3.1 Steganography

Steganography can be used to hide a message deliberate for afterward reclamation by a definite person or collection. In this case the intent is to avoid the message being perceived by any other revelry. Steganography includes the cover up of information inside computer files.. The other major area of steganography is copyright marking, where the message to be included is used to declare patent over a article. This can be further divided into watermarking and fingerprinting. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol

Digital steganography can conceal top secret data (i.e. secret files) extremely strongly by embedding them into some media data known as "vessel data." The vessel data is also referred to as "carrier, cover up, or replica data". In Steganography images used for vessel data. The embedding action put into practice is to substitute the "intricate areas" on the bit planes of the vessel image with the secret data. The most significant feature of Steganography is that the embedding capability is incredibly huge. For a 'normal' image, approximately 50% of the data might be disposable with secret data earlier than image damage becomes perceptible.

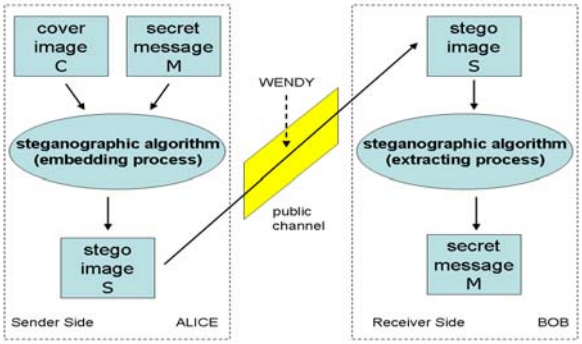

Figure 1: steganographic model

3.2 Multi-Carrier Spread Spectrum Embedding

The procedure of spread spectrum may possibly permit partially to fulfill the above requirements. The embedding technique is intended to assure the perceptual limit and advance the perceive capability as well as the embedding charge. As a substitute of the pixel rate, the histogram can be customized to embed the data. If we observe distinctive histograms of DCT coefficients we will locate some trial include high amplitudes that the widespread Gaussian technique cannot effectively established. We will believe the DCT coefficients whose amplitude is beneath a confident threshold importance. In this embedding proposal, the hidden data is widen over various test of host signal or image by totaling the DCT coefficient as the carrier.

Advantages of spread spectrum procedures are broadly well-known: Invulnerability against multi-path alteration, no necessitate for frequency preparation, high elasticity and uneven data rate transmission. The propensity of diminishing multiple access interference in direct-sequence code- division-multiple-access system is specified by the cross-correlation properties of spreading codes. In the case of multi-path transmission the ability of distinctive one section from others in the complex received signal is obtainable by the auto-correlation properties of the scattering codes. The following figures show entered data; transform data using DCT, embedded image respectively.

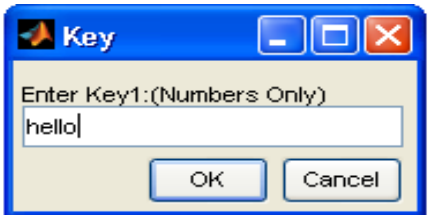

Figure 1: Data entered

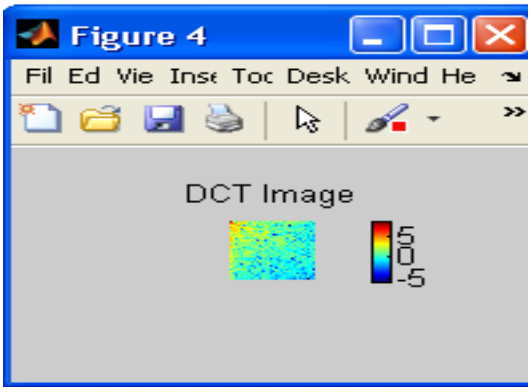

Figure 2: DCT transformation

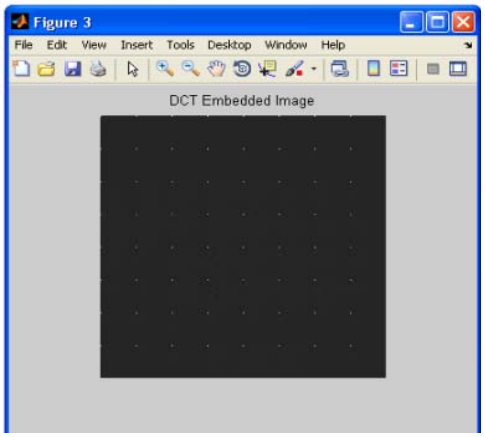

Figure 3: Embedded Image

3.3 Image encryption and watermarking

Encryption is the method of converting the information for its protection. Many image substance encryption algorithms have been projected. To create the data safe from a variety of assault and for the reliability of data we should encrypt the data prior to it is transmitted or accumulated. Government, military, financial institution, hospitals and private business covenant with confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense), product, financial status.

