ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 3, No.15 , May 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Non-blind Data hiding for RGB images using DCT-based fusion and H.264 compression concepts

Safwat Hamad[1] and Amal Khalifa[1,2]

[1] Department of Scientific Computing, Faculty of Computer and Information Sciences, Ain Shams University
Abbassia 11566, Cairo, Egypt
shamad@cis.asu.edu.eg

[2] College of Computer and Information Sciences, Princess Nora Bint Abdulrahman University
Riyadh, KSA
ASkhalifa@pnu.edu.sa

Abstract

Steganography is the field of research that provides innovative solutions to the problem of secure data communication. In this paper, a non-blind data hiding technique is proposed which is based on data fusion between both the cover and the secret images. The proposed embedding process is made in the Discrete Cosine Transform (DCT) domain of the cover image. In addition, the cover image undergoes a H.264 compression as a pre-processing step for the sake of spatial redundancy reduction. Experimental results showed that the proposed method allows an image to hide another one that is as large as itself while maintaining a remarkably outstanding invisibility performance. Furthermore, a comprehensive comparison showed that the proposed method outperformed a number of similar techniques not only in imperceptibility but also with respect to the hiding capacity.

Keywords: *information hiding, embedding, image, Discrete Cosine Transform, non-blind, invisibility, payload.*

1. Introduction

Back to 440 B.C, ancient Greek used creative ways to communicate secret information especially during war times. Beside Cryptography, information hiding techniques were used to conceal the contents of a message in some other innocent cover such that it won't raise suspicion. In 1499, Johannes Trithemius coined the term steganography as a combination two Greek words steganos (στεγανός), meaning "covered, concealed, or protected", and graphei (γραφή) meaning "writing". Since then, Steganography has been considered as an effective tool for information security.

In modern times, Steganography techniques a wide range of digital media were utilized as a host (cover) to hide or embed a piece of information (message) in such a way that it is imperceptible to a human observer but can be detected/extracted easily with a computer. These covers can take the form of any digital media such as audio tracks, Videos [1], images [2], File systems [3], networks [4], 3D objects [5], and even DNA sequences [6].

In this paper, we propose a novel technique for hiding images into other images. The proposed method is based on the properties of the recent H.264 compression technique in order to embed the secret information into the coefficients of the discrete cosine transform (DCT) of a true colored cover image. Different performance aspects of the method are measured and compared against a number of existing techniques.

The rest of the paper is organized as follows: the next section gives a quick literature review on information hiding in images. Section three describes the hiding/extraction model of the proposed technique. Experimental results are presented and analyzed in section IV, where a performance comparison was held between the proposed technique and other methods highlighting weaknesses and strengths of each one of them over the others. Finally, section V summarizes the findings and conclusions.

2. Related Work

Information hiding techniques in digital images are really diverse. Hence, a number of categorizations were proposed to group various techniques into a number of classes based on some criteria. One categorization is based on the domain of embedding. According to this categorization, techniques are classified into spatial-domain and transform-domain methods. Embedding in the spatial domain actually involves hiding the secret information directly in the pixel illumination values of the image [7-9]. On the other hand, transform-domain techniques hide the message by modulating coefficients in some transform domain, such as the Fourier Transform (FT) [10], Discrete-Cosine Transform (DCT) [11], and Discrete Wavelet transform (DWT) [12-18].Since most of the conventional transforms are irreversible, some hiding techniques employed the integer-to-integer wavelet transform to prevent coefficients from being potentially

lost through forward and inverse transforms due to any truncation or rounding errors [19, 20]. Furthermore, some methods may combine more than a transform to implement their hiding process [21, 22].

Another orthogonal categorization differentiates between blind and non-blind (cover-Screw) schemes. In blind, or oblivious, schemes allows the hidden data to be extracted directly from the modified cover without knowledge of the original image [12, 13, 18], while in non-blind schemes the original cover is needed to reveal the hidden information [21, 23]. Obviously, blind techniques are preferred over the non-blind ones since they are more practical and reliable. Dual embedding mixes both blind and non-blind algorithms where a sign image is embedded into a logo in a non-blind fashion to create a signed-logo which is then embedded into the cover image in a blind fashion [24].

