ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
DIIF 0.876

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 8, AUGUST 2015, PP 497-504

Design of an adaptive JPEG Steganalysis with UED

[1]K.Samunnisa,[2] M.Sri Lakshmi, [3]Dr S.Prem Kumar
[1](M.Tech), CSE, Assistant professor Department of Computer Science and Engineering
[2]Assistant Professor, Department of Computer Science and Engineering
[3]Professor & HOD, Department of computer science and engineering,
G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.

Abstract: Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient suspects the existence of the message a form of security through obscurity. The internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue now days. In this paper, we proposed a class of new distortion functions known as uniform embedding distortion function (UED) is presented. By incorporating the syndrome trellis coding, the best code word with undetectable data hiding is achieved. Due to hiding more amounts of data into the intersected area, embedding capacity is increased. Our aim is to hide the secret information behind the image file. Steganography hides the secret message so that intruder's can't detect the communication. When hiding data into the intersected area, thus provides a higher level of security with more efficient data mean square error is reduced and embedding capacity is increased.

Keywords: JPEG Steganography, Minimal-Distortion Embedding, Uniform Embedding, Distortion Function Design.

I. INTRODUCTION

Steganography is an art and a science of communicating in a way, which hides the existence of the communication. It is also called as covered writing because it uses a cover of a message for sending any important secret message. Steganography serves as a means for private, secure and sometimes malicious communication. Steganography is the art to hide the very presence of communication by embedding the secret message into the innocuous-looking cover media objects. Steganography is a powerful tool which increases security in data transferring and archiving. Steganography can be applied to different objects like text, picture, image, audio or video. This objects called cover object or carrier object of the steganography method. The secret message can also be of types like text, picture, image, audio or video. These objects are called message object. After application of steganography method the produced output file is called stego-object. Cryptography is an art of sending the secret information in the unreadable form. Both Steganography and Cryptography have the same goal of sending the secret message to the exact receiver. In Steganography, the secret message is hidden in any of the cover medium and then transmitted to the receiver, whereas in cryptography, the secret message is made unreadable and then transmitted to the receiver in an unreadable form. The message that is sent to receiver through cryptography, express out that some secret communication is going on between the sender and the receiver. This leads to the main drawback of the cryptography. In steganography, only the sender and receiver know the secret communication. Image steganography is carried out using different techniques. This method is broadly classified based on Spatial-domain and transform-domain. In Spatial domain, the secret messages are embedded directly. The steganography scheme embeds the secret message by modifying the Gabor coefficients of the cover image. The data hiding technique using DWT was performed on both the secret and cover images. The secret message is embedded in the high frequency coefficients in DWT performed on cover. This approach of information hiding technique has recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks of existence. This project comprehends the following objectives: To produce security tool based on steganography techniques. To reduce the distortion between the cover object and stego object is an important issue for steganography. The mainstream (and by far the most successful) approach is framing the embedding as source coding with a fidelity constraint and build the embedding around a distortion function that is minimized to embed a desired payload. Upon closer inspection of these references, one discovers that the distortion functions are always designed either in the embedding domain or in a selected model (feature) space. The first alternative can be rightfully challenged as, for example, changing a DCT coefficient has an effect on an entire block of pixels, and the detect ability of this embedding change needs to consider this fact. Designing distortion in a model space is more appealing but can only succeed with a sufficiently comprehensive source model to avoid creating security holes for the Warden who chooses to work outside of the model. In this paper, we propose a distortion function that allows careful analysis of the impact of making an embedding change on the local content and thus introduce less detectable artifacts. We work with a wavelet representation of the cover image (if the image is represented in some other domain, such as JPEG, it is first decompressed to the spatial domain prior to the wavelet transform), which can be viewed as a representation obtained using a bank of directional filters. Interpreting the highest frequency un decimated sub bands as directional residuals, one can assess the impact of an embedding change in multiple directions, which allows us to constrain the embedding changes to textures and noisy regions of the image while avoiding smooth content as well as clean edges. This is a model-free approach as we do not work with a feature representation of the cover image.

