# Stego-Based-Crypto Technique for High Security Applications

Adnan Mohsin Abdulazeez Brifcani, *Senior Member, IACSIT* and Wafaa Mustafa Abduallah Brifcani

***Abstract*—In this paper a two stage (stego-based-crypto) invertible technique is proposed based on cryptography and steganography algorithms. In order to increase the security, the proposed technique uses Rivest-Shamir-Adleman (RSA) cryptographic algorithm in the first stage for encrypting the secret message, and Integer Wavelet Transform (IWT) based lifting scheme in the second stage as a steganography algorithm to hide the secret message, To increase the capacity of secret message payload and robustness, data are embedded in the integer wavelet transform coefficients; in the low, middle and high frequency sub-bands. Through the using of present technique, imperceptibility is improved by increasing Peak Signal to Noise Ratio (PSNR) values, security improved by using public key cryptography algorithm, capacity improved by embedding data in the integer wavelet transform coefficients; in the low, middle and high frequency sub-bands (LL, LH, HL, HH).**

***Index Terms*—Cryptography, Lifting Scheme, Steganography, Wavelet Transform.**

## I. Introduction

Cyptography and steganography are related to each other. The main difference between cryptography and steganography is that cryptography scrambles the message so as to become difficult to understand, whereas steganography hides the very existence of a message. Steganography plays the central role in secret message communication [1][2]. Steganography is not intended to replace cryptography but to supplement it. Hiding a message reduces the chance of detecting a message. However, if that message is encrypted (before hiding it), in this case even if it discovered then it must be cracked (i.e. providing another layer of protection) [3].

Transform domain embedding techniques offer a higher degree of robustness to common image processing operations, compared to spatial domain ones. In most cases, the wavelet transform produces floating point coefficients, although this allows perfect reconstruction of the original image in theory.

Integer wavelet transform allows constructing lossless wavelet transform which is important for reversible data hiding [4]. Each data hiding technique must have certain properties that are dictated by the intended application. The most important properties of data hiding schemes are robustness, invisibility, security, and capacity [5].

Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system which are confidentiality, data integrity, authentication and non-repudiation [6][7].

Generally, information hiding can be divided into four phases: pretreatment phase, embedded phase, the transmission phase and the extraction phase. To achieve security for each stage, it must apply encryption techniques at the pretreatment stage. In embedded stage, it can use the algorithms based on wavelet hidden information. In the transmission stage, it can use covert channel to communication. Therefore, the processing program of information hidden will form a security system, and not only the content of information can be hidden, but also the sender and the receiver of the information can be hidden, this will lead to the establishment of hidden communications channels. Because of the advantages of information hiding technology, it has been applied in many prospects, which include e-commerce, electronic transaction protection, confidential communications, copy control, operation tracking, authentication, and signature fields [8].

This study tries to improve the security of the system by using asymmetric cryptographic algorithm (RSA) for encryption in order to achieve most goals of security system, and used transform domain for embedding the encrypted data with keeping the capacity and security of system as high as possible.

RSA algorithm gets its security from the difficulty of factoring very large integer numbers however keys have to be at least (700) bit long in order not to be broken [9]. RSA algorithm is arguably the most widely used public-key algorithm. Areas of application include browser security, the secure exchange of session keys, internet banking, and credit and debit card payments. Many applications involve the use of smart cards, for example, for the secure storage of secret keys. RSA is also used by certificate authorities [10].

## II. Related Works

In 2001, G. Xuan and et. al. [11] proposed a novel distortionless image data hiding algorithm based on integer wavelet transform that can invert the stego-image into the original image without any distortion after the hidden data are extracted. This algorithm hide data into one (or more) middle bit-plane(s) of the integer wavelet transform

Manuscript submitted in March 3, 2010. Stego-Based-Crypto Technique for High Security Applications.

