Image Hiding with Payload Reduction using Z-Transform Steganography

Thangalatha Legaz. C[1]
Assistant Professor,
Department of Information Technology,
Sri Manakula vinayagar Engineering College,
Puducherry,India

Nivetha. K[2],Saranya. R[2],Mathumathi. V[2]
UG Student,
Department of Information Technology,
Sri Manakula vinayagar Engineering College,
Puducherry,India

***Abstract* - Data Security is critical for most businesses and bank account details in which all the information is potentially dangerous when it falls into wrong hand that can have greater consequences. Steganography is an art that involves hiding of secret data in an appropriate carrier. During the process of embedding, many issues related to capacity and distortion occur which reduce the performance of the system. To overcome this, image compression technique is used which tends to reduce the pixel range to ensure payload is minimized in appropriate manner. In this proposal, image authentication has been made effective by combining Z-transform and lossless compression algorithm. This has been achieved by applying Z-transform technique to embed an image to which compression algorithm is applied to reduce the size of that particular image. As the result exact secret image is achieved during the extracting process with reasonable PSNR in comparison with existing algorithms.**

Keywords: Transform Domain Steganography, Peak signal to noise ratio(PSNR), Z transform(ZT),Least significant bit(LSB),Stego image

I.INTRODUCTION

Steganography is the technique of encoding hidden message in such a way that no one apart from the intended sender and the receiver suspect the existence of the message. Embedding the secret message into various cover media such as text, image, sound files etc. for security and authentication purpose is facilitated using this technique. There are many different forms included in steganography among which transform domain plays a major role in recent applications.

This method exploits the weakness of the human visual system (HVS) which cannot detect the variation in luminance of color vectors at higher frequency side of the visual spectrum.[1]. The most important method to make information more secure is by hiding the information into images. For example one can obtain an embedded bit stream from the various levels of rate and distortion. It was mainly used in diagnosis operations, forensic analysis, as well as scientific or clinical measurements. Transform domain are mainly used to hide messages in significant areas of the cover image.. The selected colors are specified in the color palette in the header of the compressed image. Each pixel just references the index of a color in the color palette. Present proposal is an algorithm which compresses the embedded image for secure transmission. The advantage is that the human eye perceives mainly the spatial changes of brightness than the color. This hybrid proposal provides minimum distortion of visual property and secret image is exactly achieved at the receiver side.

Rest of the paper is organized as follows. Existing methodologies are listed in Section II. Section III deals with the proposed technique. Experimental analysis are given in section IV. Concluding remarks are presented in section V and references are drawn at end.

II.EXISTING METHODOLOGIES

Least significant bit implementation (LSB) : In this method it replaces the LSB in the cover image with the bits from secret information. After altering LSB doesn't change the quality of image to human perception.[2] The drawback is given as Embedding higher bit planes may results in visible artifacts in the stego image.

Discrete cosine transformation : In this transformation Secret data is embedded in the carrier image for DCT coefficients lower than the threshold value.[5] The problem arise are probably arrangement with given stego image are high Extended for different types of carrier media such as color image.

Z transform technique in frequency domain: During Z transform One bit of the hidden data is embedded in each mask of the source onto the LSB of transformed coefficient.[3] Concept of median has been used to select the coefficient for embedding in Z-Transformed domain .The disadvantage is that increased payload can't be transformed.

Compression with reference points coding with threshold values: In this process, a threshold value is associated in the compression process[7]. It is applicable for both lossy

and lossless data compression. It has been observed that coding with threshold values involves complex process.

Encryption Algorithm: It Implements Segmented image files are merged and compress into a single image.[7] Compression method is well suited for gray scale bit map images. This way of compressing a image involve set of techniques.

Data redundancy helps compression: The technique is based on Huffman coding and decoding for scan testing to reduce test data volume, test application time.

