Image Steganography Based on Entropy Thresholding Scheme

B.S.Patil, A.H.Karode, S.R.Suralkar

Abstract— In this paper, we present image steganography based on entropy thresholding scheme via digital images that contains redundant information can be used as covers or carrier to hide secrete message. After embedding a secrete message into the cover image so called stego image is obtained. We introduce a new forensic tool that can reliably detect distortion due to steganography and watermarking and modify those images that were originally stored in the JPEG format. Due to JPEG compression we get unique fingerprints and used as a "fragile watermark" enabling us to detect changes as small as modifying the LSB of one randomly chosen pixel. The detection of changes is based on investigating the compatibility of 8×8 blocks of pixels with JPEG compression with a given quantization matrix. The use of local criteria to choose where to hide data can potentially cause de-synchronization of the encoder and decoder. This synchronization problem is solved by the use of powerful, but simple-to-implement, erasures and errors correcting codes, which also provide robustness against a variety of attacks.

The proposed system is used to hides large volume of data in an image as well as it will limit the perceivable distortion that might occur in an image while processing it. This project has an advantage over other information security software because the hidden text is in the form of images, which are not obvious text information carriers. The main advantage of this project is a simple, powerful and user-friendly GUI that plays a very large role in the success of the application.

Index Terms— Steganography, data hiding, jpeg, DCT

I. INTRODUCTION

Rapid growth in the demand and consumption of digital information in past decade has led to valid concerns over issues such as content security, authenticity and digital right management. Imperceptible data hiding in digital images is an excellent example of demonstration of handling these issues. Classical Cryptography is related with concealing the content of messages, whereas, Steganography is related with concealing the existence of communication by hiding the messages in cover. This paper presents a robust and secured method of embedding high volume of text information in digital Cover-images without incurring any perceptual distortion. It is robust against intentional or unintentional attacks such as image compression, tampering, resizing, filtering and Additive White Gaussian Noise (AWGN). The schemes available in the literature can deal with these attacks individually, whereas the proposed work is a single methodology that can survive all these attacks. Image Adaptive Energy thresholding (AET) is used while selecting the embedding locations in frequency domain.

Manuscript received October, 2013.

Mr.B.S.Patil, Student, M.E.IInd Year, S.S.B.T'S COET Bambhori,Jalgaon, India.

Mr.A.H.Karode, Assistant Professor, E&TC, S.S.B.T'S COET Bambhori, Jalgaon, India.

Mr.S.R.Suralkar, Associate Professor, E&TC, S.S.B.T'S COET Bambhori, Jalgaon, India.

Coding framework with Class Dependent Coding Scheme (CDCS) along with redundancy and interleaving of embedded information gives enhancement in data hiding capacity. Perceptual quality of images after data hiding has been tested using Peak Signal to Noise Ratio (PSNR) whereas statistical variations in selected Image Quality Measures (IQMs) are observed with respect to Steganalysis. The results have been compared with existing algorithms like STOOL in spatial domain, COX in DCT domain and CDMA in DWT domain [3].

Possible additional requirements for data hiding could be robustness to image modifications –this is the domain of sometimes confusingly called watermarking techniques, undetectability, etc. As long as the embedded signal remains invisible there is no upper bound to the amount of embedded information but the larger the amount of information the easier it is to detect the presence of an embedded signal; this might be undesirable when dealing with watermarking [7].

1. DCT Transform for Images:

The first step is the actual transformation of the image. For JPEG, the Discrete Cosine Transform (DCT) is used, but similar transforms are for example the Discrete Fourier Transform (DFT). These mathematical transforms convert the pixels in such a way as to give the effect of "spreading" the location of the pixel values over part of the image. The DCT transforms a signal from an image representation into a frequency representation, by grouping the pixels into 8 × 8 pixel blocks and the pixel blocks into 64 DCT coefficients each. A modification of a single DCT coefficient will affect all 64 image pixels in that block.

The next step is the quantization phase of the compression. Here another biological property of the human eye is exploited: The human eye is fairly good at spotting small differences in brightness over a relatively large area, but not so good as to distinguish between different strengths in high frequency brightness. This means that the strength of higher frequencies can be diminished, without changing the appearance of the image. JPEG does this by dividing all the values in a block by a quantization coefficient. The results are rounded to integer values and the coefficients are encoded using Huffman coding to further reduce the size.