Adnan Mohsin Abdulazeez Brifcani is with the University of Duhok, and Head of Computer Science Department, Duhok City, Kurdistan Region of Iraq, Iraq (phone: 009647504611970; e-mail: adnan_brifcani@yahoo.com). Wafa Mustafa Abdallah is with University of Nawroz, Computer Science Department, Duhok City, Kurdistan Region of Iraq, Iraq (phone: 009647504428943; e-mail: heevy9@yahoo).

coefficients in the middle and high frequency sub-bands (LH, HL, HH). The proposed invertible data embedding technique is able to embed about 15k-94k bits into a grayscale image of 512 × 512 × 8 imperceptibly.

In 2006, A. S. Imran and et. al. [12] presented a novel method for data hiding based on neighborhood pixels information to calculate the number of bits that can be used for substitution and modified Least Significant Bits (LSB) technique for data embedding. The modified solution is independent of the nature of the data to be hidden and gives correct results along with un-noticeable image degradation. The technique find the number of bits that can be used for data hiding, using the green component of the image as it is less sensitive to human eye and thus it is totally impossible for human eye to predict whether the image is encrypted or not. The application further encrypts the data using a custom designed algorithm before embedding bits into image for further security.

In 2007, Kh. M. Singh and et. al. [13] presented a novel least significant bit embedding algorithm for hiding encrypted messages in nonadjacent and random pixel locations in edges of images. It first encrypts the secret message using the simplified data encryption standard (S-DES), and then detects edges in the cover image. Message bits are then, embedded in the least significant bits and random locations of the edge pixels. It ensured that the eavesdroppers will not have any suspicion that the message bits are hidden in the image and the standard steganography detection methods can not estimate the length of the secret message correctly.

In 2007, K. A. Navas and et. al. [14] proposed a novel approach to blind reversible data hiding based on integer wavelet transform. The algorithm organizes wavelet coefficients to generate wavelet blocks, and applies a novel method to classify these wavelet blocks based on Human Visual System (HVS). The Electronic Patient Report (EPR) data are inserted based on the result of classification. The portions of an image which contains the significant information for diagnosis are called Region of Interest (ROI) and must be stored without distortion. This concept is implemented in the newly proposed method. It is desirable to embed data outside ROI to give better protection. Encryption of EPR is done to provide additional security. The proposed scheme also has large capacity, which is important for EPR data hiding and has higher value of PSNR.

In 2008, X. C. Guo [15] presented a reversible watermarking technique that aims at medical record protection and biometric recognition systems. The goal was to design a system that can better store sensitive information and to protect privacy. The proposed technique used the integer wavelet transform to successfully create embedding space in the high pass frequency sub-bands. The advantages of the proposed algorithm are the simplicity and robustness against common image processing operations such as compression, filtering, and additive noise.

The previous methods were depended on encrypting data with stream cipher or any other symmetric cryptographic algorithm like (S-DES) then embedding the encrypted data directly in spatial domain or embedding the encrypted data in (LL) or (LH, HL) or (LL, LH, HL) sub-bands of wavelet transform domain, or encrypting data with asymmetric cryptographic algorithm but embedding the encrypted data in spatial domain directly or embedding data in wavelet transform domain directly without encrypting data before embedding so the previous methods did not combine many cases to form integrated algorithm while the proposed algorithm in this paper comprise many cases with coordinated way to get desired results of improving the capacity with keeping the security degree as high as possible.

## III. The Wavelet Transform

The wavelet domain is growing up very quickly. A lot of mathematical papers and practical trials are published every month. Wavelets have been effectively utilized as a powerful tool in many diverse fields, including approximation theory; signal processing, physics, astronomy, and image processing.

A one dimensional discrete wavelet transform is a repeated filter bank algorithm. The input is convolved with a high pass filter and a low pass filter. The result of the latter convolution is a smoothed version of the input, while the high frequency part is captured by the first convolution. The reconstruction involves a convolution with the syntheses filters and the results of these convolutions are added [16].

The forward 2-D discrete wavelet transform can be implemented using a set of up-samplers, down-samplers, and recursive two-channel digital filter banks as shown in Fig. 1.

