Optimum segment length for embedding in the LSB of JPEG images with Minimum MSE

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

***Abstract*—Steganography is the science of hiding communication in an innocuous cover medium such as image, audio and video. In this paper, a new steganographic algorithm with optimum segment length and minimum MSE is presented, an algorithm that utilizes the redundant bits of discrete cosine transform (DCT) of JPEG images for message embedding. This algorithm offers high capacity with minimum statistical changes and minimum MSE compared to existing steganographic systems.**

***Index terms*—JPEG images, steganography, steganalysis, information hiding, JPEG hiding.**

I. INTRODUCTION

Steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new techniques for information hiding have become possible. A steganographic system hides information bits in a cover medium such as image, audio or video without disturbing the first order statistical properties of the cover medium and hence avoiding arousing a third party suspicion.

There is a major difference between cryptography and steganography in the sense that in cryptography an eavesdropper knows there is a communication is taken place, but without a decryption algorithm, the attacking is infeasible. Hence the strength of cryptography comes from how powerful the encryption algorithm to prevent any attacker from deciphering the message exchanged between sender and intended recipients.

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. [1] - [5].

In general, the process of information hiding starts by identifying redundant bits in a cover medium. Redundant bits are those bits that can be modified without destroying the integrity 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.

Embedding message bits in the redundant bits of a cover medium will change the statistical properties of that message carrier; as a result of that 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. A cover medium with hidden message is referred to as a stego medium. A stego medium should be secure against visual and statistical attacks and robust against modification such as recompression. Modern steganographic systems are robust against visual attacks and weak against statistical attacks and the ones that are robust against first order statistical attacks offer a relatively small capacity [6] - [11].

In this paper, hiding appropriate message (HAM) algorithm is introduced that globally embeds message bits in the least significant bits (LSB) of the Discrete Cosine Transform (DCT) coefficient of JPEG images. This technique hides data by dividing the message into equal segments of optimum length. The optimum segment length is obtained by measuring the ratio between even and odd nonzero AC DCT coefficients of JPEG image. Each segment has one polarity bit as a header bit which identify that whether the segment or its complement was sent. The HAM algorithm provides high capacity compared to most common steganographic techniques. A comparison between HAM algorithm and modern steganographic systems is introduced and the mean square error of the HAM algorithm is identified.

The rest of this paper is organized as follows. In section II, the HAM algorithm is introduced. Simulation results and comparisons between the proposed algorithm and the current embedding algorithms are presented in section III. The final section gives the conclusion.

II. HAM ALGORITHM

This algorithm exploits the fact that modifying the redundant bits will not affect the statistical properties of the cover media (such as image, audio, or video). JPEG images are one of most common media used for information hiding. The discrete cosine transform (DCT) coefficients of a JPEG image have redundant bits, least significant bits (LSB), which can be modified without visually attacked by an eavesdropper. Modern steganographic systems are secure with low capacity

Manuscript received May 30, 2011.

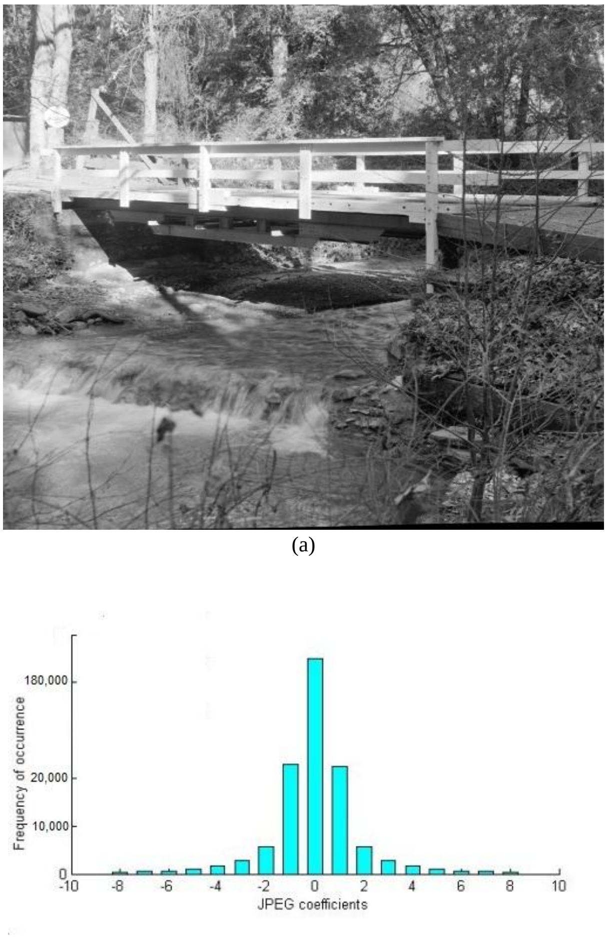
H. A. Morsy, Department of Telecommunication, Helwan University, Cairo 11792, Egypt (e-mail: hmorsy@helwan.edu.eg).

