INTERNATIONAL JOURNAL OF RECENT TRENDS IN ENGINEERING & RESEARCH
Impact Factor 4.101 ISSN -2455-1457
RECENT ADVANCES IN ELECTRONICS & COMMUNICATION ENGINEERING (RAECE-2K17)

Enhancement Of Better Image Detection Using Encryption And Decryption Techniques

D HARSHINI
STUDENT, ECE Department
Nalla Narasimha Reddy Educational Society's
Group of Institutions

G MAMATHA
STUDENT, ECE Department
Nalla Narasimha Reddy Educational Society's
Group of Institutions

Abstract—Steganography is the discipline of invisible communication by hiding the exchanged secret information (message) in another digital information media (image, video or audio). The existence of the message is kept indiscernible in sense that no one, other than the intended recipient, suspects the existence of the message. The majority of steganography techniques are implemented either in spatial domain or in frequency domain of the digital images while the embedded information can be in the form of plain or cipher message. Medical image steganography is classified as a distinctive case of image steganography in such a way that both the image and the embedded information have special requirements such as achieving utmost clarity reading of the medical images and the embedded messages. There is a contention between the amount of hidden information and the caused detectable distortion of image. The current paper studies the degradation of the medical image when undergoes the steganography process in the frequency domain.

Index Terms—Medical image, Steganography, Cryptography, Symmetric, Asymmetric, Encryption, Decryption, RSA.

I. INTRODUCTION

At the time being, there are many techniques that use either cryptography, steganography or both in order to exchange information securely by keeping the contents of the message and its existence secret. Confidentiality and integrity of information are achieved through steganography and cryptography modern protocols. Cryptography is, primarily, the study of converting a piece of information from its traditional form to an incomprehensible format keeping it unreadable without secret knowledge. At the time being, the encryption techniques represent a major issue in computer networks to keep important information secret and prevent illegal user from disclosing it [1-3]. In such way, the intended legitimate recipient can reveal the contents of the message by applying a counterpart decryption technique and using permitted secret keys. The secret keys can be exclusively exchanged between transmitter and receiver. Steganography differs from cryptography in that where cryptography discipline is the art of developing and implementing algorithms of the encryption and decryption of the stored or transmitted information, steganography is the art of writing and transmitting hidden messages in an invisible form. In such way, there is no one other than the intended users can suspect the existence of the message.

Steganography and steganalysis are two contending consorts. Steganalysis is the discipline of challenging that is in endless confronting with the security of steganography methods. The challenging problem in steganalysis is in detecting the existence of the secret message in carrier (i.e. cover image) [4]. The ability of steganalysis method depends on the payload or amount of hidden message relative to the size of the cover image. Hence, this fact imposes an upper incapacitating bound limit for embedding information. If the size of hidden data is less than the upper bound, one may ensure that the carrier is safe and the known statistical analysis methods cannot detect it. Therefore, a tradeoff between the hiding payload of a cover image and the detectability and consequently, quality of a stego-image is the main problem in steganographic schemes. Capacity, security, and robustness are different affecting aspects of steganography trinity and they are in endless battle with each other. Capacity is defined as the amount of information that can be hidden in the cover image. Steganographed medical image should achieve utmost clinical reading clarity with minimum perceptual difference compared to its original counterpart.

The current paper presents a combined implementation of both the steganography and cryptography methods to embed and hide a secret information within an image. The paper studies the degradation of the medical image when undergoes the steganography process in the frequency domain looking for the more appropriate location to hide the encrypted message.

There are several cryptography encryption techniques can be employed for this purpose. RC4 encryption technique will be applied for encryption and decryption of information for its simplicity and speed in software. Two steganography techniques will be applied for comparison purpose: the first one is the well know Least Significant Bit (LSB) technique in the spatial domain and

the other is the Discrete Fourier Transform (DFT) technique in the frequency domain. The capacity of the hidden information will be studied in the different cases as well.

This paper is organized as follows. In Section 2, a brief review is about RC4 method as one of the cryptography techniques [1-8]. In Section 3, an overview of the proposed integrated cryptography and steganography implementation is presented. Experimental results are shown in Section 4 and conclusions will be discussed in Section 5.

