Using Quaternion Fourier Transform in Steganography Systems

M.I.Khalil

Princess Norah Bent Abdurrahman University, Faculty of Computer and Information Sciences, Information Technology (networks) Department, Riyadh, Kingdom of Saudi Arabia

***Abstract*:** steganography is the discipline of exchanging information messages in such way that no one, other than the intended recipient, suspects the existence of the message. The transmitted message can be in textual or multimedia form (audio, image or video) and can be hidden within cover media. Moreover, the hidden message can be in either plain or cipher form. In steganography, the majority of hiding techniques are implemented either in spatial domain or in frequency domain of the cover media. The current contribution introduces a new a steganography technique for hiding a textual message within a cover image. Both the message and the cover image is converted to quaternion form and then only the quaternion message is converted to the frequency domain using Quaternion Fast Fourier Discrete Transform (QFFDT) technique. Simple quaternion mathematics are used to combine the message (in quaternion frequency domain) within the cover image (in quaternion form). Conversely, the hidden message can be revealed at the receiver using simple quaternion mathematics in presence of the original cover image. The proposed method allows hiding a huge amount of data and it is much complicated against steganalysis compared to the traditional methods. The method is assessed using the known performance metrics and the obtained results show that it is robust and more secure against steganalysis attacks without affecting the consumed bandwidth of the communication channel.

***Keywords*:** Quaternions, Steganography, Fourier Transform, Cryptography.

1. Introduction

Security of data and its confidentiality is essential today because of cybercrime, which is highly increased day by day. The key concept behind steganography [1,2] is that the message to be transmitted is hidden within another one (cover media) so that the presence of the hidden message is indiscernible and no one, other than the intended recipient, suspects the existence of the message. In steganography, the majority of hiding techniques are implemented either in spatial domain or in frequency domain to hide information messages. The embedded information can be either plain or cipher message. The plain message can be in textual, audio or image form and can be converted to the cipher form using one of the cryptography techniques. Cryptography [3] is primarily the discipline of converting a piece of information from its traditional form to an unintelligible form keeping it unreadable without secret knowledge. Cryptographic algorithm, also called a cipher, often rely on mathematical function used for encryption or decryption. In most cases, two related functions are employed, one for encryption and the other for decryption. Either cryptography, steganography or both can be applied to achieve privacy and confidentiality of information and keeping its existence secret.

Steganography discipline differs from cryptography in that, while cryptography is the practice of developing and implementing algorithms of the encryption and decryption [4] of the stored or transmitted information, steganography is the discipline of embedding and transmitting messages in an invisible form so that there is no one other than the intended users can suspect the existence of the message.

Steganography and steganalysis [1-4] are two contending consorts. Steganalysis is the discipline of challenging that is in endless confronting with the steganography methods. The challenging problem in steganalysis is in detecting the existence of the secret message in carrier (i.e. cover image). The ability of steganalysis method to detect messages hidden depends on the payload or amount of hidden message relative to the size of the cover media. 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 the message hidden within it. Therefore, a tradeoff between the hiding payload of a cover image and the detectability and consequently, quality of a stego-image. Capacity, security, and robustness are different affecting aspects of steganography trinity [5] 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 without overriding the upper bound. In some cases, hidden message can cause undesirable distortion of the cover media. In such a way, steganographed medical image, for instance, should achieve utmost clinical reading clarity with minimum perceptual difference compared to its original counterpart.

In cryptography, the systematic way of metamorphosing a piece of information into the undecipherable format is known as encryption, while converting it back to its original form is called decryption. The study and developing of algorithms to reveal the ciphered message without the access of key that is used for decrypting a particular message is known as cryptanalysis. Cryptographic algorithms can be classified according to several criteria and the essential one is that who is based on the number of keys that are employed for encryption and decryption. It can be categorized also according to the message as block cipher or stream cipher. A key is simply a parameter to the algorithm that allows the encryption and decryption process to take place [6].

- Symmetric key cryptography employs only one key for both encryption and decryption algorithms. Examples of symmetric algorithms are DES, 3DES (both outdated) and AES.
- Asymmetric key cryptography employs one key for

encryption and another one for decryption and are used for small block of data due to its computational complexity. RSA and PGP are examples of asymmetric cryptography algorithms.

- Hash-functions-based encryption/decryption employs mathematical transformations to irreversibly encrypt and decrypt messages. MD5 and SHA-1 are the most commonly used cryptographic hash functions.

