Hybrid Medical Colored Image LSB Steganography Based on Primitive Root Numbers

Nedhal A. M. Al-Saiyd

Department of Computer Science, Applied Science Private University
Amman, Jordan

Summary

In the age of increasing digital data transmission through network, the data security measures have become very important and crucial issue. Two main security schemes are used to protect sensitive data: cryptography and steganography. A good imperceptibility and appropriate data capacity are the two important properties that characterize Steganography technique. In this paper, a hybrid technique is proposed that utilizing the Steganography and Cryptography, to hide sensitive patient's data into pixel values of medical colored image. The medical colored image is chosen as a cover image of lossless compression PNG format. The sensitive data; which is the patient's data and the examination data, is firstly encrypted using 'Block Encryption Method' and then embedded in the image. This will make it harder to recognize or interpret it when it is attacked. In embedding algorithm, the pixels of medical cover image are chosen randomly based on the values, which are produced using primitive root numbers. The two least significant bits of the blue and alpha channels are used to hide the encrypted patient's sensitive medical data. The experimental results shows that the quality of stego-image is relatively less distortive, highly imperceptible to human eye, has good data hiding capacity, and assure more security.

Key words:

Medical Image Steganography, LSB, Data-Hiding, Cryptography, Primitive Root.

1. Introduction

Information security is the process of protecting information. Security uses two main approaches, the "cryptography" and "Steganography", but they are different. Cryptography techniques are used to obscure a sensitive message in a way that make it harder to read or to decode it, while the main goal of steganography is to send a confidential message to a receiver under the cover of a stego-carrier object [1], [2], [3].

Steganography is derived from the Greek language and means "Covered Writing" [4]. Steganography approach is the technique that is used to hide a confidential message data inside another digital object, such as text, image, audio, video and multimedia as a carrier or cover object. Images are the most common used carrier medium [1]. Figure 1 shows the security systems and the categories of steganography techniques. The more suitable object formats for hiding information is the object with a high bit redundancy. The redundant bits are those bits that can be changed without revealing the changing [5].

Basically, the objective of steganography is to prohibit the eavesdropper from suspecting the existence of secret communications and not to resist him from decoding a hidden message. The steganography is defeated when a suspicion is raised.

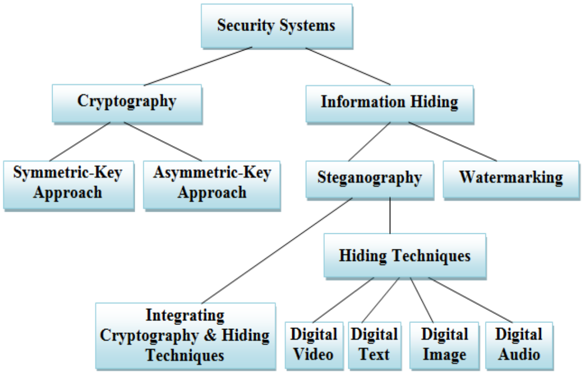

Fig. 1 Cryptography and Steganography categories

The steganography is used to build a secure communication channel, where the existence of hidden sensitive message is covert between the sender and the receiver [2], [6], as it is shown on Figure 2. The general steganography mechanism is explained in the following steps:

a. The sender selects the sensitive message to be sent.
b. The sender embeds the sensitive message into a carrier object by applying secret stego-key to change some of the carrier object's properties. The embedding is done in such a way that the third party cannot notice the existence of the message.
c. The resultant stego-object (i.e. the carrier object after hiding the sensitive data) is transmitted to the receiver.
d. At the receiver side, the sensitive message is extracted from the stego-object, depending on the shared secret stego-key between the sender and the receiver.
e. The secret stego-key should be shared between the communication entities. The key is required to be changed frequently, and a synchronization key management process is required among the entities.