The main block diagram of the developed system is shown in Fig.1, where both the plain message and cover image are loaded and provided as input to the system. The plain message is encrypted using one of the encryption algorithms yielding the cipher message. Both the cover image and the cipher messages will be provided as input to one of the steganography algorithms (either spatial or frequency domain). The generated stego-image will be transmitted to the receiver where the cipher message is extracted from the stego-image and hence decrypted yielding the plain message.

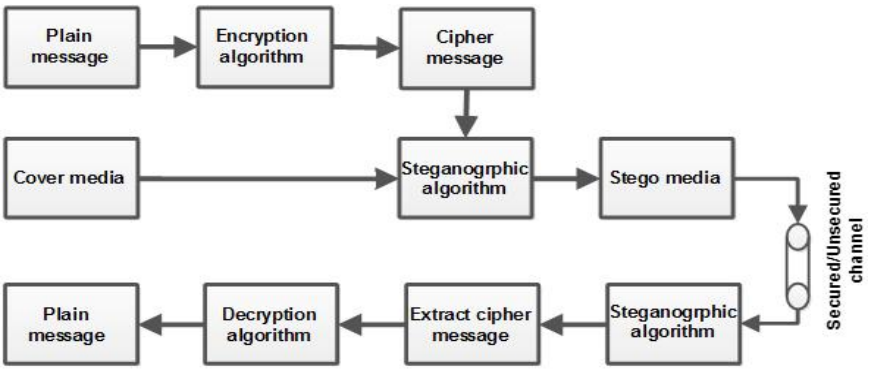


Fig.1. The Main Block Diagram of the Developed System

II. RC4 CRYPTOGRAPHY

Cryptosystems are often described as the computer programs or algorithms based on mathematical procedures. It is primarily, the study of converting a piece of information from its traditional form (plain information) to an incomprehensible format (cipher information) achieving the confidentiality and unreadability of the transmitted or stored information. As general, cryptographic systems can be classified into two main subcategories:

1- Secret-key (Symmetric) cryptosystems (Fig.2) [9,10]. This category utilizes only a unique key (i.e., a password) exchanged between the sender and receiver to encrypt and decrypt data respectively. ciphers or stream ciphers. The block ciphers algorithms handles and process the plain message in groups or blocks. Examples of block ciphers algorithms are Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. On the other side, the stream ciphers algorithms handles and process a single bit at a time as in RC4 cipher algorithm.

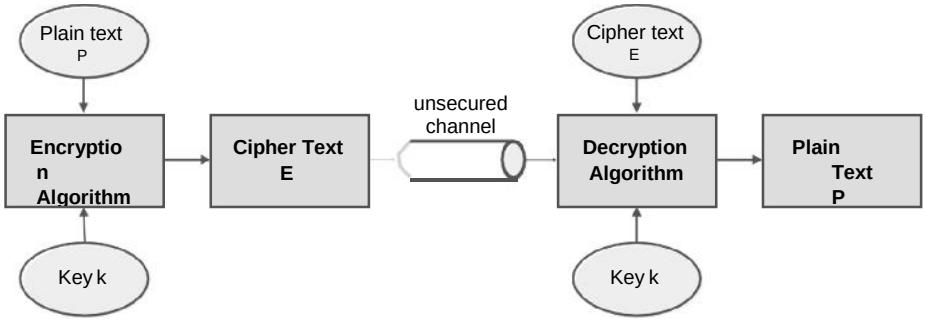


Fig.2. The Block Diagram of the Symmetric Cryptosystem

2- Public-key (Asymmetric) cryptosystems [10,11]. Asymmetric key encryption method generates and employees two different keys; private key (only known to the recipient of messages) and public key (known to everyone). Both private and public keys are mathematically related and the private one is used for encryption while the public key is dedicated for decryption process. RSA, Rabin and ElGamal are examples of public-key cryptosystems

According to the type of encryption operations, cryptographic system can be characterized by [11-16]:

1- Substitution: Each character of the plaintext is replaced or substituted by other character according to a particular substitution algorithm.
2- Transposition: In this technique, the characters of the

plaintext are rearranged forming the cipher text according to predefined permutation table.

