Pixel Indicator Technique for RGB Image Steganography

Article *in* Journal of Emerging Technologies in Web Intelligence · February 2010

DOI: 10.4304/jetwi.2.1.56-64 · Source: DOAJ

1 author:

Adnan Gutub
Umm Al-Qura University
96 PUBLICATIONS **775** CITATIONS

SEE PROFILE

Pixel Indicator Technique for RGB Image Steganography

Adnan Abdul-Aziz Gutub

Email: adnangutub@gmail.com

***Abstract*— Image based steganography utilize the images as cover media to hide secret data. The common technique used in this field replaces the least significant bits (LSB) of image pixels with intended secret bits. Several improvements to enhance the security of the LSB method have been presented earlier. This paper proposed a new improved technique that takes the advantage of the 24 bits in each pixel in the RGB images using the two least significant bits of one channel to indicate existence of data in the other two channels. The stego method does not depend on a separate key to take out the key management overhead. Instead, it is using the size of the secret data as selection criteria for the first indicator channel to insert security randomness. Our proposed technique is analyzed using security and capacity measures and compared to two other similar work. This proposed pixel indicator technique for RGB image steganography showed interesting promising result.**

***Index Terms*— Steganography, RGB Bitmaps, Pixel Indicator Algorithm, Information security, Digital watermarking.**

I. Introduction

Steganography is the art and science of hiding information by embedding data into media. Steganography (literally meaning covered writing) [1] have been used since ancient time, for example, people used etching messages in wooden tablets and covered them with wax. They used tattooing a shaved messenger's head, letting his hair grow back, and then shaving it again when he arrived at his contact point to reveal the message. Different types of steganographic techniques have been used that employ invisible inks, microdots, character arrangement, digital signatures, covert channel, and spread spectrum communications [2].

Electronic steganography techniques use digital ways of hiding and detecting processes. Steganography is different than cryptography and watermarking although they all have overlapping usages in the information hiding processes. Steganography security hides the knowledge that there is information in the cover medium, where cryptography reveals this knowledge but encodes the data as cipher-text and disputes decoding it without permission; i.e., cryptography concentrates the challenge on the decoding process while steganography adds the search of detecting if there is hidden information or not. Watermarking is different from steganography in its main goal. Watermarking aim is to protect the cover medium from any modification with no real emphasis on secrecy. It can be observed as steganography that concentrates on high robustness and very low or almost no security [3].

Steganography, in general, may have different applications. For example, steganography can be utilized for posting secret communications on the Web to avoid transmission or to hide data on the network in case of a violation. It can be useful for copyright protection, which is, in reality, digital watermarking [4]. Copyright protection is to protect the cover medium from claiming its credit be others, with no real emphasis on secrecy. Stego Applications can involve "ownership evidence, fingerprinting, authentication and integrity verification, content labeling and protection, and usage control" [25].

Steganography techniques use different carriers (cover medium in digital format) to hide the data. These carriers may be network packets, floppy disk, hard drive, amateur radio waves [5], or general computer file types such as text, image, audio and video [6]. Restrictions and regulations are thought of in using steganography due to the threat from different laws in different countries. The law and writes (such as copyright) enforcing agencies needed in organizations are aiming to secure their information [7] but do not have clear procedures nor tools. In fact, many easy to use steganography tools are available to hide secret messages on one side of communication and detect hidden info on the other side [6].

In this work, we propose a new steganography method using RGB image pixels as its cover media. The information is hidden into two of the RGB pixel channels based on the indication within the third channel. This pixel indicator technique (PIT) benefits from the advantages of several older steganography methods. We evaluate our proposed PIT in comparison to two other methods using security and capacity measures showing potential conclusions. In the next section, several related steganography methods are discussed leading to the objective of our proposed work. Section 3 presents the parameters affecting steganography design and development considered in this kind of research. The proposed pixel indicator technique is detailed in Section 4. Section 5 provides the analysis study of the PIT in regards to the parameters. The PIT work results are compared with others in Section 6. The conclusions and future work ideas are presented in Section 7

II. Related Works

Several steganography systems combine steganography with cryptography seeking more security [8]. They also tend to increase capacity and reduce file sizes utilizing file compression capabilities before or after applying cryptography [9]. The general schematic diagrams for the steganographic systems are shown in Figure 1. Figure 1a shows the basic structure of the steganography system that includes only the information regarding the steganography method, with no crypto nor compression. The reliability and security of this system totally depends on how the steganography algorithm works. Figure 1b illustrates the system that put security on the secret message through encryption first and then steganography into the image. If any eavesdropper suspects the image and attacks it, he can not reveal the secret message due to the decryption need. Security of this crypto-stego system (Figure 1b) relies mainly on the encryption algorithm and the time needed for it to be broken. Figure 1c demonstrates the advanced steganography system which has crypto security as well as file compression to increase capacity.

In the literature, crypto steganography is also subdivided based on symmetric or Asymmetric algorithms. The pros and cons of this categorization are inherited from the types and security of the crypto algorithms involved. For example, the advantage in symmetric algorithms is its fast encryption/decryption processes but its disadvantage is key management. On the other hand, asymmetric algorithms, i.e. public key crypto algorithms [2], have overcome the key management problem through large public/private keys paying the price in expensive computation timings. In addition, the size of this crypto-stego system will be affected if the system shows encryption first and then compression or vise versa. Fast communication requires small size stego object, however the sequence of these two methods are affected on the size of resultant stego object. The reader is referred to Takahashi Y. et al. paper [10] for more details in the effect of sequence of compression with encryption methods on the data size for communication.

