Information Hiding by Inverting the LSB bits of DCT Coefficients of JPEG images

Hamdy A. Morsy[*], Zaki B. Nossair, Alaa M. Hamdy, Fathy Z. Amer

Telecommunication Department, Faculty of Engineering at Helwan,
Helwan University, Cairo, Egypt
*hmorsy@helwan.edu.eg

Abstract: Embedding messages bits in a cover-object affects the first order statistical properties of the cover-object. In this paper a new technique is introduced to hide information bits in the redundant bits of JPEG images with preserving the statistical properties. This technique proved to defeat the visual and statistical attacks and offer higher capacity than existing steganographic systems.

[Hamdy A. Morsy, Zaki B. Nossair, Alaa M. Hamdy, Fathy Z. Amer **Information Hiding by Inverting the LSB bits of DCT Coefficients of JPEG images**]. Journal of American Science 2011;7(11):171-177]. (ISSN: 1545-1003). http://www.americanscience.org.

Keywords: JPEG hiding, steganography, steganalysis, information hiding.

1. Introduction

The main goal of steganography is to hide information bits in a cover-object, so that it looks innocuous to an attacker. In contrast to encryption where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an attacker.

Steganography is defined as the hiding of information in a medium (such as image, audio, or video). Any medium with redundant bits that is used for embedding data is called a cover medium. After embedding data in a cover medium, a stego medium is obtained [1, 2]. The embedding algorithm is assumed to be known to the public according to Kerckhoffs principle [3, 4]. Therefore the embedding process may use an embedding key (stego key) so that only the intended user can successfully extract the embedded data by using the extraction key in the extraction process.

The concept of hiding some information in digital media has a wider class of applications that go beyond steganography, Fig. 1. The techniques involved in such applications are collectively referred to as information hiding. Information can be gathered about an image from its electronic form or its printed form. For example, an image printed on a document could be annotated by metadata that could lead a user to its high resolution version. In general, metadata provides additional information about an image [5].

Digital watermarking is categorized as a type of information hiding and is defined as the process of embedding information into digital multimedia content such that the information (the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content. The key difference between information hiding and watermarking is the absence of an active adversary. In watermarking applications like copyright protection and authentication, there is an active adversary that would attempt to remove, invalidate or forge watermarks. In information hiding there is no such active adversary as there is no value associated with the act of removing the information hidden in the content. Nevertheless, information hiding techniques need to be robust against accidental distortions.

In a steganographic system, the information hiding starts by identifying redundant bits in a cover medium. Redundant bits are those bits that can be modified without disturbing the statistical properties of the cover medium. A steganographic system exploits those redundant bits for message embedding without changing the statistical properties of the cover medium. In most steganographic systems, modifying the redundant bits leaves detectable traces. Even if the hidden message is not exposed, the existence of it is detected.

In steganography, the communication is taken place in such a way that an attacker can not suspect that there is a hidden message is exchanged between two parties other than exchange of media files. A powerful steganographic technique exploits only the redundant bits to embed message bits without distorting the cover media statistical properties.

After embedding the message bits in an innocuous cover medium, the resulting stego medium should be secure against visual and statistical attacks and robust against modification such as recompression. Most steganographic systems are weak against visual and statistical attacks and the ones that are robust against these visual and statistical attacks offer only relatively small capacity [6, 7].

Even modifying the redundant bits doesn't affect greatly the statistical properties of the cover medium. Distortions to the histogram of the transform domain can be observed after embedding message bits. As a result, an eavesdropper can detect the distortion in the resulting stego medium's statistical properties. Statistical steganalysis is the science that concerned with finding distortions in the cover medium and hence labels the cover medium if it has a hidden message.

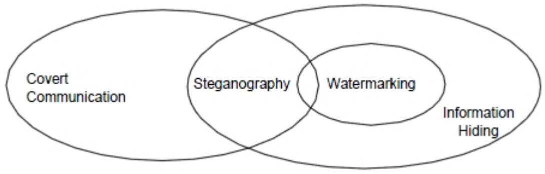


Fig. 1 Steganography and related fields [5]

Internet users transmit digital pictures over email and other Internet communication. JPEG is one of the most common formats for images. As a result, this format is the best candidate for using as a cover medium for exchanging secret messages without raising an eavesdropper's suspension. The Least-significant bits (LSB) of nonzero of discrete cosine transform (DCT) coefficients are modified for message embedding.

