Robust Steganography Based on QIM Algorithm to Hide Secret Images

Oswaldo Juarez-Sandoval, Angelina Espejel-Trujillo, Mariko Nakano-Miyatake, Hector Perez-Meana

***Abstract*—** The steganography research has grown rapidly since last decade. This technique has been used to hide different types of information, such as medical, personal and business information and also in some cases it was used in criminal act. This paper presents a robust steganographic scheme focused on the embedding of a secret image into a cover image in the DCT domain using QIM embedding algorithm. The experimental results show the robustness of the proposed scheme against the JPEG compression and noise contamination, while keeping an imperceptibility of hidden data. The proposed scheme also is robust to commercial stego-analyzers, which cannot detect the presence of the hidden data in the stegoimage generated by the proposed scheme. The better performance of the proposed scheme is shown comparing with a previously reported steganography algorithm with the same objective of the proposed one.

Keywords— Steganography, DCT, JPEG compression, QIM, payload, robustness, secret image

I. Introduction

THE growth sharing of digital files, such as images, audio and video, on social networks or Internet, animates the study of steganography as an important technique to transport and share hidden information among several world sectors. Recently this technique has been used to hide different types of information, such as medical, personal and business information and also in some cases it was used in criminal acts.

The steganography is the technique or science of hiding confidential information in a carrier file this word is derived from the Greek "Stego", meaning cover, and "Graphs" meaning writing [1]. The digital steganography must satisfy three important requirements which are: the imperceptibility of the hidden information, the capacity of large amount of hidden data and the robustness against some common signal processing procedures, such as lossy compression [2-4].

Until now several digital steganographic schemes to hide secret information into digital files have been developed such as those proposed by Stool [5], JSteg [6], F5 [7], Bit-Plane Complexity Steganography (BPCS) [8], JpHide [9], Outguess [10] and so on. Among them, Least Significant Bit (LSB) steganographic algorithms, such as Stool [5] and BPCS [8], are able to hide great amount of information, however generally they are vulnerable to statistical analysis and the hidden information is easily destroyed after lossy compression, such as JPEG compression.

The frequency domain steganographic algorithms, such as J-Steg [6], F5 [7] and Outguess [10], embed the secret data in frequency domain, which is relatively robust to lossy compression; however in general the amount of the hidden data is limited. The authors of [11] proposed a robust steganography method called RIASIWT, in which data hiding is carried out in Integer Wavelet Transform (IWT) domain. The approximation sub-band of the IWT of the cover image is divided into non-overlapping blocks of 4x4 coefficients and then the secret information bits are hidden adaptively depending on the condition number of each block. In this algorithm, a gray-scale image is considered as a secret data.

The proposed steganography scheme provides robustness to common non-intentional image processing, such as JPEG compression and noise contamination, and also it provides the high data hiding capacity, while keeping sufficient imperceptibility. In the proposed scheme, an image data is considered as secret data, because in many applications an image provides a lot of visual information. The proposed scheme is also robust to commercial analyser for steganography [12], which cannot detect the presence of hidden data in the stego-image generated by the proposed algorithm. The rest of this paper is organized as follows. Section II provides a detail description of the proposed scheme, and experimental results and performance comparison with a previous work are shown in Section III. Finally, Section IV provides the conclusions of this work.

II. Proposed Algorithm

The proposed algorithm is composed by a secret image embedding process and extraction process.

A. Embedding Stage

The block-diagram of the embedding process of the proposed steganography algorithm is shown in Fig. 1. This process is given by following steps.

1. Adjustment: Firstly the pixel values of the cover image are adjusted to avoid overflow or underflow of the range of pixel values [0,255].

O. Juarez-Sandoval is with the Instituto Politecnico Nacional, Av. Santa Ana 1000, Coyoacan, Mexico, D.F., 04430, Email joreandbins@hotmail.com
A. Espejel-Trujillo is with the Instituto Politecnico Nacional, Av. Santa Ana 1000, Coyoacan, Mexico, D.F., 04430. Angelina.et@gmail,com.
M. Nakano-Miyatake is with the Instituto Politecnico Nacional, Av. Santa Ana 1000, Coyoacan, Mexico, D.F., 04430. Email mnakano@ipn.mx.
H Perez-Meana (Corresponding author) is with the Instituto Politecnico Nacional, Av. Santa Ana 1000, Coyoacan, Mexico, D.F., 04430, Email hmperezm@ipn.mx. Phone +52-55-5656-2058,