The current paper introduces a new steganography system to hide a block of data within a digital color image. Both simple quaternion mathematics and quaternion fast Fourier transforms are employed to achieve this purpose. Hereby, both the plain message and the cover image are transformed to the quaternion form and then only the quaternion message is converted to the frequency domain using Quaternion Fast Fourier Discrete Transform (QFFDT) technique. Simple quaternion mathematics are used to combine the message (in quaternion frequency domain) within the cover image (in quaternion form). Conversely, when the intended recipient receive the image, the hidden message can be revealed using simple quaternion mathematics in presence of the original cover image. The proposed method allows hiding a huge amount of data with utmost image reading clarity with minimum perceptual difference compared to its original counterpart. The proposed algorithm makes it much complicated against steganalysis compared to the traditional methods. For instance, it overrides the defects inherent in the Least Significant Bit (LSB) insertion method [7] in terms of low rigidity against attacks and raising suspicion. The method is assessed using the known performance metrics and the obtained results show that it is robust and more secure against steganalysis attacks without affecting the consumed bandwidth of the communication channel.

This paper is organized as follows. Section II reviews some of the significant research in the field of steganography systems in both spatial domain and frequency domain. Section III illustrates the basics of quaternion mathematics. The proposed algorithm will be introduced in section IV. Section V describes the experimental framework used to evaluate the performance of the proposed method beside the obtained experimental results. The obtained results will be concluded in section VI.

2. Related work.

Digital images are the most common media for hiding information and image steganography can be classified as:

- 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).

Ki-Hyun Jung et al. have proposed semireversible data hiding method based on interpolation and LSB substitution. The interpolation method has been preprocessed before hiding the secret data for the purpose of good quality and higher capacity. Then, the LSB substitution method was applied for the embedding secret data. The cover image with the scaled down size and secret data could be extracted from the stego-image without the need of any extra information [8]. G. Raj Kumar et al., have been improved least significant bit steganalyzers by analyzing and manipulating features of the some existing least significant bit matching steganalysis techniques. They explains the LSB Embedding technique with lifting based DWT schemes by using Micro blaze Processor implemented in a FPGA using System C coding. Future work can be extended to RGB or color image processing and can be extended for video processing level also [9]. Shilpa Thakar et al, described the image steganography along with the LSB insertion method used in image Steganography. They suggested a few for future research like integrity and data capacity of cover image. Some steganographic methods need to improve security by using cryptography against attacks [10]. Gurpreet Kaur et al. have compared digital watermarking with other techniques of data hiding. Steganography, fingerprinting, cryptography and digital signature techniques are compared with watermarking. It provides ownership assertion, authentication and integrity verification, usage control and content labeling. They dedicate that all techniques of data hiding secure data with their methods, but watermarking is more capable because of its efficiency. In watermarking, they mark the information which is to be hiding. Watermarking provide us easy and efficient security solutions of digital data. Watermarking provide security of not only images, but also audio video and text [11].

Shilpa Gupta et al, has analyzed existing Least Significant Bit Algorithm and found existence of a more amount of distortion, so he proposed a new method “Enhanced Least Significant Bit (ELSB)”. The method improves the performance of the LSB method because information is hidden in only one of the three colors that is BLUE color of the carrier image. This minimizes the distortion level which is negligent to human eye [7]. Chunlin Song et al. have presented description and analysis of the recent advances in the watermarking in digital images. These techniques are classified into the several categories depending upon domain in which hidden data is inserted, size of hidden data and the requirement of which hidden data is to be extracted. The experiment shows the different effective algorithms of watermark. The result indicates frequency domain is more robustness than spatial domain. Several challenges that are often unaddressed in the literature have also been identified. Meeting these challenges is essential in advancing the current state of the art of watermarking in digital images [12]. Mariusz Dzwonkowski, et al. introduced a new quaternion-based lossless encryption technique for digital image and