II. EXISTING AND PROPOSED SYSTEMS

A. Existing System Steganography is the science and art of Secret communication where the sender embeds secret message into an original image (cover) with a shared key to generate a stego image. To conceal the very existence of communication, the stego image has to be statistically undetectable from its cover counterpart. Therefore, the two conflicting objectives un detect ability and embedding payload, should be carefully considered when devising a steganography scheme. X ∈Rn and y ∈ Rn as the cover and stego images, respectively. We then define the cost (or distortion) function of making an embedding change at i -th element of x from xi to yi as ρi (xi, yi), where $0 \leq \rho i < \infty$. Under the additive distortion model, the total impact caused by the embedding can be expressed as the sum of embedding cost over all elements, i.e., D (x, y) = _ni=1 ρi (xi, yi). In practice, the problem of designing a secure steganography scheme can be formulated as the minimal distortion embedding, i.e., to minimize the total embedding distortion D for a given payload. With properly designed ρi, the total statistical artifacts caused by the embedding are minimized and the resulting stego objects can be made less detectable. As JPEG is the most widely used format for digital image storage and transmission, JPEG steganography has become the domain of extensive research. It has witnessed the development of a lot of schemes for JPEG steganography over the last decade, such as F5, nsF5, MME and some recently emerged adaptive ones. All of these schemes can be described with a unified framework, the minimal distortion embedding framework, which consists of the coding unit and the distortion function. In the F5, the embedding impact is treated equally for each coefficient. As a result, minimizing the total distortion f or a given payload corresponds to the effort to minimize the number of coefficients to be modified, or maximize the embedding efficiency, i.e., the number of message bits embedded per embedding change. The security performance of F5 was improved by increasing its embedding efficiency through matrix encoding, which can be viewed as a special case of the minimal distortion embedding frame work with the embedding cost being identical for each coefficient. In, the wet paper code (WPC) is incorporated in nsF5, improved version of F5, to tackle the issue of shrinkage withF5, resulting in significant improvement in coding efficiency compared to the Hamming code used in F5. In the MME, for JPEG steganography, the advantage of the side-information of the original uncompressed image is taken to construct the distortion function, furthermore, only those coefficients with less distortion are selected to be modified, and more coefficients may be modified compared with the matrix coding proposed in another efficient JPEG steganography scheme, denoted as BCH opt, based on heuristic optimization and fast BCH syndrome coding. Compared with the MME, the BCH opt takes into account not only the rounding error but also the quantization step in the construction of distortion function, thus leading to significant improvement in security performance against st performance gain of both MME and BCH opt stems largely from the original BMP image as pre cover, which is, however, not always available in practice. In Filler proposed to use syndrome trellis coding (STC) as a practical approach for the implementation of minimal distortion embedding framework. They have shown that, under the additive distortion model, the STC can achieve asymptotically the theoretical bound of embedding efficiency for a user-defined distortion function.

B. Proposed System

In this paper, we focus on the design of a new additive distortion function for JPEG steganography. By following the concept in spirit of spread spectrum communication, the proposed distortion function is designed so as to guide the stego system to uniformly spread the embedding modification to the quantized DCT coefficients of all possible magnitudes. This results in possible minimal artifacts of first- and second-order statistics for DCT coefficients as a whole. It is noted that, for non side-informed JPEG steganography, our proposed distortion function is derived directly from the quantized block DCT coefficients without any pre-model training. An efficient JPEG steganography scheme is then developed by incorporating the new distortion function in the STC framework, which works quite well against the popular steganalysis with various feature sets this paper Proposed, includes several new contributions:

- The detailed analysis why the proposed UED function can lead to less average changes of second-order statistics besides the first-order ones;
- The analysis of the allowable modification (embedding) rate of DCT coefficients with different magnitude from the perspective of natural image model;
- The new scheme for side-informed JPEG 2000 steganography; and
- Implementation of all the experiments on the new BOSS• base image database, which is widely considered as a more appropriate benchmark to evaluate the performance of the steganography and steganalysis schemes.

