HVS Based Steganography

Ravi Kumar B

Abstract— The main aim of the project carried is to produce an efficient steganography method which can be avoided by identified through anti-detecting agents ,the project is combination of the two method ,First method is visual criteria and it is followed by data encryption method ,the visual criteria is the method which provide the embedded impact values of the cover image by means of this values stegno image can avoids the pixel distortion of the cover image will embedding the secret message into the cover image, the experimental results later show that the proposed information hiding system can perform well in different types of images.

Index Terms— Contrast masking, Embedding, Embedding impact, Steganography.

I. INTRODUCTION

Steganography is the art of undetectable communication. As opposed to cryptography that conceals the content of a message by encrypting and then communicating it in an overt manner, steganography achieves privacy by hiding the very existence of the message in an innocent looking cover object. Steganography is considered broken if a mere presence of secret message is detected. The concept of steganographic security (statistical undetectability) has been formalized by Caching, In below method have considered the message as image file, as the image are widely used thought the wireless network, The media with the embedded secret message known as the stego medium, which must appear to be similar to its original so that the stego medium cannot arouse suspicion. However, the anti-data hiding research has also rapidly developed to detect the presence of secret messages based on revealing visual or statistical abnormalities in the stego medium. Generally speaking, the more the embedded data, the more vulnerable the system will be to the anti-data hiding attempts, the most important property used for identifying the message is due to pixel distortion of the cover image due to poor embedding method.

In below DCT method considers Human Vision System for embedding the secret message into the cover image, Human Vision System provides the embedding frequency of the cover image, the embedding frequency values of the cover image are utilized by the Viterbi algorithm for embedding secret message into the cover image, Viterbi algorithm is known for its excellent embedding efficiency in several simple known embedding cost models, i.e., constant profile, the linear profile, and the square profile. The proposed steganography scheme can not only achieve a good embedding efficiency performance but also guarantee a high visual quality.

II. PROPOSED SCHEME

As JPEG images are widespread digital image format on Internet, work have focuses on the steganographic schemes of JPEG images. The idea of paper has modified the DCT coefficients of the JPEG image to hide information.

The proposed solution has following steps:-

[1] Divide the cover image into configurable number of blocks.
[2] DCT coefficients are computed for each block.
[3] Calculate the luminance value of each coefficient.
[4] Calculate the contrast masking of each luminance value.
[5] From the luminance value and the contrast masking value embedding impact is calculated.
[6] Sort the coefficients based on the embedding impact and then insert the secret message in these coefficients and also generate a key file with the information of coefficients affected.
[7] To get the secret message from the images, key file is also needed to get the information of affected coefficient and from it and the input image, the secret is extracted.

HVS Embedding Impact Model

DCT (The discrete cosine transforms) is a technique for converting a signal into elementary frequency components. It is widely used in image compression. The developed steganography method developed proposes some simple functions to compute the DCT and to compress images.

The modified DCT coefficients of the JPEG image is used to hide information, Each DCT coefficient has been assigned a changing cost value provided by our embedding impact model. The proposed steganographic algorithm ensures a near-optimal embedding efficiency, i.e. the total embedding impact could be minimal as far as possible.

DCT based image compression using blocks of size 8x8 is considered. An effective method of bit-plane coding of quantized DCT coefficients is proposed. Parameters of post-filtering for removing of blocking artifacts in decoded images are given. The efficiency of the proposed method for test images compression is analyzed. It is shown that the proposed method is able to provide the quality of decoding images higher than for JPEG 2000 by up to 1.9 dB.

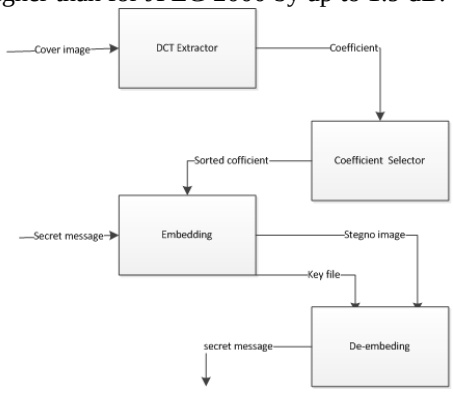


Fig1 .show the software architecture of the system.

III. STEPS TO CARRY

A .DCT EXTRACTION

As an application of information hiding, steganography

Manuscript received May, 2013.

Mr Ravi Kumar B, Information Technology, R.V. College of Engineering,Bengaluru,India.

aims to send secret messages under the cover of a carrier signal. A steganographic technique should generally possess two important properties: good visual/statistical imperceptibility and a sufficient payload. The first is essential for the security of hidden communication and the second ensures that a large quantity of data can be conveyed. While many digital watermarking techniques use characteristics of Human Vision Sensitivity, (HVS)-based steganographic techniques are also developed to embed a large amount of secret bits into a still image with high imperceptibility, in which more data are inserted into busy areas. For example, in the bit-plane complexity segmentation (BPCS) method, blocks with a bit plane of high complexity, defined as the number of transitions from 1 to 0 or from 0 to 1, are replaced with the secret data. Another technique, termed the Pixel-Value Differencing (PVD) method, segments the cover image into no overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A larger difference in the original pixel values allows a greater modification. In these methods, data embedding is performed in a block-wise fashion. In other words, the numbers of bits of secret data carried by individual pixels in the same block are made identical. In fact, however, even two adjacent pixels may have different tolerance for steganography modifications in terms of visual and statistical detestability.