Z. B. Nossair, Department of Telecommunication, Helwan University, Cairo 11792, Egypt (e-mail: znossair@helwan.edu.eg).

A. M. Hamdy, Department of Telecommunication, Helwan University, Cairo 11792, Egypt (e-mail: ahamdy@helwan.edu.eg).

F. Z. Amer, Department of Telecommunication, Helwan University, Cairo 11792, Egypt (e-mail: famer@hlewan.edu.eg).

embedding against visual and statistical attacks however the ones that offer high capacity are weak against statistical analysis. Fig. 1 shows a JPEG image with its histogram of DCT coefficients.



(a)

(b)

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

The DCT coefficients are divided into pairs of values (PoVs), for example (1, 2), (3, 4), (-1, -2) ... etc. one can notice that the odd coefficients occurs more frequently than the adjacent even coefficients (Fig. 1). As an assumption, the message bits are uniformly distributed and as a result embedding this type of message can significantly distort the first order statistical properties of the JPEG image. The first order statistical properties can be preserved by embedding message bits of ones to zeros ratios that match the distribution of even and odd DCT coefficients.

A. 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_{2c-1} and n_{2c}. 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 $n_{2c-1}>n_{2c}$. For a uniform distributed message, the number of frequency of occurrences of the LSB of nonzero AC DCT coefficients n^*_{2c-1} and n^*_{2c} will be equal due to message embedding. 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:

$$n^*_{2c} = \frac{(n2c-1+n2c)}{2} \tag{1}$$

And the Chi-square test can be calculated as:

$$x^2 = \sum_{c=1}^{k} \frac{(n_c - n_c^*)^2}{n_c^*} \tag{2}$$

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

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma(\frac{k-1}{2})}\int_0^{x^2} e^{-\frac{t}{2}} t^{\frac{k-1}{2}-1} dt \tag{3}$$

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 (2). Fig. 2 shows the histogram of stego image with 100 % embedding rate using Jsteg algorithm. It is clear that, every pair of values is equal due to embedding message of uniform distribution.

The message can be divided into small segments of equal number of bits. A polarity bit is prefixed to each segment to determine the type of data in this segment whether the data are sent directly or its complement. The segment length greatly affects the ratio of even and odd DCT coefficients.

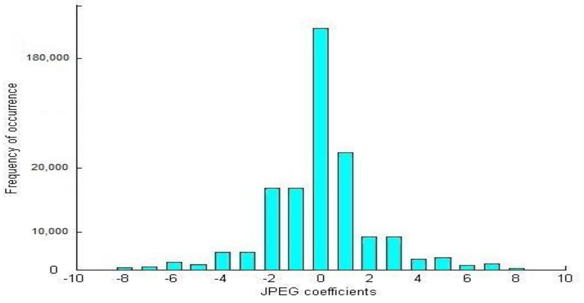


Fig. 2 The histogram of a stego image (Jsteg algorithm)

B. Optimum segment Length

The ratio of even to odd nonzero AC DCT coefficients is affected by the number of zeros and ones in the message.

Assume m_0=0 for bit of value zero and m_1=1 for bit of value one, then the probability of zeros and ones will be P(x=m_0) = P(x=m_1) =0.5. If m_1>m_0 then the number of odd coefficients will be larger than the number of even coefficients which matches the histogram of the original image. But if m_1<m_0 the complement of this segment is used for embedding. To find the optimum segment length, assume that the segment length is m, then the total number of all possible combinations of zeros and ones are equal and is give by:

$$M = mx2^{m-1} \tag{4}$$

Segments with more zeros than ones will be omitted, since the complement of these segments is used. The total number of all combinations of bits with value zero and one are given as:

$$M_0 = M - (m-k)\sum_{k=0}^{(m-1)/2} \binom{m}{k} \qquad (5)$$

$$M_1 = M - k\sum_{k=0}^{(m-1)/2} \binom{m}{k}$$

Equation (4) gives the total number of all possible combinations of zeros and ones in a segment of length m. for the whole message, (5) can be considered as the average number of zeros and ones respectively. One can obtain the optimum segment length by comparing the ratio of zeros and ones to the ratio of even and odd DCT coefficients. The ratio R_0 of zeros to the total number of bits can be calculated as:

$$R_0 = M_0 /(M_0 + M_1) \qquad (6)$$

The ratio R_0 with odd segment lengths increases with a step smaller than that with even segment lengths. However, the optimum segment length is only determined by checking the ratio of even to odd AC DCT coefficients of a given cover media.

C. Embedding Algorithm

1) Encrypt message bits with encryption algorithm (e.g. RC4 stream cipher).
2) Divide message bits into equal length of m bits (e.g. m=1, 2, 3 …).
3) Determine the polarity bit for each segment.
4) Insert the polarity bit in each segment (segment length m=m+1).
5) Apply DCT transform and quantization for image compression in JPEG image format.
6) Extract the non zero AC DCT coefficients.
7) Embed message segments into non zero AC DCT coefficients.
8) Change segment length and repeat steps from 2 to 7
9) Find segment length that provides minimum change density.
10) Use Huffman coder for image encoding.

D. Extracting Algorithm

1) Decode the compressed image using Huffman Decoder
2) Convert odd coefficients into ones and even coefficients into zeros
3) Divide the resulting data into segments of length m

4) If the segment polarity is 1 save m-1 bits in a file and if the segment polarity is 0 save the complement of this segment
5) Repeat step 4 for the rest of DCT coefficients and append the extracted segment into the previous ones
6) Decrypt the message bits using decryption algorithm.

III. SIMULATION RESULTS

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. For example, the two AC DCT coefficients 1 and 2 can be used to embed data as 1's represent a 1 bit data and 2's represent a 0 bit data. The DC DCT coefficient is avoided so it greatly affects the image average value and the zeros of AC DCT coefficients are also avoided.

Let C is the cover medium DCT coefficient matrix of size M x N and S is the stego medium DCT coefficient matrix of size M x N. Each element in C matrix consists of two parts C_{ij} for the most significant bits of the ij DCT coefficient and c_{ij} is the LSB of i and j DCT coefficient. The same notation can be applied to the S matrix. The message matrix m will have only LSB bits and represented as m_{ij}.

$$C = \begin{bmatrix} C_{11}+c_{11} & C_{12}+c_{12} & \dots & C_{1N}+c_{1N} \\ C_{21}+c_{21} & C_{22}+c_{22} & \dots & C_{2N}+c_{2N} \\ \dots & \dots & \dots & \dots \\ C_{M1}+c_{M1} & C_{M2}+c_{M2} & \dots & C_{MN}+c_{MN} \end{bmatrix} \qquad (9)$$

$$S = \begin{bmatrix} S_{11}+s_{11} & S_{12}+s_{12} & \dots & S_{1N}+s_{1N} \\ S_{21}+s_{21} & S_{22}+s_{22} & \dots & S_{2N}+s_{2N} \\ \dots & \dots & \dots & \dots \\ S_{M1}+s_{M1} & S_{M2}+s_{M2} & \dots & S_{MN}+s_{MN} \end{bmatrix} \qquad (10)$$

The message bits matrix will be

$$m = \begin{bmatrix} m_{11} & m_{12} & \dots & m_{1N} \\ m_{21} & m_{22} & \dots & m_{1N} \\ \dots & \dots & \dots & \dots \\ m_{M1} & m_{M1} & \dots & m_{MN} \end{bmatrix} \qquad (11)$$

Modifying the LSBs of nonzero AC DCT coefficients with message bits affects the distribution of the DCT of JPEG images [11], [12], [14], [15]. Each element of the stego matrix will have the value

$$S_{ij} + s_{ij} = C_{ij} + m_{ij} \qquad (12)$$

Equation (12) shows that the difference between the stego image and the cover image is in the LSB only (i.e. m_{ij} and c_{ij}).

This difference can be defined as the change density of the cover image due to message embedding and equal to:

$$D_{AC} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} m_{ij} + c_{ij} - 2m_{ij}c_{ij}}{MN} x100 \qquad (13)$$

Where D_{AC} is the change density of the cover image.