In this context, it is worth to highlight the difference between Steganography and watermarking. That is, the objective of Steganography applications is to provide a means of secret communication that is imperceptible to the human visual system [9, 23, 25]. On the other hand, watermarking algorithms are mainly concerned with copyright protection. Thus, they must be robust against certain attacks such as filtering, noise addition, and compression [13, 16-18]. These diverse goals create a tradeoff between invisibility and robustness. That is, embedding data in significant parts of the image will probably make it survive against attacks. However, this can strongly influence their perceptual quality as well as the available hiding capacity. An extensive and yet very useful review on recent image steganography techniques can be found in [2].

3. The Proposed Method

The proposed steganographic method is divided into two phases: embedding and extraction. The hiding process takes place in the DCT domain where the secret information is considered to be a true colored image. However, the same technique can be applied on grayscale images. Figure 1 depicts the overall hiding scheme. Notice that the extraction phase requires the original cover image which makes the whole method non-blind.

3.1 Data Embedding

The embedding process starts with an adjustment step that is applied on both the cover and the secret images. The purpose of this step is to ensure that changes made during the embedding process would not result in overflow in the image pixel values. Hence, the extraction process can be done with minimum errors. Notice that this adjustment operation assumes that the image is represented in floating point format. That is, the RGB values are normalized to span a range between 0.0 and 1.0.

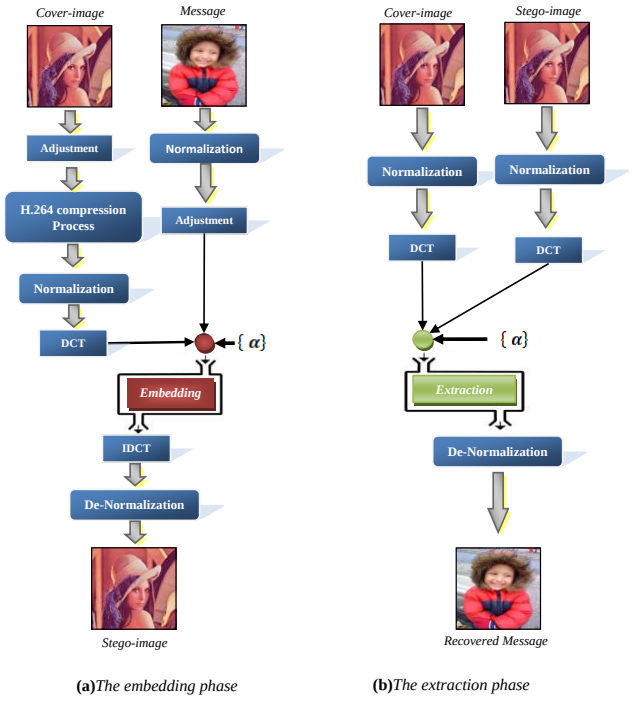


Fig. 1 The proposed steganographic model.

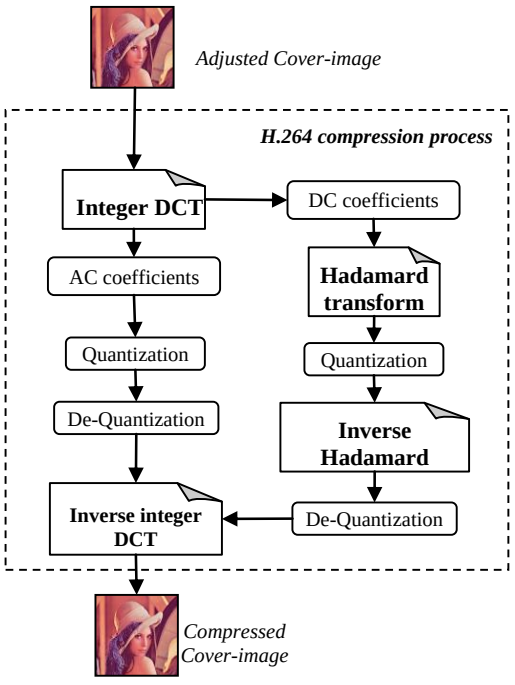


Fig. 2 The details of the H.264 compression process.