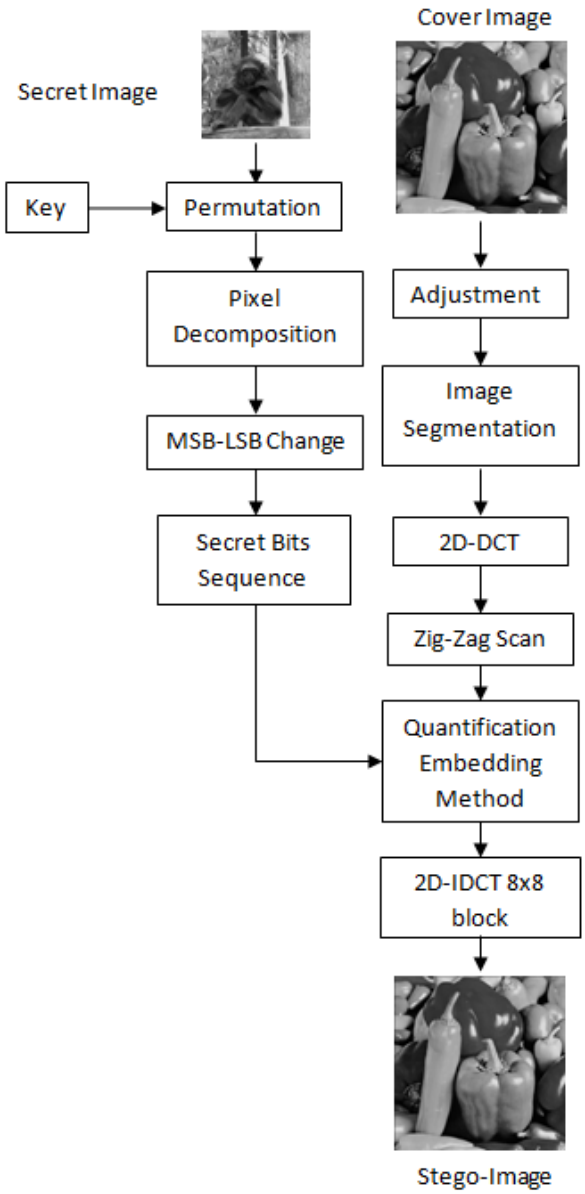

Fig.1. Block diagram of the proposed steganography scheme.

2. Image Segmentation: The adjusted cover image is divided into non-overlapped blocks with 8x8 pixels.

3. 2D-DCT: The bi-dimensional Discrete Cosine Transform (2D-DCT) is applied to each block with 8×8 pixels to obtain DCT coefficients from the DCT block.

4. Zig-Zag Scan: The DCT block of the cover image is ordered in zig-zag manner as shown by Fig. 2 to obtain a vector with 16 coefficients: $C_k = [B(1,3), B(2,2), \cdots, B(4,3), B(3,4)], k = 1..K$, where K is the total number of blocks. Here only lower 16 coefficients, except DC and two lowest ACs, are used for data hiding to reduce the visual distortion caused by data hiding.

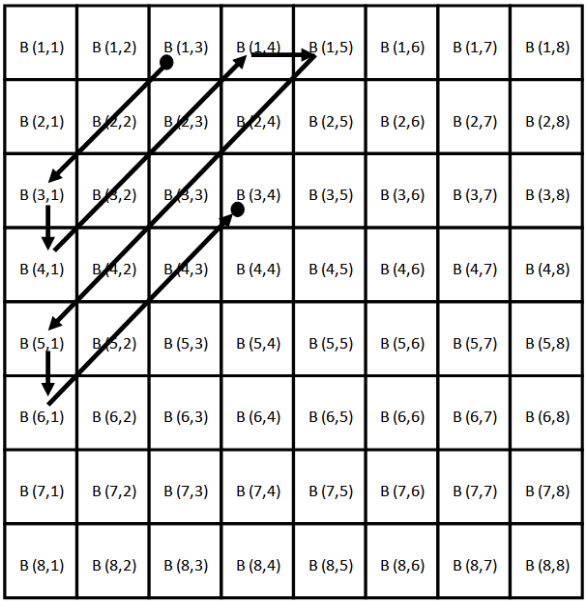

Fig. 2 Zig-Zag scan to obtain 16 DCT coefficients.

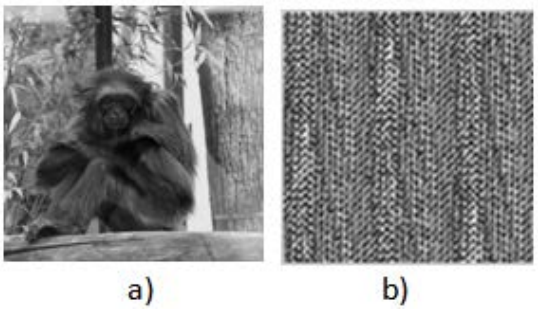

Fig 3. An example of permutation. (a) original image, (b) permuted image after applying chaotic mixing algorithm.