Originally it was thought that steganography would not be possible to use with JPEG images, since they use lossy compression which results in parts of the image data being altered. One of the major characteristics of steganography is the fact that information is hidden in the redundant bits of an object and since redundant bits are left out when using JPEG it was feared that the hidden message would be destroyed. Even if one could somehow keep the message intact it would be difficult to embed the message without the changes being noticeable because of the harsh compression applied. However, properties of the compression algorithm have been

exploited in order to develop a steganography algorithm for JPEGs.

One of these properties of JPEG is exploited to make the changes to the image invisible to the human eye. During the DCT transformation phase of the compression algorithm, rounding errors occur in the coefficient data that are not noticeable. Although this property is what classifies the algorithm as being lossy, this property can also be used to hide messages. It is neither feasible nor possible to embed information in an image that uses lossy compression, since the compression would destroy all information in the process. Thus it is important to recognize that the JPEG compression algorithm is actually divided into lossy and lossless stages. The DCT and the quantization phase form part of the lossy stage, while the Huffman encoding used to further compress the data is lossless. Steganography can take place between these two stages. Using the same principles of LSB insertion the message can be embedded into the least significant bits of the coefficients before applying the Huffman encoding. By embedding the information at this stage, in the transform domain, it is extremely difficult to detect, since it is not in the visual domain [13].

II. THE PROPOSED SCHEME

We propose a framework for hiding large volumes of data in images while incurring minimal perceptual degradation. The embedded data can be recovered successfully, without any errors, after operations such as decompression, additive noise, and image tampering. The proposed methods can be employed for applications that require high-volume embedding with robustness against certain non-malicious attacks. The hiding methods we propose are guided by the growing literature on the information theory of data hiding [22].

The key novelty of our approach is that our coding framework permits the use of local criteria to decide where to embed data. In order to robustly hide large volumes of data in images without causing significant perceptual degradation, hiding techniques must adapt to local characteristics within an image. The main ingredients of our embedding methodology are as follows.

(a) As is well accepted, data embedding is done in the transform domain, with a set of transform coefficients in the low and mid frequency bands selected as possible candidates for embedding. (These are preserved better under compression attacks than high frequency coefficients)

(b) A novel feature of our method is that, from the candidate set of transform coefficients, the encoder employs local criteria to select which subset of coefficients it will actually embed data in. In example images, the use of local criteria for deciding where to embed is found to be crucial to maintaining image quality under high volume embedding.

(c) For each of the selected coefficients, the data to be embedded indexes the choice of a scalar quantizer for that coefficient. We motivate this by information theoretic analysis.

(d) The decoder does not have explicit knowledge of the locations where data is hidden, but employs the same criteria as the encoder to guess these locations. The distortion due to attacks may now lead to insertion errors (the decoder guessing that a coefficient has embedded data, when it actually does not) and deletion errors (the decoder guessing that a coefficient does not have embedded data, when it actually does). In principle, this can lead to desynchronization of the encoder and decoder.

(e) An elegant solution based on erasures and errors correcting codes is provided to the synchronization problem caused by the use of local criteria. Specifically, we use a code on the hidden data that spans the entire set of candidate embedding coefficients, and that can correct both errors and erasures. The subset of these coefficients in which the encoder does not embed can be treated as erasures at the encoder. Insertions now become errors, and deletions become erasures (in addition to the erasures already guessed correctly by the decoder, using the same local criteria as the encoder). While the primary purpose of the code is to solve the synchronization problem, it also provides robustness to errors due to attacks.

Two methods for applying local criteria are considered. The first is the block-level Entropy Thresholding (ET) method, which decides whether or not to embed data in each block (typically 8X8) of transform coefficients, depending on the entropy, or energy, within that block. The second is the Selectively Embedding in Coefficients (SEC) method, which decides whether or not to embed data based on the magnitude of the coefficient. Reed-Solomon (RS) codes are a natural choice for the block-based ET scheme, while a “turbo-like" Repeat Accumulate (RA) code is employed for the SEC scheme. We are able to hide high volumes of data under both JPEG and AWGN attack. Moreover, the hidden data also survives wavelet compression, image resizing and image tampering attacks.