In the scope of this work, however, we do not consider combining steganography with cryptography nor compression. We focus on RGB image steganography method based on its own native definition as in Figure1a.

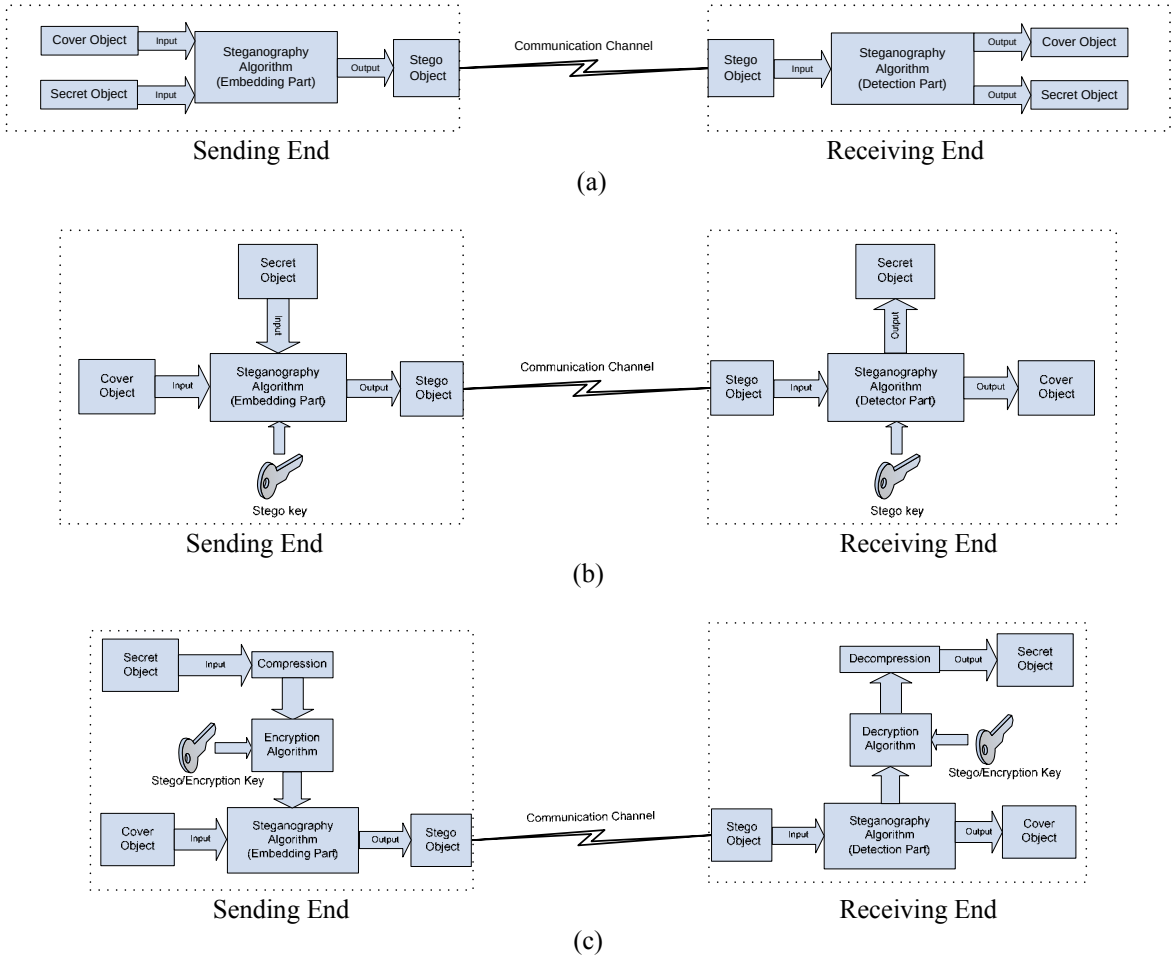

Figure 1. (a) Basic keyless steganography system, (b) Key steganography system, (c) Advanced steganography system.

It has been noted that most of the data hiding methods in image steganography used a technique utilizing the Least Significant Bits (LSB) of the pixels, i.e. the LSB of each pixel is replaced to hide bits of the secret message [11]. This, normally, produce changes in the cover media but with no significant effect. All the LSBs of pixels of cover image can be used for hiding the secret bits. The hidden information can easily be uncovered using many known statistical steganalysis techniques [12, 13], such as the X2 that can detect the concealed data inside the image with its original size as detailed in [14].

Bailey and Curran [15] described an image based multi-bit steganography technique to increase capacity hiding secrets in number of bits, i.e. Stego-1bit, Stego-2bits, Stego-3bits and Stego-4bits. Stego-1bit is the simplest of this, where it inserts the secret message data into one LSB (lower order bit) of the image pixels, which is undetectable. Hide and Seek [4] is an example of this technique. Note that if this bit insertion is performed into the higher order bit (most significant bit), the value of the pixel will show a great detectable change spoiling its security. It is known that insertion of hidden bits into lowest order LSB in all color RGB channels of the image pixels is unnoticeable [16]. In the Stego-2bits method two bits of lower order LSB in RGB image steganography is used; Stego-2bits doubled the capacity of message hiding with negligible security reduction. The capacity can be enhanced more as in Stego-3bits and even more in Stego-4bits, which are jeopardizing security accordingly. It has been claimed that these high capacity stego algorithms can be secure if images are chosen properly [15].