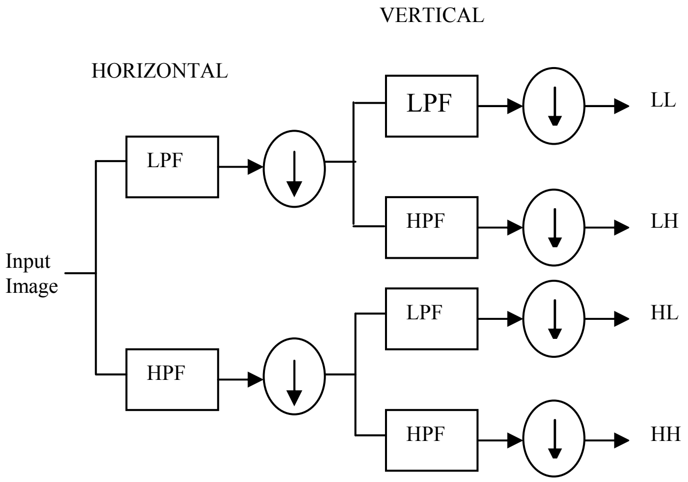


Fig. 1 The forward 2D-discrete wavelet transforms.

There are many available filters, although the most commonly used filters are Haar Wavelet Filters and Daubechies Filters. Each of these filters decomposes the image into several frequencies. When applying discrete wavelet transform on an image, four different sub-images are obtained as follows [17]:

- LL: A coarser approximation to the original image containing the overall information about the whole image. It is obtained by applying the low-pass filter on both x and y coordinates.
- HL and LH: They are obtained by applying the high-pass filter on one coordinate and the low-pass filter on the other coordinate.
- HH: Shows the high frequency component of the image in the diagonal direction. It is obtained by applying the high-pass filter on both x and y coordinates.

## IV. Integer-To-Integer Wavelet Transforms

In conventional wavelet transform reversibility is not achieved due to the floating point wavelet coefficients we get after transformation. When we take the inverse transform the original pixel values will get altered. When we transform an image block consisting of integer-valued pixels into wavelet domain using a floating point wavelet transform and the values of the wavelet coefficients are changed during watermark embedding, the corresponding watermarked image block will not have integer values. When we truncate the floating point values of the pixels, it may result in loss of information and reversibility is lost. The original image cannot be reconstructed from the watermarked image. In conventional wavelet transform done as a floating-point transform followed by a truncation or rounding, it is impossible to represent transform coefficients accurately. Information will be potentially lost through forward and inverse transforms [18]. In view of the above problems, an invertible integer-to- integer wavelet transform based on lifting is used in our proposed technique. It maps integers to integers which are preserved in both forward and reverse transforms. There is no loss of information.

## V. The Proposed Technique

Previous techniques depended on encrypting data with stream cipher or any other symmetric cryptographic algorithm, then embedding the encrypted data in (LL) or (LH, HL) or (LL, LH, HL) sub-bands of wavelet transform sub-bands, or encrypting data with asymmetric cryptographic algorithm but embedding the encrypted data into spatial domain directly, or embedding data in wavelet transform domain directly without encrypting data before embedding. In this work an integrated techniques is proposed with improving capacity and keeping the security degree as high as possible.

The proposed technique consists of four parts; the first part deals with encrypting the secret message using RSA algorithm, the second part hides the encrypted data into cover-image to get the stego-image, while the third part deals with extracting the encrypted data (cipher text) from the stego-image, and the fourth part decrypts the extracted cipher text to get the secret message, the block-diagram of the proposed technique is shown in Fig 2.