communication on medicine (DICOM) images. They have scrutinized and slightly modified the concept of the DICOM network to point out the best location for the proposed encryption scheme, which significantly improves speed of DICOM images encryption in comparison with those originally embedded into DICOM advanced encryption standard and triple data encryption standard algorithms. The proposed algorithm decomposes a DICOM image into two 8-bit gray-tone images in order to perform encryption. The algorithm implements Feistel network like the scheme proposed by Sastry and Kumar. It uses special properties of quaternions to perform rotations of data sequences in 3D space for each of the cipher rounds. The images are written as Lipschitz quaternions, and modular arithmetic was implemented for operations with the quaternions [13]. Anita Pradhan, K. Raja Sekhar, and Gandharba Swain proposed a novel steganographic method based on the compression standard according to the Joint Photographic Expert Group and an Entropy Thresholding technique. The steganographic algorithm uses one public key and one private key to generate a binary sequence of pseudorandom numbers that indicate where the elements of the binary sequence of a secret message will be inserted. The insertion takes eventually place at the first seven AC coefficients in the transformed DCT domain. Before the insertion of the message the image undergoes several transformations. After the insertion the inverse transformations are applied in reverse order to the original transformations. The insertion itself takes only place if an entropy threshold of the corresponding block is satisfied and if the pseudorandom number indicates to do so. The experimental work on the validation of the algorithm consists of the calculation of the peak signal-to-noise ratio (PSNR), the difference and correlation distortion metrics, the histogram analysis, and the relative entropy, comparing the same characteristics for the cover and stego image. The proposed algorithm improves the level of imperceptibility analyzed through the PSNR values. A steganalysis experiment shows that the proposed algorithm is highly resistant against the Chi-square attack [14]. M.I.Khalil introduced a novel method for encrypting/decrypting of audio signal based on embedding the audio samples within the quaternion frequency domain of a digital image. Hereby, the selected digital image is used as a complicated key and cover for audio signal. Each sample of the audio signal is combined with the values of the three color components of a pixel fetched from the cover image yielding a quaternion number. The absolute value of this quaternion number is then transmitted and when received, the original value of the audio sample can be extracted using simple quaternion mathematics [15]. P. M. Rubesh Anand et al. used Quaternion Julia set to generate real-time based symmetric keys for cryptography. The number of iterations, complex number and control value are the determining parameters of dynamically varying quaternion Julia image structure. The considered parameters are initialized in the proposed model of symmetric key generation during the establishment of communication between hosts. The model generates variable length, dynamic, one time usable key from quaternion Julia image to encrypt or decrypt data without involving the exchange of key. The time stamp used during the initialization process makes the quaternion Julia image to be different in real-time. The instantaneous key is generated at the hosts independently in a synchronous fashion to enhance the complexity in cryptanalysis [16]. The above-mentioned manuscripts address three significant steganographic issues: tools for hiding data within image using the least significant bit method. Second is embedding data within image in the frequency domain. The last issue is encrypting and decrypting of audio samples and hiding it within image using quaternion Fourier transform.

3. Quaternions Algebra

Quaternions mathematics were discovered by Hamilton in 1843 [13] and since that time they were not embraced. A quaternion has four components, one real and three imaginary. Quaternion is a geometrical operator to represent the relationship (relative length and relative orientation) between two vectors in 3D space. They are a generalization of complex numbers and combine by the normal rules of algebra with the exception that multiplication is not commutative. The usual notation, extended from that of the complex numbers is:

$$\mathbb{H} = \{w + xi + yj + zk : w, x, y, z \in \mathbb{R}\} \quad (1)$$

Where *w*, *x*, *y* and *z* are real, and *i*, *j* and *k* are imaginary units or complex operators that obey the following rules:

$$i^2 = j^2 = k^2 = ijk = -1 \quad (2)$$

$$ij = k,\ jk = i,\ ki = j \quad (3)$$

$$ji = -k,\ kj = -i,\ ik = -j \quad (4)$$

The signs in the products of different operators $i, j\ and\ k$ are shown in Eq. 2, 3 and 4. Using our familiar vector operations, two quaternions can be multiplied. When multiplying any pair of these operators in a clockwise sequence a positive product is produced, while a negative product is produced when any pair is multiplied in anti-clockwise sequence. The quaternion conjugate is defined as:

$$\bar{q} = w - xi - yj - zk \quad \in \mathbb{H} \quad (5)$$

In addition, the modulus of a quaternion is given by:

$$\|q\| = \sqrt{q\bar{q}} = \sqrt{w^2 + x^2 + y^2 + z^2} \in \mathbb{R} \quad (6)$$

Define the real and imaginary parts of q as:

$$Re(q) = w \in \mathbb{R},$$
$$and\ Im(q) = xi + yj + zk \in \mathbb{I} \quad (7)$$

