MATHLAB REPERCUSSION: DIGITAL IMAGE METHODOLOGIES, APPLICATION FOR PRIVACY AND SECURITY USING STEGANOGRAPHY

1. **V. R. SASIKUMAR,** Research Scholar**,** Manonmaniam Sundaranar University.

2. **DR. SANTHOSH BABOO,** G. Vaishnav College, Chennai.

Abstract:
Introduction: This tip sheet introduces the technical structure of a digital image and explains the measures for digital image characteristics. The focus is on images created by digitizing photographs, including negatives, transparencies, and prints by using steganography.
Methodology: The process of capturing a rich digital master image that achieves “Best Practice” standards in the categories noted here depends upon a variety of factors including: quality of the equipment and software, quality control processes, operator skill, and technical and administrative support throughout the process, including management of the digital image and its metadata once the digital image is created. Consulting current standards can provide the information necessary to establish a system for the digitization of photographs. Once a system is in place, benchmarking the capabilities (and understanding the limitations) of that system through testing and exploration by using targets and a sampling of representative materials will better insure a quality result in the digital images that are created.
Objectives: Understanding digital image elements can help you plan effective scanning services and create rich digital master images.
Result: The headlong development that has characterized the digital world from its very inception has not been even in all its parts: some issues have been relatively neglected and have not kept up with rapid technical and market changes. Among these are questions relating to digital identity, data security, and consumer privacy. With all the expansion in progress in this domain, and the constant innovation, the risks involved are magnified and thus assume an increasing urgency. Matters such as social participation and interaction in the digital environment are equally important to consider as they ultimately provide the backdrop for developments in this field. This chapter examines the rapidly changing technological and social environment surrounding the individual (later referred to as the “digital individual”), and the blurring boundaries between the public and private spheres of existence. Detailed consideration is then given to the establishment and management of digital identity online.
Implication: People use digital images in many ways. The same image can be viewed on a wide variety of monitors, printed in many formats, and transmitted electronically through e-mails, cell phones, and other systems.

Keywords: *Digital Image, Steganography and Digital Master Image*

1. Introduction

Amongst many carriers such as a text file, image file, audio/video file or a TCP/IP header file, that have a high degree of redundancy, image file is found to be a most popular cover object due to its confined ability of human visual system, 'innocent' data types to eavesdroppers and availability of high degree of redundancy **(Amirtharajan et. al., 2012).** For example, a 1024 x 768 image has a potential to hide a total of 294,912 bytes of information using 3-LSB insertion method. In 640 x 480 image of 256 colors (8 bits/pixel), one can hide 300 KB worth of data and it is possible to hide 15% to 20% of data in a jpeg successfully **(Ortiz, 2011).** Further, digital images are the most common on the Internet. The images are also found to be one of the best cover objects in digital steganographic applications such as for secret transactions in an inconspicuous manner. The survey for the proportion of cover objects used in digital steganographic applications done by **Johnson & Sallee (2008)** also supports it. Let C denote the set of all cover images and M be the set of all message signals. Let K be the set of all keys and C' be the set of all modified cover images. The Embedding method is a method for embedding a message signal in a cover image. According to **Chvarkova et al. (2011),** we define the embedding method, E by the mapping.

E: C x M x K C' such that c* = E(c, m, k) for all c C, m M, k K

Here, c* C' is the modified cover image. The modified cover image after embedding is also called a stego-image. The redundant space of the cover image which is available for steganographic modification and message signal transmission is called the Steganographic Channel space, SC. The extraction method is the method of decoding of the modified cover image in order to get the message signal, m. It is defined by the mapping.

D: C' x K M such that m= D(c*, k).