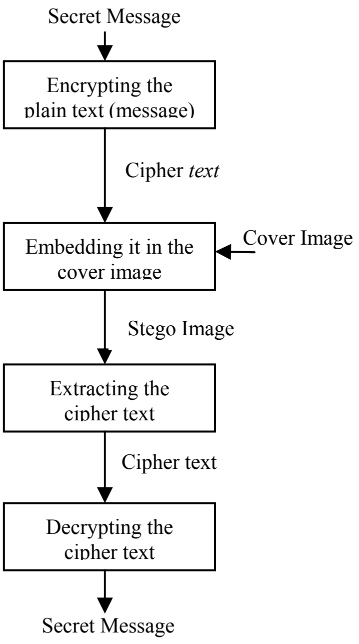

Secret Message
Encrypting the plain text (message)
Cipher text
Embedding it in the cover image
Cover Image
Stego Image
Extracting the cipher text
Cipher text
Decrypting the cipher text
Secret Message

Fig. 2 Block-diagram of the proposed technique.

### A. Encryption Stage

First of all keys are generated, this can be done by selecting two large prime numbers (p and q) randomly and independently (using Miller and Rabin Algorithm for primarily testing) such that (p ≠ q). The maximum value of both (p) and (q) is (999999) so their product determines the value of (n) that has a maximum value of (99999999999999). After selecting two random values, they are used to generate two keys (public key for encryption and private key for decryption) by computing the value of (n = p*q) and φ (n) = (p − 1)*(q − 1), then selecting an integer (e) such that 1 < e < φ (n) which is the co prime to φ (n) (i.e. the Greatest Common Divisor (GCD) between e and φ (n) is equal to 1). The Euclidean algorithm is an efficient algorithm for computing the GCD of the two integers that does not require the factorization of the integers, then the value of the private key (d) should be computed such that d*e ≡ 1 (mod φ (n)), the private key is the modular inverse of the public key. A very common method for finding modular inverses is the extended Euclidean algorithm. Hence the public key consists of (n) the modulus, and (e) the public exponent while the private key represents the value of (d) which must be kept secret.

In the proposed algorithm, the two prime numbers (p) and (q) are selected where the value of (n) is made of (14) digits in order to get a reasonable level of security and to make it hard to be attacked by adversary because the security of this algorithm (RSA) is based on the factorization problem of long integers while previous works did not use more than (12) digits. The proposed algorithm is reached up to (14-digits) and not exceeds it because of the limitations of the used language (Visual C#); otherwise the algorithm can take more than (14-digits) if it is allowable by this language.

The secret message is entered by the user and replaced with random integer values, these values are taken according to (Table 1) that adds another layer of protection to the algorithm. But the value of (n) which represents (the modulus) should not be less than the maximum ASCII code value (127) because the ASCII codes (0 – 127) are used in the proposed technique. Hence if this condition was not satisfied then an error may occur when decrypting the message. The encryption process can be performed by computing ($c = m^e$ mod n), where (m) represents the (message). Both encryption and decryption in RSA involve rising an integer to an integer power, mod n, which can be done by using fast exponential algorithm. Then the encrypted text (cipher text) is saved to a text file.

TABLE 1 LOOK UP TABLE FOR ENCODING THE SECRET MESSAGE

| ASCII Codes | Random Values | ASCII Codes | Random Values | ASCII Codes | Random Values |
|---|---|---|---|---|---|
| 0 | 82 | 4 | 123 | 8 | 96 |
| 1 | 32 | 5 | 115 | ⋮ | ⋮ |
| 2 | 12 | 6 | 28 | ⋮ | ⋮ |
| 3 | 68 | 7 | 126 | 127 | 116 |

## B. Embedding Stage

The second part of the proposed technique is the embedding stage; starting with loading the text file that contains the encrypted data (cipher text). Then it converted to binary form (stream of bits). The resultant streams of bits are all combined together to form a sequence of binary bits as shown in Fig. 3.

