International Journal of Engineering Research and Development
eISSN : 2278-067X, pISSN : 2278-800X, www.ijerd.com
Volume 2, Issue 3 (July 2012), PP. 01-07

Multimedia Data Compression by Dynamic Dictationary Approach with Stegnography Facility

[1] Kanindra Shrivastava, [2] Vinay Jain, [3] Mohan Awasthi
[1,2,3] *Dept. of E&TC, SSCET BHILAI, India*

Abstract—This paper presents a proposal for communication which is major part of daily life of today.We are living an age of science. . With the increasing communication traffic demand, data security has become very important field. Lots of data security and data hiding algorithms have been developed in the last decade. we are implementing a method of "Digital Stenography" for image data hiding. Image Steganography system allows an average user to securely transfer text messages by hiding them in a digital image file. A combination of Steganography and encryption algorithms provides a strong backbone for its security. Digital Image Steganography system features innovative techniques for hiding text in a digital image file or even using it as a key to the encryption.

I. INTRODUTION

The word steganography is of Greek origin and means "covered, or hidden writing". Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Generally, a steganographic message will appear to be something else: a picture, an article, a shopping list, or some other message. A steganographic message (the plaintext) is often first encrypted by some traditional means, producing a cipher text. image steganography system is a stand-alone application that combines steganography and encryption to enhance the confidentiality of intended message. The user's intended message is first encrypted to create unintelligible cipher text. Then the cipher text will be hidden within an image file in such a way as to minimize the perceived loss in quality. The recipient of the image is able to retrieve the hidden message back from the image with this system.

The JPEG format is currently the most common format for storing image data. It is also supported by virtually all software applications that allow viewing and working with digital images Recently, several steganographic techniques for data hiding in JPEGs have been developed .

II. IMAGE STEGANOGRAPGY ALGORITHM

The OutGuess steganographic algorithm was proposed to counter the statistical chi-square attack . In the first pass, similar to J-Steg, OutGuess embeds message bits along a random walk into the LSBs of coefficients while skipping 0's and 1's. After embedding, the image is processed again using a second pass. This time, corrections are made to the coefficients to make the stego image histogram match the cover image histogram. Because the chi-square attack is based on analyzing first-order statistics of the stego image, it cannot detect messages embedded using OutGuess. Provos also reports that the corrections are made in such a manner to avoid detection using his generalized chi-square attack .

In our attack on OutGuess, we use the fact that the embedding mechanism in OutGuess is overwriting the LSBs. This means that embedding another message into the stego image will partially cancel out and will thus have a different effect on the stego image than on the cover image.

Outguess
Proposed by Neils Provos in 2001 as a response to the ststistical chi –square attact by Andreas Westfeldin 1999.

Main feature of outguess

1. outguess hides messages in JPEG files
2. It embeds hides messages in bits in LSBs of quantized

DCT coefficients along a key –dependent walk through the image.

a) Outguess Preserves the histogram of DCT coefficients exactly.
b) Outguess cannot be detected using the chi –square attack or its generalized versions.
c) Embed secret information in DCT domain.
d) Modifies LSBs of DCT coefficients at random locations.
e) Corrects statistical deviation by modifying unused LSBs.
f) Distribution of DCT coefficients is preserved after embedding process.
g) An a priori embedding capacity for an image can be determined

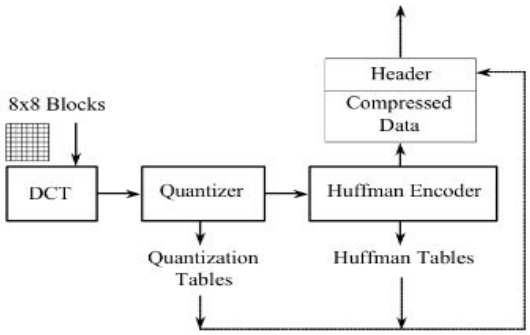
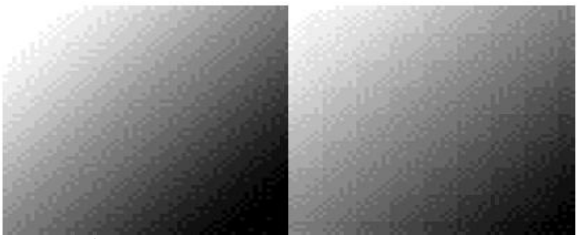