5. Permutation: The secret gray-scale image is permuted using chaotic mixing algorithm using two secret keys [13], whose objective is aggregate a security issue in the proposed scheme. The chaotic mixing algorithm is given by

$$U^{(i)} = A_N^i(k)U^{(0)},\ i = 1,2,...P-1 \qquad (1)$$

where $U^{(i)}$ is state of the input image $U^{(0)}$ after applying i times a transform matrix $A_N(k)$ to $U^{(0)}$. The transform matrix $A_N(k)$ is given by

$$A_N(k): L_N \to L_N, \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N \qquad (2)$$

where (x_n, y_n) is coordinate of each pixel at time n, k is an integer secret key which forms a transform matrix and $N \times N$ is the size of the secret image. Here k and i are two user's

keys. Figure 3 b) shows a result of this process applied to a result of this process applied to an image of Fig. 3a).

6. Pixel Decomposition: The permuted secret image is divided into pixel pairs $P_{(n,m)}$ and $P_{(n+1,m+1)}$, where (n,m) is the coordinate of each pixel . In the proposed scheme, these two pixels (P_1 and P_2) will be embedded into each DCT block of the cover image.

7. MSB-LSB swapping: Considering that a secret image is 8-bits grey-scale image, then each pixel is segmented into four MSB-bits and four LSB-bits, i.e. $P_1=MSB_1 \cup LSB_1$, $P_2=MSB_2 \cup LSB_2$. Taking in account that the four MSB-bits of each pixel have more important visual information than their four LSB-bits, therefore we arrange the bits in a sequence of 16 bits as shown by Figure 4.

8. Secret Bit Sequence Generation: In the Figure 4, P_1 and P_2 are two pixels with 8 bits data. Four MSB bits (MSB_1 and MSB_2) of both pixels are collocated in the first 8 bits of the 16 bits-sequence *S*, and four LSB bits (LSB1 and LSB2) of both pixels are collocated in the least 8 bits of the sequence, so we get $S = MSB_1 \oplus MSB_2 \oplus LSB_1 \oplus LSB_2$, where $\oplus$ indicates concatenation operation.

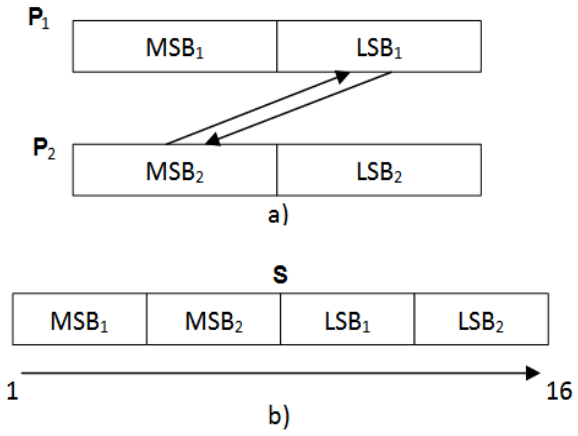

Fig. 4 Bits arrangement used in the proposed scheme. (a) two pixel P_1 and P_2 with 8 bits and (b) arranged 16 bits-sequence *S*.

This form to order the bits of two pixels ensures the embedding of the 8 MSB bits into lower AC coefficients of the DCT block, where the hidden information is more robust than the AC coefficient with higher frequency, which is shown by the Figure 5, this embedding location ensures the extraction of the most important bits of each pixel of the secret image, providing a better quality of the secret image.

9. Embedding: The arranged 16 bits-sequence S_k is embedded into *k-th* DCT block using QIM embedding algorithm [14], which is given by (3).

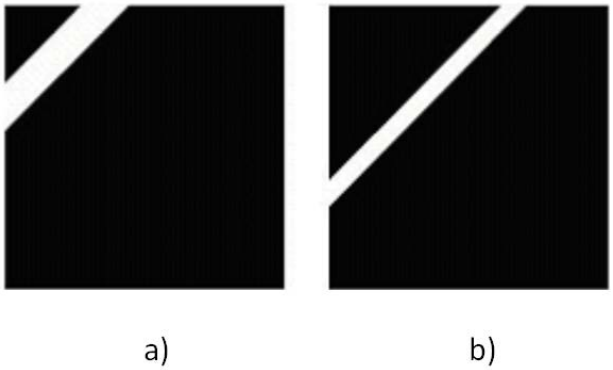

Fig. 5 Frequency representatio, (a) AC coefficients with lower frequencies where MSBs of two pixels are embedded (b) AC coefficients with higher frequency where LSBs of two pixels are embedded.

$$\begin{aligned} &\text{if} \quad S_k(b)=0 \\ &\tilde{C}_k(b)=2q \\ &\text{where} \quad q=\arg\min_j \left\| C_k(b)-2j\Delta \right\| ç \\ &\text{if} \quad S_k(b)=1 \\ &\tilde{C}_k(b)=2q+1 \\ &\text{where} \quad q=\arg\min_j \left\| C_k(b)-(2j+1)\Delta \right\| \end{aligned} \tag{3}$$

where $S_k(b)$ is *b-th* bit of 16 bits sequence of the secret data to embed in the *k-th* DCT block, $C_k(b)$ and $\tilde{C}_k(b)$ are *b-th* DCT coefficients of *k-th* block, respectively, and Δ is step-size.