Stego Color Cycle (SCC) technique [16] is another way to add security to the high capacity LSB image steganography. To confuse steganalysis attempts, the technique cyclically uses different channels of the RGB image pixels to hide the data. That is, it keeps cycling the hidden data between the Red, Green, and Blue channels, starting from any one. This SCC method uses one channel per pixel for data hiding as used in S-Tools for steganography [17], which is considered low capacity utilization.

We propose the pixel indicator technique (PIT) to increase the capacity of the SCC without degrading the security. Our new idea uses two channels for data hiding but dependent on the third channel natural as briefly introduced in [23]. We are using this natural value channel as an indicator channel for data hiding in the remaining two channels. The scope of this work does not involve stego key (keyless) relaying on the algorithm security. The study considered image steganography utilizing several LSB's insertion, to compare with Bailey and Curran multi-bit steganography. It is also compared with the SCC techniques showing attractive results.

III. Parameters Affecting Steganography Techniques

Many parameters affect steganography and its design and development. These parameters include security (or perceptual transparency), capacity, robustness, complexity, survivability, capability, and delectability [18, 19, 24]. The relationship between the first two parameters is mostly influential and considerable in most researches in the literature; they consider the following properties:

1. Capacity: This term refers to the amount of data that can be hidden in the medium. It is defined as "*the maximum message size that can be embedded subject to certain constraints*" [18].
2. Perceptual Transparency/Security: The hiding process should be performed in a way that does not raise any suspicion of eavesdropper. The secure "*information is embedded in a way such that the average human subject is unable to distinguish between carriers that do contain hidden information and those that do not*" [20].

If we increase the capacity of any cover to store data with more than certain threshold value, then its transparency will be affected; i.e. with very high capacity, the steganography is not strong to keep transparent from eavesdroppers. It is required to select the parameters in such a way that steganography can be achieved on the best level accommodating its application need. In this research, the two parameters of capacity and security/perceptual transparency are considered for comparison to other works and are used as the parameters evaluating and directing the research work.

IV. Pixel Indicator Technique (PIT)

The pixel indicator technique (PIT) proposed in this work is for steganography utilizing RGB images as cover media. The technique uses least two significant bits of one of the channels Red, Green or Blue as an indicator of secret data existence in the other two channels. The indicator channel is chosen in sequence from R, G and B, i.e. RGB, RBG, GBR, GRB, BRG and BGR. However the indicator LSB bits are naturally available random, based on image profile and its properties. The indicator relation with the hidden data and the other two channels is shown in Table 1.

Table 1: Indicator values Based action

Indicator Channel	Channel 1	Channel 2
00	No hidden data	No hidden data
01	No hidden data	2bits of hidden data
10	2bits of hidden data	No hidden data
11	2bits of hidden data	2bits of hidden data

We have selected the indicators in sequence, if the first indicator selection is the Red channel in the pixel, the Green is channel 1 and the Blue is the channel 2 i.e. the sequence is RGB. In the second pixel if we select, Green as the indicator, then Red is channel 1 and Blue is channel 2 i.e. the sequence is GRB. If in third pixel Blue is the indicator, then Red is channel 1 and Green is channel 2. The sequence of the algorithm is shown as a flowchart in Figure 2. The first 8 bytes at the beginning of the image are used to store the size of the hidden message, which is also used to define the beginning of the

indicator channel sequence. These 8 bytes consumes all LSBs of the RGB channels, assuming it is enough to store the size of the hidden bits. To choose the first indicator channel, the size stored in the first 8 bytes is used as detailed in Table 2. The indicator choice is assumed as the first level, followed by the data hiding channels as second level. All six possible selections are obtained from the length of message (N), which will control the sequence, i.e. if N is even; the indicator channel is R, leaving an option of RGB or RBG based on the parity bit of N. Similarly, if N is a prime number, Chanel B is considered as the indicator leaving R and G for data hiding. If N value is neither even nor prime, "else" row in Table 2 is chosen, selecting the indicator to be G and the channels R and B are for secret data holding.

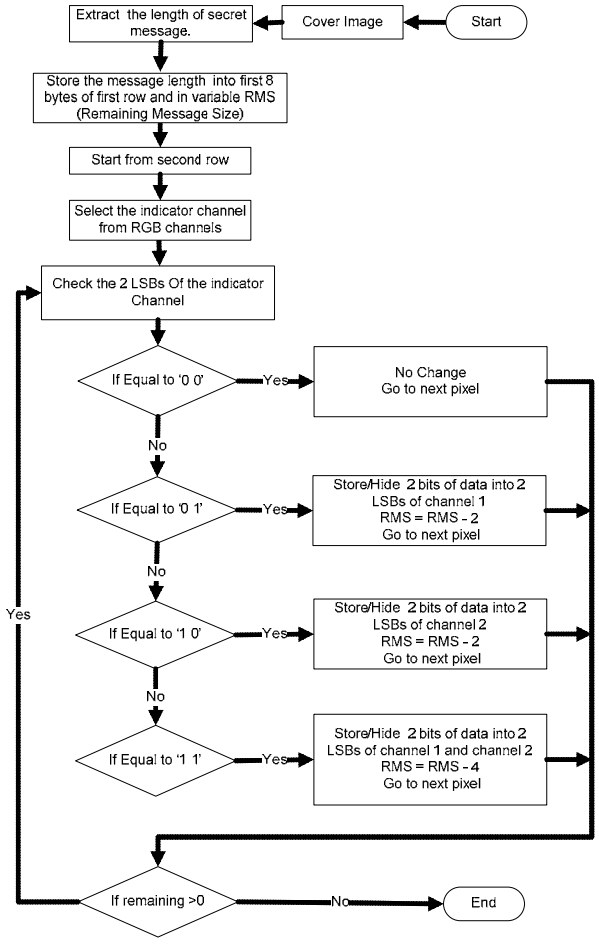

Figure 2. Construction phase (Hiding Process flowchart).