Algorithm1: The Embedding Process
Input: Cover and Secret images, α and QP
Output: Stego Image

1) Read Cover image → *Cover*.
2) Read Secret image → *Msg*.
3) Normalize both *Cover* and *Msg*.
4) Adjust extreme pixel values in *Cover* and *Msg* using the functions:

$$Cover = \begin{cases} 1-\alpha, Cover \geq 1-\alpha \\ \alpha, Cover \leq \alpha \end{cases}$$

$$Msg = \begin{cases} 1-\alpha, Msg \geq 1-\alpha \\ \alpha, Msg \leq \alpha \end{cases}$$

5) De-normalize Cover.
6) Compress Cover using H.264 concept:
 6.1) Transform *Cover* into integer DCT domain for each micro block (MB).
 6.2) Quantize and De-Quantize AC coefficients in MB using QP.
 6.3) Pick out DC coefficient in MB and apply the following:
  6.3.1) Apply Hadamard transform.
  6.3.2) Quantize Hadamard coefficients.
  6.3.3) Inverse Hadamard transform.
  6.3.4) De-Quantize the resultant coefficients.
 6.4) Apply inverse integer DCT transform on resultant MB coefficients.
7) For each MB, Transform normalized Compressed *Cover* in DCT domain.
8) Embed *Msg* pixels into Compressed *Cover* coefficients using the following equation:

$$Stego = sign\{Cover\}[(1-\alpha)\times|Cover| + (\alpha \times Msg)]$$

9) Apply inverse DCT transform on resultant *Stego* coefficients.
10) De-normalize *Stego*.
11) Return the *Stego* image.

The next step can be considered as a preprocessing step that takes place on the adjusted cover image. Here we suggest the image to undergo a H.264 compression process using an integer DCT. As shown in figure 2, the image is divided into 16×16 blocks where each block is divided into 4×4 Micro block (MB). Then, a 4×4 Integer DCT is applied on each MB independently resulting in a 16-element DCT transform that consists of 1 DC coefficient and 15 AC coefficients. The DC coefficient represents the average color of the 4x4 region while the 15 AC coefficients represent color change across the block. After that, a quantization step takes place in order to scale down the transformed coefficients using a Quantization Parameter (QP). Finally, a De-Quantization and Inverse integer DCT are applied to reconstruct the compressed cover image. Notice that a 4×4 Hadamard transform is applied on the 16 DC coefficients in each block as a second-level transform before the reconstruction process takes place. The reason behind that is called a hierarchical transform [26, 27].

Now, the embedding process can start using the resultant compressed cover image. In fact, the hiding process is based on the idea of data fusion. Fusion refers to the processing and synergistic combination of information from various knowledge sources and sensors to provide a better understanding of the situation under consideration [28]. Here, the fusion operation takes place in the DCT domain between the compressed cover coefficients (Cover) and the adjusted normalized secret pixels (Msg) using the following equation:

$$Stego = sign\{Cover\}[(1-\alpha)\times|Cover| + (\alpha \times Msg)] \quad (1)$$

where α is the embedding strength which ranges from 0.0 to 1.0. Algorithm1 summarizes the steps of the embedding module.

3.2 Data Extraction

In the extraction process, the steps carried out in the embedding process are generally reversed to recover the hidden message. The steps of the extraction module are listed in Algorithm2. Once again, the proposed method is non-blind which means that the original cover image is required to extract the hidden data.