III.SYSTEM STUDY

Data Embedding Steps

1. Preprocessing

2.Embedding operation

3. Distortion function

4. STC coding

5. Post processing

1. Preprocessing

The preprocessing is adopted to generate the cover, i.e., the quantized DCT coefficients for data embedding. When input image is original BMP image, the process starts from the implementation of JPEG compression. In this way, the side information, i.e., the rounding error is available for a more secure data embedding. Then the rounding errors obtained .When the input image is in JPEG format, the entropy decoding is applied to generate the quantized DCT coefficients c directly.

Quantization table – Some researchers modified standard quantization tables for their research purposes. JPEG digital image uses a standard 8×8 quantization table, as Table 1(standard brightness quantization table). The standard quantization tables can get a very good image processing effect, so the table is commonly used. Chang et al. presented to change middle frequency coefficient of the standard quantization table to1 and get a new 8×8 quantization table, as Table 2.In our proposed method, we produced an 8×8 quantization table, as Table 3. For embedding purposes, the middle and higher frequency of the produced quantization table were set to be 1 in the Table.3.

2. Embedding Operation

The scramble stego DCT coefficients and embedding operation are performed. For scrambled AC coefficients the distortion of a modified coefficient, the embedding operation itself should be defined. The important of reducing a chance of the information being detected during the transmission

Embedding algorithm – The procedure of embedding a secret message in a cover image is in Figure 1. It can be described as follow:-

1. The message (M) to be embedded in the cover image.

2. The cover image is divided into non-overlapping blocks of 8×8 pixels and applies DCT to each block to get DCT coefficients.

3. The DCT coefficients are quantized by the modified 8×8 quantization table (Table.3). In this quantization

table, the values 1 represent the middle and high frequency to be used for embedding (54 values).

4. The least two-significant bits of each middle and high frequency coefficient in the quantized DCT blocks are modified to embed two secret bits.

5. The JPEG entropy coding (Run-Length coding and Huffman coding) is applied to compress these resultant blocks, and then the stego image is obtained.

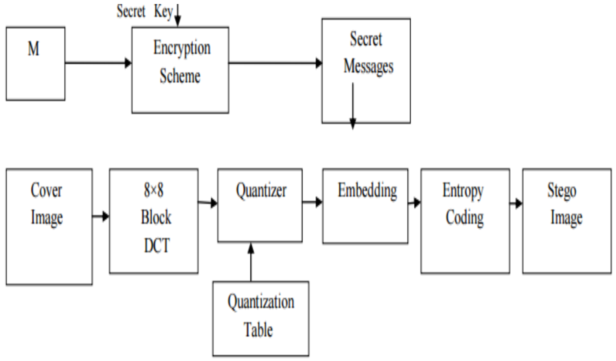


Figure 1 Embedding Procedure Block Diagram

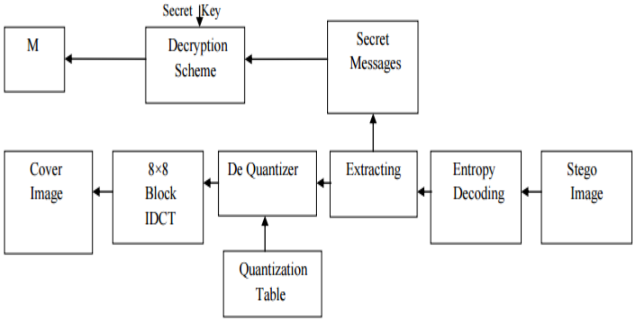


Figure 2 Embedding Procedure Block Diagram

Extraction algorithm – The extraction process is the inverse of the embedding process. The procedure of extracting a secret message from a cover image is in Figure 2. 1. The stego- image is entropy decoded using the coding tables (Huffman tables) located in the image header. 2. As a result, we get the blocks of quantized DCT coefficients modified according to the secret message. From each predefined middle and high frequency coefficients of each block, we retrieve least two significant bits (secret bits). 3. We put these retrieved bits in the same order of embedding to get the secret message (M).