10. Inverse 2D-DCT: Finally stego-image is obtained applying inverse DCT to each DCT block with hidden 16 bits sequence (S_k).
In the proposed scheme, two pixels of the secret image are embedded into each DCT block of the cover image obtaining the stego-image; therefore there is a relationship between size of the gray-scale cover image and that of the gray-scale secret image, which is given by

$$L \geq \frac{8N}{\sqrt{2}} \tag{4}$$

where $(N \times N)$ is the size of secret image and $(L \times L)$ is the size of the cover image.

B. Hidden Data Extraction Process

The hidden data extraction process is similar to the embedding process. This process is shown in the Fig.6.

1. Image segmentation: The stego-image is divided into non-overlapped blocks with 8x8 pixels.

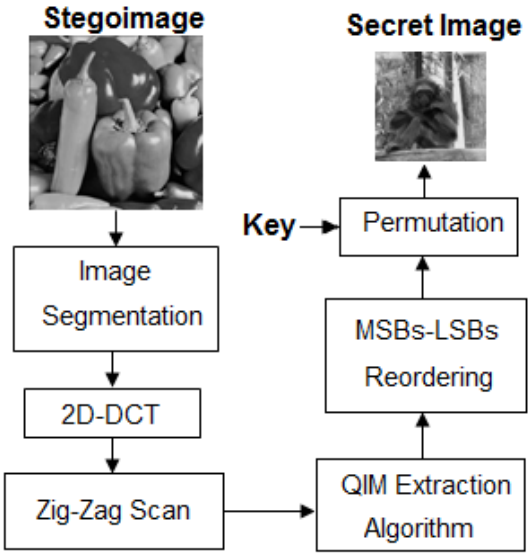

Fig. 6 Block diagram of the extraction of the proposed steganography scheme.

2. 2D-DCT: The 2D-DCT is applied to each block of the stego-image obtained in the previous process.

3. Zig-Zag scan: The Zig-Zag scan is applied to each DCT block to obtain 16-coefficients per block, as shown in Figure 2.

4. QIM Extraction: The 16 bits of the secret sequence from the 16 coefficients obtained in the previous process, are extracted using the QIM extraction algorithm, which is given by

$$\hat{S}_k(b) = \mathrm{mod}\left(\hat{C}_k(b), 2\Delta\right) \tag{5}$$

where $\hat{C}_k(b)$ is the zig-zag ordered *b-th* coefficient of the *k-th* DCT block of the stego-image, which is probably distorted by non-intentional attacks, such as JPEG compression and noise contamination, and $\hat{S}_k(b)$ is the extracted *b-th* hidden bit and Δ is the same step-size used in the embedding process.

5. MSB-LSB Reordering: The extracted 16 bits secret sequence in the previous process is rearranged to generate two pixels values (P_1 and P_2) with 8 bits. All pixel values are obtained at the same way.

6. Inverse permutation: Applying inverse process of the chaotic mixing algorithm [13] to all extracted data to obtain the secret image. The inverse chaotic mixing algorithm is given by

$$\tilde{U}^{(0)} = A_N^{-i}(k)\tilde{U}^{(i)},\ i = 1,2,...P-1 \tag{6}$$

Fig. 7 Cover Images used in the experiments.

where $\tilde{U}^{(i)}$ is the extracted secret data in the step 5, whose pixels are disordered and $\tilde{U}^{(0)}$ is the resultant image after applying inverse permutation process, i.e. the extracted secret image.

III. Evaluation Results

In this section the performance of the proposed scheme is evaluated from the several points of view, such as the hidden data imperceptibility, the payload that indicates the hiding capacity, the quality of the recovered secret images and hidden data robustness. These evaluations are carried out using several cover images and secret images with different characteristics. Some of the cover images used in the evaluation are shown by Figure 7. Firstly the step-size Δ of the QIM algorithm must be determined adequately, because the hidden data imperceptibility, the quality of the extracted secret

image and the robustness of the hidden data are directly related to this value. Figure 8 shows the relationship between the step-size Δ and the quality of stego-images respect to their original one and Figure 9 shows the relationship between the step-size Δ and the quality of the extracted secret images respect to their original one when the stego-image is compressed by JPEG compression with quality factor 80. In both cases, the payload of the secret image is 100%. For example if the dimension of the host image is 512 × 512, the dimension of the secret image is 90 × 90, applying (4) it follows taht

$$N = \frac{512 \times \sqrt{2}}{8} \approx 90$$

Obviously using smaller step-size Δ, we can get higher quality of stego-image, however the quality of the extracted secret image is affected, and using a lager Δ, we can extract a secret image with higher quality, however in this situation the quality of the stego-image is affected.