Imperceptible digital watermarks are a innovative technology which could solve the “trouble” of make compulsory the patent of content transmitted across shared networks. They allow a patent holder to insert a concealed message (invisible watermark) within images, moving

pictures, sound files, and even raw text. Moreover, the author can supervise traffic on the shared network for the occurrence of his or her watermark via network system. Because this method obscure both at ease of the message (cryptography) and the occurrence of the message (steganography) an imperceptible watermark is very hard to eradicate.

The host image is an 8-bit or privileged grey height image which has to perfectly be the similar dimension as the basic text image or else resized consequently with the same magnitude.

Pre-conditioning the cipher and the complication practice are take on using a Discrete Cosine Transform (DCT).The output will comprise negative hovering point numbers ahead pleasing the real constituent of a intricate array. The array must be correct by totaling the biggest negative rate in the output array to the equivalent array prior to normalization. For color host images, the twofold coded text can be included into single or entire of the RGB components. The binary plaintext image should include homogeneous margins to minimize the special effects of buzzing due to 'edge effects' when dealing out the data using Cosine transform. The following figure shows the embedding of watermark and detecting watermark.

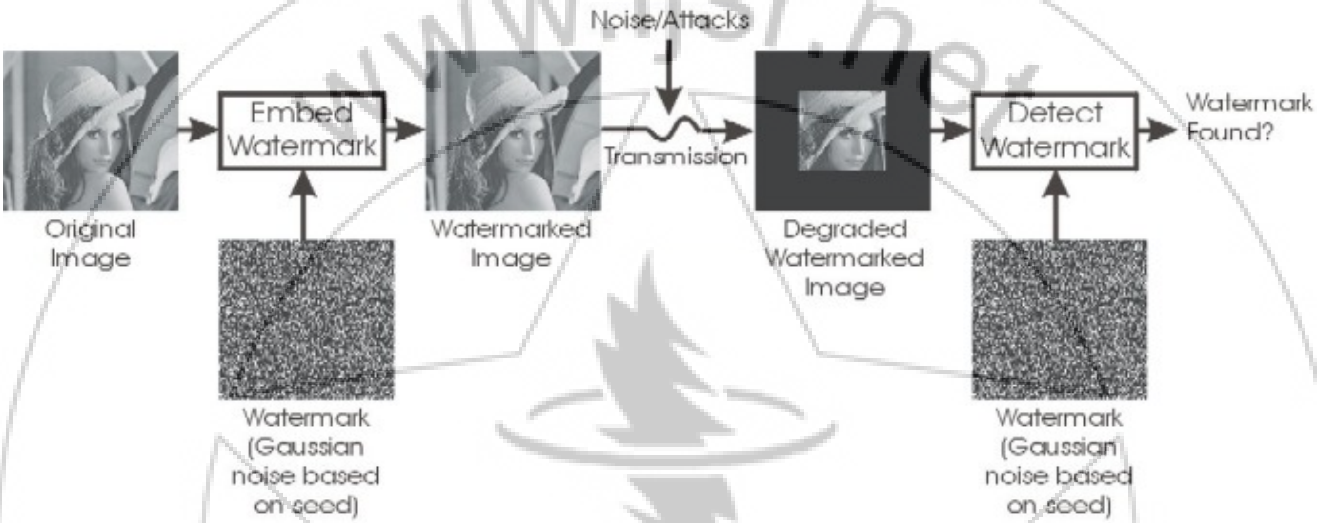

Figure 4: Watermarked Image

3.4 Image decryption and extraction

Decryption is exactly the reverse procedure of encryption. When the receiver obtains encrypted image, extraction of the data from random values and flag values are to be done. This extraction of data from image is considered as the highlighting factor.

The steps to perform M-IGLS algorithm for extracting data from an image is as follows:

Initialize B^ irrationally and swap step wise step among (1) and (2) to accomplish at every pace conditionally indiscriminate least squares rough of one matrix bound particular the further.
The equations used above for computation are

$$V^{\wedge}_{GLS}=\arg_{V\epsilon R}{}^{LxR}\|R_z^{-1/2}(Y-VB)\|^2_F$$
$$=YB^T(BB^T)^{-1} \quad (1)$$

$$B^{\wedge binary}_{GLS}=\arg_{B\epsilon\{\pm1\}}{}^{KxM} \min \|R_z^{-1/2}(Y-VB)\|^2_F$$
$$\approx \text{sgn}\{(V^TR_y^{-1}V)^{-1}V^TR_y^{-1}Y\} \quad (2)$$