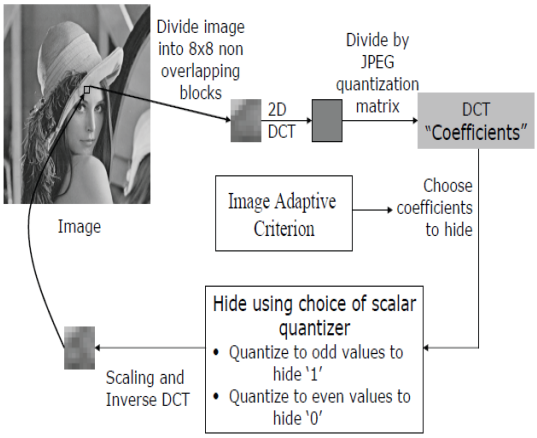

Figure 1: Image-adaptive embedding methodology

It is observed that the perceptual quality as well as the PSNR is better for the image with hidden data using local criteria. Note that though the PSNR is only marginally better, the actual perceptual quality is much better. This indicates that the local criteria must be used for robust and transparent high volume embedding.

Although we do not use specific perceptual models, we refer to our criteria as `perceptual' because our goal in using local adaptation is to limit perceivable distortion. Figure 1 shows a high-level block diagram of the hiding methods presented. Both embedding methods, the entropy thresholding (ET) scheme, and the selectively embedding in coefficients (SEC) scheme, are based on joint photographic experts group (JPEG) compression standard. As seen in the Figure 3.1, the techniques involve taking 2D discrete cosine transform (DCT) of non-overlapping 8X8 blocks, followed by embedding in selected DCT coefficients [13].

1. Entropy Thresholding

The entropy thresholding scheme uses the energy of an 8 x 8 block to decide whether to embed in a block or not. Only those block whose entropy exceeds the predetermined threshold are used to hide data.8 x 8 blocks by aij and the corresponding DCT coefficients by Cij ,
where I, j €{ 0,1……7}.
Thus

$$C=DCT2 \quad \ldots\ldots\ldots\ldots (1)$$

Where, DCT2 denotes a two-dimensional DCT.
Next, the energy of block is computed as follows

$$E=\sum ij \| cij \|2 \ , \ i, j \in \{0,1\ldots..7\}, (I, j) \neq 0 \quad \ldots.. (2)$$

It should be noted that the dc coefficient is neither used for entropy calculation nor for information embedding. This is because JPEG uses predictive coding for the dc coefficients and hence, any embedding induced distortion would not be limited a single 8 x 8 block.
The embedded procedure is as follows: The image is divided into 8 x 8 non overlapping blocks, and 8 x 8 discrete cosine transform (DCT) of the blocks is taken. For a quantizer hiding scheme based on JPEG, one observes less distortion when embedding in low frequency DCT coefficients because of JPEG's finer quantization in this range. However, JPEG uses predictive encoding for the DC coefficients, x00, of successive blocks, so the additive uniform noise model does not apply. Furthermore, distortion induced in these coefficients would not be localized to their 8x8 block. We therefore do not use these to embed data.
Next, we computed the 2-norm entropy of each 8x8 block as follows,

$$E = \sum ij \| xij \| 2, \quad (i, j) \neq (0, 0) \ldots\ldots\ldots\ldots\ldots (3)$$

Only those coefficient blocks whose entropy exceeds a predetermined threshold are used to hide data. Likewise, the decoder checks the entropy of each 8_8 block to decide if data has been hidden. The threshold entropy is determined by the desired embedding rate (or allowable distortion) for a particular image.
In general, compression will decrease the entropy of the coefficient blocks. Therefore, it is necessary to check that the entropy of each block used to embed information, compressed to the design quality factor, still exceeds the threshold entropy. If a particular block fails this test, we keep it as such, and embed the same data in the next block that passes the test.