3- Product: Where the previous two methods are combined together to generate the cipher text.

Historically, RC4 [8] was designed by Ron and it became the base for designing of some commonly used encryption protocols and standards, such as WEP and WPA [5,6,7]. RC4 is based on generating a pseudorandom stream of bits (a keystream) which can be used in both encryption and decryption processes by combining it with the plaintext using bit-wise exclusive-or. The key-stream is generated by making use of a secret internal state, which consists of two parts (as shown in Fig.3):

a- A table or string of 256 bytes (denoted as —S‖) where all the 256 possible bytes are permutated.

b- Two 8-bit index-pointers (denoted "i" and "j").

The permutation is initialized (as shown in List-1) with a variable length key, typically between 40 and 256 bits, using the key-scheduling algorithm (KSA) while another algorithm named pseudo random generation algorithm (PRGA) is utilized to generate the stream of bits.

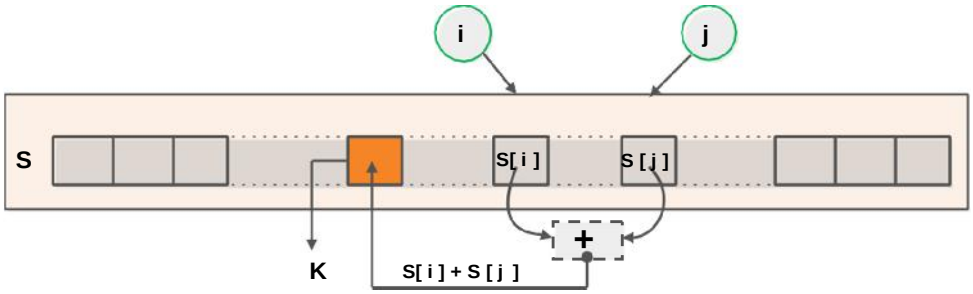


Fig.3. Pseudo-random Generation Algorithm (PRGA)

A. *Key-scheduling algorithm (KSA)*

The key-scheduling algorithm is responsible of initializing the permutation in the array "S". The term "keylength‖ refers to the number of bytes in the key where it varies from 1 to 256. First, the array "S" is initialized to the identity permutation and S is then undergone more processing of 256 iterations in a similar way to the main PRGA, except that it also simultaneously mixes in contents of the key.

List-1: RC4 initialization

```
i := 0
j := 0
while GeneratingOutput:
   i := (i + 1) mod 256
   j := (j + S[i]) mod 256
   swap values of S[i] and S[j]
   K := S[(S[i] + S[j]) mod 256]
   output K
endwhile
```

B. *Pseudo-random generation algorithm (PRGA)*

According to number of required iterations, the PRGA updates the state and a byte of the key stream is generated. In each iteration, the following steps are performed:

- The PRGA increments *i*, looks up the i^{th} element of S(i) and j^{th} of S(j),
- Adding S(i) and S(j) and then, swaps the values of S(i) and S(j),
- Getting modulo 256 of the sum S(i) + S(j) and use the result as an index to fetch a third element of S; i.e. S(S(i) + S(j)),
- The obtained value is then bitwise exclusive OR'ed with the next byte of the message yielding the next byte of the ciphertext (or plaintext).
- Each element of S is then swapped with another element at rate at least one swaping every 256 iterations.

C. *RC4 Cipher: Encryption*

The RC4 encryption algorithm uses variable length key and its length ranges from 1 to 256 bytes. A state table of 256 bytes is used and initialized by the key. This key is then used to initialize a 256-byte state table, which is later used for subsequent generation of pseudo-random bytes. The state table is then used to generate a pseudo-random stream which is bitwise exclusive XORed with the plaintext yielding the ciphertext. Each element in the state table is swapped with another element at least once.

The cipher internal state consists mainly of:

– A 256-byte array S, which contains a permutation of 0 to 255, and accordingly the total number of possible states is 256!
– Two indexes: i, j

The pseudo code of RC4 encryption algorithm is shown in List-2.