The set of coding and decoding methods executed with steganographic objects, applying the restriction on steganographic channel space, is called the Steganographic System, SS. Mathematically we define SS as the pair < SSEsc, SSDsc>, where SSESC: C x M x K C' is defined by

SSEsc (c, m, k) = c* for all c SC, m M, k K

and SSDsc: C' x K M is defined by

SSDsc (c*, k) = m

2. Problem Statement

Step 1 - Encoding the message by some appropriate codes to convert the data into a bit pattern

Step 2 - To determine the redundant bits/pixels in the cover or its transformed image that can be modified so that the image quality is not degraded.

Step 3 - Embedding the secret data bit stream into the selected redundant coefficients of cover image or into the subbands obtained by applying transformation to cover image, thus creating the stego-image.

3. Algorithm

Reed-Muller code based algorithm

In this section a secure steganographic technique based on Reed-Muller codes, RM(r, m), as depicted in Figure 2.2.1, is proposed. RM(r, m) codes are summarized. The details can also be seen in the text by **Raaphorst (2003).**

…………………………………………..

Embedding

…………………………………………..

Input: Cover image, A, Message m; and the Parity Check Matrix, H

Output: Stego-image, key3

Step 1. Given the cover grayscale image, first decompose it into 8 bit-planes.

Step 2. Then, compute the complexity of second, third and fourth bit-planes. The variance of a bit-plane is used as a measure of its complexity.

Step 3. Select the bit-plane, 'I' by determining if the complexity of the bit-plane is greater or equal to a threshold value which is a function of the mean value of that bit-plane, denoted by' key1'.

Step 4. A cover bit-plane, I is reshaped into n-columns by padding required zeroes, denoted by, CI , where n=2m -1.

Step 5. Choose k-blocks, Ck, out of n-blocks, CI.

Step 6. Encode Ck to a (n, k) RM-code by multiplying it with its generator matrix, G(r,m), where r is the order of the code (taken =1) and m determines the length of code, n = 2 m, the resulting vector is denoted by C.

Step 7. Encode the original message with Huffman / T-codes and reshape the binary string into m-columns by padding zeroes, if required. Let the resulting string be ‘nmsg’ and the encoding key is ’key3’.

Step 8. Convert the binary string ‘nmsg’ into decimal

Step 9. Now, using the error mapping, each error related to message bit is added to the n-bit code C, randomly, using the random key, denoted by key2. The resulting vector is the vector with message embedded in it. Let it denote by I’.

Step 10. Reshape the stego-bit-plane, I’, remove the padded zeroes and merge all the bit-planes to recreate the image, called ‘stego-image’.

…………………………………………

Extraction

………………………………………..

Input: Stego-image, key1, key2, key3

Output: Original message, m

Step 1. Decompose the stego-image into bit-planes and choose the plane containing the message, using key1.

Step 2. Reshape the selected plane into n-columns; say ‘st-plane’

Step 3. Get the codeword, Cs , containing message from ‘st-plane’ using the random-

key, key2.