In this paper, a new technique, the Inverted Steganographic Algorithm (ISA), is introduced for message embedding in the LSB of nonzero AC DCT of JPEG images. This steganographic system is based on inverting each LSB bit flipped by message bit with the corresponding bit in the pair of values (PoVs) of the DCT coefficients. The nonzero AC DCT coefficients are divided into pairs of values , for example (1,2), (-1,-2)… etc, if the selected bit is different from the data bit, the LSB bit will be inverted and the first next LSB bit in the same PoVs will be inverted too . As a result, the total changes due message embedding will be zero given that the maximum message embedding limited to the lower number of bits in each PoVs. This algorithm provides maximum capacity compared to the state of the art steganographic algorithms. The performance will be studied on both spatial domain and transform domain.

The rest of this paper is organized as follows. In section II, JPEG image format is introduced. ISA algorithm is presented in section III. Comparisons between the proposed algorithm and the current steganographic algorithms and simulation results are presented in section IV. Conclusions are presented in section V.

2. Jpeg Images

2.1 Steganography

In JPEG image format, each 8 x 8 block of pixels of the image are transformed into 64 DCT coefficients. The DCT coefficients $F(u, v)$ of an 8 x 8 block of image pixels $f(x, y)$ are given by:

$$F(u,v)=\frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7}f(x,y)*\cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16};\right] \quad (1)$$

Where $C(x)=\begin{cases}\frac{1}{\sqrt{2}} & \text{x} = 0\\ 1 & \text{otherwise}\end{cases}$

Afterwards, the following operation quantizes the coefficients:

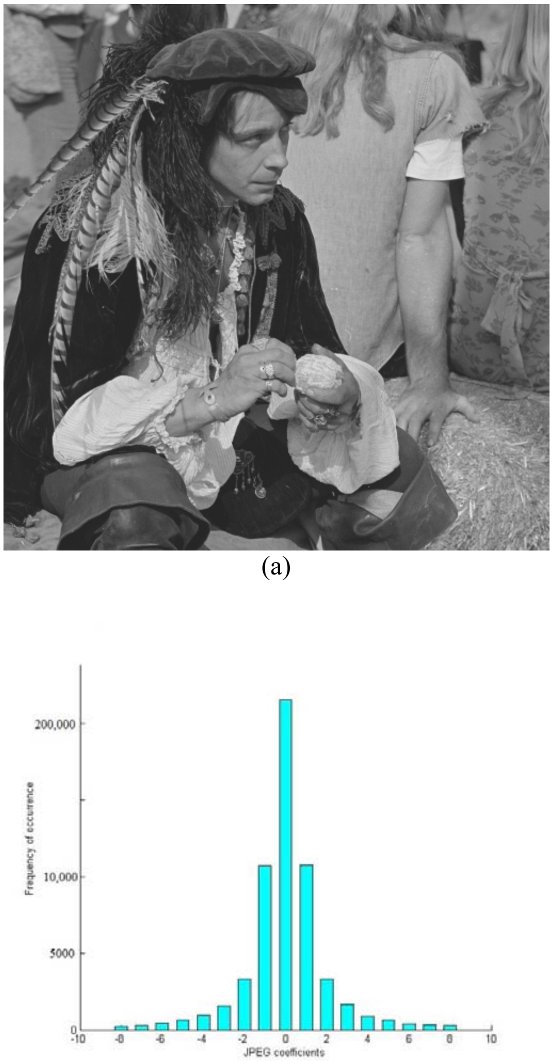
$$F^{Q}(u,v)=\left\lfloor\frac{F(u,v)}{Q(u,v)}\right\rfloor, \quad (2)$$

Where $Q(u, v)$ is a 64-element quantization table.

We can use the least-significant bits of the quantized DCT coefficients as redundant bits in which the secret message can be embedded. The modification of a single DCT coefficient affects all 64 image pixels [8]. Fig. 2 shows an image (standard pirate test image 512x512) with its frequency of occurrences of DCT coefficients.