Manuscript received February 5, 2017
Manuscript revised February 20, 2017

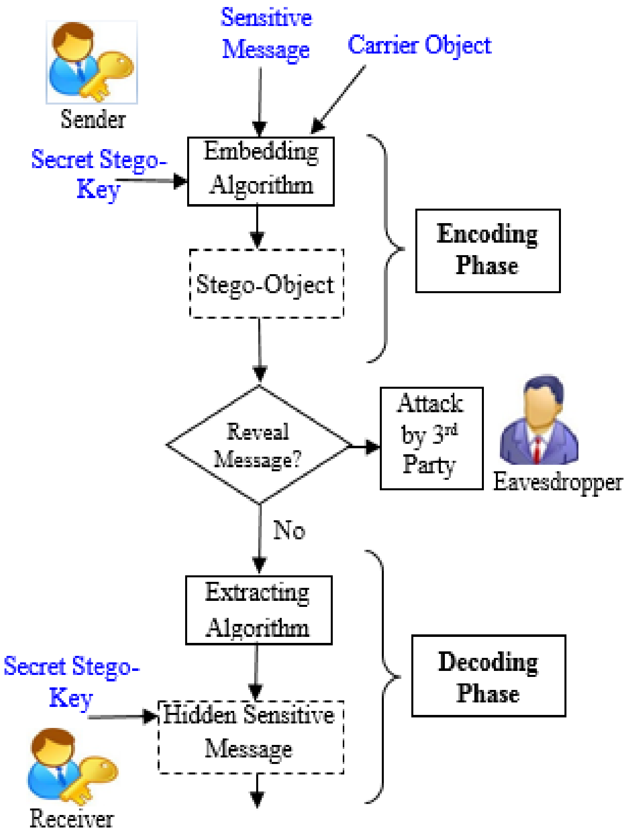

Fig. 2 The basic model of steganography mechanism

2. Motivation and Solution Objectives

Lesser Work is done on RGB color images than gray level (almost 25% on comparison scale) [7]. Very few techniques are working on hiding data according to RGB color perceptibility while the blue color plane provides maximum data than green or red.

A lot of examination medical images are transferred and transmitted among different hospitals, medical laboratories, and scientific research centers. The examination medical images, the sensitive patient data, and the patient examination results are transmitted separately, which may raise the amount of transmitted data, cost and consume more bandwidth. Sometimes the results may be lost or link to another patient. Therefore, it is necessary to keep the existence of the patient examination results embedded and combined to the specific patient medical image (i.e. steganography), try at the same time to keep the data contents secret and protected (i.e. cryptography) from unwanted parties and attackers. By combining steganography with cryptography, the strength of steganography can be increased.

In this paper, a new technique is proposed that integrate the steganography and the cryptography using random generated key depending on primitive roots of prime numbers; that will be applied in encrypting the sensitive data using block ciphering, and in identifying certain LSBs to embed the encrypted sensitive patient medical examination results into patient medical colored image.

The rest of the paper is organized as follows. Section 2 presents the motivation and the solution objectives of this research. Section 3 explained in general Steganography of utilizing LSB techniques. In section 4 literature review are briefly covered. Section 5 explains the design considerations for the proposed methodology. The proposed medical colored image steganography is explained in details in section 6. The experimental results are illustrated in section 7, and finally conclusions are provided in section 8.

3. LSB in Image-Based Steganography

In general, the image steganography techniques are classified into three main categories, according to their mechanisms, characteristics, complexities, and payload:

I. *Spatial domain image steganography techniques*:
The secret data is hidden directly into image pixel's value. They are considered as simple techniques that embed the secret message directly into image pixels. This may cause noticeable change to the image. Hence, the embedding algorithms use the lossless image compression. Least Significant Bit (LSB) is a commonly used type of spatial domain technique [8].

II. *Transform image steganography techniques*:
The cover image is converted from spatial domain into frequency domain using Discrete Cosine, Discrete Wavelet, Integer Wavelet or Discrete Fourier transform. Then the secret data is embedded, through quantizing and modifying the spectrum coefficients of the converted image [9], [10].

III. *Dynamic masking and filtering image steganography technique*:
This technique is implemented on colored or grey-level images. The embedded message is relatively very smaller than the cover image, which limits the number of safely be embedded bits. It uses a mathematical expression to identify the pixel in significant areas of image to embed the secret data [11].

LSB is one of the commonly used techniques. The least significant bit of each image pixel is replaced with one bit of the secret message and the process repeated for all the bits of the message. [12]. The drawback of old LSB techniques was to replace the image LSBs in sequential order and the extraction of message bits from image are done in sequential manner, which may lead to reveal the hiding algorithm. Also, it is considered as low capacity stego algorithms. This caused a risky model of uncovering the model and subsequently threatened its security [3]. Therefore, a pseudo random number generator (PRNG) is used to produce a stego-key, which is used to select randomly image pixels to hide secret data. The stego-key is shared between the sender and receiver synchronously, and is needed to be changed frequently. This will demand extra effort and cost for key management technique [13].

Chang et al, in 2008 [14] proposed an method to embed a large payload of secret data in color images by modifying the blue color value of the pixel because the blue value is an undetectable color to human eyes.