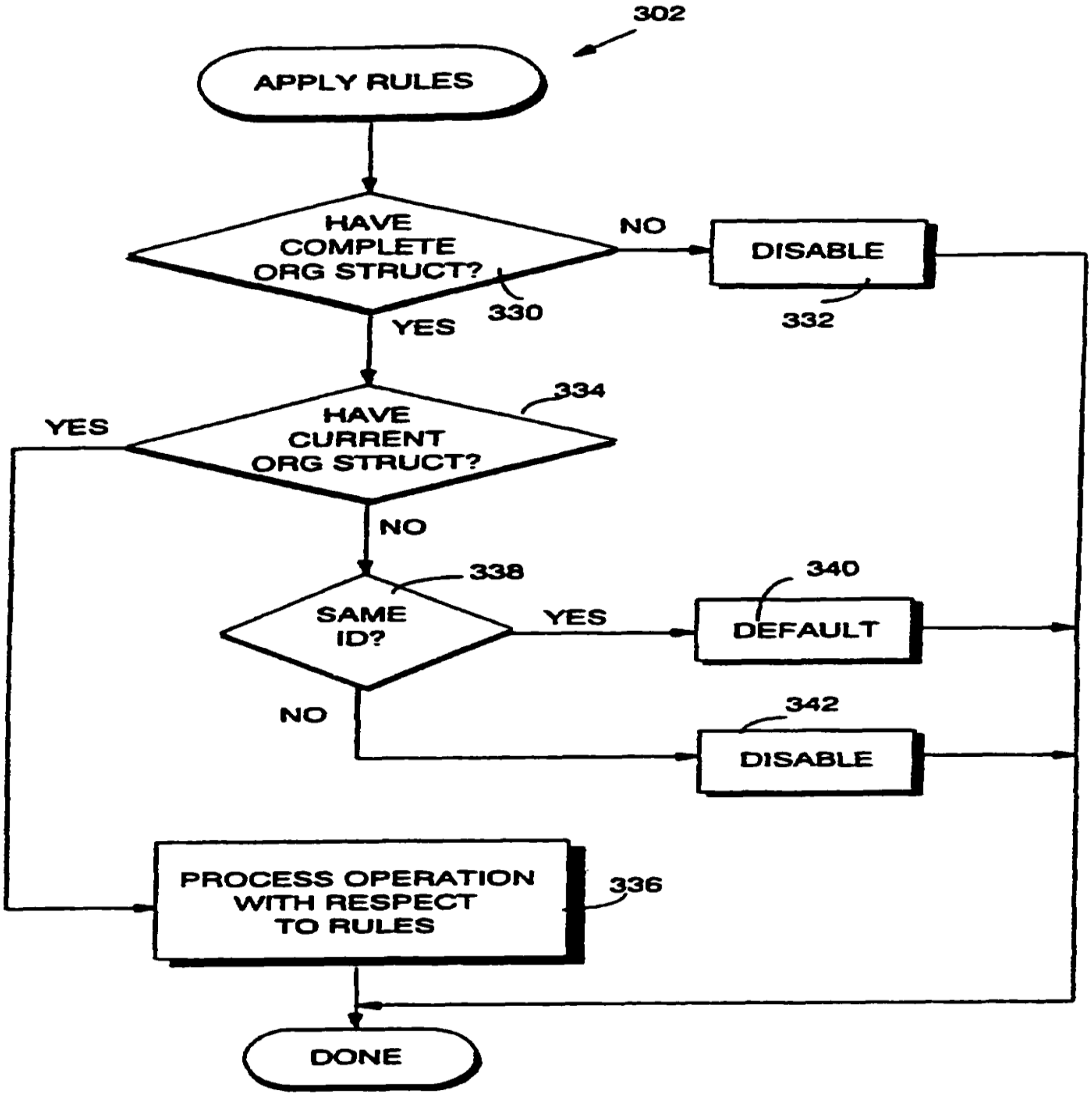
Step 4. The received codeword, Cs , is compared with all the codewords in the Hadamard matrix, row-wise. The codeword, r, which has the least distance compared to the received codeword, is taken as the corrected codeword.

Step 5. Subtracting these two codewords, C – r, we get the error, y

Step 6. Decoding y with Huffman/T-decoding using key 3, message, m, is obtained.

………………………………

Methodology



1. Using digital vision technology the distance between the objects will be calculated effectively.
2. The disparity between the two object is calculated using 3D vision.
3. In this method the computation speed is calculated.

4. This method can cope with much more difficult cases like repetitive patterns, complex scene, etc.
5. This algorithm is proposed to visits small fraction of disparity space in order to find the disparity map.
6. This method can be easily adapted for multi-image matching.
7. Accurate matching on 2-megapixel images of complex scenes is routinely obtained in a few seconds with minimal seed without limiting the disparity search range.

