three Phase disintegration

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Discrete Wavelet Transformation consists of its own best space frequency localization correctly. In every dimension, DWT is applied on 2 dimensional images which is corresponds to 2 dimensional filter image processing. When wavelet transform is useful to an image, it is disintegrating into four sub-bands LL1, LH1, HL1 and HH1 by the filters. LL1 is the low frequency sub band and holds estimate coefficients. The important descriptions of the image are controlled in this sub band. Previous three sub-bands are high or greater frequency sub-bands and hold fewer important features. It is potential to rebuild the image by allowing for only LL. To get the after that coarser of wavelet coefficients, the LL1 sub band is processed till a few ultimate scale 'M' is reached. After 'M' is reached, we will get 3M+1 sub bands which is contain multi resolution sub bands i.e. LLM, LHY, HLY, and HHY where 'Y' is from 1 to till 'M'. Normally many of the energy of an image get accumulated in these sub divided sub bands. Due to the best space frequency localization function of DWT, identification of areas within in the cover image and then sensitive data can be hiding or embed efficiently. The implanting or hiding of secrete image in lower frequency sub bands significantly may confuse the image. However hiding in low frequency sub bands considerably improves the robustness.

3.5 Data Extraction

Generally, data extraction is the process of extracting the required data from the obtained data. Similarly, in the proposed system data is extracted from the stego image. Data extraction is performed by preprocessing the received stego image. After preprocessing, knight tour algorithm is applied to generated blocks of the stego image later Inverse transformation is applied. Finally data is extracted by applying the decryption technique of RSA algorithm to extract the signature from the inverse transformed image. Data can be successfully extracted if extracted signature or key is equal to the signature which is added at the time of secret data encryption. Algorithm 3 presents the decryption process of RSA algorithm.

A. ***Decryption***

Decryption is the procedure of converting the cipher data to the original clear (i.e. plain) data. Further decryption steps are presented in below section:

Step.1. The receiver requests the transmitter for the data.

Step.2. Transmitter verifies the receiver authentication and sends the encrypted data i.e. A.

Step.3. The Receiver then decrypts the data (S*) by using Eq. (2).*

After obtaining A *(Encrypted data), the receiver can obtain the original data by reversing the padding method.*

IV. Experimental Results

There are many ways are available to evaluate the system performance. In the proposed technique most important two parameters i.e. Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) is considered. Mean Square Error (MSE): - Mean Square Error is the important parameter. MSE can be define as the computing the average value of square of the difference between the cover image and stego image intensities and it shows the distortion rate in the stego output (i.e. image) which is collected. The mathematical formula for Mean Square Error (MSE) is represented in below Eq. (8).

$$MSE = \left(\frac{1}{a * b}\right) \sum_{j=1,k=1}^{a,b} \left(u_{jk} - v_{jk}\right)^2 \quad (8)$$

u_{jk} = Value of pixel at (j, k) in the cover image

v_{jk} = Value of pixel at (j, k) in the stego image

$a * b$ = Size of the image.

PSNR (Peak Signal to Noise Ratio): - The PSNR depicts the quality of the reconstruction of the transformed image. This parameter is utilized to analyze the robustness and effectiveness of the proposed technique by considering cover and stego image PSNR value. In the same manner sensitive data (secret image) is compared with the extracted sensitive data's PSNR. The PSNR value of the stego outcome is computed by utilizing the Eq. (9) and it is expressed in dB (decibel format).

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (9)$$

The quality of image and system performance is measured by considering PSNR and MSE value. Initially in the transmission side, the cover images are pre-processed and blocks are generated. Knight tour technique is applied for generated blocks. Secret image is pre-processed and processed image is encrypted by adding signature using RSA technique. Finally encrypted sensitive data (i.e. secrete image) is embedded in cover image using DWT (Discreet Wavelet Transform) method.

The performance analysis of the proposed technique is analyzed by considering PSNR and MSE parameters. Figure 7 shows the cover image, secret image and stego image, extracted secret image from the stego image respectively. For Comparative analysis, we have considered two steganography methods, (i). Artificial Bee Colony Algorithm based Steganographic method, and (ii). Adaptive Artificial Bee Colony Algorithm based Optimum Pixel Adjustment Algorithm. The average PSNR and MSE values obtained for the existing and proposed methods are tabulated in Table 2.