Algorithm2: The Extraction Process
Input: α, Stego and Cover Image
Output: Secret image

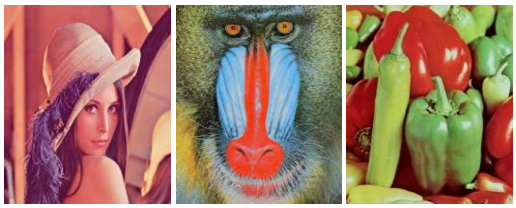
1) Read Stego image → *Stego*.
2) Read Cover image → *Cover*.
3) Normalize *Stego* and *Cover*.
4) For each MB, Transform *Stego* and *Cover* into DCT domain.

$$Rec\ Msg = \frac{1}{\alpha}[|Stego| - (1-\alpha)\times|Cover|]$$

5) De-normalize the extracted *Rec Msg* pixels
6) Return the *Rec Msg* as Secret image.

4. Experimental Results

Throughout the following sets of experiments, three standard test images (Lena, Baboon, and Pepper) were used as covers. Another 512x512 colored image is used as the secret message. These images are shown in figure 3.



(a) Test images

(b) Secret image

Fig. 3 Images used for testing the performance of the proposed algorithm.

Table 1: The invisibility performance of the proposed method with varying values of α and QP

	QP=18			QP=20			QP=22			QP=24			QP=26			QP=28		
α	0.01	0.05	0.1	0.01	0.05	0.1	0.01	0.05	0.1	0.01	0.05	0.1	0.01	0.05	0.1	0.01	0.05	0.1
Lena	46.52	37.94	35.18	45.26	37.77	35.18	43.79	37.59	35.2	42.34	37.55	35.42	41.15	37.76	35.87	39.9	37.75	36.16
Baboon	47.18	38.57	36.01	46.01	38.44	35.97	44.54	38.27	35.92	42.84	38.01	35.82	41.18	37.72	35.77	39.47	37.28	35.61
Pepper	45.01	35.75	33.64	44	35.65	33.61	42.7	35.48	33.58	41.32	35.37	33.62	40.09	35.37	33.77	38.81	35.31	33.94

Table 2: The accuracy of extraction provided by the proposed method at varying values of α and QP

	QP=18			QP=20			QP=22			QP=24			QP=26			QP=28		
α	0.01	0.05	0.1	0.01	0.05	0.1	0.01	0.05	0.1	0.01	0.05	0.1	0.01	0.05	0.1	0.01	0.05	0.1
From Lena (%)	98.37	99.81	99.48	98.37	99.78	99.41	98.38	99.75	99.33	98.38	99.75	99.28	98.39	99.74	99.25	98.41	99.74	99.24
From Baboon (%)	98.34	99.82	99.62	98.33	99.81	99.61	98.31	99.79	99.59	98.32	99.78	99.58	98.31	99.76	99.56	98.31	99.75	99.54
From Pepper (%)	98.32	99.86	99.8	98.3	99.85	99.8	98.3	99.85	99.78	98.3	99.85	99.78	98.3	99.86	99.78	98.31	99.86	99.77

The invisibility performance is measured in terms of the Peak Signal-to-Noise Ratio (PSNR). PSNR is measured in decibels (dB) and can be computed as in equation 2, where p(x,y) represents the shade level of a pixel, whose coordinates are (x,y) in the original image, and represents the same pixel in the distorted image. Generally, PSNR values of 40 dB or higher indicate acceptable, less suspicious images.

$$PSNR = 10 \times \log\left(\frac{(\max p(x,y))^2}{MSE}\right) \quad (2)$$

$$MSE = \frac{1}{X \times Y}\sum_{x,y}(p(x,y) - \tilde{p}(x,y))^2 \quad (3)$$

Furthermore, since the extracted message is expected to be only an estimate of the original one, we need some measure to quantify similarity between the original secret message and the extracted one. Here, we employ the normalized correlation (NC) coefficient to indicate how much of the original message was successfully extracted. It can be computed as follows:

$$Sim(x, x^*) = \frac{(X \times X^*) \div (\sqrt{X \times X^*})}{(X \times X) \div (\sqrt{X \times X})} \times 100 \quad (4)$$

where X is the original message components organized as a vector, and X* is the recovered vector. Obviously, the higher similarity is the better quality of the retrieved watermark.