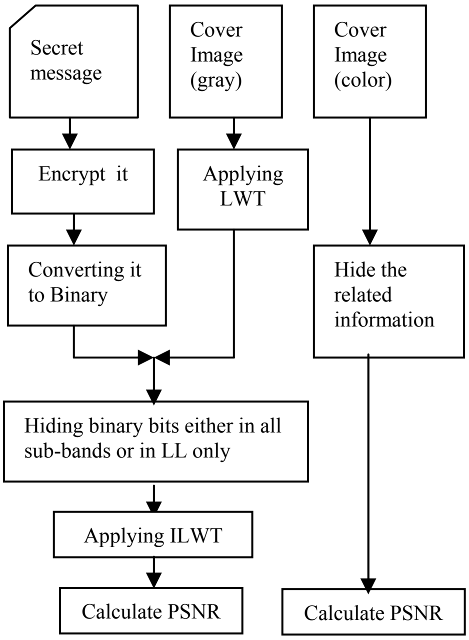


Fig. 3. Block diagram of the embedding process

Each encrypted character (cipher text) has a different length. So, when retrieving the binary bits at extraction side, it will be difficult to restore each cipher text according to its length without knowing these lengths, therefore the proposed technique uses two images for hiding: one is used for hiding the encrypted data which is grayscale image and the other one is used for hiding the related information like lengths of each encrypted character which is the color image.

The proposed technique uses two embedding methods that are based on Integer Wavelet Transform (IWT) which is used to ensure lossless transform. To achieve that, wavelet transform based on lifting scheme is used with filter type (cdf 2.2) to guarantee the perfect reconstruction, and the image is decomposed into four sub-bands (approximation coefficients matrix CA and detail coefficients matrices CH, CV, and CD), then performing the embedding process.

There were two ways or methods for embedding; the first one is based on inserting the stream of bits (data to be hidden) into Least Significant Bits (LSB) of approximation coefficients (CA) that are larger or equal to zero. While the second one is based on inserting the data into the four sub-bands (CA, CH, CV and CD) respectively by inserting the first bit in CA's coefficients then inserting the second bit in CH's coefficients then the third bit in CV's coefficients then the fourth bit in CD's coefficients and so on until all bits of sequence are embedded, therefore data are distributed into all sub-bands, as a result the overall capacity will be increased.

It should be noted that the proposed technique also hides the data into the colored image which contains the related information to add another level of security.

The lengths of encrypted characters (cipher text) should be hidden in the colored image, the embedding process is done in spatial domain directly by replacing pixel values which are smaller than (60) with these lengths, because the values of these lengths are ranging between the range (40 to 50). So replacing these pixels will not affect quality of the cover image and the distortion will be eliminated. After embedding process is completed, the PSNR of the stego image is computed in order to measure the distortion of the stego image comparing with the cover-image, higher PSNR means less distortion between the two images.

## C. Extraction Stage

The third part of the proposed technique deals with extraction of the encrypted message. Second image which contains the related information (lengths of encrypted characters) should be recovered first to extract the information and used it when retrieving the encrypted message. Information about the type of embedding method is extracted from the colored image, so according to this number if it's equal to 1 then the data should be extracted from the CA coefficients, but if the extracted number is equal to 2 then the data should be extracted from (CA, CH, CV and CD) coefficients respectively. Then the extracted data (stream of bits) should be converted from binary form to integer form again, and the cipher text is saved to a text file.

## D. Decryption Stage

The last stage of the proposed technique deals with decryption, which starts by reading the cipher text from the text file. Then the decryption process is performed by applying (M = $C^d$ mod n) using fast exponential algorithm. Resultant data (random integer values) are replaced with their corresponding ASCII codes, and then converted back to characters to restore the original message.

## VI. Performance Measure

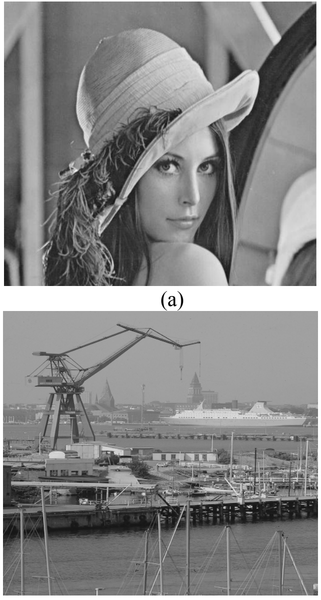
Peak-Signal-to-Noise Ratio (PSNR) which is used as performance measure for image distortion is applied on both stego and original images. It is defined below as in [19]:

$$\left[\begin{array}{l} PSNR = 10\log_{10}\dfrac{255^2}{MSE} \\ MSE = \dfrac{1}{n}\sum_{x=1}^{N}\sum_{y=1}^{M}\left[Steg_{x,y} - Cov_{x,y}\right]^2 \end{array}\right]$$