Figure - 1

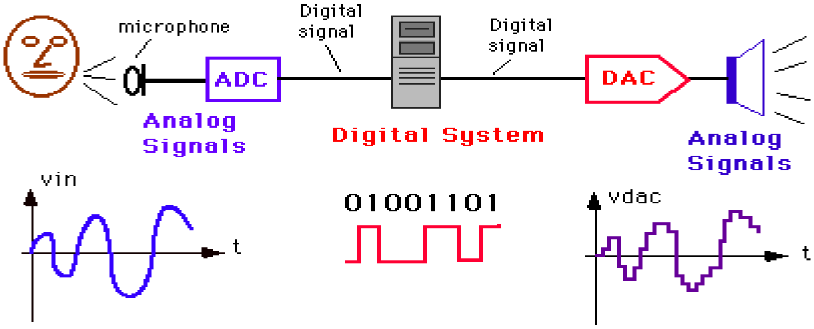


Figure - 2

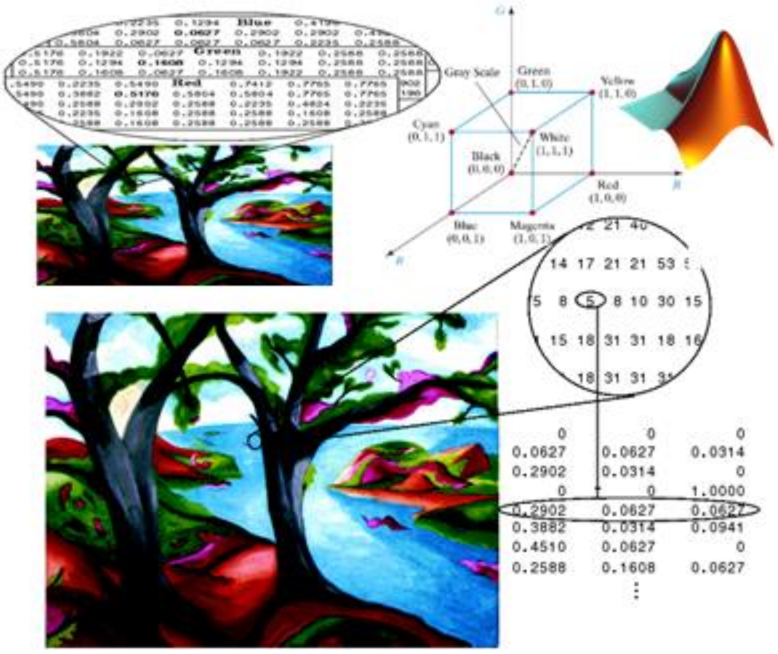


Figure - 3

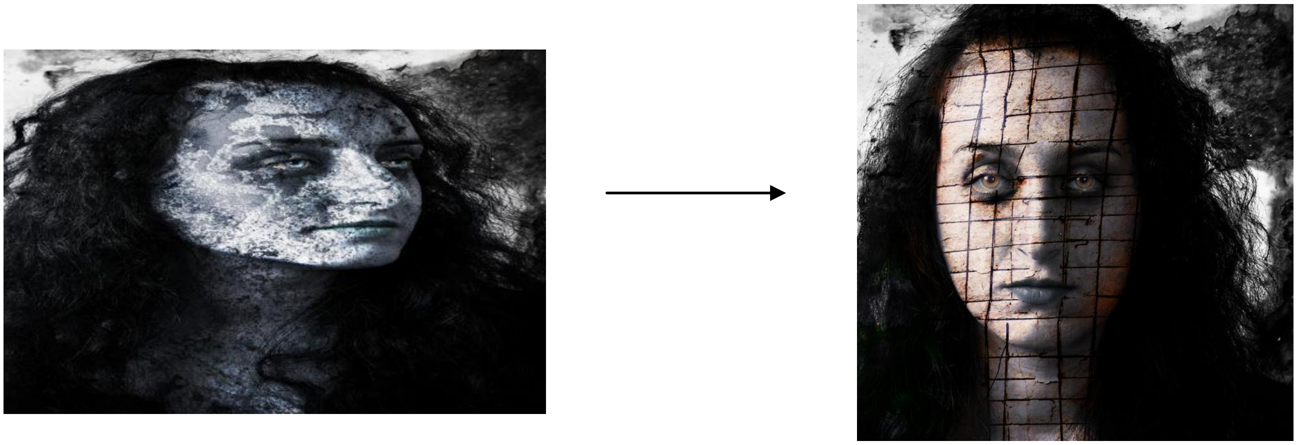