***Fig 1* Block diagram of Algorithm**

III. JPEG STEGANOGRAPHY AND ALGORITHMS

3.1 JPEG Format

Strictly speaking, JPEG refers only to a family of compression algorithms; it does not refer to a specific image file format. The JPEG committee was prevented from defining a file format by turf wars within the international standards organizations. JFIF has emerged as the de-facto standard on Internet, and is what is most commonly meant by "a JPEG file. JPEG works by extracting coefficients describing 8x8 pixel blocks and then compressing these coefficients. The blocks can be revealed by saving a JPEG of a gradient pattern with the lowest possible compression quality. The blocks, which start in the upper left-hand corner, are shown in Fig. Partial blocks will be included on the right and lower edges if the dimensions are not divisible by 8 pixels



Left: gradient with high quality compression
Right: gradient with low quality compression

Fig 2

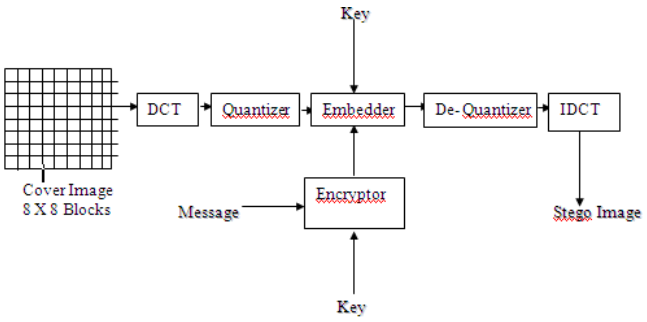


Fig 3 Block Diagram of Encoding

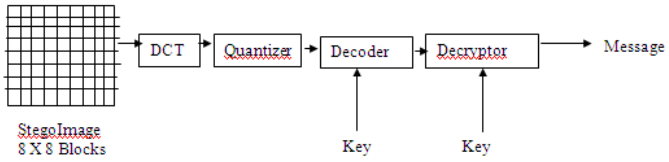


Fig 4 Block Diagram of Decoding

IV. ALGORITHM FOR ENCODING

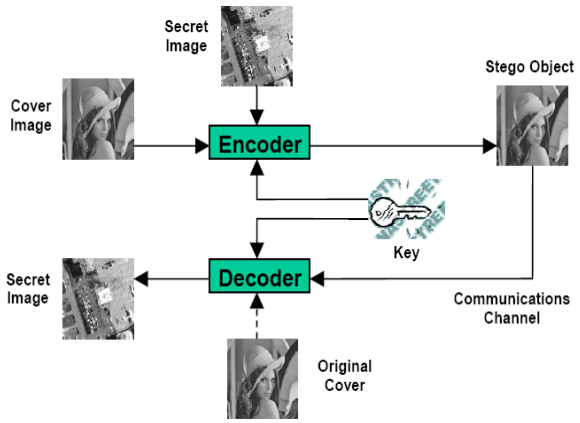
1) The input is a Buffered Image object, which contains a Color Model and a matrix representing the image with pointers aimed at indices of the Color Model. The RGB values of the uncompressed input image are converted into three components: one luminance component and two chrominance components (YUV). The luminance component is considered more important.
2) The image is separated into 8x8 pixel blocks starting from the upper left-hand corner.
3) The component signals for each 8x8 block are transformed into the frequency domain by using the two-dimensional discrete cosine transform (DCT). This transformation is similar to the two-dimensional fast Fourier transformation.
4) While the coefficients closest to 0 are eliminated, the remaining coefficients are quantized using various degrees of accuracy. This can be modified by changing the quantization tables. The DC luminance coefficients are the most important and are quantized with the most accuracy.
5) Since the DC luminance coefficients are quantized with the most accuracy, we will hide the information inside them
6) Finally, the quantized coefficients are compressed using a Huffman encoder

V. ALGORITHM FOR DECODING

The decoding scheme is much simpler than encoding. The averages of the luminance of the 8x8 blocks just need to be calculated and converted back to bits.

Basically what we exactly do in decoding process is:-

1) The user needs to provide a Source Image and any Keys used when the Source Image was generated.
2) If a non-default key was used in text hiding process, the receiving party must have prearranged knowledge of the key for use in retrieving the text.
3) After the Source Image and any required Keys are loaded into the application, the hidden text can be retrieved by selecting Extract Text from the Tools menu



The generic process of Encoding and Decoding is demonstrated in this diagram

Fig 5

VI. SYSTEM ANALYSIS

6.1 System Analysis Methodology

The methodology used for System Analysis is the Object Oriented Analysis. The OOA process begins with an understanding of a manner in which the system is used by people. Once the scenario of usage is defined, the modeling of the software begins.

Use Cases model the system from the end user's point of view. The use case diagram for our system is as follows The use case achieves the following objectives:

a) Define the functional and operational requirements of the system by define a scenario of usage that is agreed upon by the end user and the software engineering team.
b) Provide a clear view of the system's functionality.