2. DESCRIPTION OF AN ENTROPY BASED EMBEDDING TECHNIQUE

Our embedding technique is based on the modification of the least significant bits. In order not to compromise the overall image quality, the algorithm adapts the number of embedded bits to the image content. The steps of the algorithm are the following (we assume that the image is defined on 8 bits):
A. The image is divided in 8x8 pixels wide blocks.
B. For each 8x8 block, denoted by B, compute the entropy H (B) on the 4 most significant bits. If the entropy is larger than 2, then embed information in the 4 least significant bits of B , else go to step 3.
C. For each block compute the entropy H (B) on the 5, most significant bits. If the entropy is larger than 2, then embed information in the 3 least significant bits of B, else embed information in the 2 least significant bits of B.
Because the entropy computed during step 2 is based on the 4 most significant bits, there are only 16 possible values and therefore the entropy is contained in the [0, 4] interval. The threshold of 2 was chosen to be in the middle of this interval. The entropy computed during step 3 is different from that of step 2 as the computation is based on 5 bits; accordingly the entropy is contained in [0, 5]. In all cases, the algorithm provides a minimum of embedded bits per pixel. But in the best case, the number may raise to 4 bits.
At the reception side, a similar algorithm is used in order to extract the embedded message:

1. The image is divided in 8x8 pixels wide blocks.
2. For each 8x8 block, denoted by B, compute the entropy H (B) on the 4 most significant bits. If the entropy is larger than 2, then retrieve from 4 least significant bits of B, else go to step 3.
3. For each block compute the entropy H (B) on the 5, most significant bits. If the entropy is larger than 2, then retrieve from the 3 least significant bits of B, else retrieve from the 2 least significant bits of B.

Figure 2 shows images and several statistics like the original size, the entropy per pixel H(C) and the maximal size of the message that might be embedded. The last row provides the average number of embedded bits per pixel. In the case of the Dice image, the upper size of the embedded image is exactly equal to bits per pixel as could be expected. Because the algorithm adaptively determines the number of bits to embed based on the image content, we expect no subjective difference between an original image and that image after information embedding; however, this assumption has not been tested on an exhaustive list of image samples [14].

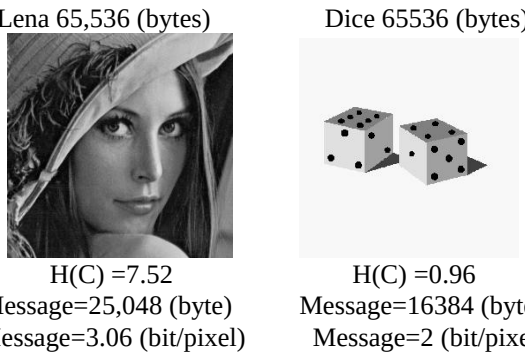

Figure 2: Images and sizes of the message that can be embedded.

III. SIMULATIONS AND RESULTS

1. Data hiding capacity

Initially all the images from image data set have been applied as the input to the embedding algorithm to embed 1000 ASCII characters of a text file 'A-message.txt'. Out of 3545 images from the image data set 3025 images were eligible with VCs more than the encrypted number of bits. The proposed CDCS scheme saves lot of coding bits that are needed to be embedded in Cover-images as shown in Table 1. This saving can further be increased with increase
in message length as well as increase in r as shown in Fig. 5. It can be observed that increase in data hiding capacity is the result of saving the number of bits while coding the characters with proposed CDCS mechanism.

2. PSNR variations

The PSNR is most commonly used as a measure of perceptual quality of Stego image. The signal in this case is the original

Cover-image (C), and the noise is the error introduced due to embedding in Stego-image (S). PSNR is used as an approximation to human perception of reconstruction quality. A higher PSNR would normally indicate that the reconstruction is of better quality. PSNR is computed in terms of Mean Squared Error (MSE) of two m × n monochrome images C and S as,

PSNR = 10 log10 MAX2/MSE = 20 log10 MAX/MS …….. (4)

Where,

MAX is the maximum possible pixel value of the image

And,

MSE = 1/mxn ∑x=1, M ∑y=1, N (p(x, y) - p'(x, y)) 2 …….. (5)

TABLE I Variation in PSNR

	Proposed Scheme	IWT [15]	HDWT [15]
Images Bits	Lena		
10332 Bits	36.34	31.8	33.58
	Mandril_gray		
15260 Bits	34.76	33	-

IV. CONCLUSION

We have proposed a scheme for data hiding in images uses entropy thresholding schemes. In this scheme the message is embedded in to cover image that will produced stego image. This stego image quality is analized by using various parameters like PSNR, MSE, SSIM. This method is an adaptive data hiding method with which one can adjust capacity factor to balance between the image quality and the embedding capacity dynamically. Furthermore, the proposed method is securer than most of its predecessors.