Huffman coding suffers from the fact that the uncompresser need have some knowledge of the probabilities of the symbols in the compressed files this can need more bit to encode the file if this information is unavailable compressing the file requires two passesfirst pass: find the frequency of each symbol and construct the huffman tree second pass: compress the file.This image compression method is well suited for gray scale (black and white) bit map images .[8]

III.PROPOSED TECHNIQUE

In this proposed algorithm Z-Transform is applied on a 2*2 masks of a cover image to transform original sub image (cover image) block to its corresponding frequency domain. The dimension of the hidden image is extracted. Along with the hidden image , the dimensional values are also embedded into the real part of the host image mask on fourth LSB bit of the transformed coefficient where the coefficient is chosen based on median of the coefficient of 2 x 2 mask. In the embedding process, dimension of the hidden image followed by the content of the message are embedded.. Huffman coding is then applied here.

Huffman coding is mainly based on the frequency of the data items in which the images are in pixels. In order to encode the data we use the principle of lowering the number of bits in each images .Then the stego image 2*2 matrices are derived from 2*2 cover image matrices and the transformation matrix. In this proposed algorithm transform domain steganography, the cover image are embedded by using Z transform in frequency domain and the stego image is derived.It combines the algorithm of frequency domain Z-transform technique and Huffman lossless compression in steganography. Reverse process is followed during decoding to receive the cover image.

ALGORITHM

The process of steganography is used to make sure that the confidential data is secure by hiding it in any media. The transform domain technique which suggest to cover the message in an image by replacing the least significant bits of original image to corresponding bits of the secret message. This process plays an important role in image authentication to protect the document from unauthorized user. The embedding process is achieved in 2x2 mask in row major order. Using Z-transform the 2x2 gray scale image is transformed from spatial domain to frequency domain.The algorithm for the z transform to embed a secret image and the lossless Huffman compression algorithm to minimize the payload after the embedding process is given below.

\\ Hiding Image Within Another Image

Step 1 : Obtain the size of hidden image ie. p x q .

Step 2: For each hidden image read the input image mask of 2 x 2 in row major order.

Step 3: To obtain the coefficients in transform domain for the selected cover image apply Z-transform.

$$X(z) = \sum_{k=0}^{n} \mathrm{x[k]z^{-k}}$$

Step 4: To choose the byte for embedding get the median from the four frequency coefficients.

Step 5: Embed one secret bit towards left of the byte onto the fourth LSB position.

Step 6: To make the coefficient to be the median of the mask after embedding adjustment can be done.

\\Compressing The Image

Step 7 : Convert the input color image into gray scale image.

Step 8: Identify the pixel value using the function and calculate the probability of each symbol/pixel.

Step 9: Arrange the probability of pixel values in decreasing order and the values which are less or merged.

Step 10: The above step is repeated until two probabilities are left.

Step 11: The compressed data will be given as output only when it is mapped with its corresponding codes.

Step 12: The performance of the process is analysed using PSNR, capacity and the robustness.

.

Here, an image is being hidden in an source image. To encrypt the secret image within an original image it is also necessary to embed the dimension of the secret image. This dimension helps the receiver to verify the decrypted image is same as the cover image. The values are embedded in the fourth least significant bits(LSB) of the image.

The process accepts input as an image which in the secret image and the output of this Z-transform method is an embedded image. Again compression technique is applied to the embedded image to reduce the size and capacity which provide reasonable PSNR. This is facilitated by identifying the probabilities and merging them after arranging in decreasing order. Reverse process is followed during decoding, as the result the secret image is achieved at the receiver .

IV.EXPERIMENTAL ANALYSIS

The statistical and mathematical analysis is given by comparing with various algorithms.. We use the peak-to-signal noise ratio (PSNR) to evaluate qualities of the stegoimages. The table shows the PSNR values for Lenna image in existing methods like SCDFT, QFT and DCT.[9] In all the techniques the dimension of Lenna JPEG image is 512 x 512. In all the existing technique the PSNRs are low, means bit-error rate are high but in the proposed scheme more bytes of authenticating data can be embedded and the PSNR values are significantly high. In DCT based watermarking scheme do not embed watermarks in every single block of image. Here selectively pick the regions that do not generate visible distortion for embedding, thus decreasing the authenticating data size. In QFT based watermarking compensation mark allows the watermark to be undetected even if the strength of it is high.[9] For low compression factor it cannot completely recover the embedded message. In this proposed algorithm the embedding capacity is maximum with higher average PSNR which completely recover the secret image.