Where MSE denotes to the Mean Square Error, Cov denotes to the original image, Steg denotes to the Stego image, N and M denotes to the image dimensions, while x and y denotes to the image coordinates. The number 255 in the above equation refers to the highest possible image level in an 8-bit image. In general, the higher the PSNR, the better the signal quality becomes [15]. The PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality (i.e., distortion caused by embedding can be obvious). A high quality stego should strive for 40 dB and above [19].

## VII. Results

The proposed technique is tested by using 20 gray-scale standard images of size 512*512 with three formats (BMP, GIf and JPEG) like Lena, Barbara, Boat and a variety of sceneries as shown in Fig. 4 (a,b,c,d). In addition, a number of colored images are used with different sizes; two of them are shown below in Fig. 4 (a,b).


(a)

(b)

(c)

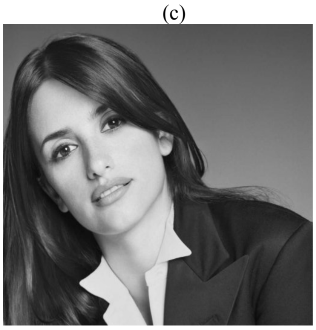

(d)

Fig. 4 Test images for the proposed technique.

(a) (b)

Fig. 5 Cover image for the proposed technique.

Table 2, Table 3, Table 4, and Table 5 show the results of the proposed technique using the mentioned test images.

TABLE 2 RESULTS WHEN EMBEDDING IN ( LL) SUB-BAND

| Images of 512*512*8 bit | Message Size Characters | Pay-Load (bits) | PSNR of Stego-Image (dB) | Embedding Duration Time (msec) |
|---|---|---|---|---|
| 1. lena.jpg | 1250 | 53540 | 53.1164 | 2.9375 |
| 2.harbour.gif | 1250 | 53540 | 53.2174 | 3.35938 |
| 3. boat.bmp | 1250 | 53540 | 53.1136 | 2.45313 |
| 4. girl.bmp | 1250 | 53540 | 53.1309 | 2.5625 |

TABLE 3 RESULTS WHEN EMBEDDINH IN THE FOUR SUB-BANDS

| Images of 512*512*8 bit | Message Size Characters | Pay-Load (bits) | PSNR of Stego-Image (dB) | Embedding Duration Time (msec) |
|---|---|---|---|---|
| 1. lena.jpg | 1250 | 53540 | 55.4131 | 2.875 |
| 2.harbour.gif | 1250 | 53540 | 55.2605 | 3.23438 |
| 3. boat.bmp | 1250 | 53540 | 54.8810 | 3.21875 |
| 4. girl.bmp | 1250 | 53540 | 55.6164 | 3.10938 |

TABLE 4 RESULTS WHEN EMBEDDINH IN THE FOUR SUB-BANDS FOR MESSAGE OF 4000 CHARACTERS

| Images of 512*512*8 bit | Message Size Characters | Pay-Load (bits) | PSNR of Stego-Image (dB) | Embedding Duration Time (msec) |
|---|---|---|---|---|
| 1. lena.jpg | 4000 | 176561 | 50.0098 | 9.48438 |
| 2.harbour.gif | 4000 | 176561 | 49.6327 | 8.10938 |
| 3. boat.bmp | 4000 | 176561 | 49.5518 | 9.14063 |
| 4. girl.bmp | 4000 | 176561 | 50.1157 | 8.45313 |

TABLE 5 RESULTS OF SAMPLE TEST ON THREE SUB-BANDS DONE BY THIS ALGORITHM.