List-2: RC4 encryption

```
for i from 0 to 255
  S[i] := i
endfor
j := 0
for i from 0 to 255
  j:= (j + S[i] + key[i mod keylength]) mod 256
  swap values of S[i] and S[j]
endfor
```

III. STEGANOGRAPHY

Steganography is the discipline of hiding information into another digital information media (image, video or audio) in such a way that no one other than the sender and intended recipient suspects or realizes that there is hidden secret message within the transmitted media (Fig.4). Digital images are the most common media for hiding information and image steganography can be classified as [12-17]:

- Spatial domain steganography: where the bits of secret message directly replace some or all of the least significant bits (LSB) of the cover image pixels. This method is simple and straightforward but secret data can be easily disclosed by extracting whole LSB plane.
- Frequency domain steganography: the cover image is transformed (decomposed) using DCT or DFT to the frequency domain coefficients prior to embedding the secret message. The stego-image is transformed again to the spatial domain to be transmitted in an unsecured channel. The intended recipient then inversely transforms it again to the frequency domain to retrieve the secret message. One of the frequency domain transformations can be applied in this method such as: Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) or Discrete Fractional Fourier transform (DFrFT).
- Adaptive steganography: it is a special case of the two previous methods and is defined as the mechanism of choosing the amount of the bits for hiding according to the characteristics of the human visual system (HVS).

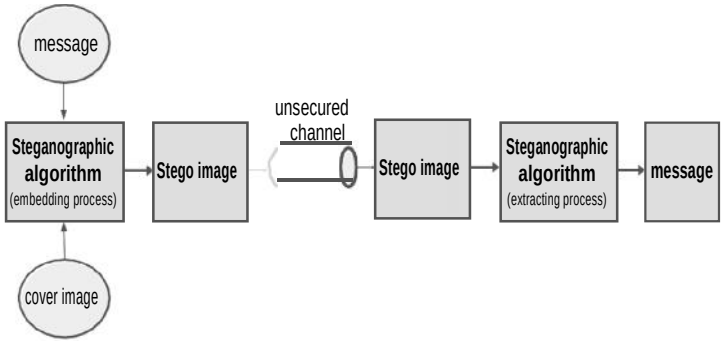


Fig.4. The Block Diagram of the Steganographic System

the cover. The Discrete Fourier Transform (DFT) will be image in the frequency domain by decomposing it into its sinusoidal (sine and cosine) fundamental components in different frequencies. The number of yielded frequencies corresponding to the number of pixels of the image in the spatial domain and in the frequency domain are of the same size. Given a 2D discrete function g(u,v) defined on M x N grid, the Discrete Fourier Transform is defined as:

Using transform-domain techniques, it is possible to embed a secret message (low amplitude signal with low bandwidth) more securely in different frequency bands of a medium that presents a much larger bandwidth called the cover. The Discrete Fourier Transform (DFT) will be considered in this paper while the another transforms can be applied as well.

The process for embedding the cipher message within the frequency domain of the digital image is illustrated in List-3.

$$G(m,n) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} g(u,v) e^{-i2\pi \frac{mu}{M}} . e^{-i2\pi \frac{nv}{N}} = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} g(u,v) e^{-i2\pi \left(\frac{mu}{M} + \frac{nv}{N}\right)} \quad (1)$$

The plain message is encrypted using RC4 encryption method and the image is transferred into the discrete Fourier domain prior to transferring the image again into the spatial domain to be transmitted.

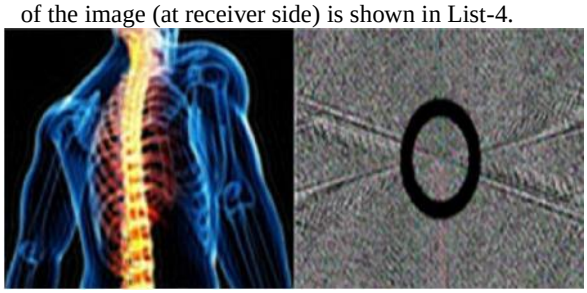
$$g(u,v) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} G(m,n) e^{-i2\pi \frac{mu}{M}} . e^{-i2\pi \frac{nv}{N}} = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} G(m,n) e^{-i2\pi \left(\frac{mu}{M} + \frac{nv}{N}\right)} \quad (2)$$

List-3: Hiding cipher message in the frequency domain of

the image (at transmitter side)

- Load the cipher or plain message
- Load the image data.
- Transfer the image into the frequency domain
- Select the frequency band with as size as that of the cipher message and replace it with the message
- Transfer the image data (in frequency domain) back into the spatial domain
- Transmit the image in secured/unsecured communication channel

When the image containing the encrypted message is received, it is transferred to the frequency domain and the cipher message is extracted. The cipher message is then decrypted yielding the original message. The process of extracting the cipher message from the frequency domain of the image (at receiver side) is shown in List-4.