The DCT coefficients are divided into pairs of values (PoVs), for example (1, 2), (-1, -2), (3, 4)... etc. Fig. 2 shows the histogram of frequency of occurrences of DCT coefficients, one can notice that the odd DCT coefficients occur more frequently than the adjacent even DCT coefficients. As an assumption, the message bits are uniformly distributed. As a result, embedding this type of message can significantly distort the first order statistical properties of the JPEG image.

The Jsteg algorithm, by Derek Upham, was the first publicly available steganographic system for JPEG images. Its embedding technique sequentially replaces the least-significant bit of DCT coefficients with the message's data. This algorithm excludes the DC DCT coefficients and the values zeros and ones of AC DCT coefficients. With uniformly distributed message bits, every pair of value will be equalized after embedding [11,12,13].



(a)

(b)

Fig. 1. Standard test image and its histogram:
(a) Bridge, (b) The histogram

2.2 Steganalysis

Assume k is the distinct AC DCT coefficients of a JPEG image and c is the nonzero AC DCT coefficient index of DCT transform and the frequency of occurrence of two adjacent DCT coefficients are n_i and n_{i+1}. One can observe that the absolute value of frequency of occurrences of the histogram is monotonically decreasing as shown in Fig. 1, which means that $n_i > n_{i+1}$. For a uniform distributed message, the number of frequency of occurrences of the LSB of nonzero AC DCT coefficients n^*_i and n^*_{i+1} will be equal due to message embedding. The following relation can be hold:

$$|n_i - n_{i+1}| \geq |n_i^* - n_{i+1}^*|. \tag{3}$$

Based on this observation, Westfeld and Pfitzmann designed a first order statistical test to detect the similarity of the PoVs of stego images [9, 10]. This statistical steganalysis is known as Chi-square attack.

The average number of each pair of values is given by:

$$n_i^* = \frac{(n_i + n_{i+1})}{2} \tag{4}$$

And the Chi-square test can be calculated as:

$$x^2 = \sum_{i=1}^{k} \frac{(n_i - n_i^*)^2}{n_i^*} \tag{5}$$

The probability of embedding as a function of Chi-square value is given as:

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}} \Gamma(\frac{k-1}{2})} \int_0^{x^2} e^{-\frac{t}{2}} t^{\frac{k-1}{2}-1} dt \tag{6}$$

Where k is the degree of freedom – 1, the distribution of DCT coefficients of a JPEG image can be tested for uniform distribution using equation (5). Fig. 2 shows the histogram of stego image with 100 % embedding rate using Jsteg algorithm. It is clear that, every pair of values are equal due to embedding message of uniform distribution.

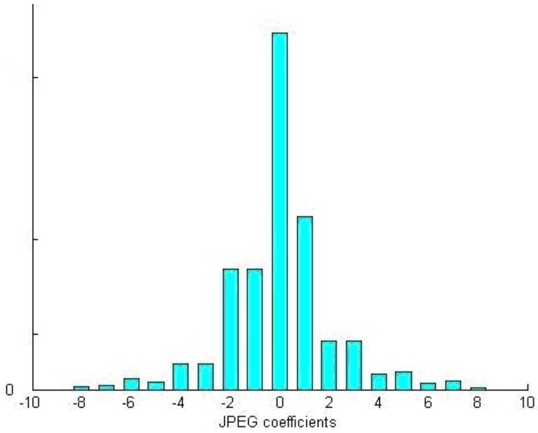


Fig. 2 The histogram of a stego image (Jsteg algorithm)

3. ISA algorithm

The Isa Algorithm Embeds Message Bits By Modifying The Redundant Bits In The Cover Medium (Such As Image, Audio, Or Video). Jpeg

Image Format Is The Most Widely Used Image Format On The Web, As A Result, It Is A Good Cover Medium For Information Hiding. Modifying The Least Significant Bits Of The Nonzero Ac Discrete Cosine Transform (Dct) Will Be Secured Against Visual Attacks [14, 15]. An Encryption Key Is Needed To Transmit The Minimum Number Of Each Pair Of Values Povs, So More Message Bits Can Be Embedded To The Dct Coefficients On The Account Of Adding Distortions To The First Order Statistical Properties.