REFERENCES

[1] Lee Yeuan-kuen et al. An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding [J]. 2009, Pg. No. 349-360

[2] Omid Zanganeh, "Image Steganography Based on Adaptive Optimal Embedding", Faculty of Computer Science and Information Systems University Technology Malaysia Johor, Malaysia.2009 Pg. No. 600-605

[3] Suresh Mali & Pradip Patil, "Robust And Secured image adaptive Data Hiding", Faculties from VIT COE Pune 2011.

[4] Kevin Curran, Internet Technologies Research Group, "An Evaluation of Image Based Steganography Methods" University of Ulster Karen Bailey, Institute of Technology, Letterkenny, Ireland , International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2.

[5] MasoudNosrati Kermanshah, "An introduction to steganography methods" University of Kermanshah Medical Science, Kermanshah, Iran World Applied Programming, Vol. (1), No (3), August 2011. 191-195

[6] N.Wu and M. Hwang. "Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan. 2007.

[7] Marc Van Droogenbroeck And JérômeDelvaux, "An Entropy Based Technique For Information Embedding In Images" IEEE Benelux Signal Processing Symposium (SPS-2002), Leuven, Belgium, March 21–22, 2002 Pg. No. S02-81-84

[8] W. Bender,W. Butera,D. Gruhl,R. Hwang,F. J. Paiz, Pogreb Applications, "for data hiding" IBM systems journal, vol. 39, nos. 3&4, 2000 Pg.no. 547-568

9] Neil F. Johnson & Stephen C. Katzenbeisser "A Survey Of Stegnographic Technique" Chapter no. 3 Pg. No. 43-78

[10] Kaushal Solanki, Student Member, IEEE, "Robust Image-Adaptive Data Hiding Using Erasure and Error Correction" IEEE Transactions On Image Processing, Vol. 13, No. 12, December 2004 Pg. No. 1627-1639.

[11] Chin-Chen Chang, "High Capacity data hiding in JPEG-Compressed images", Information, 2004, Vol. 15, No. 1, 127–142

[12] Jessica Fridrich, MiroslavGoljan, Rui Du, "Steganalysis Based on JPEG Compatibility", Centre for Intelligent Systems, Department of Electrical Engineering, SUNY Binghamton, Binghamton.

[13] Prof. Akhil Khare, Meenu Kumari, Pallavi Khare, "Efficient Algorithm For Digital Image Steganography", journal of information 2009 to 10 vol.1 ISSN 0975-6728

[14] Marc Van Droogenbroeck And JérômeDelvaux, "An Entropy Based Technique For Information Embedding In Images", Proc.3rd IEEE Benelux Signal Processing Symposium (SPS-2002), Leuven, Belgium, March 21–22, 2002

[15] R.O.EI Safy, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", Faculty of Engineering, Brenham University 2009. Pg. No. 111-117

Mr. Bhushan S. Patil received his B.E. degree in Electronics & Telecommunication Engineering from S.R.E.S.COE Kopargaon , Pune University in 2008. He is M.E. Student in S.S.B.T'S C.O.E.T Bambhori, Jalgaon, and North Maharashtra University. He is working as H.O.D. in Industrial Electronics Department in Smt.S.S.Patil Institute of technology (Polytechnic) Chopda, Dist.Jalgaon. He has 5 years of teaching experience. His research interest includes Image Processing.

Mr. Atul H Karode received his B.E. degree in Electronics Engineering from S.S.B.T'S C.O.E.T Bambhori, Jalgaon, and North Maharashtra University in 1999. He received his M.E degree from Professor Ram Meghe Institute of Technology & Research Badnera Amravati, SGBAU Amravati University in 2010. Recently, he is working as Assistant Professor in Electronics & Telecommunication Engineering Department in S.S.B.T'S C.O.E.T Bambhori, Jalgaon. He has 12 years of teaching experience. His research interest includes Image Processing & Pattern recognition.

Mr. Shekhar R. Suralkar received his BE degree in Electronics and Telecommunication Engineering from SSGM College of Engineering Shegaon, Amravati University, and received his ME degree from Motilal Nehru Regional College of Engineering Allahabad University, Now he is pursuing P.hD. in the same Department, recently he is working as Head and Associate Professor in Electronic and Telecommunication Engineering Department in SSBT`s College of Engineering Bambhori, He has 22 Years Teaching Experience, His research interest includes pattern recognition and Biometrics authentication.