3. Distortion Calculation

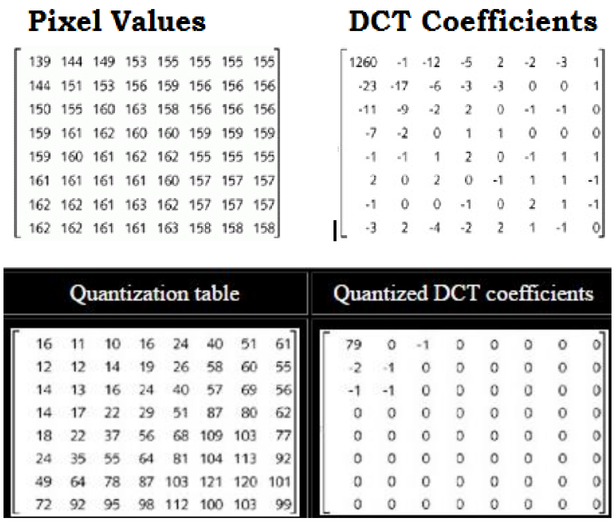
Compute the embedding distortion for each scrambled nonzero AC coefficient using the sided UED defined in where the additional rounding error of the embedding distortion for each scrambled non-zero AC coefficient using the JC-UED defined.

4. STC Coding Since the embedding operation is deterministic as in which is guided by the rounding error we can only use the binary STC. Let the binary vector are used in corresponding embedding cost ρ as input parameters, the binary STC coding is then applied to embed secret message m. The output of coding is scrambled.

Discrete Cosine Transform

The remaining values are transformed, 8x8 blocks at a time, by a forward Discrete Cosine Transform, which is going to transform your values into frequencies. It sounds complex but it's not. It's just a matter of describing your numbers no more by their values, but by coefficients of a mathematical expression. Think about how easier it is to describe a line by the two coefficients a and b in the mathematical formula "y = ax + b" than by keeping the coordinates of hundreds of points that belong to that line. Ah, beauty of mathematics: you can describe infinity of very particular points with just two coefficients! The formula here is more complex than a simple linear one, and, as its name implies, it involves a decomposition of your signal into several cosines functions of different frequencies. A little bit like Fourier transform. You will transform the 64 values into 64 frequency coefficients. In other words, you will describe 64 values with 64 coefficients. Now you're thinking... So what is the point? Replacing 64 values by 64 new values? No gain of space! Well, the point is that in "natural" images (remember JPEG is made for photography), most of these coefficients will be very low, and we can get rid (at the next step) of a lot of them, and still reconstruct the original values with a good accuracy. At this point you have the DCT coefficients.

Still trying to give visual examples, here is on the left an example 8x8 block of pixel values. It could be luminance or chrominance data, whatever you want. The 8x8 block on the right is after a forward DCT transform. The low frequency coefficient is on the top left. It's the highest value, because it encodes the data with the highest importance and the lowest frequency: basically the average value of this entire block pixel. See how these coefficients are still high around the top left corner, and then, the more you go to the bottom right (the high frequencies), they go down. We will remove a lot of these small values at the next step. Right now, if you do an inverse cosine transform from these coefficients, you will recover exactly the starting pixels values, minus the rounding errors.