The recovery phase of the algorithm is shown in Figure 3 flowchart; it is the exact reverse of the hiding process starting with reading the length 'N' from the first 8 bytes of the image. Then, this N will specify the sequence of the channels as indicators and will stop based on the length of the secret message.

A BMP image is selected to run the experimentations for testing the proposed PIT algorithm. The PIT method is compared to the Stego-1bit, Stego-2bit, Stego-3bit, Stego-4bit and Stego Color Cycle techniques. The BMP image size is 512 X 384 used to hide a text message of 11,733 characters length (i.e. 93,864 bits). The algorithm is applied to hide 1-bit, 2-bits, 3-bits, 4-bits, and 5-bits to find the effect of increasing the bits on image security and capacity parameters. Tests conducted showed different levels of visual inspections and histograms based analysis. For capacity requirement the numbers of pixels used are recorded in each test run to hide data. The analysis with respect to the security and capacity is detailed in the next section. All analysis used *ImageJ 1.38v* (an image processing tool) [21] to get results.

Table 2: Indicator Channel Selection Criteria

Type of length (N) of secret message	I Level Selection Select indicator channel, first element of sequence	II Level Selection Binary N parity-bit	
		Odd Parity	Even Parity
Even	R	GB	BG
Prime	B	RG	GR
Else	G	RB	BR

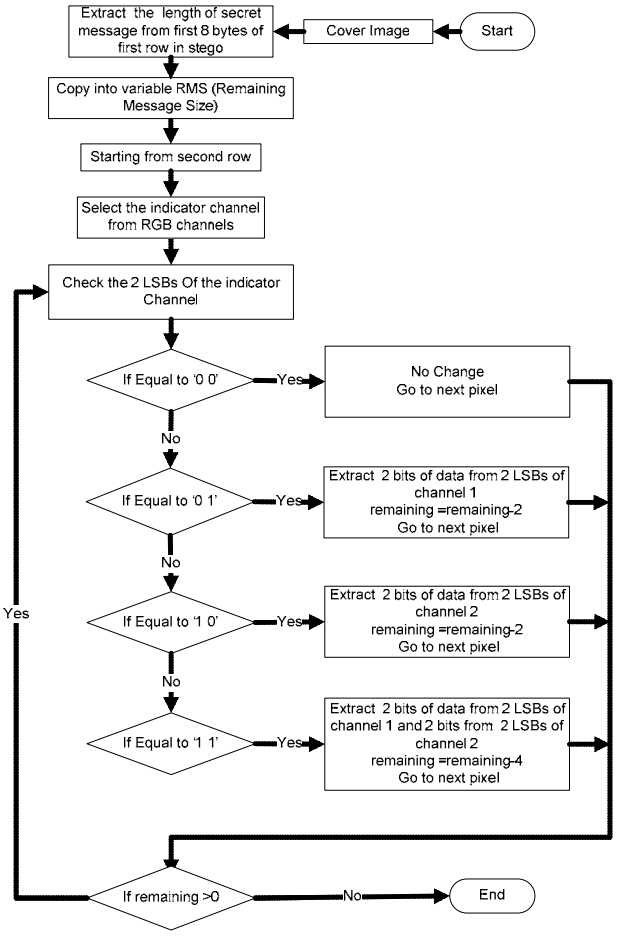

Figure 3. Recovery phase (Recovery Process flowchart).

Table 3: Measured values of the original and modified image

Measured values	Mean			Standard deviation		
Channels	Original	Modified	% Difference	Original	Modified	% Difference
Red channel	140.695	140.683	12	76.646	76.645	1
Green channel	116.266	116.261	5	76.574	76.570	4
Blue channel	90.710	90.694	16	74.451	74.411	40

V. ANALYSIS

The pixel indicator The analysis considers the security and capacity parameters. Security relates to minimal probability for breaking a steganography system for all adversaries [22].

1. Security:

The security analysis compares the original image with the stego image based on histogram of images. Comparing the histogram of the original channels, before and after modifying channels can give a clear idea of the security; i.e. if change is minimal then the stego system is considered secure. Figure 4 shows the original 512×384 image. The modified image (stego) after applying the PIT algorithm using 2-bits LSB's did not release any identifiable visual difference. The histogram of the original and stego images are shown in Figure 5a and Figure 5b, respectively. The histogram showed no change in the lower part of the image, however in the upper part it shows the difference in graph. We, furthermore, applied XOR operation between original and stego images to mark differences. The XORing revealed spots on the top area showing modification of the image as shown in Figure 5c.

Figure 4. Original 512×384 BMP image (cover image).

For further elaboration, the RGB original and stego images are split into Red, Green and Blue channels images with there histograms compared. Figures 6, 7, and 8, shows the histograms of the different channels, of R, G, and B from original and stego images, respectively, pre and post application of the PIT algorithm based on 2-bits LSB's. Histogram of all pairs of Red, Green and Blue channels in original and modified images, respectively, shows increasing changes. To be specific, consider mean and standard deviations of the channels as shown in Table 3. The major change occurred is in the Blue channel. This distribution is based on the natural randomization in choosing the indicator due to secret message length. If message length is changed then the selection of the sequence of R, G, and B will change reflecting on the distribution in all channels.