| Images of 512*512*8 bit | Message size characters | Pay-load (bits) | PSNR of stego-image (dB) | Embedding duration time (msec) |
|---|---|---|---|---|
| 1. lena.jpg | 1250 | 53540 | 56.0988 | 3.34375 |
| 2.harbour.gif | 1250 | 53540 | 55.9209 | 2.93750 |
| 3. boat.bmp | 1250 | 53540 | 55.5539 | 3.21875 |
| 4. girl.bmp | 1250 | 53540 | 56.2174 | 2.32813 |

It's obvious from the tables that the maximum capacity when embedding in (LL sub-band) is 1250 characters while the maximum capacity is 4000 when embedding in the four sub-bands, comparing this with [14] which had a maximum capacity of 3400 by embedding in three sub-bands (LH,HL,HH). Maximum embedding reached in this work is (176000 bit) comparing with [11] which had (94000 bit) and embedded in the middle bit or bits of high frequencies coefficients (LH,HL,HH). In addition the imperceptibility of the proposed technique in this work is improved.

The value of (n) which determines the length of public key in this work is selected to be consist of (17) digit so the maximum value of (n) is (99999999999999), comparing this with reference [20] which had a value of (n) between values of range between (256) and (512).

The PSNR is adversely proportional with the capacity; the higher capacity of the cover image has lower PSNR. Also, the embedding duration time is directly proportional with the capacity; the higher capacity of the cover image has the higher embedding time.

It can be seen from the tables there is a small difference in the value of PSNR, this is due to the difference in high and low frequency contents of the images.

By comparing results of (Table 3) with (Table 5), it is clear that when embedding (1250) character in three sub-bands of any test image, will produce a PSNR value ranging between (55 to 56)dB which is not much different from embedding the same data into four sub-bands of the same test images which will produce a PSNR values ranging between (54 to 55) dB. So, from imperceptibility point there is no variance between both methods, but from capacity point there is, because the maximum capacity (data that can be embedded) when using three sub-bands is (3000) character, while the maximum capacity when using four sub-bands is (4000) characters. So the proposed technique could increase the capacity and at the same time keeps the imperceptibility as high as possible.

## VIII. CONCLUSIONS

In this paper a stego-based-crypto technique is proposed, which is a hybrid of RSA algorithm and lifting wavelet transform. RSA algorithm has been used to increase the security of the system were a key of 14 digits has been used. Two methods of embedding have been used for the embedding; embedding either in the low frequency sub-band of the lifting wavelet transform or embedding in all sub-bands of the lifting wavelet transform. Both methods of embedding obtained high imperceptibility improvement were PSNR values ranged between 49-55 db. In addition to that the capacity of embedding is increased when it done in all sub-bands of the lifting wavelet transform were a message of 4000 characters has been embedded.

## REFERENCES

[1] N.F. Johnson, "Exploring Steganography, Seeing the Unseen", IEEE Computer, George Mason University, (February 1998), (pp. 26-34), available: http://www.jjtc.com/pub/r2026.pdf.

[2] K. Curran, K. Bailey, "An Evaluation of Image Based Steganography Methods," International Journal of Digital Evidence, Volume 2, Issue 2, (2003), (pp. 1-40).

[3] O. Khalind, "A Coding Approach for Image Steganography Using Frequency Domain", M.Sc. Thesis, University of Salahadin, (2008).

[4] K. A. Navas, S. A. Thampy, and M. Sasikumar," EPR Hiding in Medical Images for Telemedicine", international Journal of Biomedical Sciences, Volume 3, Number 1, (2008).

[5] S. Cacciaguerra , S. Ferretti," Data hiding: Steganography and copyright marking ", Department of Computer Science, University of Bologna, Italy, 2000.

[6] A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, Inc., (1996).

[7] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms", (2005). Available: http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.html

[8] J. Wang, R. Jiao, et.al. "Research on Information Hiding", ISSN1548-6613, USA, volume 5, Number 3, (May 2006), PP.(77-81).