To increase the imperceptibility, Stego Color Cycle (SCC) technique is used to hide data into different RGB channels, using one channel as a data carrier at a time. The channels are selected cyclically [14].

An adaptive data hiding approach for 24-bits RGB colored images is proposed to embed secret data in relation to data size. In embedding process, one of the three channels is selected randomly depending on integer random number ranged from 0 to 3. If the random number is 1, then green and blue channels are chosen to hide data. If the random number is 2, then red and blue channel are chosen to hide data. If the random number is 3, the red and green channels are chosen to hide data Otherwise, nothing is done [15].

In 2013 W. W. Zin proposed a hybrid method to hide information in PNG format image by combining cryptographic and steganographic techniques. For data confidentiality, the important message is encrypted using RC4 algorithm. Then the encrypted message is embedded in PNG image file based on the Blum-Blum-Shub (BBS) pseudo random number generator that generates the random sequences where the embedding will take place [16].

In 2014, Rawashdeh and Al-Saiyd proposed hybrid technique that integrate colored image steganography with encryption to achieve high-level of security [17]. In the encryption process the secret key generation depends on primitive roots of prime numbers is used. The embedding process of steganography is done randomly and based on stego keys that are also derives from primitive roots of prime numbers.

In 2015, Manjula and others proposed a technique called “Hash Based Least Significant Bit (2-3-3)” to insert 8 bits of secret data in LSBs of pixel value of the colored cover image; where 2 bits is inserted in Red, 3 bits is inserted in Green, and 3 bits is inserted in Blue channels respectively. LSB bit position within the pixel is calculated from (the position of each hidden image pixel % number of bits of LSB). This hash function distribution produced better results. [18].

Steganography is in contrast to the cryptography concept, is about concealing the secret message existence and it is invisible to an ordinary observer, while cryptography is about protecting the content of messages [9].

Cryptography uses Encryption and Decryption processes. Encryption process secure and be unreadable without adequate knowledge. The receiver can decrypt the encrypted data and understand the actual meaning. Cryptography methods can be classified into symmetric-key and Asymmetric-key algorithms, depending on the key(s). In the symmetric-key cryptography, the sender and the receiver share the same secret key in encryption and decryption processes. While in the asymmetric-key cryptography, there are two keys: the encryption key (public key) that is published and known to all senders and used in encryption process, and the private key that is used by the receiver to decrypt the encrypted messages [19].

4. Related Work of Medical Digital Image Steganography

We found that few attempts were done on medical colored image steganography and applied hybrid security scheme that integrate cryptography and steganography; as:

Petitcolas [20] explained an application, which embedded the patient’s information in the medical image. Confidentiality is considered in the separation between patients’ image data (DNA sequences) and the patient's personal data.

The patient data is embedded into medical image at different sub-bands using wavelet coefficients of the cover image [20].

Miaou et al. [22] presented an LSB embedding technique for electronic patient records based on bi-polar multiple-base data hiding technique and transmit the patient image on the internet among different hospitals and countries.

Yue Li and et al. [23] proposed an algorithm to protect mammographic image from illegally obtained or changed the image content. It hides patients' data into mammogram images without altering the important details of the grey-scale images.

5. Design Considerations of the Proposed System

Any steganography technique is characterized by two significant properties; a good imperceptibility and sufficient data capacity. There are different algorithms, where each of them has different strong and weak influences. One embedding algorithm may have reduction in payload capacity, while the other may have reduction in robustness against most type of attacks [24]. The eavesdropper is unable to detect the existence of hidden data by naked eye. The decision about which steganographic technique is more appropriate to apply depends on the application type, security level, perception level, payload and it needs some of features compromising [24]. The main purpose of image steganography is to preserve the quality of cover image and the sensitive data, and eliminate the amount of modification in cover images.

For the proposed design, many issues are taken into our consideration, and data are gathered, analyzed and designed, such that:

A. A medical colored images are chosen, since color imaging is widely used in medical diagnosis. The format of medical colored image is suggested to be the lossless compression PNG that has 32-bit for Red, Green, Blue, and Alpha (RGBA) color channels. They are supported across multiple file systems and operating systems. The PNG large file size has good advantage for hiding data with less distortion and with high payload capacity. PNG can compress more than a GIF file can do on the same image in approximately from 5% to 25% [16]. It offers more flexibility features when it is used in Steganography. Therefore, larger amount of data will be embedded into image, unlike an 8-bit gray level digital image. The major drawback to PNG images is their large size.