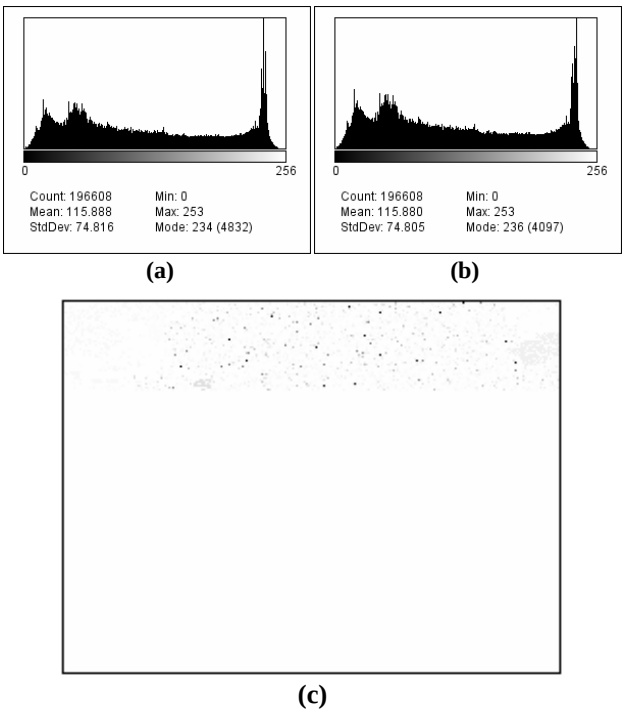

Figure 5. (a) Histogram of original image, (b) Histogram of stego image, (c) Images differences spots through XOR operation.

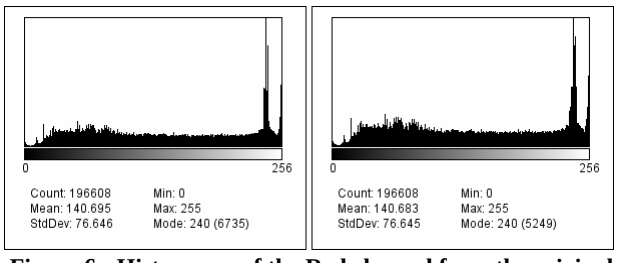

Figure 6. Histograms of the Red channel from the original (left) and stego image (right).

In order to measure the security vs. capacity effect, the algorithm is modified for hiding multi-bits per channel, i.e. 1, 2, 3, 4, and 5-bits (LSBs) in the same cover image of Figure 4. The simple visual evaluation showed differences in using PIT for 4 and 5-bits (LSBs) as shown

in Figures 9 and 10, respectively. However, the histograms of all multi-bits PIT tests showed the changes as in Figure 11. The mean and standard deviation figures decrease from 1-bit LSB insertion to 5-bit LSB insertions as listed in Table 4. This made the choice for PIT with 2-bits LSB insertion to be a practical recommended compromise between security and capacity.

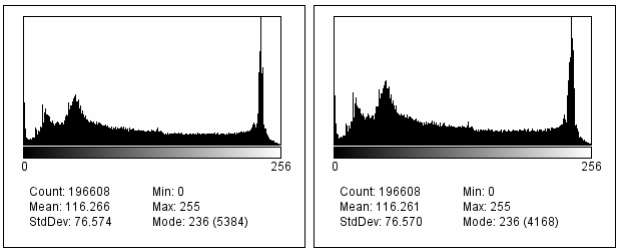

Figure 7. Histograms of the Green channel in the original (left) and stego image (right).

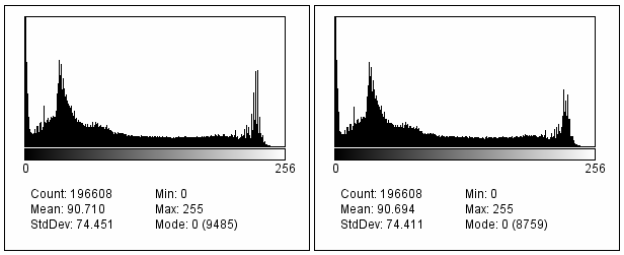

Figure 8. Histograms of the Blue channel in the original (left) and stego image (right).

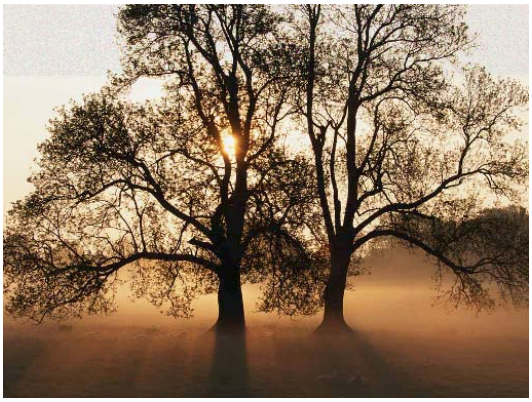

Figure 9. Stego image of PIT algorithm for 4 bits hidden.

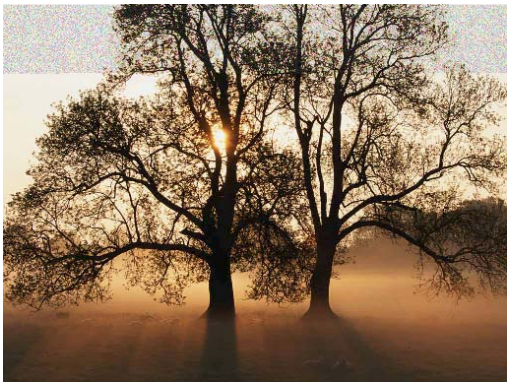

Figure 10. Stego image of the PIT algorithm when 5 bits are hided.