End when convergence is accomplished. Observe that (2) stimulate understanding of the autocorrelation matrix Ry, which can be conservative by figure averaging over the expected data interpretation,

$$R^{\wedge}y = 1/M \sum^{M}_{m=1} y(m)y(m)^{T.}$$

The M-IGLS extraction algorithm is review in Table I. Superscripts signify iteration index. The computational density of every iteration of the M-IGLS algorithm is

$$O(2K^3+2LMK+K^2(3L+M)+L^2K)$$

and, experimentally, the number of steps is accomplished between 20 and 50 in broad-spectrum

Table-1
Multi-carrier iterative generalized least squares Algorithm

1) d := 0; initialize B^(0) 2 {±1}K×M arbitrarily.
2) d := d + 1;
V^(d) := $Y(B^{\wedge(d-1)})^T[B^{\wedge(d-1)}(B^{\wedge(d-1)})^T]^{-1}$;
B^(d) := $\text{sgn}\{(V^{\wedge(d)})^TR_y{}^{\wedge-1}(V^{\wedge(d)}))^{-1}(V^{\wedge(d)})^T R_y{}^{\wedge-1} Y\}$
3) Repeat Step 2 until B^(d) = B^(d−1).

4. Results

The proposed technique is to remove the concealed data from the digital media. Here blindly improvement of data is measured. That is the original host end embedding carrier is not necessitating to be known. This technique uses multicarrier embedding and DCT transformation for the embedding the data into the host image. The M-IGLS algorithm is used for the extraction purpose. The following figure shows extracted data and graph for existing and proposed.

Figure : Extracted data

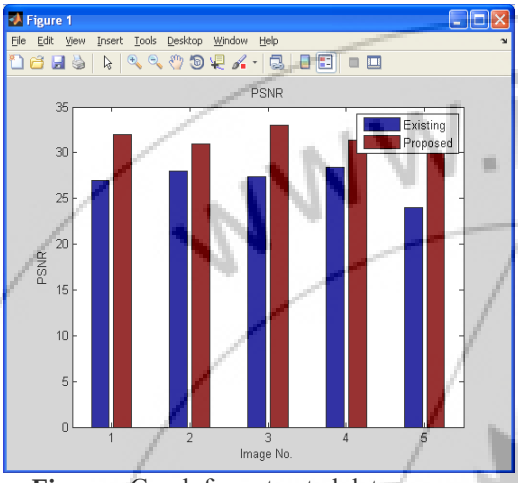

Figure : Graph for extracted data

5. Conclusion and Future Work

Data tracking and tampering is speedily growing in communication. So we have to lock the data from the trackers .Hence we require a vigorous and protected data hiding and extraction format. The most important accord of the proposed system is to afford a good quality extraction technique which measured the blindly improvement of data. This technique uses the M-IGLS algorithm for the extraction. The data is entrenched via DCT transform by multicarrier SS embedding. This extraction procedure will afford high signal to noise fraction and it will achieve the possibility of fault improvement equals to notorious host and embedding carriers. This method is improved by using harmony search algorithm where it offers small time utilization and high assault confrontation.

References

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn."Information hiding. A survey," ,Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.
[2] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 111–119, Mar.2006.
[3] G. Gul and F. Kurugollu, "SVD-based universal spatial domain image steganalysis," IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp.349–353, Jun.2010.
[4] M. Gkizeli, D. A. Pados, and M. J. Medley, "Optimal signature design for spread-spectrum steganography," IEEE Trans. Image Process., vol.16, no.2, pp. 391–405, Feb. 2007
[5] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of watermarking algorithms for improved resistance to compression," IEEE Trans. Image Process., vol. 13, no. 2, pp. 126–144, Feb. 2004.
[6] C. Qiang and T. S. Huang, "An additive approach to transform-domaininformation hiding and optimum detection structure," IEEE Trans. Multimedia, vol. 3, no. 3, pp. 273–284, Sep. 2001.
[7] T. Li andN.D. Sidiropoulos, "Blind digital signal separation using successive interference cancellation iterative least squares," IEEE Trans Signal Process., vol. 48, no. 11, pp. 3146–3152, Nov. 2000

Author Profile

Ch. Anusha received the B. Tech degree in Information technology from Audisankara College of engineering and technology affiliated to JNTU Anantapur during 2008 and now pursuing M.Tech in Computer Science and Engineering from Audisanka institute of technology affiliated to JNTU Anantapur.

V. Sireesha is working as Associate professor at Audisanka institute of technology affiliated to JNTU Anantapur. She received M. Tech in CSE and pursuing PhD in CSE