Figure – 4: Respective frequency plane decomposition

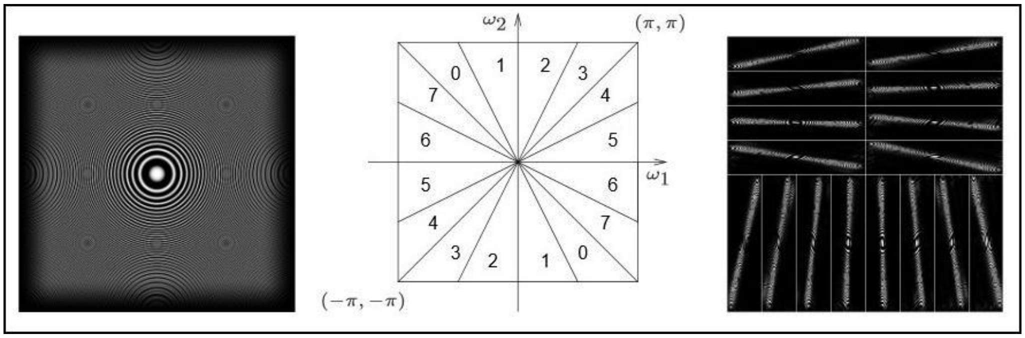
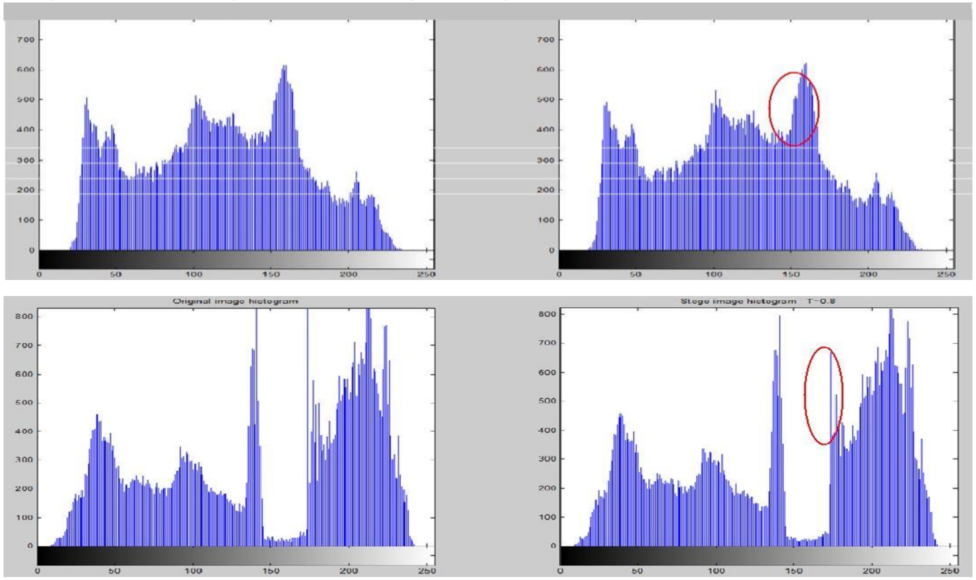
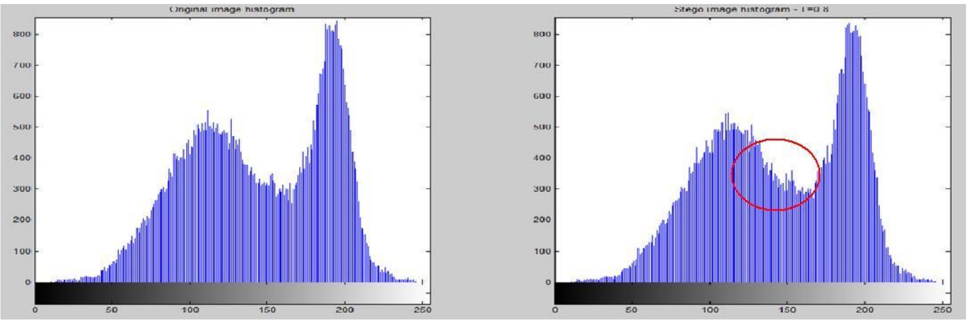