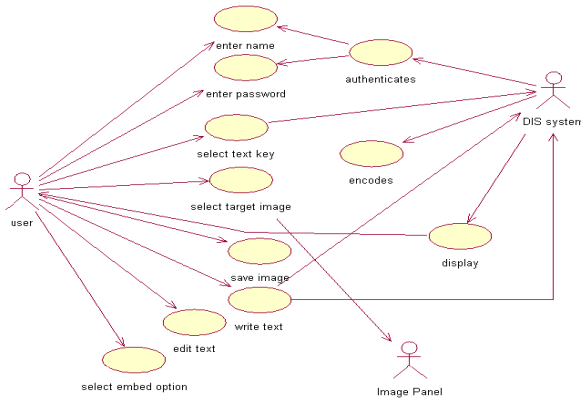


***Fig. 6* Use Case Diagram**

6.2 User Interface

User interface consist of three main panels are Main Panel, Key Panel, & Source/Target Panel.

Main Panel: The main panel of the application contains a Text tab and an Image tab as described below. Both the text and image cannot be viewed at the same time in the main panel; however, a scaled version of the image is always shown in the Source/Target pane, so both will be visible if the text tab for the main panel is selected.

i) Text Tab: This is the main text area into which the user types the text to be hidden within an image. In the case of extracting text from an image, the text would be loaded into this same tab.

ii) Image Tab: This tab is also located within the main panel. Its sole purpose is to display an image that has been produced as a result of embedding text within another image.

Key Panel: The Key Panel will have a text key tabs that will display the selected key. The selected key will be the key the program uses.

i) Text tab: The user may type directly into the text tab. He can also use Open Text Key from the Tools menu to load text as a key. The text continues to be editable once a text file has been loaded.

Source/Target Panel: The Source/Target Panel shows the image that will contain hidden text, or an image, which we would like to extract text from. An image can be loaded into the Source/Target Pane either from the Image Bar via the Load Image button that will load highlighted image or through File menu ‡ Open Image File.

6.3 Activity Diagram

An activity diagram is essentially a flowchart, showing flow of control from activity to activity. It is used to model the dynamic aspects of the system. An activity is an ongoing execution in the system. Activities ultimately result in actions, which is made up of executable atomic computations that result in a change in state of the system or return of a value.