[9] B. Agarwal, A. B. Amara, et.al. ,"Cryptography",(November 2004). Available:-http://www.cc.gatech.edu/classes/AY2005/cs4235_fall/papers/Crypto2.pdf.

[10] T. L. Grobler, W. T. Penzhorn "Fast Decryption Methods for the RSA Cryptosystem". Available: http://www.satnac.org.za/proceedings/2006/papers/No%20208%20-%20Grobler.pdf

[11] G. Xuan, J. Zhu, et.al. " Distortionless Data Hiding Based on Integer Wavelet Transform ", New Jersey Institute of Technology, (2001). URL:-http://202.120.189.34/files/InforWeb/news2003-10-30_zig6F3nuek/IEE-6-14-02-submit.pdf.

[12] A. S. Imran, M. Y. Javed, and N. S. Khattak "A Robust Method for Encrypted Data Hiding Technique Based on Neighborhood Pixels Information", International Journal of Computer Science and Engineering, Volume 1, Number 3, (2006), pp. (159-164).

[13] Kh. M. Singh, S. B. Singh and L. Sh. S. Singh," Hiding Encrypted Message in the Features of Images", IJCSNS International Journal of Computer Science and Network Security, Volume 7, Number 4, (April 2007).

[14] K. A. Navas, S. A. Thampy, and M. Sasikumar," EPR Hiding in Medical Images for Telemedicine", international Journal of Biomedical Sciences, Volume 3, Number 1, (2008).

[15] X. C. Guo, " Methodologies in Digital Watermarking: Robust and Reversible Watermarking Techniques for Authentication, Security and Privacy Protection ", M.Sc. Thesis, University of Toronto, (2008).

[16] M. Fahmy Tolba, M. AI-Said Ghonemy, Ismail Abdoul-Hameed Taha, Amal Said Khalifa, " High Capacity Image Steganography using Wavelet-Based Fusion",IEEE, (2004), pp.(430-435).

[17] Ahmed A. Abdelwahab and Lobna A. Hassaan, "A DISCRETE WAVELET TRANSFORM BASED TECHNIQUE FOR IMAGE DATA HIDING",25th NATIONAL RADIO SCIENCE CONFERENCE, (2008).

[18] S. Kurshid Jinna1, Dr. L. Ganesan," Lossless Image Watermarking using Lifting Wavelet Transform", International Journal of Recent Trends in Engineering, Volume 2, Number 1, November (2009), pp. (191-195).

[19] A. Cheddad, J. Condell, et.al., " Enhancing Steganography In Digital Images", IEEE, (2008), pp. (326-332).

[20] Z. K. Ibrahim, "Image Based Steganography System", M.Sc. Thesis, Nahrin University, Iraq, (2002).

BIOGRAPHY

**Adnan Mohsin Abdulazeez** (M.Sc.'98–Ph.D.'07) became a Member (M) of IEEE in 2009 and Member in IACSIT in 2010. Born in Aqra District, Duhok City, Iraq, 1970. Got his B.Sc. in Electrical and Electronic Engineering from Baghdad, University of Technology, College of Al-Rasheed for Engineering and Science 1993, his M.Sc. in Control Engineering from the same college, 1998, and Ph.D. from Mosul University, Department of Computer Engineering. Currently working as Assistant Professor and Chairman of the Computer Science Department in Duhok University, Duhok City, Kurdistan Region of Iraq. Major Fields of studies are soft computing, security.

He worked as Assistant Lecturer in the Al-Rasheed College of Engineering and Science in University of Technology, Baghdad, and Lecturer in several colleges in University of Duhok. Published many papers in the Scientific Journal of Duhok University and a paper in the University of Philadelphia, Jordan. Author of the booklet "The Road to Wavelet Theory, Duhok, Iraq, Assyrian Center in Duhok City".

**Assist. Prof. Dr. Eng. Brifcani** is a member in Engineering Syndicate of Kurdistan Region of Iraq, and a member in the Iraqi Engineering Syndicate.