List-4: Extracting cipher message from the frequency domain of the image (at receiver side)

- Load the received (stego) image
- Transfer the image into the frequency domain
- Select the frequency band and extract the cipher message.
- Decrypt the cipher message using RC4 decryption algorithm yielding the plain message.

IV. Experimental Results and Comparisons

In this section, several experiments are carried out on a selected color image to hide an encrypted message within the frequency domain of the image. The plain, and accordingly the cipher message, is of fixed length (~19 Kbyte). The plain message is encrypted using RC4 method. The selected image is transferred to the frequency domain using Discrete Fourier Transform (DFT). A circular slip of the frequency domain data with area equals that of the cipher message is selected to embed the cipher message where every digit within the circular slip is replaced with a character of the cipher message. The location of the circular slip is initially chosen at the center of the frequency domain area and gradually moved far from the center. The frequency domain, containing the embedded cipher message, is then transferred back to the spatial domain to be transmitted in secure (or unsecured) channel. The same procedure is performed again with a rectangular shape slip instead of the circular one. The original image (plain image) is shown in Fig.5 while the yielded image in frequency domains beside the frequency domain

Fig.5. The Original Medical Image

The assessment of yielded color image quality is a necessary procedure. PSNR is used as performance parameter to assess the ratio between the signal and noise in different cases. PSNR can be defined via the mean squared error (*MSE*). Given an original image (noise-free) *m*×*n* image*I* and its noisy approximation *K*, *MSE* is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (3)$$

$$PSNR = 10\,log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20\,log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \qquad (4)$$

figure are shown in Fig.6. The location of the circular slip (and the rectangle one) is gradually varied faring from the center of the frequency domain shape. The original image has dimensions of 427x259 pixels and the embedded text is 19 KB length.

Where, MAX_I is the maximum possible pixel value of the image. The noise her is the embedded data. The relation between the location of the circular (rectangle) slip where the cipher message is embedded and the PSNR is shown in Fig.7. It is noticed that the signal to noise ratio (PSNR) increases with the moving of the circular (rectangle) slip far from the center. Moreover, the PSNR has a higher value in the rectangular slip shape compared with circular one.

V. Conclusion

In this paper, a proposed method has been introduced where one of the cryptography algorithms and another steganography algorithm have been combined together to embed an amount of secret data within a cover image in the frequency domain. There is a contention between the amount of hidden information and the caused detectable

distortion in the image. The embedded data is considered as noise and attenuates the frequency bands of the cover image. The current paper studied the degradation of the medical image when undergoes the steganography process in the frequency domain. The secret message is embedded separately in different bands of the image's frequency domain starting from the DC up to the maximum frequency. It has been found that the quality of the image is extremely degraded when embedding data close to the low frequency bands (DC) and this effect decreases in the upper frequency bands. A strip of the frequency domain is selected to embed the data, and this strip took one of two shapes, either circular or rectangular one. The peak signal to noise ratio (PSNR), the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation, is used as a measuring metric to assess the quality of the image in both cases. It is found that PSNR value is improved when the rectangular strip shape is used compared to the circular one. Accordingly, it is preferable when it is required to embed data within an image in the frequency domain, to embed the cipher text in higher frequency bands in rectangular strip.