The inverse of a non-zero quaternion $q \neq \mathrm{H}$ is:

$$q^{-1} = \frac{\tilde{q}}{|q^2|} \quad (8)$$

The pure quaternion is that quaternion with zero real part while the quaternion with unit modulus is called a unit quaternion. A quaternion is also expressed as the sum of scalar **S**(q) and vector parts **V**(q):

$$q = S(q) + V(q) \quad (9)$$

Quaternion Fourier transforms have been mainly defined over $\mathbb{R}^2$ as signal domain space. This quaternion domain Fourier transform (QDFT) transforms quaternion valued signals defined over a quaternion domain (space-time or other 4D domains) from a quaternion position space to a quaternion frequency space [17]. The traditional quaternion Fourier transform (QFT) [18,19] is only defined for real or quaternion valued signals over the domain $\mathbb{R}$, while the quaternion discrete Fourier transform (QDFT) for $h \in \mathrm{H}$ can be defined, based on the concept of quaternion multiplication and exponential and non-commutative property of the quaternion multiplication , as three different types:

a) The two-sided DQFT:

$$F_{L-R}(u,v) = \frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} e^{-\mu 2\pi\frac{xu}{M}} f(x,y) e^{-\mu 2\pi\frac{vy}{N}} \quad (10)$$

b) The left-sided DQFT:

$$F_L(u,v) = \frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} e^{-\mu 2\pi\left(\frac{xu}{M}+\frac{vy}{N}\right)} f(x,y) \quad (11)$$

c) The right-sided DQFT:

$$F_R(u,v) = \frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\ e^{-\mu 2\pi\left(\frac{xu}{M}+\frac{vy}{N}\right)} \quad (12)$$

μ is any unit pure quaternion.

$$F_f^{-q}\left[F_f^q\right](m,n) = f(m,n) = \frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F_f^q(u,v) e^{\mu 2\pi\left(\frac{mu}{M}+\frac{nv}{N}\right)} \quad (13)$$

Due to its important properties, quaternion discrete Fourier transform (QDFT), its counterparts quaternion discrete cosine transform (QDCT) and quaternion wavelet transform have been widely used and applied to both single and two dimensional signals in the fields of image processing, radar, robotics and cryptographic.

4. The Proposed System

In terms of development, the proposed steganography system is comprised of two algorithms, one for embedding the textual message and one for extracting it. The embedding process is concerned with hiding a secret textual message within a cover image, and is the most carefully constructed process of the two. A great deal of attention is paid against steganalysis to ensuring that the secret message goes unnoticed if a third party were to intercept the cover image. The extracting process is a much simpler process, where the secret message is revealed at the end.

4.1 The Embedding Process

The block diagram of the entire embedding process of steganography is presented in Fig.1. Traditionally, two inputs are required for embedding process. One is secret message that usually an image, audio, or text file that contains the message for transform, text message will be considered in the proposed algorithm. And cover image is used to be the stego media or a stegogramme that contains a secret message. The input image is copped to be square image with both width *w* and height *h* equal the maximum of the original width and height of the input image and is called stego image. The maximum length of the secret message that can be embedded $L = h\,w = h^2 = w_2$.

The pixels of the stego image are decomposed into its *R*, *G* and *B* (red, green and blue) components whose values are used to create a square array of quaternion numbers Q_A with zero-real part:

$$Q_A = 0w + Ri + Gj + Bk \quad (14)$$

A secret message with length ≤ L is acquired as a string, and the value of each character *c* of this string is used to set the real part of a quaternion number of array Q_S:

$$Q_S = cw + 0i + 0j + 0k \quad (15)$$

From Equation 14, the quaternion Fourier transform of Q_S is computed as:

$$Q_B = QFFT(Q_S) = mw + xi + xj + xk \quad (16)$$

The magnitude of three vector components of the yielded Q_B are equal and it is a quaternion property: when the magnitude of the three vector components of a quaternion number are zeros, so the yielded quaternion Fourier transform of such input is in the form shown in Eq.(16). This is a significant property and much helper in constructing the embedding process, where it is possible to use only two components of the quaternion Q_B : *m* and *x*.

The next step is to embed the secret message Q_B (in the quaternion frequency domain) inside the stego image Q_A (in the quaternion form). To ensuring that the secret message goes unnoticed, a very small ratio of Q_B is added to a very high ratio of Q_A. Two ratios α and γ, will be used for this purpose and it is assumed that $\alpha + \gamma \cong 1$. For such a way, the very small ratio = γ = 1/256, and the very high ratio = α = 255/256 will be used to construct the stego image as following:

Using Equations 14 and 16,

$$Q_T = \alpha(0w + Ri + Gj + Bk) + \gamma(0w + mi + xj + 0k)$$

$$Q_T = 0w + (\alpha R + \gamma m)\,i + (\alpha G + \gamma x)\,j + \alpha B \quad (17)$$

The array represents the stego image and is transmitted in secure or unsecure channel and goes unnoticed if a third party were to intercept it. The pseudo code of hiding algorithm is shown in List-1.