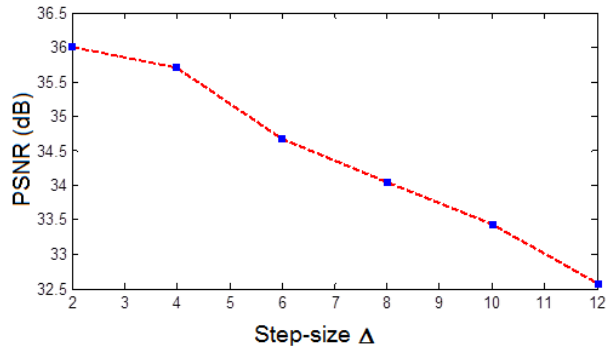

Fig. 8 Relationship between Step-size and quality of stego-images.

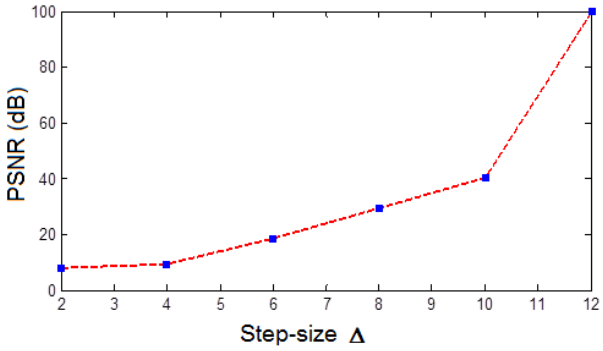

Fig. 9 Relationship between step-size and quality of recovered secret images.

Considering trade-off between the quality of the stego-images and the quality of the extracted secret image, we consider that an adequate step-size Δ is equal to 7.

A. *Imperceptibility of hidden image*

The quality of stego-image is inversely proportional to the quantity of the hidden data. In the Table I, the quality of the color stego-image with different quantities of hidden data, respects to their original one are given. The size of the color images is 512× 512. The image quality is assessed by the Peak Signal to Noise Ratio (PSNR), which is given by (7) and (8).

$$PSNR = 10 \log_{10}\left(\frac{256^2}{MSE}\right) \tag{7}$$

$$MSE = \frac{\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}(Ic - Is)^2}{N_1 N_2} \tag{8}$$

If the host image is color image, the payload defined by (4) increases three times, because three color channels, Red, Green and Blue, are available for the secret image hiding.

Table I. Quality of stego-image with different hidden data quantities.

Hidden data quantities pixels / payload (%)	Quality of steo-image PSNR (dB)
6,075 (25%)	44.40
12,288 (50%)	41.28
18,252 (75%)	39.61
24,300 (100%)	38.44

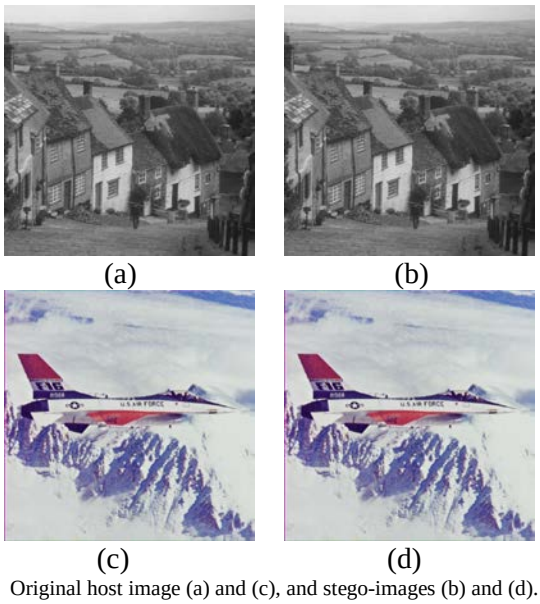

Fig. 10 Original host image (a) and (c), and stego-images (b) and (d).

Figure 10 shows gray-scale and color stego-images with 100% payload, together with their original cover images for visual comparison purpose.

B. *Quality of the extracted secret image and Robustness to JPEG compression*

The qualities of the extracted secret image using the proposed algorithm, when the stego-images are compressed by JPEG compression, are also evaluated. These evaluations reflect the

robustness of the proposed scheme to non-intentional image processing.