Embedding Algorithm

1) Encrypt message bits with encryption algorithm.
2) Apply DCT transform and quantization for image compression in JPEG image format.
3) Find the minimum of each pair of values in DCT transform excluding the DC and the zero AC DCT coefficients.
4) Determine the maximum embedding capacity by adding up the results in step 3
5) Sequentially embed the message bits in the selected AC DCT coefficients
6) Stop embedding in any given PoVs if you reach the maximum limit for this PoVs.
7) Use Huffman coder for image encoding.

Extracting Algorithm

1) Decode the compressed image using Huffman Decoder.
2) Determine the minimum of the frequency of occurrences of nonzero AC DCT coefficients of each PoVs
3) Convert odd coefficients into ones and even coefficients into zeros.
4) Append only the ones and zeros in the limited number of each PoVs
5) Repeat step 4 for the rest of DCT coefficients and append the extracted data into a file.
6) Decrypt the message bits using decryption algorithm.

In ISA technique, the maximum embedding capacity depends mainly on the minimum in every pair of values (PoVs). Assume H is a one dimensional matrix representing the frequency of occurrence of DCT coefficients of a JPEG image and h_i is the frequency of occurrence of quantized value *i*, then

$$H = [\dots \; h_{-2}, h_{-1}, h_0, h_{-1}, h_{-2}, \dots] \qquad (7)$$

To fully utilize and divide the H matrix into integer number of PoVs, all nonzero AC DCT coefficients the minimum and maximum quantized coefficients should be even. The minimum and maximum values of quantized coefficients can be calculated as

$$h_{\min} = \begin{cases} \min(H) & \text{if min(H) is even} \\ \min(H) - 1 & \text{otherwise} \end{cases} \qquad (8)$$

$$h_{\max} = \begin{cases} \max(H) & \text{if max(H) is even} \\ \max(H) + 1 & \text{otherwise} \end{cases} \qquad (9)$$

And the total number of nonzero AC DCT coefficients n_{AC} is given by:

$$n_{AC} = N - n_{DC} - n_0 \qquad (10)$$

Where N is the total number of DCT coefficients, n_{DC} is the DC DCT coefficients , and n_0 is the zeros AC DCT coefficients.

After dividing the quantized AC DCT coefficients into integer number of PoVs, the maximum embedding capacity is limited by the lower value in every PoVs and can be calculated as:

$$C = \sum_i \left| \min(h_i, h_{i+1}) \right| \qquad (11)$$

The embedding efficiency is given by:

$$\eta = \frac{C}{n_{AC}} \qquad (12)$$

4. Simulation results

ISA algorithm preserves the histogram of frequency of occurrences as long as the message size doesn't exceed the maximum embedding limit C. As more data bits embedded to the cover medium, the histogram starts to show deviation from the histogram of the original image. Embedding data in the nonzero AC DCT coefficients are based on pairs of values method which means that every two adjacent coefficients can exchange values. The histogram of the DCT coefficients will be affected by the message bits when exceeding the maximum limit and cause some distortions that can be detected [15, 16, 17].

Let's define D_{AC} as the difference between the cover medium and the stego medium histogram of the frequency of occurrence of DCT coefficients and define it as the change density and M as the message size in bits. For M < C the change density will be zero for M > C, the following relation can be hold:

$$D_{AC} = p_M \frac{M - C}{n_{AC}} x100 \qquad (13)$$

Where p_M is the probability that the messages bits is different from the LSB of AC DCT coefficients. For uniform distributed messages bits p_M=1/2.

The change density D_{AC} is zero, when the message size is within the limit of maximum limit. A comparison of change density between Inverting Steganographic Algorithm (ISA) and Jsteg and F5 algorithms based on the absolute value of changes made to the nonzero AC DCT coefficients of an image (pirate image) [18] is shown in Fig. 3. DEA is a direct embedding algorithm which is a modified version of the Jsteg algorithm without any processing on the AC DCT coefficients and including the value one for embedding [19].

The state of the art algorithms that can be take as a reference for measuring the performance of ISA algorithm are Jsteg, Outguess and F5 algorithm. Since Outguess utilize only 50 % of the available capacity, it is not included in this comparison. From Fig. 3 it can be noticed that ISA algorithm doesn't affect the first order statistical properties of the standard test image until reach the maximum embedding limit determined by this techniques which in this case approximately 40 %. The size of an image and its textural properties affect the maximum limit of embedding data bits using different steganographic systems.