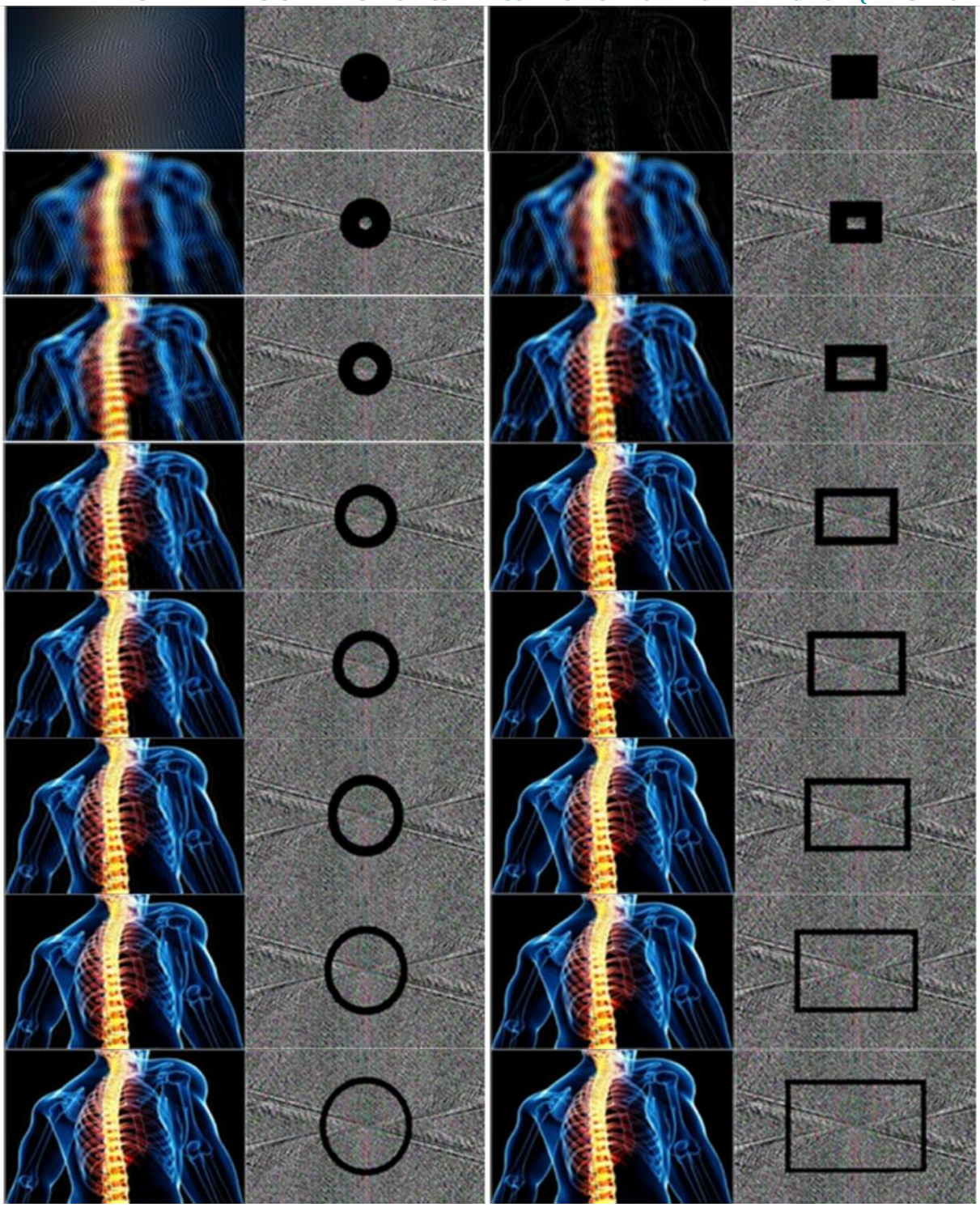


Fig.6. (part2): Degradation of the Stego-image Depending on the Location of the Embedding Process within the Different Frequency Bands

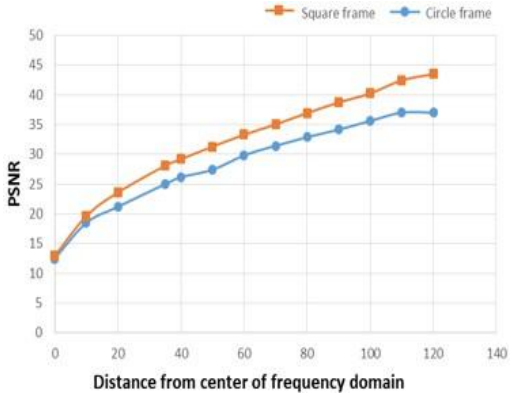


Fig.7. Relation between the Location of the Circular (Or Rectangular) Slip and PSNR