4.1 Invisibility Performance

In our first set of experiments, we are going to investigate the effect of the two embedding parameters α and QP on the fidelity of the stego-images when applying the maximum payload. The results are listed in table 1. However, these results can't be useful without simultaneously studying their effect on the correctness of the extracted image. So, table 2 shows the similarity between the secret image and the extracted secret image. In addition, figures 4 and 5 show respectively the computed PSNR of the stego-images as well as the similarity of the extracted messages at different values of α while QP is fixed at 18. The results show that α at 0.02 achieves a good tradeoff between the visual quality of the stego image and the accuracy of the extracted message.

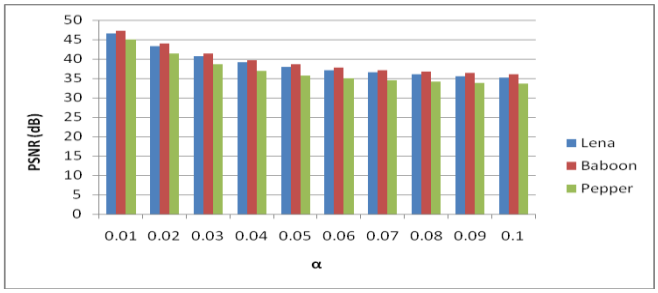


Fig. 4 The invisibility performance of the proposed method on the three test images at QP = 18 using different values of α.

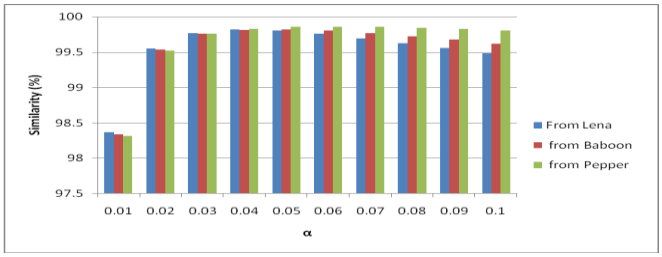


Fig. 5 The accuracy of the extracted message from the three test images at QP = 18, using different values of α.

Now, at α = 0.02, different values for QP were investigated to judge their effect on the hiding quality. Figures 6 and 7 show the results highlight that 20 can be the recommended value for QP. A closer look on the resultant images using these recommended values are shown in figure 8. With a simple visual inspection, the results show that the proposed method succeeded to hide into an image another image that is as large as itself while maintaining the fidelity of the stego-image and providing almost perfect retrieval of the secret message.

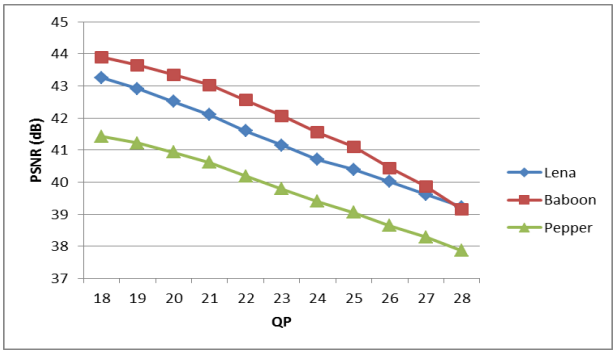


Fig. 6 The invisibility performance of the proposed method on the three test images using different values of QP, α = 0.02.