Pixel Values

139	144	149	153	155	155	155	155
144	151	153	156	159	156	156	156
150	155	160	163	158	156	156	156
159	161	162	160	160	159	159	159
159	160	161	162	162	155	155	155
161	161	161	161	160	157	157	157
162	162	161	163	162	157	157	157
162	162	161	161	163	158	158	158

DCT Coefficients

1260	-1	-12	-5	2	-2	-3	1
-23	-17	-6	-3	-3	0	0	1
-11	-9	-2	2	0	-1	-1	0
-7	-2	0	1	1	0	0	0
-1	-1	1	2	0	-1	1	1
2	0	2	0	-1	1	1	-1
-1	0	0	-1	0	2	1	-1
-3	2	-4	-2	2	1	-1	0

Quantization table

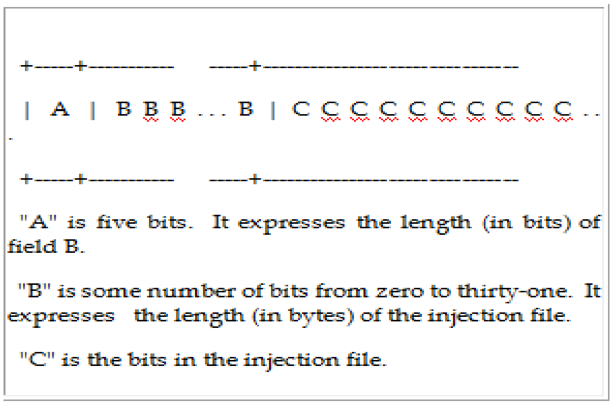
16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Quantized DCT coefficients

79	0	-1	0	0	0	0	0
-2	-1	0	0	0	0	0	0
-1	-1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

5. Post processing

Once the modified pattern is obtained, the cover x is modified with to obtain stego y. The k is defined as secret key function. For both cases, the entropy coding is then applied to generate stego JPEG image after y is descrambled. Although JSteg deals with the complex JPG format, it embeds the hidden information in a very simple way, which is even detailed nicely in the readme file. The hidden information is not even encrypted, and that's why I chose this steganography program as an introduction to JPG steganography. Basically, the DCT coefficients which are equal to zero or one are not modified. The other ones are used to embed sequentially one bit of the hidden information, by overwriting their Least Significant Bit (LSB). The hidden information has this format (copy-pasted from the readme, a bit simplified):



```
+-----+-----------     -----+--------------------------------
| A | B B B . . . B | C C C C C C C C C C C . .
+-----+-----------     -----+--------------------------------
```

"A" is five bits. It expresses the length (in bits) of field B.

"B" is some number of bits from zero to thirty-one. It expresses the length (in bytes) of the injection file.

"C" is the bits in the injection file.

So now I know this, I simply extract one bit at a time the LSBs of the first five DCT coefficients to get the size of the size (the field "A"), get the of the next bits to have the size of the hidden data (the field "B"). And finally I can extract the hidden data (the field "C"), reconstructing bytes from the extracted bits.

6. Cover image

To conceal the very existence of communication, the stego image has to be statistically undetectable from its cover counterpart. Steganography hides the existence of the message so that intruders can't detect the communication and thus provides the major requirements of data hiding are that the hidden data must be imperceptible. Therefore, the two conflicting objectives, i.e., undetectability and embedding payload, should be carefully considered when devising a steganographic scheme. The embedding operation is deterministic as in which is guided by the rounding error is scrambled into stego image in the data embedding operation.

C. Data Extraction

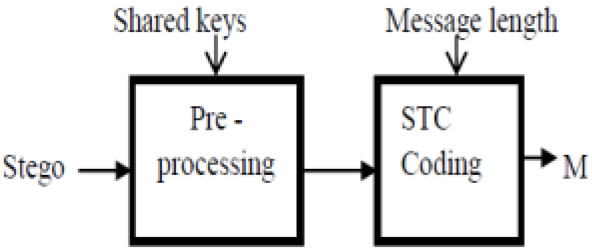


Fig 3. Data Extraction.

1. Data Extraction steps

Data extraction is the process of extracting the original image from the stego image of the scrambled message.

Preprocessing: For a stego JPEG image, the quantized DCT coefficients are obtained by entropy decoding, which are then scrambled with the shared key K to generate the scrambled non-zero AC coefficient.