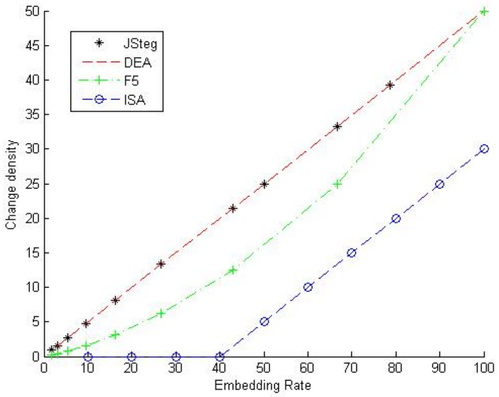


Fig. 3. A comparison between ISA algorithm and DEA, Jsteg and F5 algorithm

There is a tradeoff between the capacity of embedding and change density; the maximum capacity required the maximum change density will be introduced to the histogram. Fig. 4 shows some standard test images of size 512x512 of different textural properties used for capacity measurements. ISA algorithm offers high capacity with minimum change density as shown in Table 1.

Fig. 4. Standard test images from left-top Barbara, Boat, Camera man, and Jungle and from left- bottom Lena, Living room, Mandrill, and Pirate

Table I: Capacity measurements (in bits) using various embedding algorithms

Test images	Capacity in bits			
	ISA	Jsteg	F5	Outguess
Barbara	59838	40050	39892	20025
Boat	67843	41966	45229	20983
Camera man	30589	22572	20393	11286
Jungle	103279	71522	68853	35761
Lena	40488	28035	26992	14017
Living room	46537	34041	31025	17020
Mandrill	38985	26555	25990	13277
Pirate	46801	34126	31201	17063

From Table I, one can notice that the ISA algorithm outperform the current existing algorithm. This maximum embedding capacity came with price that the hidden message can be detected easily using the Chi-square test. To fully utilize the available nonzero AC DCT coefficients, the rest of the coefficients can be handled separately by adding control bits to maximize the ratio between even and odd DCT coefficients. For example the ratio of the PoVs (1, 2) is changes if more data are embedded that the frequency of occurrence of the number. As message size increases beyond the maximum limit, the value one will be used for message embedding without inverting the corresponding value 2. In this case, the Chi-Square test can detect the distortions in the first order statistical attach. To minimize this distortion, the rest of the DCT coefficients are divided into segments with one control bit denoted as a sign bit. If the sign bit is one, decode the bits directly and if it a zero, invert the bits before decoding. The data or its inverted form is utilized to minimize the distortion made by embedding data.

5. Conclusion and future work

ISA algorithm outperform current existing algorithm and can not be detected in both visual and statistical attack. The maximum embedding capacity is limited to the lowest of the values of each pair of values PoVs. This technique minimizes the changes introduced to the first order statistical properties of the cover media due to message embedding by limiting the message size to the available capacity of the cover medium.

The embedding capacity can be maximized by handling the difference of each pair of values PoVs separately in such a way that minimizing the distortions added to the cover medium due to message embedding.

Corresponding author
Hamdy A. Morsy
Telecommunication Department, Helwan University,
Cairo Egypt
hmorsy@helwan.edu.eg