Table 4: Measured Mean and St. Dev. from resultant image of 1 to 5 bits LSB insertion

Modified image	Mean	Standard deviation
1 bit LSB	115.891	74.810
2 bit LSB	115.881	74.807
3 bit LSB	115.841	74.805
4 bit LSB	115.823	74.764
5 bit LSB	115.173	74.037

For comparison of PIT with Stego Color Cycle (SCC), 2-bits and 4-bits LSB's insertion in the same original image, of Figure 4, have been tested. The two SCC scenarios, 2-bits and 4-bits, did not show visual changes that can be detected. However, the differences can be observed in the R, G and B channels histograms as in Figures 12 and 13, for 2-bits and 4-bits, respectively.

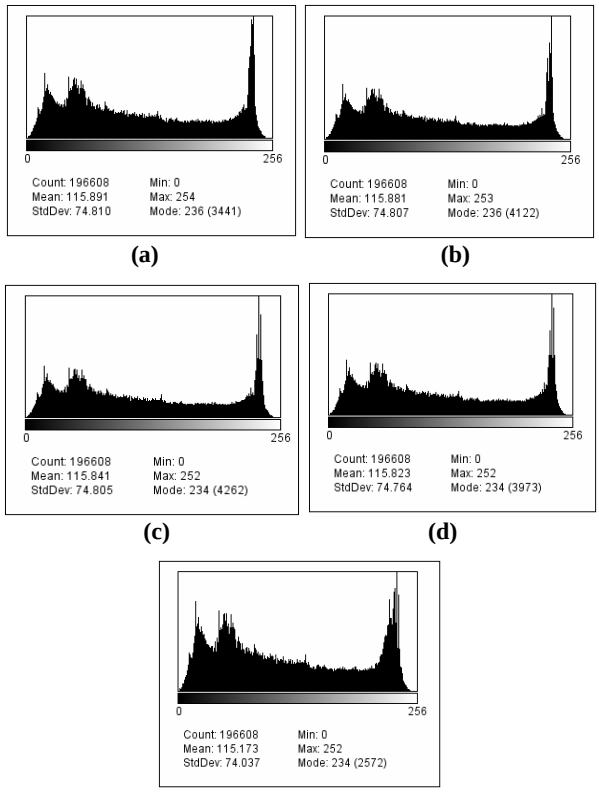

Figure 11. Histograms of multi-bit stego images: (a) 1-bit, (b) 2-bits, (c) 3-bits, (d) 4-bits, (e) 5-bits.

The histograms comparisons for the R and G channels with 2-bits and 4-bits LSB insertion showed that the means and standard deviations are decreasing. Unlike the B channel, were its standard deviation increased from 2-bits to 4-bits LSB insertion. This showed that the distribution in SCC is not homogeneous even though hiding the secret bits is put in a cyclical manner.

2 Capacity:

For the capacity analysis, the required number of pixels needed to hide the secret message is recorded. This capacity is measured using the PIT with multi-bit

features, i.e. 1-bit, 2-bits, 3-bits, 4-bits and 5-bits as shown Table 5.

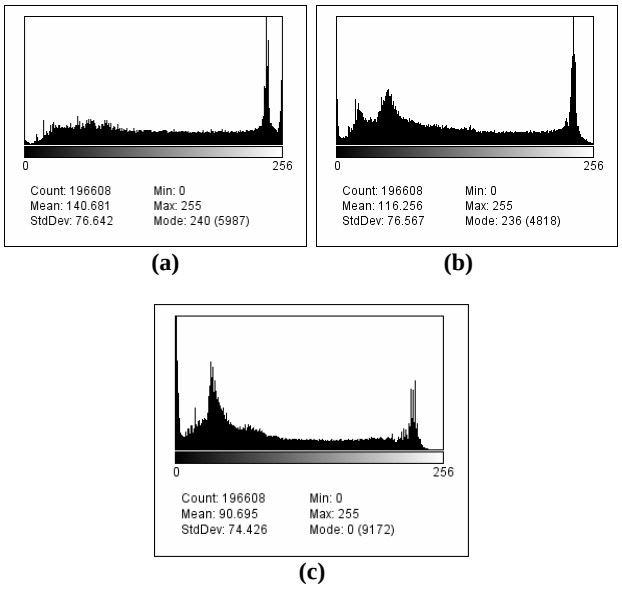

Figure 12. Histograms of SCC 2-bits stego image of separate channels: (a) Red, (b) Blue, (c) Green.

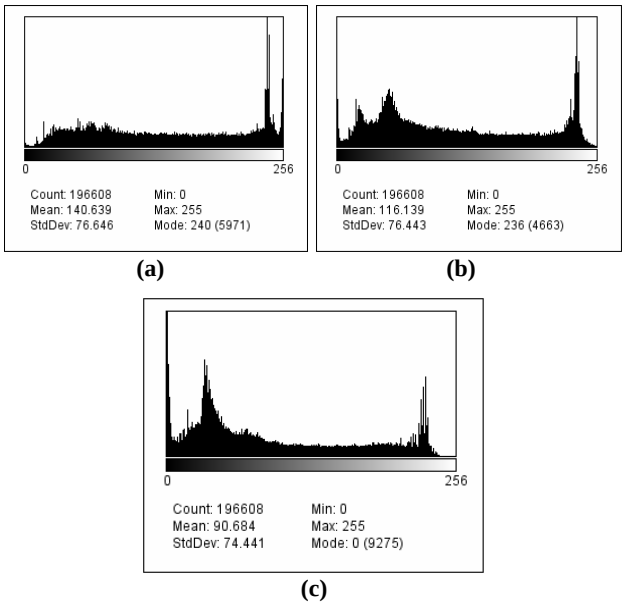

Figure 13. Histograms of SCC 4-bits stego image of seperaste channels: (a) Red, (b) Blue, (c) Green.