Table II shows the quality of the extracted secret image under JPEG compression with different quality factors, in which "Inf" means the lossless extraction of the secret image. Here gray-scale images showed in the Fig. 7 are used as cover images and the values of this table are average using 10 cover images. Figure 11 shows the extracted secret image with 90 ×90 pixels from the stego-images with 512×512 pixels, which is compressed by the JPEG compression with quality factor 80. In this case the payload is 100%.

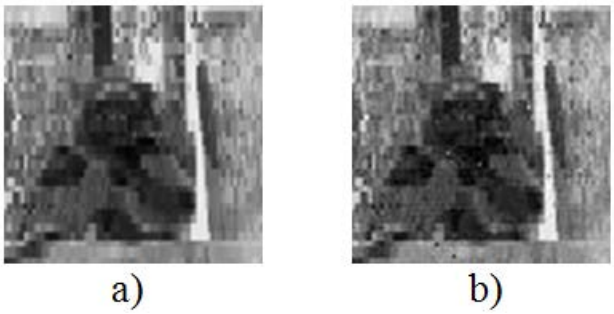

Fig. 11 a) Secret image, b) recover image with 38.45 dB.

From this Table and the Fig. 11, we can conclude that in the proposed scheme, the extracted secret image from the compressed stego-image by JPEG compression with quality factor 70 provides sufficiently good visual information to the receptor.

A. Robustness to noise contamination

The hidden data robustness to the Gaussian noise in the proposed steganography is also evaluated. Table III shows the quality of the extracted secret image respect to its original one, when the stego-image is contaminated by Gaussian noise with different variances σ^2 of noise distribution. The Figure 12 shows an extracted secret image from the stego-image that is compressed by JPEG compression and contaminated by Gaussian noise with a variance $\sigma^2 = 10^{-5}$. The PSNR of this image respect to its original one is approximately 21.5 dB.

Table II. Quality of the extracted secret image when stego-image is compressed by JPEG compression with different quality factors.

	Payload			
σ^2 $\times 10^{-6}$	25%	50%	75%	100%
	Extracted secret image quality in PSNR (dB)			
1.0	29.93	28.23	27.88	27.17
5.0	23.52	23.11	23.51	24.12
10.0	21.34	20.70	21.39	21.52

Fig. 12 Extracted secret image under contamination by Gaussian noise with a variance $\sigma^2 = 10^{-5}$ and JPEG compression with quality factor 90.

Table III. Quality of the extracted secret image when stego-image is contaminated by Gaussian noise with different variances

	Payload			
QF	25%	50%	75%	100%
	Extracted secret image quality in PSNR (dB)			
60	15.90	15.86	16.03	15.34
70	25.57	25.12	25.47	25.25
80	37.43	37.43	36.50	36.21
90	Inf	Inf	Inf	Inf
100	Inf	Inf	Inf	Inf

From Table III and Figure 12, we can conclude that the proposed steganography algorithm provides a sufficiently good quality of the extracted secret image when the stego-image is compressed by JPEG compression and contaminated by Gaussian noise.

C. Performance Comparison with RIASIWT [11]

The performance of the proposed steganography algorithm is compared with that of the RIASIWT [11]; because the purpose of the RIASIWT is hide a secret image into the cover image, which is the same purpose of the proposed algorithm.

Firstly, the imperceptibility of the stego-image is compared under the same payload, i.e. the number of pixels of secret image to be hidden. In the RIASIWT [11], the condition number is calculated to determine if the block of 4×4 IWT coefficients is proper or not for data hiding, then the payload is varied depending on the characteristics of the cover image. Generally the maximum payload of a specific image is much lower than that of our proposed algorithm. So the number of pixels of the secret image is unified among two algorithms. Table IV shows a comparison of the hidden data imperceptibility between the proposed algorithm and the RIASIWT [11].

Table IV. Comparison of stego-image quality

Payload # of pixels (%)	PSNR (dB)	
	Proposed	RIASIWT [11]
6,075 (25%)	42.30	31.64
12,288 (50%)	39.23	31.63

Table V. Comparison of the maximum payload in the proposed algorithm and RIASIWT.

Images 512×512	Maximum payload (pixels number)	
	Proposed	RIASIWT [11]
Lena	8100	3218
Chiles	8100	3093
Baboon	8100	4795
Boat	8100	2844
Gold-Hill	8100	3796
Barbara	8100	3085

Table VI. Quality of the extracted secret image under JPEG compression

JPEG - QF	100		70	
Size of secret image (pels)	6075	12288	6075	12288
Proposed	40.66dB	39.76dB	36.55dB	35.70dB
RIASIWT	14.89dB	14.78dB	14.85dB	14.71dB

As we can observe from the Table IV, the proposed algorithm provides a better quality of the stego-image than that of the RIASIWT when the secret image is the same size.