Table 2: Comparison of Proposed Method Performance Analysis with Existing Methods

Steganography Methods	Image Size	PSNR(dB)	MSE
ABC based Steganographic method	512*512	26.9137	0.939189
ABC based OPA	512*512	29.9123	0.899170
Proposed Method	512*512	31.792	0.866123

Table 2 shows the comparison of performance of the proposed technique with existing system. It shows that proposed system enhance the quality of stego image with improved PSNR. The proposed method and existing method's PSNR performance graph is shown in Figure 8.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

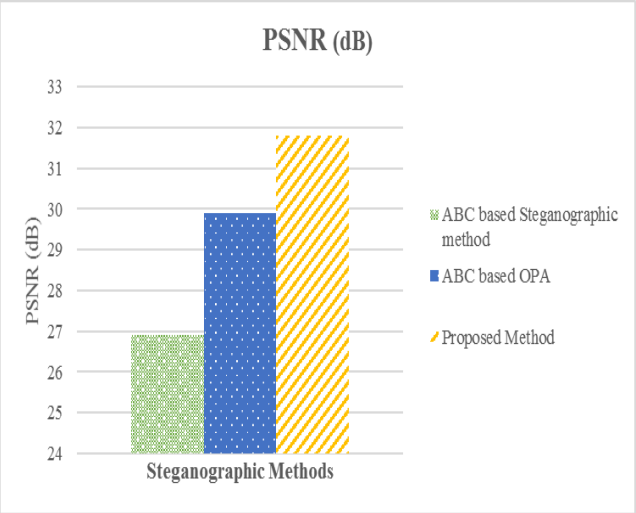


Figure 8: PSNR Comparison Graph

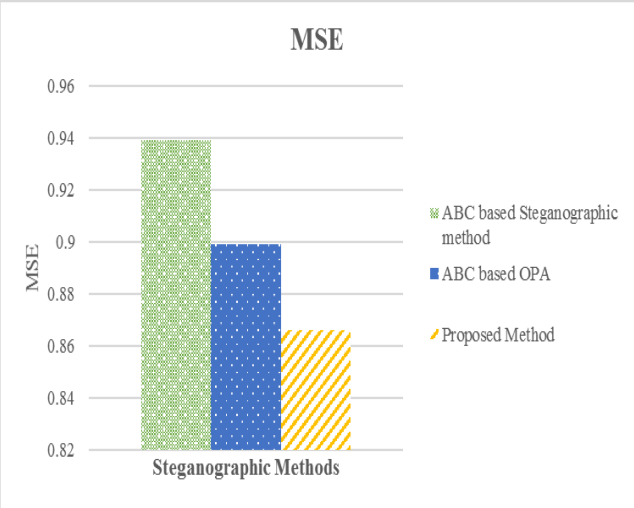
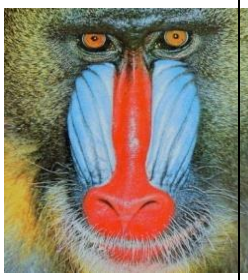
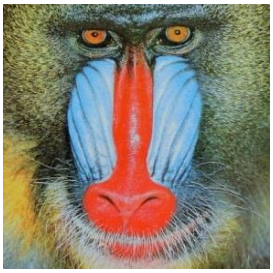
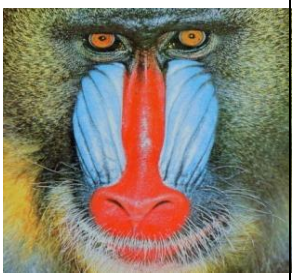


Figure 9: MSE Comparison Graph

The bar chart in the Figure 8 shows the detailed analysis of three steganographic algorithms using standard images for PSNR. The obtained PSNR values are 29.9137, 29.9123 and 31.792 for Artificial Bee Colony Algorithm based Steganographic method, Artificial Bee Colony Algorithm based Optimum Pixel Adjustment Algorithm and Proposed method respectively. A high PSNR value for the steganographic method indicates better secured transmission of the images. From above graph, it is clear that Proposed method shows better PSNR value as compared with other methods.In addition to PSNR, the plot of MSE for proposed method and existing methods has been shown in Figure 9. A low MSE value for the steganographic method indicates better robustness against to transmission errors. By observing the MSE plot one can easily notice that the Proposed method's MSE is least among existing methods, hence proposed method performs well when compared to existing methods.

				
a	b	C	d	e
Figure 7: (a) Cover Image;	**(b) Secret Image;**	**(c) Transmitted Stego Image**	**(d) Received Stego Image;**	**(e) Extracted Secret Image**

V. CONCLUSION

Steganography is one of the most important techniques for secure data transmission. In this proposed scheme, steganography designed for the secure data transmission. This steganography technique is designed using RSA and DWT techniques. The secret image (sensitive data) is encrypted using RSA algorithm after adding signature to it and mean while cover image is pre-processed. Block generation and knite tour algorithm is applied to pre-processed cover image. Finally the encrypted secret image is hided within the cover image using DWT method and stego image is generated. Similarly secret image is extracted from the cover image in the receiver side by extracting and verifying the signature. In this proposed work, system performance is improved in an efficient manner using existing algorithms. The proposed system shows that, performance of the proposed method is improved efficiently when compare to existing method. In our further research work will work on improving the efficiency of the proposed system.