B. Colored image steganography using LSB technique is proposed. The LSBs of Blue and Alpha channels are be selected as embedding positions, because embedding into LSBs of blue channels is less perceptive by human eye and hence, has relatively the best quality [25]. The number of embedded bits into blue channels will be dynamic and the modification of pixels in image. It will provide relatively high payload data to be embedded.

C. To empower the security, the patient secret data is encrypted before embedding it into image, because cryptography is used, to provide data confidentiality, integrity, authentication, and non-repudiation problem solutions [26], where both steganography and cryptography ensure data confidentiality.

D. A pseudo random key is generated from the prime number depending on the primitive roots of prime numbers. Random key generator generates keys will be applied in the block encrypting algorithm of patient's data and examination results, where the sensitive data is partitioned into non-lapping blocks. The randomized key will be used to determine the indices of bit-permutation within the block of sensitive patient's text data.

E. The encrypted sensitive patient medical data is then embedded in randomized pixels in the first and second LSBs of the Blue and Alpha channels of some selected image pixels instead of embedding them in the pixels sequentially. This will make it harder to the eavesdropper to predict the embedded data size and its value or detect the modifications in the medical image.

6. The Proposed Research Methodology

The proposed methodology has four integrated components: random key generator, the encryption of sensitive patient's examination data, the selecting and embedding process, and the extracting process of sensitive patient's data.

Figure (3) illustrates the four integrated components of the proposed methodology.

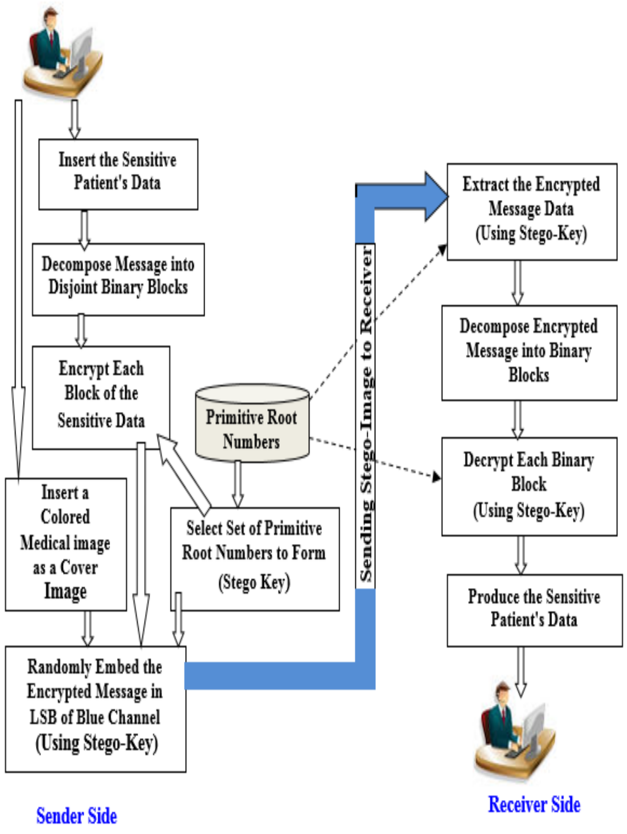
Insert the Sensitive Patient's Data
Decompose Message into Disjoint Binary Blocks
Encrypt Each Block of the Sensitive Data
Insert a Colored Medical image as a Cover Image
Primitive Root Numbers
Select Set of Primitive Root Numbers to Form (Stego Key)
Randomly Embed the Encrypted Message in LSB of Blue Channel (Using Stego-Key)
Sending Stego-Image to Receiver
Extract the Encrypted Message Data (Using Stego-Key)
Decompose Encrypted Message into Binary Blocks
Decrypt Each Binary Block (Using Stego-Key)
Produce the Sensitive Patient's Data
Sender Side
Receiver Side

Fig. 3 The three integrated components of the proposed system

6.1 Randomized Key Generator

For the implementation of encryption and the embedding processes, the generation of randomized keys is requested. They are used in the identification and permutation of bits each block of the non-lapped blocks of the sensitive patient's data. Depending on the values of stego-key, the locations of carrier bits in Blue and Alpha channels are needed to be identified to embed the sensitive patient's into the patient's medical image. The prime numbers and their primitive root numbers are used to assure the randomness of byte selection. In this research, 809 is being used as a prime number. It is considered as a stego-key.