Table V shows a comparison of the maximum payload (pixel number) that both algorithms can provide. As mentioned before, in the proposed algorithm, we can calculate the maximum payload from the size of cover image using (4), however in the RIASIWT, the maximum payload depends strongly on the characteristics of the cover image. From this table, the proposed algorithm provides a higher hiding capacity than that of the RIASIWT. In the best case, the proposed algorithm can hide three times larger secret images than that of the RIASIWT.

Also the hidden data robustness against the JPEG compression of both algorithms is compared. The comparison results under the same condition are shown by Table VI. In this table, the quality degradations of the extracted secret image caused by JPEG compression are measured in terms of PSNR. Two secret images with different size: 6075 pixels and 12,288 pixels, which are 25% and 50% of the maximum hiding capacity of the proposed algorithm, are used. It is because the maximum hiding capacity of the RIASIWT is approximately 50% of the maximum hiding capacity of the proposed algorithm.

The table VI shows that the robustness of the hidden data in the proposed algorithm is much higher than that of the RIASIWT. The secret image extracted from the compressed stego-image generated by the proposed algorithm is sufficiently clear, while the secret image extracted from the compressed stego-image of the RIASIWT is too noisy to observe the contents of the image.

D. Robustness to Commercial Analyzer

Recently the SARC (Steganography Analysis and Research Center) published in his web site that the quantity of Steganographic applications in his SAFDB (Steganography Application Fingerprint Database) is approximately 1150. The main purpose of the analyzers (StegAlyzerAS and StegAlyzerSS) provided by SARC is the detection of stego-files generated by several steganographic algorithms [12].

In other hand, the principal objective of steganographic algorithms is generating a stego-image that any commercial steganographic analyzer cannot detect as stego-image. All stego-images generated by the proposed steganographic algorithm are classified as natural images by the StegAlyzerAS and StegAlyzerSS, meaning that analyzers cannot detect the presence of the hidden data into the stego-images generated by our algorithm.

IV. CONCLUSION

This paper proposed a steganographic algorithm, which embeds and extracts a secret image in the DCT domain using the Quantization Index Modulation (QIM) embedding algorithm, in which unlike the previous reported methods, such as RIASIWT, the maximum payload is independent on the characteristics of either cover image or secret image. The maximum hiding capacity of the proposed algorithm is much higher than that of some conventional steganographic algorithms and it allows hiding a secret image.

The experimental results show that the proposed steganographic algorithm provides a high imperceptibility of the hidden information using DCT domain hiding technique, which allows taking advantage of the human visual system deficiency. This fact is shown in the Table I, in which the stego-image quality respect to the cover image is close to 40dB.

Also the proposed steganographic algorithm provides the hidden data robustness to the JPEG compression and the Gaussian noise contamination, extracting sufficiently high quality of the secret image from the stego-image attacked by the JPEG compression and the noise contamination. This robustness is obtained by the robust QIM algorithm and the rearrangement of the nibbles (MSB and LSB) of the pixels before the hiding operation. Additionally the proposed steganographic algorithm provides a stego-image in which the commercial stego-analyzer cannot detect the presence of the hidden data in it.

The performance of the proposed steganographic algorithm is compared with the previous reported RIASIWT [11], whose objective is same with that of the

proposed algorithm. The comparison results show the better performance of the proposed algorithm than the RIASIWT from the hidden data imperceptibility and robustness points of view. Also the proposed steganographic algorithm provides a twice or three times higher hiding capacity than that of the RIASIWT.

ACKNOWLEDGMENT

We would like to thank to the National Science and Technology Council of Mexico (CONACYT) and to the National Polytechnic Institute of Mexico for the support provided for the realization of this research.

REFERENCES

[1] S. Katzenbeisser, F.A.P. Petitcolas, *"Information Hiding Techniques for Steganography and Digital Watermarking"*, Comput. Security Ser., Artech House Books,2000.

[2] Suresh N. Mali, Pradeep M. Patil, Rajesh M. Jalnekar, *"Robust and Secured Image-Adaptive Data Hiding"*, Digital Signal Processing, Vol.22, 2011,pp 314-323.

[3] E. Chandy, L. Moucary and E. Hassan,*" A Novel Blind Digital Watermarking Technique for Stegano-Encrypting Information Using Nine-AC-Coefficient Prediction Algorithm with an Innovative Security Strategy"*, WSEAS-Transactions on Signal Processing, 2009, pp 359-36

[4] S. Torres Maya, M. Nakano-Miyatake and H. Perez-Meana, *"An Image Steganography Systems Based on BPCS and IWT"*, WSEAS-Transactions on Communications, May 2006,Vol.5, pp 814-820.

