An Innovative Approach For Spectral Domain Based Data Hiding Using Nearest Neighbour Interpolation

S.Thenmozhi kavitha[1], M.Suresh Thangakrishnan[2]

[1]*M.E. Scholar, Dept. Of CSE, Einstein college of Engineering, Tirunelveli, thenmozhi12694@gmail.com.*

[2] *Associate Professor, Dept. Of CSE, Einstein College of Engineering, Tirunelveli.*

Abstract— **The main objective of this work is to develop a innovative approach for hiding the data. The steganography is the process of concealing one medium of information within another. There are lots of techniques available to achieve steganography like least significant bit insertion method and transform domain technique. In this work, the secret message is to embedded into the image and then this embedded image is used for further sending purpose. It is a technique designed to secure a message by hiding that message within another object so that it can be kept secret from everyone except the intended recipient. The amount of data that can be hidden inside the cover image chosen depends on the properties of the image like number of noisy pixels. This is quite different from cryptography that renders the message (which is typically visible or audible) unintelligible to unauthorized viewers to prevent access.**

Keywords— **data embedding, stegnography, curvlet transform, LSB insertion.**

I. Introduction

Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity).

The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography's goal is to keep its mere presence undetectable, but steganographic systems because of their invasive nature leave behind detectable traces in the cover medium. Even if secret content is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called statistical steganalysis.

Three different aspects in information-hiding systems contend with each other: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stegomedium can withstand before an adversary can destroy hidden information.

Information hiding generally relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity,which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it. A classical steganographic system's security relies on the encoding system's secrecy.

Transform domain techniques embeds the hidden information in the transform domain. Image samples are decorrelated .Toachieve this, key is used. This technique enhances the value of transmission coefficients significantly. The benefit with this method is it becomes easy to embed more data. A quantization technique is used to embed the hidden data. Quantization is another technique that comes handy to retrieve information in a secure manner. The decoding process also involves a key which is same as encoding process. The key is very important in this process because its unavailability at decoder makes the retrieval of information impossible.

LSB Insertion Method is the most popular technique when dealing with images. The simplicity of this method is at the cost of compression which is inherently lossy. The traditional LSB technique takes into account every possible bit. 3 bits are safeguarded in every pixel since there is a option to use red, green or blue. The method works by choosing last bit to store the information. For enhancing security encryption technique is used. This security is achieved at the cost of added complexity. LSB insertion is of prime significance with a gray scale palette. The challenge in LSB technique is the issue of corruption. This means that the integrity of the message is not really taken into consideration. The decoding is relatively simple making it less secure.

digital watermark is digital data that can be embedded into all forms of media content, including digital images, audio, video and even certain objects. Digital watermarks can be easily detected and read by computers, networks and a variety of digital devices, validating the original content and/or initiating actions. Digital watermarking relates to a technology known as steganography, which literally means covered writing. It is a technique designed to secure a message by hiding that message within another object so that it can be kept secret from everyone except the intended recipient. This is quite different from cryptography that renders the message (which is typically visible or audible) unintelligible to unauthorized viewers to prevent access.

During embedding process, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored. If a person makes a modification, then the digital content is said to be attacked. A watermark attack is an attack on digital data where the presence of a specially crafted piece of data can be detected by an attacker without knowing the encryption key. Special attention has to be paid to the kind of attacks as they can help to develop better watermarking techniques and defined better benchmarks. Watermark attacks can be classified into four main groups. The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

II. OUTLINE OF PROPOSED SYSTEM

A. *OVERALL SYSTEM DESIGN*

The work has two main processing parts, they are embedding and extraction. In embedding process the cover image and the secret message is given as the input, and the stego image is produced as the output. In extraction process the stego image is given as the input image and the secret message is produced as the output.

Embedding Process: The embedding process is used to produce the stego image. To do this first the cover image is divided into blocks and then the prediction algorithm is applied to each block to find the blocks which contains the texture information. The prediction error helps to find out the texture blocks. These blocks only used to embed the secret message for providing high visual perception. Then these blocks are collapsed for providing additional security, and then the secret message is encrypted using the encryption technique is applied to produce multilayer security and then the encrypted message is collapsed for avoiding attacks. After that the curvelet transform is applied on the detected blocks and then normalization process is applied and then the collapsed secret image bit is fused with the curvelet normalized curvelet coefficients. Finally the inverse curvelet transform and denormalization is applied. And then the blocks are combined to get the stego image.