Figure – 5: Histograms for original and Stego-images for Contourlet-based MLSB-FM method





The main research thrust in image steganography has been more towards finding the applications of Wavelet-like transforms such as Slantlet transform, Contourlet transforms and Complex Wavelet transforms (DD DWT and DD DT CWT) that they fulfill the basic characteristics of steganography or not. We have further extended our work of investigation towards the use of error correction codes, mainly linear block codes such as Hamming codes, RM-codes and RS-codes in steganography. We have also studied issues of security (in terms of KLDiv) and steganalysis (in terms of histogram analysis).

10. Conclusion

The Complex Wavelet Transforms (CWTs) and Error Correction Codes (ECCs) have been investigated in this thesis for image steganography. So far, it was an understanding that imperceptibility is the most important criterion for the image steganography, but recent progress in steganalysis has forced to change this ideology and researchers have now agreed that Undetectability is the most important criterion for image steganography. For the Steganography, there is still a challenge to come up with a steganographic scheme that fulfills the six criterion of image steganography as mentioned in the research. One may this summarized this problem in steganography as to develop a steganography technique that is robust to different types of attacks (statistical and image carrier-attacks) and to which, the majority of contemporary techniques fail to detect the presence of secret messages. We have considered two other requirements, robustness and self-synchronization in the design of an image steganography algorithm. One solution in this directions is to embed the exactly the same data in all the local hiding regions (multiple time embedding). This way one can resist to cropping. Since Complex Wavelet transforms provide number of real and imaginary subbands at the higher stage, one may think of using different subbands in different direction carrying the same data. There can be other intelligent coding schemes where different parts of the message can be embedded in different regions.

References

- Adams M. D. (2002, September). Reversible integer-to-integer wavelet transform for image coding, Ph.D. thesis, Department of Electrical & Computer Engineering, The University of British Columbia,
- Agrawal V. K. (2007, June). Perceptual Watermarking of Digital Video using the Variable Temporal Length 3D-DCT, M.Tech thesis, Department of Electrical Engineering, I.I.T., Kanpur.
- Bruen, A. A., Forcinito, M. A. (2005). Cryptography Information Theory and Error Correction, John Wiley & Sons, Inc., New Jersey.
- Cachin C. (1998). An information-theoretic model for steganography, 2nd International Workshop Information Hiding, Vol. LNCS 1525, 306-318.
- Do M.N. and Vetterli M. (2005). The Contourlet transform: An efficient directional multiresolution image representation, IEEE Trans. On Image Processing, 14(12), 2091-2106.
- Eggers J. J., Bauml R. and Girod B. (2002, January). A Communication approach to Image Steganography, Proceedings of SPIE., Security and Watermarking of Multimedia Contents IV, Vol. 4675, San Jose, CA.
- Ling, W., Na, W. L. (2009). A Novel Steganography Algorithm Based on CRC, International Conference on Multimedia Networking and Security.
- Xu-Ren Luo, TE-Lung Yin (2011, April). Reversible Data Hiding Exploiting in Wavelet Coefficients, JCS & T, Vol. 11, No. 1.
- Zhang W., Wang S. and Zhang X. (2007, August). Improving embedding efficiency of covering codes for applications in steganography, IEEE Communications Letters, 11(8): 680-682.