Shared keys: To conceal the very existence of communication, the stego image has to be statistically undetectable from its cover counterpart of the generating the secret messages.

STC Decoding: The STC decoding binary STC and ternary STC is then applied to extracted message. The decoding is the reverse operation of the encoding method. The syndrome trellis coding method is the used for both binary and ternary.

IV.SYSTEM ARCHITECTURE:

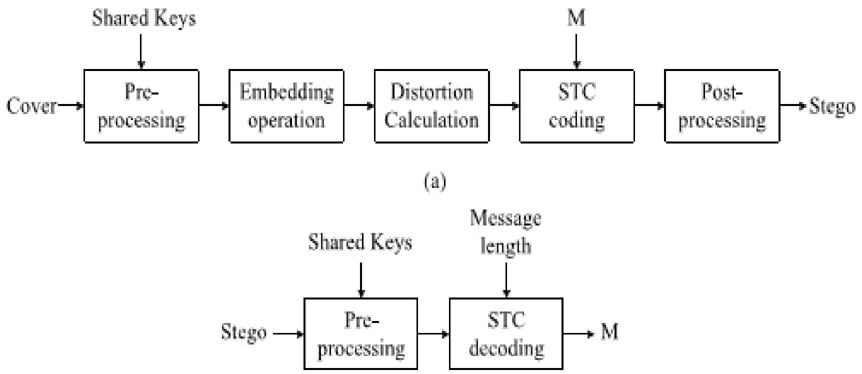
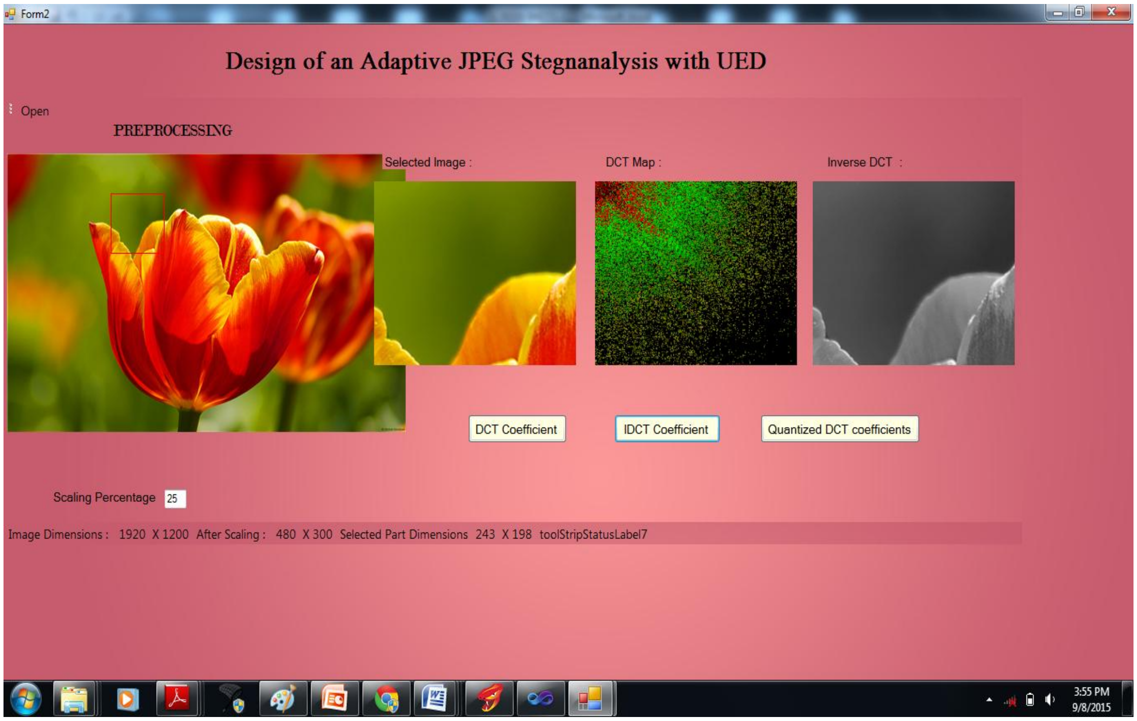