Extraction Process: The extraction process is used to get the original secret message from the stego image. To do this first the stego image is divided into blocks and then the prediction algorithm is applied to each block to find the blocks which contains the texture information. The prediction error helps to find out the texture blocks. These blocks only used to extract the secret message for providing high visual perception. Then these blocks are collapsed for providing additional security. After that the curvelet transform is applied on the detected blocks and then normalization process is applied and then extract the secret image bit. Finally these message bit is decrypted to get the original secret message.

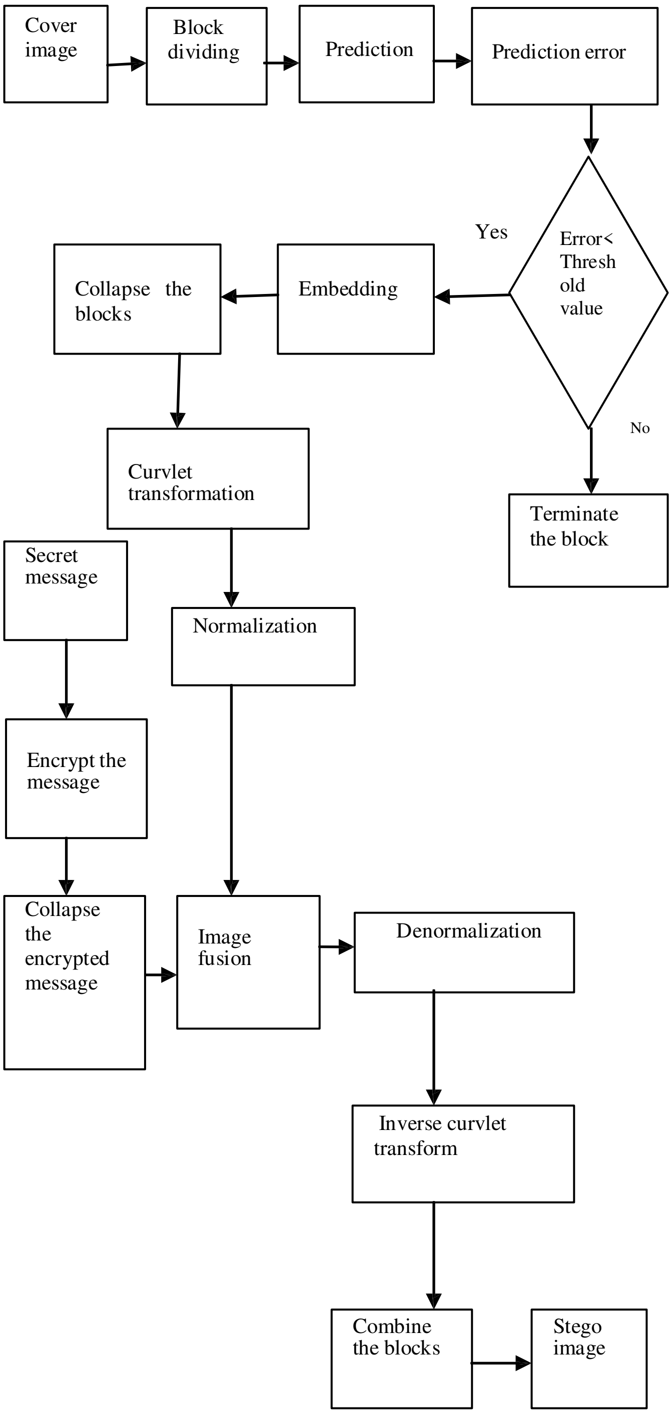

Fig 1. Process Flow Diagram of Embedding

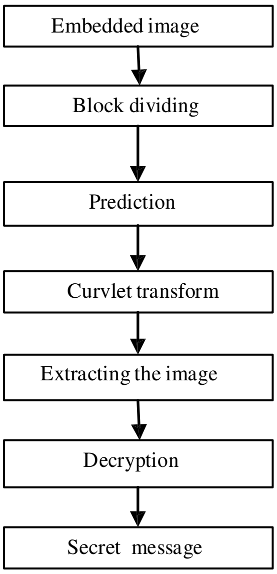

Fig 2: Process Flow Diagram of Extraction

III. METHODOLOGY

In this modern era, computers and the internet are major communication media. They connect different parts of the world and have made the world one global virtual world. As a result, people can easily exchange information without distance being a hindrance. However, the safety and security of long-distance communication is an important consideration. The need to solve this problem has led to the development of steganography schemes. Steganography is a strong security tool that provides a high level of security. But this is particularly when it is combined with encryption. In image steganography image is one of the most popular cover objects. Schemes like LSB insertion and JPEG steganography makes the steganalysis very simple for the opponent. The increasing need of better methods of image steganography has motivated this new concept.

A. Sender Module

The sender module takes the cover image and secret data to be hidden as the input. It performs the encryption of secret data using a password chosen by sender . By embedding bits in the LSB of noisy pixels it hides this encrypted secret data.

B. Block Dividing

The original cover image sized M × N as I, and it is divided into the non-overlapping n × n blocks. For simplicity, assume that M and N can be divided by n with no remainder. Denote all k divided blocks in raster scanning order as Bi, j, where k = M × N/ n2, i = 1, 2, . . . , M/n, and j = 1, 2, . . . , N/n.

C. Prediction and Prediction Error

After block dividing the next step is to find the texture information block. To identify this the interpolation method is used. For do this take the current processing block as Bx,y and its left blocks are Bx,y−1 and upper blocks Bx−1,y, respectively. To find the average value of these two blocks and calculate the difference value of interpolated blocks and the current processing blocks. Then compare the difference value with the threshold value. If the difference value is greater than the threshold value the block contains the structure information so eliminate these blocks. Otherwise the block contains the texture information. These blocks are considered as the embedding blocks.