Depending on Fermat's Little Theorem and Difiee-Hellman secret-key exchange protocol [27], the randomization key generator function G(Ind), will be computed from a prime number ‘P’, and given the least positive residue of PrInd that is produced for all integers in [1, P-1] interval, and Pr is a primitive root of P. A primitive root of modulo n or a primitive root of n, is a positive integer such that the powers of it runs through all the integers modulo n [27].

$$\textbf{Key} = \boldsymbol{G(Ind) = Pr^{Ind}\ (mod\ P)} \qquad \textbf{(1)}$$

Where:
G(Ind): The generated key or new index;
Where: 0 < G(Ind) < P.
Pr: A primitive root of prime number P, is considered as a sub-key, where not all integer numbers have primitive roots. The prime number has many incongruent primitive roots [27].
Ind: The current index of the block element to be permutated in encryption process or embedded in embedding process.
P: Prime positive number that is equal to or larger than the indexing range, and is a positive number; P > 0.

The above function produces unique values for stego-keys within a certain range [1, P-1], with the help of Fermat's little theorem [27]. Assuming that the sender and the intended recipient share a key that is used to encrypt the message.

6.2 The Encryption Method of Sensitive Patient's Examination Data

The sensitive patient's text data will be segmented into fixed-length blocks; B_1, B_2, …, B_n, each block has 101-bytes (808 bits), if B_n has less than 101 bytes it can padded with zeros. A selected keys K from a sequence of generated keys are applied on each block of bits. The encryption function corresponded to the selected key is denoted by $E_i(K_i)$.

For confidentially, the encryption process is performed. The sensitive data is partitioned into blocks of 101 characters (i.e. block size), convert each of them into binary array of 808-bits, and the permutation of the block bits is done according to the new location that is indexed by:

$$f(x) = Pr^{x}\ \%\ 809 \qquad (2)$$

Pr: Primitive Root of prime number 809.
X: represents the current bit location, and
f(x): new calculated index within the block size.
809 has 400 primitive roots, so we can choose any subset.

The permutation process is customized using key generated in step 5 on each index of bits in Block[BlockID, Ind]. To eliminate patterns and make it harder for eavesdropper to extract the message. Different permutation rounds use different primitive root numbers as keys. Each block uses different set of keys. The pseudo code is:

```
Encrypt(Keys[],Block[][])
  For each (k in Keys)
    For each (s in Block[][])
      For i=0 to s.length-1 step 1
      Encrypted[s.index][$key^{i+1}$ % (BlockSize-1)-1]
          = Block[s.index][i]
Returned Encrypted[][];
```

6.3 Embedding of Sensitive Patient's Examination Data

Step 1: The sender selects patient's color image of PNG format, to represent the input cover-object and the related sensitive patient’s data and transforms it into binary format.
Step 2: The sensitive patient data is partitioned into non-lapped blocks, where each block size equal to 808-bits, and if the last block is less than 808, it is padded with zeros. Each block is identified by Block[BlockID , Ind].
Step 3: The key is generated as it is discussed in equation 1. The prime number is chosen to be slightly larger than value of array length. The key value is computed from primitive roots of chosen prime number.
Step 4: Then the embedding process of encrypted message is done in the two LSBs of Blue and Alpha channels of (RGBA) PNG color images. The bits of the encrypted block are embedded in randomized order, which are identified using the key generated in step 5. To embed one character of encrypted sensitive data, two pixels are needed, because the embedding is done in the two LSBs of Blue and Alpha channels. The pseudo code of the embedding is:

```
Embed(Encrypted[][], rKey, cKey)
j=-1
For each(s in Encypted[])
j=j+1
For i=0 to s.length-1 step 8
   If ((i+1) % 513 ==0)
    j=j+1
    cIndex=($cKey^{((i+1)\% 513)}$) % 513
    rIndex=($rKey^{(j+1)}$) % 513
    image[cIndex].Blue=replace
         LSB(Image[cIndex][rIndex].Blue,s[i+4]
                  image[cIndex].Alpha=replace
         LSB(Image[cIndex][rIndex].Alpha,s[i+6]
return Image[][]
```

Step 5: The ‘BlockID’ in ‘Block[BlockID, Ind]’ is increment to work on the next block, if any. Steps 3 and 4 are repeated on all the blocks. If the colored cover image has (5000) pixels, then (4969) prime numbers ‘P’ are needed. The number of prime numbers must be chosen larger than the block size to cover block indexing.