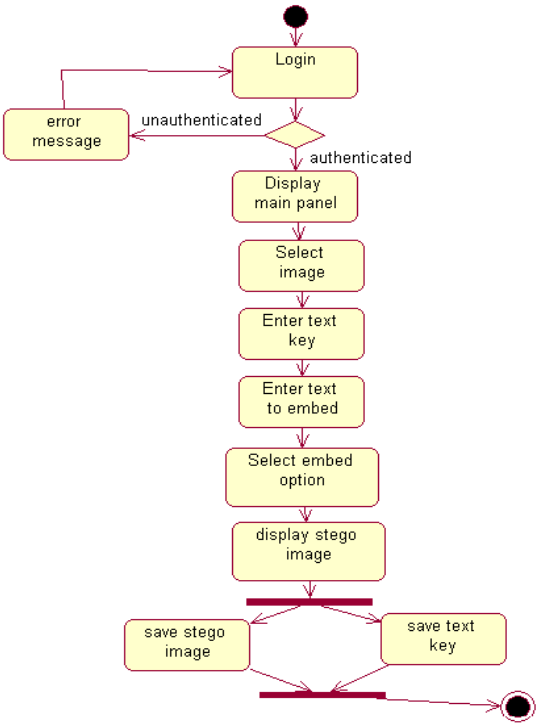


Fig. 7 **Activity Diagram for embedding**

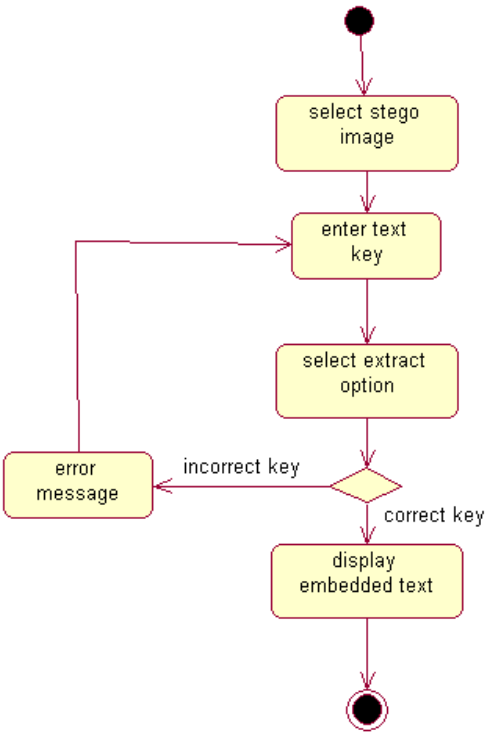


Fig. 8 **Activity Diagram for Extracting**

6.4 Input/Output Screens

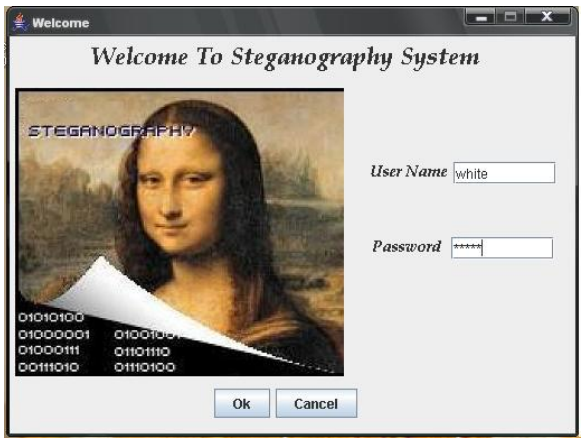


Fig.9 **Login Screen**

Fig.10 Main Panel

VII. CONCLUSION

The application is primarily intended to be used to inconspicuously hide confidential and proprietary information by anyone seeking to hide information. This software has an advantage over other information security systems because the hidden text are in the form of image, which is not obvious text information carriers.

Because of its user-friendly interface, the application can also be used by anyone who wants to securely transmit private information. The main advantage of this program for individuals is that they do not have to have any knowledge about steganography or encryption. The visual way to encode the text, plus the visual key makes it easy for average users to navigate within the program. To send a message, a source text, an image in which the text should be embedded, and a key are needed. The key is used to aid in encryption and to decide where the information should be hidden in the image. A short text can be used as a key. To receive a message, a source image containing the information and the corresponding key are both required. The result will appear in the text tab after decoding.

The common Internet-friendly format is offered. It is inherently more difficult to hide information in a JPEG image because that is exactly what the designers of JPEG wanted to avoid: the transmission of extra information that doesn't affect the appearance of the image.

REFERENCES

[1]. Daniel L.Lau, Robert Ulichney, Gonzalo R.Arce, "Fundamental Characteristics of Halftone Textures: Blue-Noise and Green-Noise", Image Systems Laboratory, HP Laboratories Cambridge, March 2003.
[2]. C.Yang and C.Laih, "New colored visual secret sharing schemes", Designs, Codes and Cryptography, vol.20, 2000, pp.325-335.
[3]. C.Chang, C.Tsai, and T.Chen, "A new scheme for sharing secret color images in computer network", in Proc. of International Conference on Parallel and Distributed Systems, 2000, pp. 21-27.
[4]. R.L.Alder, B.P.Kitchens, M.Martens, "The mathematics of halftoning", IBM J. Res. & Dev. Vol.47 No.1, Jan. 2003, pp. 5-15.
[5]. R.Lukac, K.N.Plantaniotis, B.Smolka, "A new approach to color image secret sharing", EUSIPCO 2004, pp.1493-1496.
[6]. H.Ancin, Anoop K.Bhattacharjya, Joseph Shu, "Improving void-and-cluster for better halftone uniformity",International Conference on Digital Printing Technoogies.
[7]. N . Provos, "Defending Against Statistical Steganography," Proc 10th USENEX Security Symposium 2005.

[8]. N . Provos and P. Honeyman, "Hide and Seek: An introduction to Steganography," IEEE Security & Privacy Journal 2003.
[9]. S . Katzenbeisser and Petitcolas , "Information Hiding Techniques for Stenography and Digital watermaking" Artech House, Norwood, MA. 2000 .
[10]. L. Reyzen And S. Russell , "More efficient provably secure Steganography" 2007.
[11]. S.Lyu and H. Farid , "Steganography using higher order image statistics , " IEEE Trans. Inf. Forens. Secur. 2006
[12]. Venkatraman , s, Abraham , A . & Paprzycki M." Significance of Steganography on Data Security " , Proceedings of the International Conference on Information Technology : Coding and computing , 2004.
[13]. Fridrich , J ., Goljan M., and Hogea , D ; New Methodology for Breaking stenographic Techniques for JPEGs. " Electronic Imaging 2003".
[14]. http:/ aakash.ece.ucsb.edu./ data hiding / stegdemo.aspx.Ucsb data hiding online demonstration . Released on Mar .09,2005.