[5] A. Brown, S-Tool for Windows, Shareware, 1994, ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/s-tool3.zip

[6] D. Upham, Steganographic Algorithm JSteg [Online].Available: http://zooid.org/paul/crypto/jsteg

[7] A. Westfeld, F5-A Steganographic Algorithm (2001) LNCS, 2137 Moskowitz, I.S. (ed.) IH 2001 , pp. 280-302.

[8] S. Khaire, L. Nalbalwar, *"Review: Steganography – Bit PlaneComplexity Segmentation (BPCS) Technique"*, International Journal of Engineering Science and Technology, Vol. 2, No. 9, 2010, pp. 4860-4868.

[9] http://linux01.gwdg.de/~alatham/stego.html

[10] http://www.outguess.org/

[11] Raja, K.B., Sindhu, S., Mahalakshmi, T.D., Akshatha, S., Nithin, B.K., Sarvajith, M., Venugopal, K.R., Patnaik, L.M., *" Robust image adaptive steganography using integer wavelets "*, 3rd IEEE/Create-Net International Conference on Communication System Software and Middleware, COMSWARE , 2008 , pp. 614-621

[12] StegAnalyzer, http://www.sarc-wv.com/

[13] A. Tefas and I. Pitas, *"Image authentication using chaotic mixing systems"*, The 2000 IEEE International Symposium on Circuits and Systems, Proceedings. ISCAS 2000 Geneva, pp 216-219.

[14] Luis Rosales-Roldan, Manuel Cedillo Hernandez, Mariko Nakano Miyatake and Hector Perez Meana, Brian Kurkoski, *"Watermarking-based image authentication with recovery capability using halftoning technique"*, Journal of Signal Processing: Image Communication, Vol. 28, January 2013, pp 69-83.

O. Juarez-Sandoval received the B.S. degree in Communications and Electronics Engineering in 2010 and her from The Mechanical and Electrical Engineering School Culhuacán Campus of The National Polytechnic Institute of Mexico. Currently he is a Master student in Graduate Department of The Mechanical and Electrical Engineering School of the National Polytechnic Institute of Mexico. His Research interests are in image processing, secret sharing scheme and steganographi.

A. Espejel-Trujillo. She received her B.S. degree in Computer Engineering in 2007 and her M.E. degree in 2009 in the Graduate Department of The Mechanical and Electrical Engineering School Culhuacán Campus of The National Polytechnic Institute of Mexico. During her master degree she realized an international student exchange, in the University of Electro-Communications, Tokyo Japan in 2008-2009. Currently she is studying Ph. D course in Graduate Department of The Mechanical and Electrical Engineering School on the National Polytechnic Institute of Mexico. Her Research interests are in image processing, secret sharing scheme, and visual cryptography.

Mariko Nakano-Miyatake received the M.E. degree in Electrical Engineering from the University of Electro-Communications, Tokyo Japan in 1985, and her Ph. D in Electrical Engineering from The Universidad Autonoma Metropolitana (UAM), Mexico City, in 1998. From July 1992 to February 1997 she was a Department of Electrical Engineering of the UAM Mexico. In February 1997, she joined the Graduate Department of The Mechanical and Electrical Engineering School of The National Polytechnic Institute of Mexico, where she is now a Professor. Her research interests are in information security, image processing, pattern recognition and related field. Dr. Nakano is a member of the IEEE, RISP and the National Researchers System of Mexico.

Hector Perez-Meana received his M.S: Degree on Electrical Engineering from the Electro-Communications University of Tokyo Japan in 1986 and his Ph.D. degree in Electrical Engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 1989. From March 1989 to September 1991, he was a visiting researcher at Fujitsu Laboratories Ltd, Kawasaki, Japan. From September 1991 to February 1997 he was with the Electrical Engineering Department of the Metropolitan University of Mexico City where he was a Professor. In February 1997, he joined the Graduate Studies and Research Section of The Mechanical and Electrical Engineering School, Culhuacan Campus, of the National Polytechnic Institute of Mexico where he was the Dean from August 2006 to December 2009. In 1991 he received the IEICE excellent Paper Award, and in 2000 the IPN Research Award and the IPN Research Diploma. In 1998 he was Co-Chair of the ISITA'98, and in 2009 he was the General Chair of The IEEE Midwest Symposium on Circuit and Systems (MWSCAS). Prof. Perez-Meana has published more that 100 papers and two books. He also has directed 19 PhD theses and more than 35 Master theses. He is a senior member of the IEEE, member of The IEICE, The Mexican Researcher System and The Mexican Academy of Science. His principal research interests are adaptive systems, image processing, pattern recognition, watermarking and related fields.