Fig 4. System Architecture

V.EXPERIMENTAL RESULTS

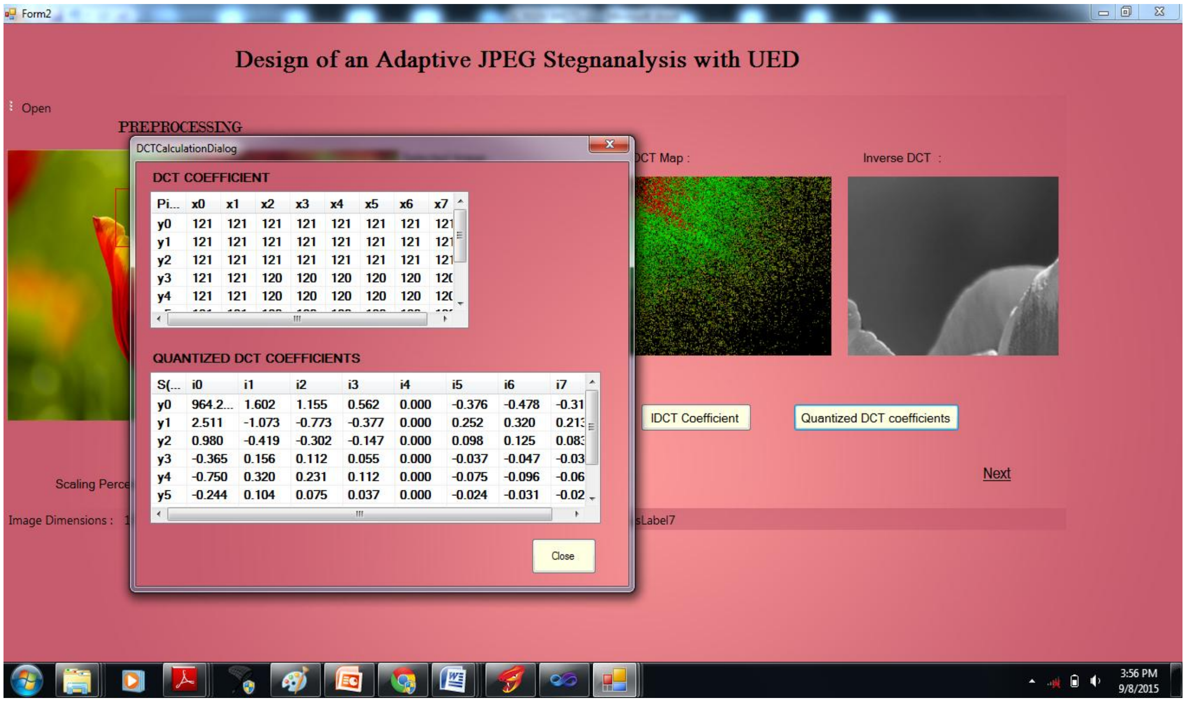


Scaling Percentage 25

Image Dimensions : 1920 X 1200 After Scaling : 480 X 300 Selected Part Dimensions 243 X 198 toolStripStatusLabel7

Fig 3. Quantized DCT Coefficients generated image

Description: here with this screen generation of Quantized DCT Coefficients from generated DCT image.