REFERENCES

[1] Jingli Zheng, Zhengbing Hu, Chuiwei Lu, –A Light-weight Symmetric Encryption Algorithm Based on Feistel Cryptosystem Structure‖, IJCNIS, Vol. 7, No. 1, December 2014, pp. 16-23.

[2] Mamta. Juneja, and Parvinder S. Sandhu, –A Review of Cryptography Techniques and Implementation of AES for Images‖, International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 1, Issue 4 (2013) ISSN 2320-401X; EISSN 2320-4028.

[3] Koumal Kaushik and Suman, –An Innovative Approach for Video Steganography‖, IJCNIS, Vol. 7, No. 11, October 2015, pp. 72-79.

[4] R.Gnanajeyaraman, K.Prasadh , Dr.Ramar, Audio encryption using higher dimensional chaotic map, International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.

[5] Sheetal Sharma and Lucknesh Kumar, Encryption of an Audio File on Lower Frequency Band for Secure Communication, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013 ISSN: 2277 128X

[6] Ali M. Meligy, Mohammed M. Nasef, Fatma T. Eid, –An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys‖, IJCNIS Vol. 7, No. 7, June 2015, pp. 24-29.

[7] M.I.Khalil, Real-Time Encryption/Decryption of Audio Signal‖, I. J. Computer Network and Information Security, 2016, 2, 25-31, DOI: 10.5815/ijcnis.2016.02.03.

[8] Fluhrer, S., Mantin, I. and Shamir, A. –Weaknesses in the key scheduling algorithm of RC4‖ Eighth Annual Workshop on Selected Areas in Cryptography (August 2001)

[9] Matthews, Jr., Donald P. –System and method for a fast hardware implementation of RC4‖ Compaq Computer Corporation , November 23, 1998 US Patent 6,549,622

[10] Allam Mousa (1) and Ahmad Hamad, –Evaluation of the RC4 Algorithm for Data Encryption‖, International Journal of Computer Science &Applications, Vol. 3. No.2, June 2006.

[11] Habutsu T., Nishio Y., Sasase I., and Morio S., –A secret key cryptosystem by iterating chaotic map,‖ Lect. Notes comput. Sci, Advances in Cryptology-EuroCrypt'91, 1991, vol. 547, page(s): 127-140.

[12] Pichler F. and Scharinger J., –Finite dimensional generalized baker dynamical systems for cryptographic applications,‖ Lect. Notes in Comput. Sci, 1996, vol. 1030, pp. 465-476.

[13] T. ElGamal, –A prublic key cryptosystem and a signature scheme based on discrete logarithms‖, in Advances in Cryptology (CRYPTO '84), Springer, 1985, vol. 196, pp. 10–18.

[14] Ueli Maurer and Björn Tackmann, –On the Soundness of Authenticate-then-Encrypt: Formalizing the Malleability of Symmetric Encryption‖, Proceedings of the 17th ACM Conference on Computer and Communication Security, ACM, pp. 505–515, Oct 2010.

[15] Ueli Maurer and Stefano Tessaro, Basing {PRF}s on Constant-Query Weak {PRF}s: Minimizing Assumptions for Efficient Symmetric Cryptography Advances in Cryptology — ASIACRYPT 2008, Lecture Notes in Computer Science, Springer-Verlag, vol. 5350, pp. 161–178, Dec 2008.

[16] Thiruppathy Kesavan, V, –Secret Key Cryptography based Security Approach for Wireless Sensor Networks‖, Recent Advances in Computing and Software Systems (RACSS), 2012 International Conference, IEEE.

[17] Anupam Mondal and Shiladitya Pujari, –A Novel Approach of Image Based Steganography Using Pseudorandom Sequence Generator Function and DCT Coefficients‖, IJCNIS Vol. 7, No. 3, February 2015 pp.42-49.