Table 5: Capacity comparison

No. of bits used	No. of pixels required to hide the data
1 bit	94512
2 bits	47287
3 bits	35112
4 bits	23370
5 bits	12146

The capacity increases normally as the bits to insert increase. This leaves the decision of the best number of bits to insert, to the application and its need. In general, the transparency of the image is affected clearly after 3-bits insertion n, making the recommendation to not exceed 3-bit PIT for acceptable secure systems. It has been observed also for SCC that the transparency is affected noticeably in the insertion of more than 2-bits in LSB's.

VI. Evolution Results

The multi-bit steganography, i.e. Stego-1bit, Stego-2bits, Stego-3bits, Stego-4bits and Stego Color Cycle (SCC) results given by Bailey and Curran [15] were considered to compare with our pixel indicator technique (PIT). Different PIT scenarios are compared to others based on similar number of bits to be inserted. The evolutional results are pointed out in Table 6. Note that the proposed PIT showed better results when compared to Stego-1bit and Stego-2bits, while it is kind-of similar when Stego-3bits and Stego-4bits are considered. Comparing to SCC, the PIT is always better.

VII. Conclusion and Future Work

The multi-bit Image steganography has many techniques to hide data. We have proposed a new pixel indicator technique (PIT) for RGB image based steganography. The PIT novelty is that it uses one channel for indication of secret data in the other channels. This indication channel changes from pixel to another with natural random value depending on the image pixels.

The study considered other available similar techniques to compare with; i.e. Stego-1bit, Stego-2bits, Stego-3bits, Stego-4bits, and Stego Color Cycle (SCC). The comparison is based on the commonly used parameters of security and capacity, which showed through histograms and statistical analysis that PIT has more capacity with same level of security. The PIT is found promising for further improvements and more

security enhancing; as future work example, we plan to improve this method replacing the indication channel sequence by pseudo random number generator (PRNG) controlled by the secret message length. This will keep the keyless feature but improve the security through the randomness of PRNG. If a key is to be used, it can be the seed of the PRNG which will make security responsibility on the user and application. The PIT can further be enhanced through a complete steganography security system using encryption and compression. In fact, this PIT may be a seed to develop state of art image steganography security system.

Table 6: Evolution results details

	Score		1 Bit		2 Bits		3 Bits		4 Bits		2 Bits		4 Bits	
			Stego 1-bits	PIT	Stego 2-bits	PIT	Stego 3-bits	PIT	Stego 4-bits	PIT	Stego Color Cycle	PIT	Stego Color Cycle	PIT
Histogram Based statistical analysis	Not Susceptible			✓		✓						✓		
	Susceptible	Low	✓								✓			✓
		High			✓		✓	✓	✓	✓			✓	
Visual Inspection of the image	Not Susceptible			✓		✓					✓	✓		
	Susceptible	Low	✓		✓			✓		✓				✓
		High					✓		✓				✓	

ACKNOWLEDGMENT

Thanks to the Center of Excellence in Information Assurance (CoEIA) at King Saud University, Riyadh, Saudi Arabia, for financially supporting this research. Similar thanks to King Fahd University of Petroleum & Minerals (KFUPM), Dhahran, Saudi Arabia, for facilitating this research work. Special appreciation to the students *Aleem Alvi, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen* and all other students of the course COE 509: Applied Cryptosystems - Techniques & Architectures for their valuable initiatives and positive cooperation.

REFERENCES

[1] Gutub, A., Fattani, M., 'A Novel Arabic Text Steganography Method Using Letter Points and Extensions', WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE), Vienna, Austria, May 25-27, 2007.

[2] Anderson R. J., 'Stretching the Limits of Steganography', 1st Information Hiding Workshop, Springer Lecture Notes in Computer Science, Vol. 1174, pp. 39–48, 1996.

[3] Gutub, A., Ghouti, L., Amin, A., Alkharobi, T., Ibrahim, M.K., "Utilizing Extension Character 'Kashida' With Pointed Letters For Arabic Text Digital Watermarking", Inter. Conf. on Security and Cryptography - SECRYPT, Barcelona, Spain, July 28 - 31, 2007.

[4] Provos, N., Honeyman, P., 'Hide and seek: an introduction to steganography', Security & Privacy Magazine, IEEE, Vol. 1, No. 3, pp. 32-44, May-June 2003.

[5] Westfeld A., 'Steganography for Radio Amateurs—A DSSS Based Approach for Slow Scan Television', J. Camenisch et al. (Eds.): LNCS 4437, pp. 201-215, Springer-Verlag Berlin Heidelberg, 2007.

[6] Johnson N. F., 'Steganography Software', http://www.jjtc.com/Steganography/tools.html, Accessed on Dec. 10, 2007.

[7] Karyda, M., Mitrou, L., 'Internet Forensics: Legal and Technical Issues', *IEEE Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007*), Greece, 2007.

[8] Bloisi, D., Iocchi, L., 'Image based Steganography and Cryptography', International Conf. on Computer Vision Theory and Applications (VISAPP), 2007.