References

1. Hamdy A. Morsy, Zaki B. Nossair, Alaa M. Hamdy, and Fathy Z. Amer, "Utilizing Image Block Properties to Embed Data in the DCT Coefficients with Minimum MSE," International Journal of soft computing and Engineering vol. 1, no. 4, pp. 449-453 , 2011.
2. Hamdy A. Morsy, Zaki B. Nossair, Alaa M. Hamdy, and Fathy Z. Amer, " Optimum segment length for embedding in the LSB of JPEG images with Minimum MSE," International Journal of Computer and Electrical Engineering vol. 3, no. 3, pp. 72-77 , 2011.
3. Kerckhoffs, “La Cryptographie Militaire”, Journal des Sciences Militaires, 9th series, IX pp 5–38; Feb. pp 161–191, Jan. 1883.
4. R. J. Anderson, and F.A. Petitcolas, “ On the limits of Steganography,” J. Selected Areas in Comm., vol.16, no. 4, pp. 474–481, 1998.
5. Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon " Image Steganography: Concepts and Practice," WSPC/Lecture Notes Seriesm, April 22, 2004.
6. Westfeld, “F5—A Steganographic Algorithm High Capacity Despite Better Steganalysis,” Springer-Verlag Berlin Heidelberg, 2001.
7. N. Provos, and P. Honeyman, “Detecting Steganographic Content on the Internet,” CITI Technical Report 01-11, 2001.
8. N. Provos, and P. Honeyman, “Hide and Seek: An introduction to steganography,” IEEE Computer security 15407993/03, 2003
9. A. Westfeld, “Detecting Low Embedding Rates, “, 5th Information Hiding Workshop. Nooerdwijkerhout, Netherlands, Oct. 7−9, 2002.
10. Westfeld, and A. Pfitzmann, “Attacks on Steganographic Systems,” in Andreas Pfitzmann (ed) Information Hiding. Third International Workshop, LNCS 1768, Springer- Verlag Berlin Heidelberg. pp. 61–76. 289, 291, 293, 299, 2000.
11. Hung, “PVRG-JPEG Codec, 1.1,” Stanford niversity, 1993. http://archiv.leo.org/pub/comp/os/unix/graphics/jpeg/PVRG 291.
12. Manoj Kumar Meena, Shiv Kumar, Neetesh Gupta “ Image Steganography tool using Adaptive Encoding Approach to maximize Image hiding capacity” IJSCE Volume-1, Issue-2, May 2011.
13. Cachin,” An Information-Theoretic Model for Steganography,” Cryptology ePrint Archive, 2002.
14. N. Memon, and M. Kharrazi, “Performance study of common image steganography,” Journal of Electronic Imaging 15(4), 041104 (Oct-Dec), 2006.
15. G. Cancelli, and M. Barni, “New techniques for steganography and steganalysis in the pixel domain, “, Ph.D. dissertation - Ciclo XXI. Report 2000 /028, 2009. www.zurich.ibm.com/˜cca/papers/stego.pdf.
16. T. Pevn'y, J. and Fridrich, “Benchmarking for Steganography,” Information Hiding.10th International. Workshop, Santa Barbara, CA, LNCS vol. 5284, 2008.
17. D. Upham, “Steganography software for Windows,” 1997, http: //members.tripod.com/steganography/stego/ software.html
18. J. Fridrich, M. Goljan, and D. Hogea, “new methodology for breaking steganographic techniques for JPEGs,” in Proc. of SPIE: Security and Watermarking of Multimedia Contents, vol. 5020, pp 143–155, 2003.
19. Jan Kodovský, Jessica Fridrich ”Quantitative Steganalysis of LSB Embeddingin JPEG Domain” MM&Sec’10, September 9–10, 2010, Roma, Italy.2010 ACM 978-1-4503-0286-9/10/09

Hamdy A. Morsy is a PhD student at Faculty of Engineering at Helwan University, Cairo, Egypt. He received his M.Sc. (2002) from Stevens Institute of Technology, Hoboken, NJ, USA. He is currently working as a senior teaching assistant at faculty of engineering at Helwan University.

Zaki B. Nossair received his B.Sc. in electronics and communications engineering, Helwan University (1978) and M.Sc. in electrical engineering (1985), Stevens Institute of Technology, NJ, USA. His PhD in electrical engineering, Old Dominion university , Norfolk, Virginia, USA, 1989. He is currently an associate professor at Helwan University. His current research interests in the field of image processing, speech processing.

Alaa M. Hamdy received his M.Sc. degree in computer engineering from Helwan University in1996 and his PhD degree from the faculty of electrical engineering, Poznan University of technology, Poland in 2004. Currently he is an assistant professor at faculty of engineering, Helwan University. His research interests in the field of image processing, pattern analysis and machine vision.

Fathy Z. Amer is the professor of Electronics in the department of Communications and Electronics, Helwan University, Cairo, Egypt. Previously, He was an associate professor at faculty of training at El ahsaa, Saudi Arabia from 1995 to 2004. His research interests include Microelectronics and Testing and Information Hiding.

11/1/2011