This can be exploited to accommodate more secret data without introducing additional detectable traces. The work have provided an alternative steganographic method in which the data to be hidden are re-expressed based on a multiple-base notational system and then embedded into pixels according to the different degree of pixel value variation in the immediate neighborhood. Embedding strength is varied over the entire host image on a pixel-by-pixel basis, allowing more secret data to be carried in busy areas. On them receiving side, the original image is not needed for recovering the embedded message.

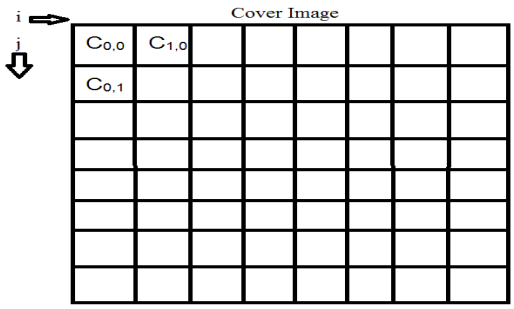


Fig 2.DCT extractor – which split the image to blocks, extracts the coefficients

The cost of a flipping at one pixel when embedding, ρ, could be computed as follow:

• Get the DCT coefficients of the cover image by block $C_{i,j,k}$ where i, j ($0 \le i, j \le 7$) index the DCT frequency in the individual block, and k indexes the block number.

$$c_{i,j,k} = t_{i,j,k} \left(c_{0,0,k} \sqrt{c_{00}} \right)^{\alpha t} .$$

Eq. (1) Compute the luminance masking of every DCT coefficient.

where $t_{i,j}$ should be made a assuming display luminance, and initial values are shown in Table1;$c_{0,0,k}$ is the DC coefficient of the k_{-th} block, which represents the average brightness of the block k; $C_{0,0}$ is the DC coefficient, which represents the average brightness of whole image; and a_T controls the degree to which this masking occurs, where in it suggests 0.649 . Equation (1), I can find the higher the average brightness of image blocks are, the greater the luminance masking, $t_{i,j,k}$ is.

$$m_{i,j,k} = \max[t_{i,j,k} \left| C_{i,j,k} \right| w_{i,j} \; t_{i,j,k}^{1-w_i}].$$

Eq. (2) Calculate the contrast masking, $m_{i,j,k}$, with the above $t_{i,j,k}$.

Here, $w_{i,j}$ is an exponent that lies between 0 and 1, and a typical empirical value is 0.7. Obviously, contrast masking effect on the different band of image is different, and it depends on the different band information contained. The equation (2) is widely used in vision models, which indicates that, the smaller the value of $m_{i,j,k}$ is, the more sensitive human eye on the frequency would be, i.e., the higher the cost of modifying the carrier element is. Therefore, The work suggest to avoid modifying the carrier elements with smaller value $m_{i,j,k}$.

$$\rho_{i,j,k} = 1/ \, m_{i,j,k}$$

Eq. (3) calculates the Embedding impact.

The $\rho_{i,j,k}$ means the embedding impact caused by flipping the cover element $C_{i,j,k}$ for data hiding. When the value of $\rho_{i,j,k}$ is bigger, the distortion caused by modifying $C_{i,j,k}$ is greater.

1.40	1.01	1.16	1.66	2.40	3.43	4.79	6.56
1.01	1.45	1.32	1.52	2.00	2.71	3.64	4.93
1.16	1.32	2.24	2.59	2.98	3.64	4.60	5.88
1.66	1.52	2.59	3.77	4.55	5.30	6.28	7.60
2.40	2.00	2.98	4.55	6.15	7.46	8.71	10.17
3.43	2.71	3.64	5.30	7.46	9.62	11.58	13.51
4.79	3.67	4.60	6.28	8.71	11.58	14.50	17.29
6.56	4.93	5.88	7.60	10.17	13.51	17.29	21.15