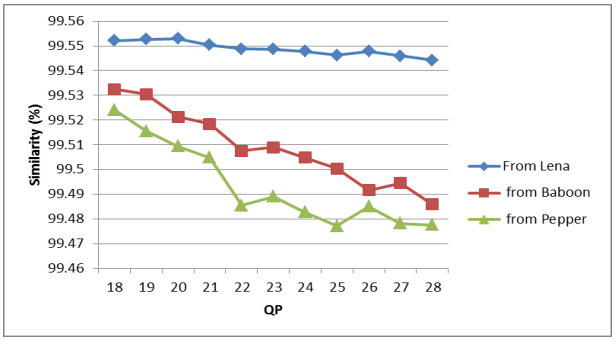


Fig. 7 The accuracy of the extracted message from the three test images using different values of QP, α= 0.02.

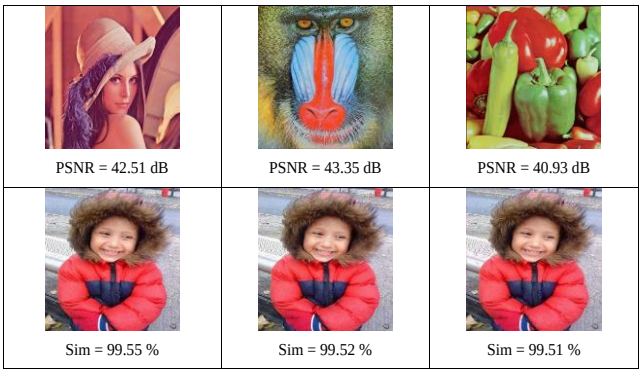


Fig. 8 Resultant stego- and the extracted images at α = 0.02 and QP = 20.

4.2 Comparisons with other methods

In this section, we are going to compare the performance of the proposed method with other existing techniques. The comparison is made with respect to a number of criteria such as the domain of embedding and the maximum hiding capacity. For the sake of standardization, this set of experiments used the 512x512 colored Lena as the test image. Furthermore, the PSNR values are computed at the maximum embedding capacity offered by each method.

The results listed in table 3 show that the proposed algorithm outperforms the other existing schemes in terms of invisibility. In addition, although another technique [29] provides the same capacity, it still cannot reach the high imperceptibility of the proposed method. However, it still has an advantage of being blind where the hidden data can be retrieved without referring to the original cover image.

Table 3: Performance comparisons with other hiding techniques

Method	*Domain of embedding*	*PSNR (dB)*	*Hiding Capacity*
Kawaguchi and Eason, 1998 [30]	Spatial (BPCS)	NA	30%-50%
Spaulding et al., 2002[31]	DWT	30	25%
Tolba et al. 2005[32]	Integer WLT (**N=4**)	39.36	50%
Chang et al. 2007 [33]	DCT	30.34	1.76%
Lin and Shiu, 2009 [34]	DCT	34.30	2.75%
Lin et al. 2010 [11]	DCT	35.28	4.30%
Jinna and Ganesan, 2010 [19]	Integer WLT	37.89	5%
Hamad et al. 2014 [29]	DWT (β=40)	37.41	100%
Proposed	DCT (α= 0.02, QP=20)	42.51	100%

5. Conclusions

This paper presents a non-blind steganographic scheme that is based on the idea of data fusion. The method actually merges the normalized pixels of the secret image with the DCT coefficients of the cover image. Before this fusion phase, the cover image undergoes a compression step to reduce spatial redundancy using H.264 compression standard concepts. In addition, the algorithm applies an adjustment operation on the normalized cover pixels to guarantee that the message will be recovered with acceptable accuracy even when the value of embedding strength factor (α) is kept low.
Experimental results showed that the proposed method can successfully hide an image into another one that is as large as itself while maintaining the fidelity of the stego-image and providing almost perfect retrieval of the embedded secret message. When compared with other existing techniques, the results showed that the proposed algorithm achieved an outstanding invisibility performance as well as a remarkably high hiding capacity.