D. Curvelet Transform

After collapse the blocks then apply the curvelet transform on it. Before apply the curvelet transform the normalization process is applied. After applying the curvelet transform and then the encrypted secret bit is fused with the curvelet transform. Finally the inverse curvelet transform to get the stego image.

Image fusion is the process of merging two images of the same scene to form a single image with as much information as possible. Several fusion algorithms have been proposed extending from the simple averaging to the curvlet transform.

The concept of curvlet transform is based on the segmentation of the whole image into small overlapping tiles and then applying ridegelet transform on each tile.Algorithm for curvelet transform is given below:

1. Split the input images into sub bands using additive wavelet transform.
2. Perform tiling on each of the sub bands .
3. Perform discrete ridgelet transform on each of tile on all the sub bands.

The curvelet transform can be expressed as

$$C(j,l,k)=<f,\varphi_{j,l,k}> \qquad (1)$$

here, j = 0, 1, 2, …, is a scale parameter; l = 0, 1, 2, …, is an orientation parameter; and k = (k1, k2) Z2 is a translation parameter. The mother curvelet is φj (x), its Fourier transform is φj (ω) = Uj (ω), where Uj is frequency window defined in the polar coordinate system such as:

$$U_j(r, \theta) = 2^{-3j/4}W(2^{-j}r)V(2(j/2)\theta/2\pi) \qquad (2)$$

W and V are radial and angular windows respectively and will always obey certain admissibility conditions.

Curvelet at scale 2^{-j}, orientation θ_l and positioncan be expressed as

$$\varphi_{j,l,k}(x) = \varphi_j [R_{\theta l} (x_k^{j,l}) \tag{3}$$

E. Encryption

Encryption includes a message or a file encrypting. Encryption involves converting the message to be hidden into a cipher text. Encryption can be done by passing a secret key. Secret key can be used for encryption of the message to be hidden. It provides security by converting it into a cipher text. This makes it difficult for hackers to decrypt. Greater security is added if the message is password protected. Then while retrieving message, the retriever has to enter the correct password for viewing the message.

The Data Encryption Standard (DES) is a symmetric-key method of data encryption.DES works by using the same key to encrypt and decrypt a message,so both the sender and receiver must know and use the same private key.