6.4 The Extracting Method of Sensitive Patient's Data

At the receiver side, the sensitive data is extracted first from the medical image and then is decrypted is done using the same stego-keys, and secret key of the encrypted process. The Pseudo code of decryption is:

```
Decryt(Keys[], Encypted[],[])
 For each (key in K)
   For each (s in Encypted[])
     For i = 0 to .length-1 step 1
       Decrypted[s.index][i] = s[s.index][key_i +1 % 809)-1]
  Return Decrypted[][];
```

7. Evaluation Results

A. The proposed technique is applied to medical colored images, as shown in figures 4 through 8. They are selected with PNG format images and image size has (512x512) pixels.

B. The perception evaluation of the hidden secret message is measured using Peak Signal-to-Noise Ratio (PSNR) for color image, that is consider as a measurement of imperceptibility degree [28]:

$$PSNR = 10\log_{10}\frac{255x255}{MRE_B+MRE_A)/_2}\,\text{dB} \qquad (3)$$

Where:
MSE_B: is mean square error for Blue channel, and
MSE_A: is mean square error for Alpha channel.

The PSNR is decreased, and this means that the embedding scheme does not degrade the quality of the cover image; where the stego-image is closest to the original cover image. The embedded message is not perceptible or detectable to the viewer.

C. Since the last two least significant bits are changed in the pixel of 32-bit (RGBA colors) PNG image and only two color channels of 255 are only changed. The degradation ratio will be 1.5625%. Therefore, the minor changes and degradation in stego-images are completely imperceptible to human eye.

D. The payload capacity is increased, where the acceptance results shows that the number of hidden messages exceeds 560 characters and it is still hard for human eye to detect the changes in image or predict the existence of sensitive data, as it is shown in figure 4 through 8.

E. The size of generated random key is dynamically changed with respect to the changing in the length of sensitive patient’s data. This complicates the key distribution between sender and receiver, and the algorithms of encryption and embedding.

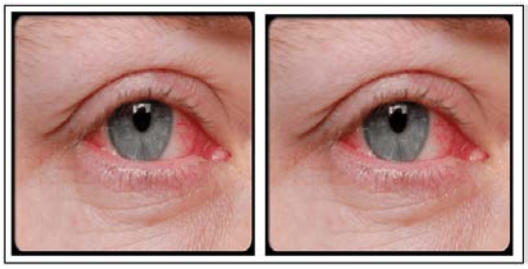

Fig. 4 (left) Cover image (right) Stego image after embedding message data of 486 character with spaces (415 characters without spaces)

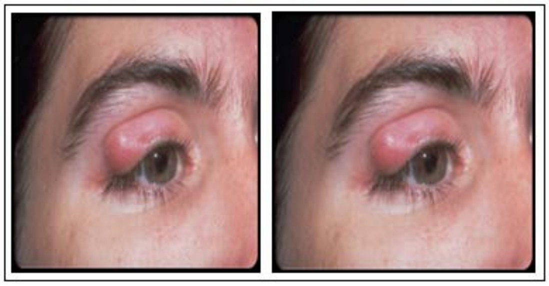

Fig. 5 (left) Cover image (right) Stego image after embedding message data of 423 character with spaces (359 characters without spaces)

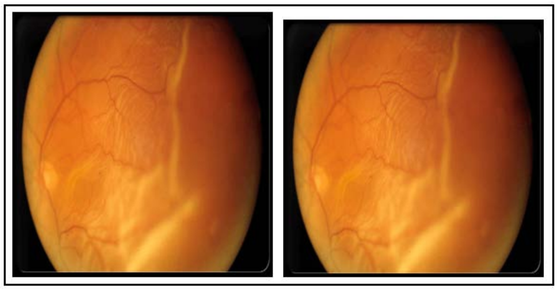

Fig.6 (left) Cover Image (right) Stego image after embedding message data of 662 character with spaces (560 characters without spaces)

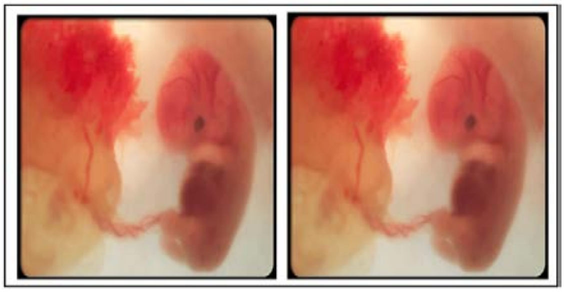

Fig.7 (left) Cover Image (right) Stego Image after embedding message data of 428 character with spaces (353 characters without spaces)