References

[1] Y.-C. Liao, C.-H. Chen, T. K. Shih, and N. C. Tang, "Data hiding in video using adaptive LSB," in *Pervasive Computing (JCPC), 2009 Joint Conferences on*, 2009, pp. 185-190.
[2] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, pp. 727-752, 2010.
[3] R. Anderson, R. Needham, and A. Shamir, "The steganographic file system," in *Information Hiding*, 1998, pp. 73-82.
[4] S. J. Murdoch and S. Lewis, "Embedding covert channels into TCP/IP," in *Information Hiding*, 2005, pp. 247-261.
[5] K. Wang, G. Lavoué, F. Denis, and A. Baskurt, "A comprehensive survey on three-dimensional mesh watermarking," *Multimedia, IEEE Transactions on*, vol. 10, pp. 1513-1527, 2008.
[6] A. Khalifa and A. Atito, "High-capacity DNA-based steganography," in *Informatics and Systems (INFOS), 2012 8th International Conference on*, 2012, pp. BIO-76-BIO-80.
[7] Y.-K. Lee and L.-H. Chen, "An adaptive image steganographic model based on minimum-error lsb replacement," in *Ninth National Conference on Information Security*, 1999, pp. 8-15.
[8] D. Neeta, K. Snehal, and D. Jacobs, "Implementation of LSB steganography and its evaluation for various bits," in *Digital Information Management, 2006 1st International Conference on*, 2006, pp. 173-178.
[9] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, pp. 1613-1626, 2003.
[10] W.-Y. Chen, "Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation," *Applied Mathematics and Computation*, vol. 185, pp. 432-448, 2007.
[11] C.-C. Lin and P.-F. Shiu, "High capacity data hiding scheme for DCT-based images," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, pp. 220-240, 2010.
[12] H. A. Abdallah, M. M. Hadhoud, A. A. Shaalan, and F. E. Abd El-samie, "Blind Wavelet-Based Image Watermarking," *International Journal of Signal Processing, Image Processing & Pattern Recognition*, vol. 4, 2011.
[13] N. Kashyap and G. Sinha, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)," *International Journal of Modern Education & Computer Science*, vol. 4, 2012.
[14] A. Khan, S. A. Malik, A. Ali, R. Chamlawi, M. Hussain, M. T. Mahmood, *et al.*, "Intelligent reversible watermarking and authentication: Hiding depth map information for< i> 3D</i> cameras," *Information Sciences*, vol. 216, pp. 155-175, 2012.
[15] L. Fan, T. Gao, and Q. Yang, "A novel zero-watermark copyright authentication scheme based on lifting wavelet and Harris corner detection," *Wuhan University Journal of Natural Sciences*, vol. 15, pp. 408-414, 2010.
[16] S. Lagzian, M. Soryani, and M. Fathy, "Robust watermarking scheme based on RDWT-SVD: Embedding Data in All subbands," in *Artificial Intelligence and Signal Processing (AISP), 2011 International Symposium on*, 2011, pp. 48-52.
[17] G. Thirugnanam and S. Arulselvi, "Wavelet Packet based Robust Digital Image Watermarking and Extraction using Independent Component Analysis," *International Journal of Signal & Image Processing*, vol. 1, 2010.
[18] C.-C. Wu, Y. Su, T.-M. Tu, C.-P. Chang, and S.-Y. Li, "Saturation Adjustment Scheme of Blind Color Watermarking for Secret Text Hiding," *Journal of Multimedia*, vol. 5, 2010.
[19] S. K. Jinna and L. Ganesan, "Reversible image data hiding using lifting wavelet transform and histogram shifting," *arXiv preprint arXiv:1004.1791*, 2010.
[20] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform,"