Extensive analysis has been made by using Z transform techniques for hiding the secret image into the original image.we incorporate gray scale images for the implementation of z transform technique. It shows a précised output for the given images. Fig(a)shows the input image in which the secret image is to be embedded. Fig(b) shows the secret image which is confidential. Fig(c) shows the embedded image after compression which is the output.

Fig (a) input image

Fig (b) secret image

Fig(c) embedded image

TABLE I. PSNR VALUES OBTAINED FOR VARIOUS TECHNIQUE

TECHNIQUE	PSNR (BITS)
SCDFT	30.104
QFT	30.928
DCT	30.406
Z-TRANSFORM	43.154

Peak signal-to-noise ratio, is a term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. From the survey it is clear that acceptable PSNR ranges from 50-80 Db. In the algorithm like SCDFT (sine cosine discrete fourier transform),QFT (quaternion fourier transform),DCT(discrete cosine transform) shows the ratio below 40 Db. In the Z-transform algorithm after the embedding process 40.14Bps is the value of PSNR. In the compression process it ranges upto 53.14Db which is shown in the graph.(Z-transform with compression).

TABLE II. PAYLOAD MINIMIZATION

VALUES	EMBEDDED IMAGE
PSNR	43.154
NEW PSNR	53.154
ORIGINAL BITS	127004
COMPRESSED BITS	90000

The payload minimization in embedded image which incorporate lossless image compression technique.In the host image Z-transform is applied to embed a secret image into it. After the embedding process the size of the image is increased which is referred as payload. The amount payload is reduced with the lossless Huffman image algorithm. The embedded image has 125400 Bps which is increased amount of payload in an stego image. It is reduced to the considerable value of 90000 after completion of compression process.

V.CONCLUSION

The proposal is based on transformation of confidential data by combining frequency based Z transform technique and huffman image compression. From the result it is clear that the proposed technique obtained consistent PSNR ratio along with good image fidelity for various images which confirm that Z-transformed based image steganography can obtain better visibility/quality along with compression method. This algorithm provides the payload pixels that are converted into binary and while embedding, two bits are considered at a time. At the destination, the secret image is extracted by adopting reverse process of embedding technique. It is observed that with acceptable PSNR and capacity, security has improved compared to existing algorithms .

REFERENCES

1. K B Shiva Kumar, R K Chhotaray, Sabyasachi Pattnaik "Steganography Based Payload Transformation" , International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011
2. V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy "Implementation of LSB Steganography and its Evaluation of different file formats" , Int. J. Advanced Networking and Applications 868 ,2011
3. J. K. Mandal, "A Frequency Domain Steganography using Z Transform (FDSZT)" Association for the Advancement of Modelling and Simulation Technique in Enterprises (AMSE), AMSE journal of Signal Processing and Pattern Recognition, Vol. 51,2012
4. Soumyendu Das , Bijoy Bandyopadhyay "SteganoGraphy and Steganalysis: Different approaches"
5. Hardik Patel, Preeti Dave, "Steganography Technique based on DCT Coefficients" International Journal of Engineering Research and Applications, Vol. 2, Issue 1,Jan-Feb 2012, pp.713-717
6. Ran-Zan Wang,Chi-Fang Lib and Ja-Chen Lin,"Image hiding by optimal LSB substitution and genetic algorithm,"2001 Pattern Recognition Society. Published by ElseivierScience Ltd.
7. A survey in various lossless compression. Dr.Gaurav vijayvargiya, Dr.sanjay silakari,Dr.Rajeev Pandey. Published by International Journal of Computer Science and Information Security, Vol. 11, No. 10, October 2013.
8. Lossless Image Compression Algorithm For Transmitting Over Low Bandwidth Line. Dr.E.KANNAN Registrar &Dean(Academics) Vel Tech Dr.RR & Dr.SR Technical University, G. Murugan Research Scholar,CMJ University Vel ech Dr.RR & Dr.SR TechnicaUniversity Meghalaya Chennai,TN-INDIA INDIA. Published by International Journal of Advanced Research in Computer Science and Software Engineering,volume 2 , issue 2,February-2012
9. Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation (IATFDDFT). Nabin Ghoshal1, J. K. Mandal2 1Department of Engineering and Technological Studies, University of Kalyani, Kalyani, Nadia-741235, West Bengal, India