[9] Al-Najjar A. J., Alvi A. K., Idrees S. U., Al-Manea A. M., 'Hiding Encrypted Speech Using Steganography', 7th WSEAS International Conference on Multimedia, Internet & Video Technologies (MIV '07), Beijing, China, September 15-17, 2007.

[10] Takahashi Y., Matsui S., Nakata Y., Kondo T., 'Communication Method with Data Compression and Encryption for Mobile Computing Environment', Proceeding of INET96 Conference, Montreal, Canada, 24-28 June 1996.

[11] Hempstalk, K., 'Hiding Behind Corners: Using Edges in Images for Better Steganography', Department of Computer Science, University of Waikato, Hamilton, New Zealand, 2006. http://diit.sourceforge.net/files/HidingBehindCorners.pdf

[12] Dumitrescu, S., Wu, X., Memon, N., 'On steganalysis of random lsb embedding in continuous-tone images', IEEE International Conference on Image Processing, Rochester, New York, September 2002.

[13] Fridrich, J., Goljan, M., Du, R., 'Detecting LSB steganography in color and gray-scale images', IEEE Multimedia Special Issue on Security, pp. 22-28, October-November 2001.

[14] Sabeti, V., Samavi, S., Mahdavi, M., Shirani, S.,'Steganalysis of Pixel-Value Differencing Steganographic Method', IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, (PacRim), pp. 292-295, 22-24 Aug. 2007.

[15] Bailey, K., Curran, K., 'An evaluation of image based steganography methods', Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88, July 2006.

[16] Neeta, D., Snehal, K., Jacobs, D., 'Implementation of LSB Steganography and Its Evaluation for Various Bits', 1st International Conference on Digital Information Management, pp. 173-178, Dec. 2006.

[17] Andy Brown, Steganography tools (S-Tools) for windows, 1996, Accessed in December 2007. ftp://idea.sec.dsi.unimi.it/pub/security/crypt /code/s-tools4.zip

[18] Chandramouli, R., Memon, N.D., 'Steganography capacity: A steganalysis perspective', Proc. SPIE Security and Watermarking of Multimedia Contents, Special session on Steganalysis, 2003.

[19] Pal, S.K., Saxena, P.K., Muttoo, S.K., 'Image steganography for wireless networks using the handmaid transform', International Conference on Signal Processing & Communications (SPCOM), 2004.

[20] Kraetzer, C., Dittmann, J., Lang, L., 'Transparency benchmarking on audio watermarks and steganography', In: Security, steganography, and watermarking of multimedia contents VIII; SPIE (u.a.), pp. 60721J-1--60721J-13, San Jose, California, 19 January 2006.

[21] Rasband, W.S., ImageJ, *U. S. National Institutes of Health,* Bethesda, Maryland, USA, http://rsb.info.nih.gov/ij/, Accessed in January 2008.

[22] Robert Kunnemann, 'Planning a Jailbreak: Use Steganography', Course slides, August 11, 2007. http://www.infsec.cs.uni-sb.de/teaching/ SS07/Proseminar/slides/kuennemann-stego.pdf

[23] Gutub A., Ankeer M., Abu-Ghalioun M., Shaheen A., and Alvi A., "Pixel Indicator high capacity Technique for RGB image Based Steganography", *WoSPA 2008 - 5th IEEE International Workshop on Signal Processing and its Applications*, University of Sharjah, Sharjah, U.A.E. 18 - 20 March 2008.

[24] Parvez M. T. and Gutub A., "RGB Intensity Based Variable-Bits Image Steganography", *APSCC 2008 - Proceedings of 3rd IEEE Asia-Pacific Services Computing Conference*, Yilan, Taiwan, 9-12 December 2008.

[25] Mohanty, S. P., and Bhargava, B. K., "Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks", *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP)*, Vol. 5 , No. 2, Article 12, November 2008.

Adnan Abdul-Aziz Gutub is currently holding the rank of an associate professor in Computer Engineering from King Fahd University of Petroleum and Minerals (KFUPM) in Saudi Arabia. He received his Ph.D. degree (2002) in Electrical & Computer Engineering from Oregon State University, USA. Adnan received his BSc degree (1995) in Electrical Engineering and MSc degree (1998) in Computer Engineering, both from King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia.

Adnan's research interests are in modeling, simulating, and synthesizing VLSI hardware for crypto and security computer arithmetic operations. He worked on designing efficient integrated circuits for the Montgomery inverse computation in different finite fields. He has some work in modeling architectures for RSA and elliptic curve crypto operations. His interest in computer security also involved steganography such as simple image based steganography and Arabic text steganography.

Adnan has been awarded the UK visiting internship for 2 months of summer 2005 and summer 2008, both sponsored by the British Council in Saudi Arabia. The 2005 summer research visit was at Brunel University to collaborate with the Bio-Inspired Intelligent System (BIIS) research group in a project to speed-up a scalable modular inversion hardware architecture. The 2008 visit was at University of Southampton with the Pervasive Systems Centre (PSC) for research related to advanced techniques for Arabic text steganography and data security.

Adnan participated in many conferences and delivered number of short courses and technical speeches inside and outside Saudi Arabia .

His participation also involved him in international/local research affiliations including:

-Security Research Group, Information & Computer Science Department, KFUPM.

-Cryptography Research Group, Computer Engineering Department, KFUPM.

-Cryptographic Hardware and Embedded Systems (CHES) Research Group.

-Information Security Laboratory, at Oregon State University, Corvallis, Oregon, USA.

Adnan Gutub filled many administrative and academic positions in KFUPM. Lately (2006~2009), he has been the chairman of computer engineering department (COE) at KFUPM in Dhahran, Saudi Arabia.