Information Forensics and Security, IEEE Transactions on, vol. 2, pp. 321-330, 2007.
[21] V. Santhi and A. Thangavelu, "DC Coefficients Based Watermarking Technique for color Images Using Singular Value Decomposition," *International Journal of Computer and Electrical Engineering*, vol. 3, pp. 1793-8163, 2011.
[22] T. Minamoto and K. Aoki, "A blind digital image watermarking method using interval wavelet decomposition," *International Journal of Signal Processing, Image Processing & Pattern Recognition*, vol. 3, 2010.
[23] M. F. Tolba, M.-S. Ghonemy, I.-H. Taha, and A. S. Khalifa, "High capacity image steganography using wavelet-based fusion," in *Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on*, 2004, pp. 430-435.
[24] S. Tripathi, N. Ramesh, A. Bernito, and K. Neeraj, "A DWT based Dual Image Watermarking Technique for authenticity and watermark protection," *Signal and Image Processing: an international journal (SIPIJ)*, vol. 1, pp. 34-45, 2010.
[25] M. Khatirinejad and P. Lisoněk, "Linear codes for high payload steganography," *Discrete Applied Mathematics*, vol. 157, pp. 971-981, 2009.
[26] H. S. Malvar, A. Hallapuro, M. Karczewicz, and L. Kerofsky, "Low-complexity transform and quantization in H. 264/AVC," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 13, pp. 598-603, 2003.
[27] H. S. Malvar, *Signal processing with lapped transforms*: Artech House, 1992.
[28] D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," in *International Conference on Image Processing*, 1997, pp. 544-547.
[29] S. Hamad, A. Khalifa, and A. Elhadad, "A Blind High-Capacity Wavelet-Based Steganography Technique for Hiding Images into other Images," *Advances in Electrical and Computer Engineering*, vol. 14, pp. 35-42, 2014.
[30] E. Kawaguchi and R. O. Eason, "Principles and applications of BPCS steganography," in *Photonics East (ISAM, VVDC, IEMB)*, 1999, pp. 464-473.
[31] J. Spaulding, H. Noda, M. N. Shirazi, and E. Kawaguchi, "BPCS steganography using EZW lossy compressed images," *Pattern Recognition Letters*, vol. 23, pp. 1579-1587, 2002.
[32] M. F. Tolba, M. A.-S. Ghoniemy, I. A.-H. Taha, and A. S. Khalifa, "Reliable blind informamtion hiding into colored images using reversible wavelet transforms," *I. J. Comput. Appl.*, vol. 12, pp. 133–140, 2005.
[33] C.-C. Chang, C.-C. Lin, C.-S. Tseng, and W.-L. Tai, "Reversible hiding in DCT-based compressed images," *Information Sciences*, vol. 177, pp. 2768-2786, 2007.
[34] C.-C. Lin and P.-F. Shiu, "DCT-based reversible data hiding scheme," in *Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication*, 2009, pp. 327-335.

Safwat Hamad currently works as an assistant professor of Scientific Computing at Faculty of Computer & Information Sciences, Ain Shams University, Egypt since 2009. He graduated in 2000 and worked as a teaching assistant for a number of undergraduate courses till 2004. He got his MSc degree in the field of Modelling Simulation and Visualization. He earned his PhD degree in 2008 in the area of High performance Computing. The PhD was under a joint supervision between Computer Science and Engineering Department at University of Connecticut, USA and the Faculty of Computer and Information Sciences at Ain Shams University, Egypt. His main research interests are Computer Graphics and Visualization, Image and Video Processing, High Performance Computing and Cryptography.

Amal Khalifa currently works as an assistant professor of Computer Science at College of Computer and Information Sciences, Princess Nora Bint Abdulrahman University, Riyadh KSA since 2013. She was working as an assistant professor of Scientific Computing at Faculty of Computer & Information Sciences, Ain Shams University, Egypt since 2009 (now on leave). She got her M.Sc. degree in the field of Information Hiding in Digital Images. In 2005 she was granted a 2 years research scholarship in University of Connecticut, USA. She earned her PhD degree in 2009 in the area of High performance Computing. Her main research interests are Steganography, computational biology, parallel computing, encryption and Security.