DCT COEFFICIENT

Pi...	x0	x1	x2	x3	x4	x5	x6	x7
y0	121	121	121	121	121	121	121	121
y1	121	121	121	121	121	121	121	121
y2	121	121	121	121	121	121	121	121
y3	121	121	120	120	120	120	120	120
y4	121	121	120	120	120	120	120	120

QUANTIZED DCT COEFFICIENTS

S(...	i0	i1	i2	i3	i4	i5	i6	i7
y0	964.2...	1.602	1.155	0.562	0.000	-0.376	-0.478	-0.31
y1	2.511	-1.073	-0.773	-0.377	0.000	0.252	0.320	0.213
y2	0.980	-0.419	-0.302	-0.147	0.000	0.098	0.125	0.083
y3	-0.365	0.156	0.112	0.055	0.000	-0.037	-0.047	-0.03
y4	-0.750	0.320	0.231	0.112	0.000	-0.075	-0.096	-0.06
y5	-0.244	0.104	0.075	0.037	0.000	-0.024	-0.031	-0.02

Fig 4. DCT Calculation Dialog

Description: here with this screen calculation of DCT Coefficients

VI.CONCLUSSION:

In this paper we review the process of Image compression with secret information with DCT Techniques , while embedding secret information into image how the values of DCT Coefficients and its quantized calculations among embedding and decoding images, finally we demonstrate the process of UED with DCT and IDCT Process.

REFERENCES:

[1] C. C. Chang, T. S. Chen and L. Z. Chung, “A steganographic method based upon JPEG and quantization table modification”, Information Sciences, vol. 141, 2002, pp. 123-138.

[2] Parvinder Singh, Sudhir Batra, H R Sharma, "Message Hidden in 6th and 7th Bit", Proceedings of International Conference on Controls, Automation and Communication System, Dec. 22-24, 2004, Allied Publishers, pp-281- 284.

[3] Parvinder Singh, Sudhir Batra, HR Sharma, "Evaluating the Performance of Message Hidden in 1st and 2nd Bit Plane", WSEAS Transactions on Information Science and Applications, issue 8, vol 2, August 2005, pp 1220- 1227.

[4] Parvinder Singh, Sudhir Batra, HR Sharma, "Message Hidden in 1st and 2nd Bit Plane", Proceedings of 9th WSEAS International Conference on Computers, Athens, Greece, July 14-16, 2005, pp 1-5.

[5] Parvinder Singh, Sudhir Batra, H R Sharma, "Steganographic Methods Based on Digital Logic", 6th International Conference on Signal Processing, Dallas, USA, March 22-24,2007.

[6] Prince Kumar Panjabi, Parvinder Singh, “An Enhanced Data Hiding Approach using Pixel Mapping Method with Optimal Substitution Approach”, International Journal of Computer Applications, vol.74(10), July 2013, pp. 36- 43.

[7] Parvinder Singh, Sudhir Batra, HR Sharma, "Hiding Credentials in Biological Images", A & B Research, vol 22(1), Jan 2006, ISSN 0970-1970, pp 22-25.

[8] Sonam Chhikara, Parvinder Singh, “SBHCS: Spike based Histogram Comparison Steganalysis

Technique", International Journal of Computer Applications, vol.75, 2013.

[9] Sudhir Batra, Parvinder Singh, "A Class of $ q $-ary 2-IPP Codes", Journal of Informatics and Mathematical Sciences 5 (2), 65-76.

[10] Parvinder Singh, Sudhir Batra, HR Sharma, "A review of digital signatures and status in India", WSEAS Transactions on Computers 4 (4), 408-410.

[11] Jasvinder Kaur, Manoj Duhan, Ashok Kumar, "Digital Logic Embedding Using Single Row." International Journal on Computer Science & Engineering, vol. 3, no. 12 , 2011.

[12] Penne baker, William B., and Joan L. Mitchell, "JPEG: Still Image Data Compression Standard", Van Nostrand Reinhold, 1993.

[13] H. W. Tseng and C.C. Chang, "Steganography using JPEG- compressed images", Fourth International Conference on Computer and Information Technology, CIT '04, 14-16 Sept 2004, pp .12-17.

[14] Kobayashi, H., Y. Noguchi and H. Kiya (1999), "A method of embedding binary data into JPEG Bitstreams" IEICE Trans. Information and Systems, J83-D-II, 1469–1476.