Minimum change density can be achieved by limiting the message size or by modifying the message distribution so it matches the distribution of the DCT coefficients of the JPEG image. A comparison of change density between Hiding Appropriate Message (HAM) algorithm and Jsteg and F5 algorithms based on the absolute value of changes made to the nonzero AC DCT coefficients of an image (Bridge image) [13] is shown in Fig. 3. A reference algorithm is added in this comparison which has the property of embedding data directly into nonzero AC DCT coefficients without any processing or adding control bits; a modified version of Jsteg called symmetric Jsteg [17]. In addition to the randomly generated message bits, HAM algorithm is applied on a text file (Matlab readme file). Outguess is excluded from this comparison, since its maximum capacity is limited to 50 % of the available AC DCT coefficients. From Fig. 3 it can be noticed that F5 behaves very well when the message size is less 10 % and the intersection in the figure can not be obtained with F5 algorithm for the total number of available DCT coefficients. Once the message size exceeds this limit, HAM algorithm outperforms other algorithms on both computer generated data and on real text files.

The size of an image and its textural properties affect the maximum limit of embedding data bits using different steganographic systems. Assume C is the maximum number of message bits that can be embedded into the non-zero AC DCT coefficients and M x N is the total number of DCT coefficients, the relation between C and N is given as:

$$C = \eta(MN - n_0 - n_{DC}) \qquad (14)$$

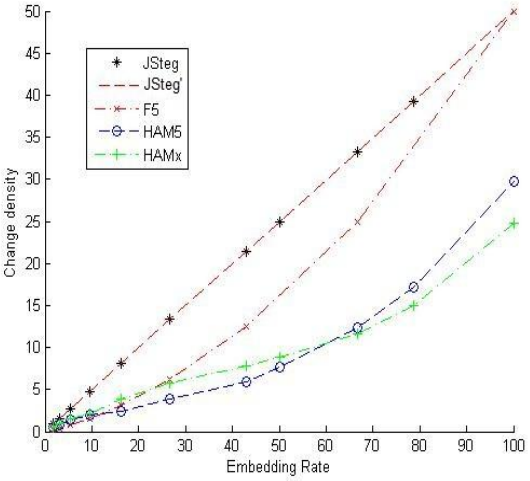


Fig. 3. A comparison between HAM algorithm and DEA, Jsteg and F5 algorithm

Where $\eta = \dfrac{m}{m+1}$ is the efficiency of embedding,

n_{DC}= MN/64 is number of DC DCT coefficients, and

n_0 = the number of zero AC DCT coefficients.

Equation (14) defines the relation between the capacity of embedding and the DCT coefficients. There is a tradeoff between the capacity 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. HAM algorithm provides high capacity in all gray images used in testing with different textural properties as shown in table I.

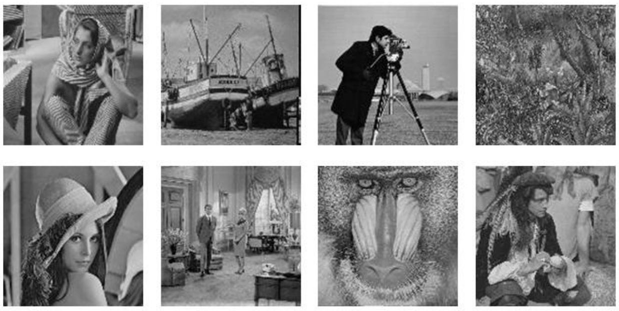


Fig. 4. Standard test images from left-top Barbara, Boat, Camera man, and Jungle and from left- bottom Lena, Living room, Mandrill, and Pirate

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

Test images	Capacity in bits			
	HAM	Jsteg	F5	Outguess
Barbara	47072	40050	39892	20025
Boat	53370	41966	45229	20983
Camera man	24064	22572	20393	11286
Jungle	81246	71522	68853	35761
Lena	31849	28035	26992	14017
Living room	36609	34041	31025	17020
Mandrill	29761	26555	25990	13277
Pirate	36817	34126	31201	17063

The HAM algorithm gives different values of capacity measurements with different images. This is due to the variation of textural properties from one image to another.