When encrypting a message or data using the algorithm, the key is chosen at random from the pool of possible keys.

F. Receiver module

The receiver module takes the cover image with the hidden data as the input. The encrypted secret data is then retrieved by applying suitable algorithm.The secretdata is obtained by using DES decryption algorithm.

It involves retrieving the embedded message from the file. After retrieval the message has to be converted into original message or file. The read data will be in the bytes format. It is essential that the message is in the suitable output file format.

G. Decryption

Decryption involves converting the cipher text into decrypted format. Decryption involves use of a secret key. It enhances security by converting the cipher text, into the original data message or file. The robustness of the system can be increased further if the message is password protected. Then while retrieving message, the retriever has to enter the correct password for viewing the message.

IV. Existing technology

Most image steganographic algorithms adopt an existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion encountered in the stego image. This leads to two drawbacks. First, since the size of the cover image is fixed, the more secret messages which are embedded allow for more image distortion. Consequently, a compromise must be reached between the embedding capacity and the image quality which results in the limited capacity provided in any specific cover image.

Recall that image steganalysis is an approach used to detect secret messages hidden in the stego image. A stego image contains some distortion, and regardless of how minute it is, this will interfere with the natural features of the cover image. This leads to the second drawback because it is still possible that an image steganalytic algorithm can defeat the image steganography and thus reveal that a hidden message is being conveyed in a stego image.

Pixel-based algorithms generate the synthesized image pixel by pixel and use spatial neighborhood comparisons to choose the most similar pixel in a sample texture as the output pixel. Since each output pixel is determined by the already synthesized pixels, any wrongly synthesized pixels during the process influence the rest of the result causing propagation of errors.

V. Conclusions

We In this project a novel approach for hiding is proposed. In the novel approach the prediction algorithm is applied to find the texture information. The prediction error is also applied to find out the texture blocks. In this project multilayer security is also included. Before embed the secret message the encryption technique is applied and then the encrypted message is collapsed for avoiding attacks. In this project the embedding process is done on the curvelet transform. It increases the payload and the quality of the embedded image. The curvelet transform is applied on the detected blocks and then normalization process is applied and then the collapsed secret image bit is fused with the curvelet normalized curvelet coefficients. Experimental results shows that the proposed method performs better than the existing approaches.In future instead of curvelet transform other transform such as ridgelet transform, counterlet transform will be used. Not only that multiple security layers will be included for additional security.

References

[1] Babita Ahuja and, Manpreet Kaur.(2009),'High Capacity Filter Based Steganography', International Journal of Recent Trends in Engineering, Vol. 1, No. 1, pp.672-674.

[2] Chang-Chu Chen, and Chin-Chen Chang(2008), 'LSB-Based Steganography Using Reflected Grey Code', The Institute of Electronics Information and communication Engineers Transaction on Information and System, Vol. E91- D(4), pp. 1110-1116.

[3] Chin- Chen Chang, Yung- Chen Chou and Chia- Chen Lin. (2009), 'A steganography scheme based on wet paper codes suitable for uniformly distributed wet pixels', IEEE International Symposium on circuits and Systems, pp. 501-504.

[4] Debnath Bhattacharyya, Poulami Das, Samir kumar Bandyopadhyay and Tai-hoon Kim.(2009), 'Text Steganography: A Novel Approach', International Journal of Advanced Science and Technology, Vol.3, pp.79-85.

[5] Gaetan Le Guelvouit.(2008),'Trellis-Coded Quantization for Public-Key Steganography', IEEE International conference on Acostics, Speech and Signal Processing, pp.108-116.

[6] Giuseppe Mastronardi, Marcello Castellano, Francescomaria Marino.(2001), 'Steganography Effects in Various Formats of Images. A Preliminary Study', International Workshop on Intelligent data Acquisition and Advanced Computing Systems Technology and Applications, pp. 116-119.

[7] Jan Kodovsky, Jessica Fridrich.(2008), 'Influence of Embedding Strategies on Security of Steganographic Methods in the JPEG Domain', Proceedings of SPIE, the International Society for Optical Engineering, Vol. 6819, pp. 681902.1-681902.13.