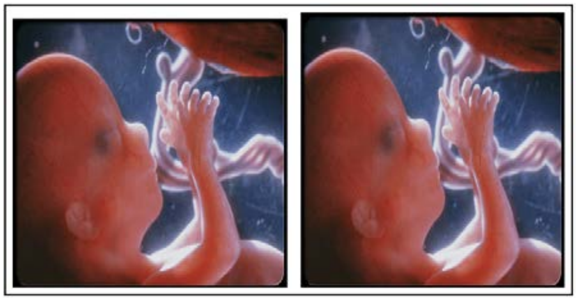

Fig.8 (left) Cover Image (right) Stego Image after embedding message data of 231 characters with spaces (194 characters without spaces)

8. Conclusion

- In this paper, a new hybrid technique is presented that integrate cryptography and steganography to encrypt the sensitive patient data and embed it into medical image. Both steganography and cryptography enhance medical data security, and ensure data confidentiality, and integrity.
- Random numbers generator algorithm, is derived primitive roots of prime numbers to generate unique value that are used in encryption and embedding processes. This complexity increases the security level.
- To protect the patient sensitive data, an effective block ciphering algorithm is applied using the random numbers as the index for permutation of bits inside non-lapped blocks of data.
- Steganography is done by embedding the encrypted data into the two LSBs of PNG Blue and Alpha channels of the medical images.
- The experimental results shows that the quality of stego image is relatively less distortive, preserve the sensitive data and increase the data payload.
- The maximum embedding data inside the image is equal to ((Number of image pixels/2)-1), because 2 pixels are needed to store one message character, and the value is subtracted by 1, because one pixel is needed to store the length of data. The embedding data rate is variable
- The generated random keys used in encrypting the patient data and embedding it into patient's image increases the cost and the complexity of the system since it depends on exponential mathematical operations.

Acknowledgment

The authors are grateful to the applied science private university, Amman-Jordan, for the full financial support granted to cover the publication fee of this research article.

References

[1] M. Mahajan, and A. Sharma, Steganography in Colored Images Using Information Reflector with 2k Correction, International Journal of Computer Applications (0975 – 8887), Vol. 1, No. 1, 2010. Available at: http://www.ijcaonline.org/journal/number1/pxc387130.pdf

[2] S. Natanj, and S. R. Taghizadeh, Current Steganography Approaches: A survey, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 1, Issue 1, PP. 836-842, Dec. 2011.

[3] S. Venkatraman, A. Abraham, and M. Paprzycki, Significance of Steganography on Data Security, International Conference on Information Technology: Coding and Computing (ITCC'04), Las Vegas, Vol. 2, 5-7 April 2004.

[4] R. K. Nithya, C. Palaninehru, and T. Balas Ubramaniam., Optimal Pixel Adjustment Based Reversible Steganography, (IJITR) International Journal of Innovative Technology and Research, Vol. No.2, Issue No. 3, April–May 2014, PP. 963–966.
Available at: http://www.ijitr.com/index.php/ojs/article/viewFile/314/pdf

[5] G. S. Sravanthim B. Sunitha Devi, S. M. Riyazoddin and M. Janga Reddy, A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method, Global journal of computers Science and Technology Graphics & Vision, Vol. 12, Issue 15, Version 1.0, 2012.

[6] P. Jajoo, S. Sharma, A. Bhadu, and V. Sharma, Hiding Information By Using Image Steganography, 3rd International Conference on Machine Learning and Computing (ICMLC 2011), Singapore, 26-28 Feb 2011, Vol. 4, PP. 70-74, 2011.

[7] M. Juneja, P. S. Sandhu, A New Approach for Information Hiding in Color Images using Adaptive Steganography and Hybrid Feature Detection with Improved PSNR and Capacity, International Journal of Engineering and Technology (IJET), Vol 5, No 2, PP. 1853- 1862, Apr-May 2013.

[8] H. Reddy, K. Raja, Steganography based on Adaptive Embedding of Encrypted Payload in Wavelet domain, International Journal of Scientific & Engineering Research, Volume 3, Issue 8, August-2012.

[9] A. Almohammad, G. Ghinea, and R. M. Hierons, JPEG Steganography: A Performance Evaluation of Quantization Tables, 2009 International Conference on Advanced Information Networking and Applications, 26-29 May 2009, Bradford, PP. 471- 478.

[10] S. Gupta and R. Biswas, A Performance Evaluation of JPEG Steganography Techniques, International Journal of Computer Science and its Applications, Mar. 2013, PP. 1-8

[11] S. M. Thampi, Information Hiding Techniques: A Tutorial Review, ISTE-STTP on Network Security & Cryptography, LBSCE, PP. 1-19m 2004

[12] R. Kefa, Steganography - The Art of Hiding Data, Department of Physics, Eastern Mediterranean University, Mersin, 2004.