Another criterion can define the performance of image embedding which is the mean square error (MSE) of an image in the spatial domain. The MSE occurs due to embedding message bits in the frequency domain and can be calculated as:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j) - S(i,j))^2 \qquad (15)$$

Where C(i,j) and S(i,j) are the image pixel values before and after embedding respectively and M and N are the dimension of the image. MSE can be used to calculate the peak signal to noise ratio as follows:

$$PSNR = 20\log_{10}(\frac{255}{\sqrt{MSE}}) \qquad (16)$$

This criterion can measure the effect of embedding message bits in the frequency domain on the spatial domain. Another criterion which measures the changes due to message embedding is cross correlation and is given by:

$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-M_1)(S(i,j)-M_2)}{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-M_1)^2} \qquad (17)$$

A comparison between HAM algorithm and Jsteg' algorithm (symmetric Jsteg) is shown in table II and table III. HAM algorithm outperforms the symmetric Jsteg' algorithm based on PSNR but the cross correlation depends on the textural properties. The cross correlation of HAM algorithm is higher than the Jsteg' algorithm with images with high textural properties.

TABLE II: THE MSE AND PSNR OF STANDARD TEST IMAGES OF HAM ALGORITHM AND STANDARD EMBEDDING ALGORITHM.

Test Image	Jsteg'		HAM	
	MSE	PSNR	MSE	PSNR
Mandrill	177	25.65	146.10	26.48
Jungle	230	24.51	78.21	29.20
Boat	105	27.92	53.41	30.85
Barbara	108	27.8	63.65	30.09
Living room	56	30.65	22.14	34.68
Pirate	55	30.73	20.71	34.97
Lena	41	32	14.04	36.66
Camera man	32	33,08	24.01	34.33

TABLE III: THE CC OF STANDARD TEST IMAGES OF HAM ALGORITHM AND STANDARD EMBEDDING ALGORITHM.

Test Image	Jsteg'	HAM
Mandrill	96.92	90.16
Jungle	91.06	93.40
Boat	95.99	97.13
Barbara	94.68	96.51
Living room	98.94	98.82
Pirate	99.19	98.97
Lena	99.39	99.97
Camera man	100	99.85

IV. CONCLUSION

HAM algorithm proved to outperform current algorithm when high capacity of embedding is a requirement. This algorithm minimizes the changes introduced to the first order statistical properties of the cover media due to message embedding by matching the distribution of the message bits with the DCT distribution of the cover medium. HAM algorithm proved to defeat both visual and statistical attacks exploiting the fact that uniformly distributed messages have non uniform distribution over small segments of the message bits. The peak signal to noise ratio and the cross correlation increase with images of low textural properties.

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 Computer and Electrical Engineering* vol. 3, no. 3, pp. 449-453 , 2011.
2. 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
3. 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.
4. A. Kerckhoffs, "La Cryptographie Militaire", *Journal des Sciences Militaires*, 9th series, IX pp 5–38; Feb. pp 161–191, Jan. 1883.
5. N. Provos, and P. Honeyman, "Detecting Steganographic Content on the Internet," *CITI Technical Report* 01-11, 2001.
6. C. Cachin," *An Information-Theoretic Model for Steganography*," *Cryptology ePrint Archive*, 2002.
7. N. Memon, and M. Kharrazi, "Performance study of common image steganography," *Journal of Electronic Imaging* 15(4), 041104 (Oct-Dec), 2006.
8. 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.
9. A. Westfeld, "F5—A Steganographic Algorithm High Capacity Despite Better Steganalysis," *Springer-Verlag Berlin Heidelberg*, 2001.
10. A. Westfeld, "Detecting Low Embedding Rates, ", 5th *Information Hiding Workshop.* Nooerdwijkerhout, Netherlands, Oct. 7−9, 2002
11. A. 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.
12. N. Provos, and P. Honeyman, "Hide and Seek: An introduction to steganography," *IEEE Computer security* 15407993/03, 2003
13. T. Pevn'y, J. and Fridrich, "Benchmarking for Steganography," *Information Hiding.10th International. Workshop,* Santa Barbara, CA, LNCS vol. 5284, 2008.
14. C. Hung, "PVRG-JPEG Codec, 1.1," Stanford University, 1993. http://archiv.leo.org/pub/comp/os/unix/graphics/jpeg/PVRG 291.
15. D. Upham, "Steganography software for Windows," 1997, http: //members.tripod.com/steganography/stego/ software.html
16. 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.
17. *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*

AUTHORS PROFILE

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.