Table I Frequency Perception Table

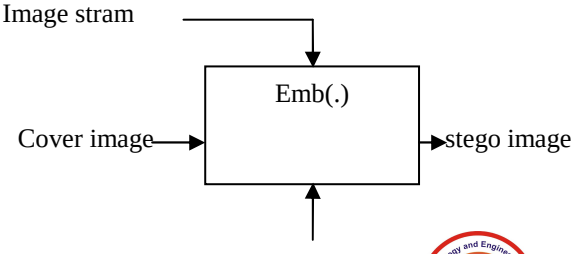
B. Data Embedding Procedure

Assuming binary embedding operation, let sequence s =($s1$, $s2$, ..., sm)Є$\{0,1\}^m$ be secret messages, and x = ($x1$, $x2$, ...,xn)Є$\{0,1\}^n$ ($m < n$) be elements of cover object, here, I use least significant bit (LSB) of DCT coefficients to embed the secret messages. After slightly modifying some of elements in x for hiding s, stego object y is produced, that is, y = ($y1$, $y2$, ...,yn)Є$\{0,1\}^n$. I also define the function of total embedding impact $D(x, y)$,

$$D(x, y) = \left\| x - y \right\|_{\rho} = \sum_{i=1}^{n} \rho_i \left| x_i - y_i \right|.$$

Eq. (4) calculate the total embedding impact $D(x, y)$.

Fig.(1) shows the proposed embedding procedure. Here, stegnography method just uses the JPEG image as cover image. The cover stream x$\{0,1\}^n$ derived from the LSB of DCT coefficients, except the DC and zero ones. For security consideration, the DC and zero ones should avoid flipping during the information hiding. The embedding impact $\rho_{i,j,k}$ of each element in cover with DCT coefficient $C_{i,j,k}$ from Equation (2) and Equation (3).



Secret image ————————

Fig 3:- Shoes the Data Embedding procedure.

Then, work begin to embed the secret sequences by Modifying the cover stream x which is shown in the central Part of the Fig. 3.The relation between secret messages s and stego medium can be expressed as matrix form as (5),

$$Hy^{T} = s^{T}$$

Eq .(5) calculates the parity check method.

First, we have to construct a good and practical parity check matrix H sized m×n, which means H should be easily generated and restored. The paper suggest, H can be generated by a Small sub matrix H^{s} of size h×w . Here, the height h of H^{s} is called the constraint height (in the pseudo code, h=10), and the Width w equals to 1/α where α is the embedded rate.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

In terms of embedding capacity and distortion, the performance of our method is measured by comparing with the F5 algorithm. Usually there are several approaches to measure the distortion or image quality induced by data embedding, such as peak signal to noise ratio (PSNR), root mean squared error (RMSE). But these simple mathematically defined metrics in the literature are image-independent without consideration of the HVS characteristics, here, stegnography method use the universal quality index (short Q) which performs significantly over simple mathematical measures as a combination of correlation loss, luminance distortion, and contrast distortion.

In the first experiment, to carry by taking Lena, Peppers, Baboon and Bridge of 256×256 with quality factor 30, 50, 70, 90 respectively as cover images, and compare the universal quality index of our method and F5 under the same quality factor and the same bits of hidden messages. In Fig. 3, it shows that our method always has higher Q values than F5, which means a better visual quality.

V. CONCLUSION

The proposed method achieves a good rate-embedding efficiency performance as well as guarantees the high visual quality. Introduction of the Watson's work, stegno method build a HVS embedding distortion model which assigns an imbedding cost for each DCT coefficient of the cover elements. The syndrome-trellis codes help to minimize the total imbedding impact. Our experimental results indicate that it outperforms the F5 significantly in visual quality and statistic characteristics under different types of images and different payload. The problem to embed a given payload with minimal embedding impact always drew data hider's attention. In the future, the study can be carried on dynamic distortion model during the embedding processing.

ACKNOWLEDGMENT

The author would like to thank Mr. B K Srinivas, Assistant Professor, Department of Information Science and Engineering, RVCE for his help, sharing his technical expertise and expert advice.

Last but definitely not the least I would like to thank my parents and friends who have always supported me in every path of life.

REFERENCES

[1] Willems F. and Dijk M., "Capacity and codes for embedding information in Gray-Scale Signals," IEEE Trans. Information Theory, 2005, pp. 1209-1214.

[2] Zhang X and Wang S, "Efficient Steganographic Embedding by Exploiting Modification Direction,"IEEE Communications Letters, 2006, pp. 781-783.

[3] Fridrich J. and Filler T., "Practical methods for minimizing embedding impact in steganography, " Proc. SPIE, 2007, pp. 650502.1-15.

[4] Zhang W., Zhang X., and Wang S., "Maximizing steganographic embedding efficiency by combining hamming codes and wet paper codes," Proc.10th Information Hiding Conf., 2008, pp. 60-71.

[5] Fridrich J., "Asymptotic behavior of the ZZW embedding construction," IEEE Transactions on Information Forensics and Security, 2009, pp.

[6] Filler T., Judas J., and Fridrich J., "Minimizing embedding impact in steganography using trellis-coded quantization," Proc. SPIE, Electronic Imaging, Media Forensics and Security XII, San Jose, CA,January 17, 2010, pp. 501-514.

Mr. RAVI KUMAR B was born in Bellary, completed his Diploma at TMAE's Polytechnique , completed his Bachelor if degree at City Engineering College, present studying Masters of technology in Information Technology at RV college of Engineering.