[8] Jaya.S, Varalatchoumy.M, Meghali.C, Jitendra.K, Nagesh.H (2013) , 'A Secure Mosaic Image Transmission By Reversible Integer Color Transformation Technique' , International Journal Of Computer Science And Information Technologies, Vol.5 (6) , pp.7443-7445.

[9] Jen Lai.I and Wen Hsiang Tsai.(2011), 'Secret Fragment Visible Mosaic Image - A New Computer Art and Its Application to Information Hiding', IEEE Transactions on Information Forensics and Security, Vol.6 (3).

[10] Jessica Fridrich and David Soukal (2006), 'Matrix Embedding for Large Payloads', SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents , Vol. 6072, pp. 727-738.

[11] Jessica Fridrich, Miroslav Goijan and David Soukal(2003), 'Higher-order statistical steganalysis of palette images', Proceeding of SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents, Vol. 5020, pp. 178-190.

[12] Jun Zhang, Ingemar J. Cox and Gwenael Doerr.G.(2007), 'Steganalysis for LSB Matching in Images With High-frequency Noise', IEEE Workshop on Multimedia Signal Processing, Issue 1-3, pp.385- 388.

[13] Kuo-Chen Wu and Chung-Ming Wang.(2015), 'steganography reversible texture synthesis', IEEE Transactions on Image Processing,Vol.24, No 1.

[14] Lisa M.Marvel and Charles T. Retter.(1998), 'A Methodlogy for Data Hiding using Images', IEEE conference on Military communication, Vol. 3 , Issue 18-21, pp. 1044-1047.

[15] LIU Tong, QIU Zheng-ding.(2002)), 'A DWT-based color Images Steganography Scheme', IEEE International Conference on Signal Processing, Vol. 2, pp.1568-1571.

[16] Mahdavi.M, Samavi.Sh, Zaker.N and Modarres-Hashemi.M.(2008), 'Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram', Journal of Electrical and Electronic Engineering, Vol. 4, No. 3, pp. 59-70.

[17] Merlin.S (2010), 'Covert Image Transmission Technique Using Mosaic Image', Journal of Emerging Trends in Computing and Information Sciences, Vol. 8, No.11.

[18] Mohammed Ali Bani Younes and Aman Jantan.(2008), 'A New Steganography Approach for Images Encryption Exchange by Using the Least Significant Bit Insertion', International Journal of Computer Science and Network Security, Vol. 8, No. 6, pp.247-257.

[19] Neil F. Johnson and Sushil Jajodia. (1998), 'Steganalysis: The Investigation of Hidden Information', IEEE conference on Information Technology, pp. 113-116.

[20] Por.L.Y, Lai.W.K, Alireza.Z, Ang.T.F, Su.M.T, Delina.B.(2008), 'StegCure: A Comprehensive Steganographic Tool using Enhanced LSB Scheme', Journal of WSEAS Transctions on Computers, Vol. 8, pp. 1309-1318.

[21] Raja.K.B, Indhu.S, Mahalakshmi.T.D, Akshatha.S, Nithin.B.K, Sarvajith.M, Patnaik.M.(2008), 'Robust Image Adaptive Steganography using Integer Wavelets', International conference on Communication Systems Software, pp. 614-621.

[22] Ruisong Ye, Weichuang Guo(2013) , ' A Chaos-based Image Encryption Scheme Using Multimodal Skew Tent Maps', Journal of Emerging Trends in Computing and Information Sciences, Vol. 4, No.10.

[23] Shilpa P. Hivrale, Sawarkar.S.D, Vijay Bhosale, and Seema Koregaonkar.(2008), 'Statistical Method for Hiding Detection in LSB of Digital Images', An Overview World Academy of Science Engineering and Technology, Vol. 32, pp. 658-661.

[24] Shruti Sarwate.M.(2014), ' An Approach to Securely Transfer a Secret Image Using Reversible Color Transformations and HSV Color Model', International Journal of Computer Science and Information Technologies, Vol. 5 (6).

[25] Yuan-Yu Tsai, Chung-Ming Wang.(2007), 'A novel data hiding scheme for color images using a BSP tree', Journal of systems and software, Vol.80, pp. 429-437.