REFERENCES

1. Virupakshappa, Dr. Basavaraj Amarapur," Cognition based MRI brain tumor segmentation technique using modified level set method", Cognition, Technology & Work, https://doi.org/10.1007 /s10111-018-0472-4, Springer, 2018.
2. Virupakshappa, Dr. Basavaraj Amarapur," An Approach of using Spatial Fuzzy and Level Set Method for Brain Tumor Segmentation", International Journal of Tomography & Simulation, Issue No. 4, **Vol. 31, 2018.**
3. Ambika, Rajkumar L. Biradar "Secure medical image steganography through optimal pixel selection by EH-MB pipelined optimization technique" Health and Technology https://doi.org/10.1007/s12553-018-00289-x December 2018.
4. Virupakshappa, Dr. Basavaraj Amarapur, "Computer-Aided Diagnosis applied to MRI images of Brain Tumor using Cognition based Modified Level Set and Optimized ANN Classifier", Multimedia Tools and Applications, DOI: 10.1007/s11042-018-6176-1, Springer, 2018.
5. Sachinkumar Veerashetty, Dr Nagraj Patil, "Novel LBP based texture descriptor for rotation, illumination and scale invariance for image texture analysis and classification using multi-kernel SVM", Multimedia Tools and Applications, DOI:10.1007/s11042-019-7345-6, Springer, 2019.
6. Virupakshappa, Dr. Basavaraj Amarapur," An Improved Level Set Method with New Speed Function and Optimized KPCM for Initial Contour for Brain MRI Segmentation", Health and Technology, https://doi.org/10.1007/s12553-018-00288-y, Springer, 2018.
7. Yuan Ziqian, Guan Zijie, and Feng Hao, "An Improved Information Hiding Algorithm Based on Image", IEEE, pp. 169-172, 2017.
8. Vojetech Holun and Jessica Fridrich, "Digital Image Steganography Using Universal Distortion", ACM, 2013.
9. Saiful Islam, Mangat R Modi and Phalguni Gupta, "Edge Based Image Steganography", Springer, 2014.
10. Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal and Paramartha Dutta, "A Novel Secure Image Steganography Method Based on Chaos Theroy in Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 3, No. 1, 2014.
11. Hamidreza Rashidy Kanan and Bahram Nazeri, "A Novel Image Steganography Scheme with High Embedding Capacity and Tunable Visual Image Quality based on a Genetic Algorithm", Elsevier, Vol. 41, pp. 6123-6130, 2014.
12. Della Baby, Jitha Thomas, Gisny Augustine, Elsa George, Neenu Rosia Michael, "A Novel DWT based Image Securing Method using Steganography", Elsevier, Vol. 46, pp. 612-618, 2015.
13. Xinyi Zhou, Wei Gong, WenLong Fu and LianJing Jin, "An Improved Method for LSB Based Color Image Steganography Combined with Cryptography", IEEE, pp. 1-4, 2016.
14. Hayat Al – Dmour and Ahmed Al – Ani, "A Steganography Embedding Method Based on Edge Identification and XOR Coding", Elsevier, Vol. 46, pp. 293 – 306, 2016.
15. Parsi Kalpana, and Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm", IJRCCT, Vol. 1, No. 4, pp. 143-146, 2012.
16. Md Mijanur Rahman, Tushar Kanti Saha, and Md Al-Amin Bhuiyan, "Implementation of RSA Algorithm for Speech Data Encryption and Decryption", International Journal of Computer Science and Network Security (IJCSNS), Vol. 12, No. 3, pp. 74, 2012.
17. Della Baby, Jitha Thomas, Gisny Augustine, Elsa George and Neenu Rosia Michael, "A novel DWT based image securing method using steganography", Elsevier, Vol. 46, pp. 612-618,2015.

AUTHORS PROFILE

Ambika received the Bachelor of Engineering degree from the University of Visvesvaraya Technological University, Belagavi, in 2011, the M. Tech degree from the University of Visvesvaraya Technological University, Belagavi in 2014, and pursuing the Ph.D. degree from the University of Visvesvaraya Technological University, Belagavi. From 2011 to 2012, she worked as a lecturer in Department of Computer Science & Engineering, Appa Institute of Engineering & Technology, Kalaburagi. she is currently working as an Assistant Professor in the Department of Computer Science & Engineering, Appa Institute of Engineering & Technology, Kalaburagi. Her research interests are in digital image processing, multimedia computing and cryptography.

Dr. Rajkumar L. Biradar received the B.E. degree from the University of Gulbarga, Karnataka, India, in 2001, the M. Tech degree from the VTU, Belgaum, Karnataka, India, in 2004, and the Ph.D. degree from VTU, Belgaum, Karnataka, India, in 2014. From 2007 to 2016, he worked as an Associate Professor in ETM Dept., GNITS, Hyderabad, India. He is currently working as **Professor in** ETM Dept., GNITS, Hyderabad, India. His research interests are in wireless communication, signal and image processing. Received best paper award in two international conferences. Published twenty-nine journal papers in SCI & peer reviewed journals and five papers in international conference.

Dr. Vishwanath Burkpalli received his Ph.D. degree from VTU, Belgaum, Karnataka, India. He is working as Professor in Poojya Doddappa College of Engineering Kalaburagi, Karnataka, INDIA. His research area of interest are Image Processing, Pattern Recognition. He has total experience of 13 years in which 8 years were dedicated to research and development. He has published many paper in various national and international journals.