[13] A. A. Gutub, Pixel Indicator Technique for RGB Image Steganography, Journal of Emerging Technologies in Web Intelligence, Vol. 2, No. 1, Feb. 2010.

[14] Yung-Chen Chou, Chin-Chen Chang, Kuan-Ming Li ," A Large Payload Data Embedding Technique for Color Images", Fundamenta Informaticae, Vol. 88, No. 1-2, PP.47-61, 2008.

[15] M. K. Meena, S. Kumar, N.h Gupt, Image Steganography tool using Adaptive Encoding Approach to maximize Image hiding capacity, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-2, May 2011.

[16] W. W. Zin, Message Embedding in PNG File Using LSB Steganographic Technique, International Journal of Science and Research (IJSR), Volume 2 Issue 1, PP. 227-230, January 2013. Available at: http://www.ijsr.net/archive/v2i1/IJSR13010217.pdf

[17] O. A. Rawashdeh, N. A. Al-Saiyd, A Novel Approach for Integrating Image Steganography and Encryption, International Journal of computer Technologies and Applications (IJCTA), Volume 5, Issue 6, November-December 2014, PP. 1917-1923, 2014. Available at: http://www.ijcta.com/documents/volumes/vol5issue6/ijcta2014050614.pdf

[18] G. R. Manjula1 and AjitDanti, A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography In Spatial Domain, International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015. https://arxiv.org/ftp/arxiv/papers/1503/1503.03674.pdf

[19] M. Bellare, A. Boldyreva and S. Micali, Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, , Vol. 1807, PP. 259-274, 2000.

[20] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, (2000), “Introduction to information hiding” Proceedings of the IEEE, special issue on protection of multimedia content, Vol. 87, 7, PP. 1062-1078, July 1999.

[21] S. Dandapat, J. Xu, O. Chutatape and S. M. Krishnan , Wavelet Transform Domain Data Embedding In A Medical Image, Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. February 2004, PP. 1541-1544, 2004. DOI: 10.1109/IEMBS.2004.1403471

[22] S. Miaou, C. Hsu, Y. Tsai, H. Chao, A Secure Data Hiding Technique With Heterogeneous Data-Combining Capability For Electronic Patient Records, in: Proceedings of the IEEE 22nd Annual EMBS International Conference, Chicago, USA, July 23–28, 2000, pp. 280–283, 2000.

[23] Y. Li, C. Li, C. Wei, PROTECTION OF MAMMOGRAMS USING BLIND STEGANOGRAPHY AND WATERMARKING, in Proceedings of the IEEE International Symposium on Information Assurance and Security- IAS 2007, pp. 496–499, 2007.

[24] P. Jajoo, S. Sharma, A. Bhadu, and V. Sharma, Hiding Information By Using Image Steganography, 3rd International Conference on Machine Learning and Computing (ICMLC 2011), Singapore, 26-28 Feb 2011, Vol. 4, PP. 70-74.

[25] M. Xiu-ying and L. Jia-jun, HVS-Based Imperceptibility Evaluation for Steganography, P. Mueller, J.-N. Cao, and C.-L. Wang (Eds.): Infscale, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), Volume 18, pp 152-161, 2009.

[26] V. Gupta, G. Singh, and R. Gupta, Advance Cryptography Algorithm for Improving Data Security, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 1, Jan. 2012.

[27] K. H. Rosen, Elementary Number Theory and Its Applications, 6th Ed., Addison-Wesly, 2011.

[28] M. H. Hassan, S. A. M. Gilani, A Fragile Watermarking Scheme for Color Image Authentication, Proceedings of World Academy of Science, Engineering and Technology, pp. 312–316, 2006.

Dr. Nedhal A. Al-Saiyd. She got her B.Sc. degree in Computer Science from University of Mosul-Iraq in 1981, M.Sc. and PhD degrees from University of Technology, Baghdad-Iraq in 1989 and 2000 respectively. She is an Associate Prof. at Computer Science Dept., Faculty of Information Technology, in Applied Science University, Amman, Jordan. She has got more than 25 years of teaching experience. She has published several papers in major international journals and peer-reviewed international conference proceedings. Her research interests include: Software Engineering, Ontology Engineering, Intelligent Systems, User Authentication, Security, Image Processing and Speech Processing