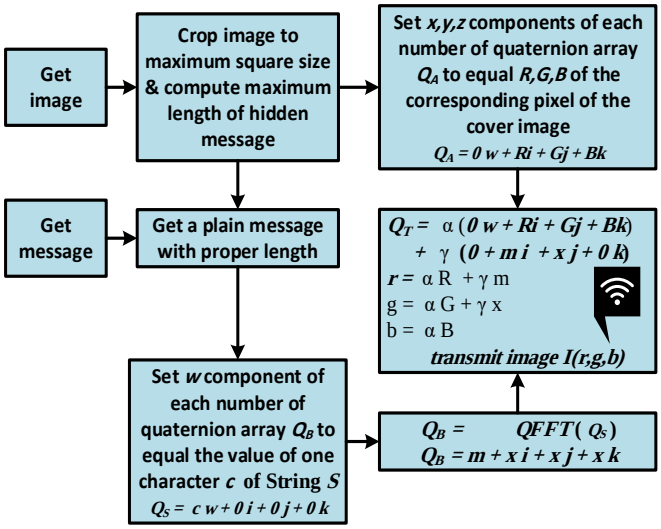

Fig.1: The block diagram of the embedding process of the proposed steganography system

List 1. Pseudo code of the hiding algorithm

```
// input α , γ
// get cover image
// get text message
// crop image to be in square dimensions
// construct quaternion array  Q_A form image pixels
for each pixel  p_{i,j}  in the frame
{
    R_{i,j}, G_{i,j}, B_{i,j}  ←  p_{i,j}
    Q_A(i,j)      ← 0 w + Rr_{i,j} i + G_{i,j} j + B_{i,j} k
}
// construct quaternion array  Q_S form secret message
for each character c_n in the secret message
{
    Q_S(i,j)  ← c_n w + 0 i + 0 j + 0 k
}
// convert  Q_S  to quaternion fast Fourier transform
Q_B       ←   QFFFT( Q_S)
Q_B (takes the form)  ≡  m w + x i + x j + x k
Q_T ← α(0w + Ri + Gj + Bk) + γ( m w + x i + x j + x k )
r  ←  α R + γ  m
g  ←  α G + γ  x
b  ←  α B
Transmit Stego image f(r,g,b)
```

4.2 The Extraction Process

The block diagram of the extraction process is shown in Fig.2. Two inputs are required for this process: one is the received image, and second is the original image.

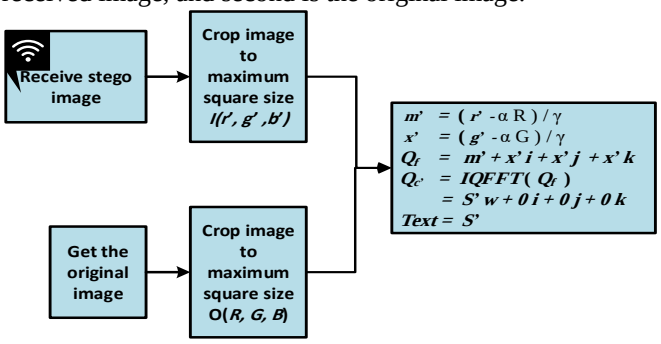

Figure 2. The block diagram of the extraction process for the proposed steganography system

As explained in the previous section, the original image is cropped and then represented as quaternion array:

$$Q_A = 0w + Ri + Gj + Bk \quad (18)$$

Similarly, the received image is cropped and the represented in the quaternion form as:

$$Q_a = 0w + r'i + g'j + b'k \quad (19)$$

Given α and γ, and using Equations 18 and 19, the secret message can be computed as:

$$m' = (r' - \alpha R) / \gamma \quad (20)$$

$$x' = (g' - \alpha G) / \gamma \quad (21)$$

$$Q_f = m' + x' i + x' j + x' k \quad (22)$$

And getting the inverse quaternion fast Fourier transform of Q_f yields:

$$Q_{c'} = IQFFT (Q_f) = S' w + 0 i + 0 j + 0 k \quad (23)$$

The extracted text message = S'

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

List 2. Pseudo code of the extraction algorithm

```
// input α, γ
// get original image I(R, G, B)
Q_A = 0w + Ri + Gj + Bk
// get received image f(r', g', b')
Q_a = 0w + r'i + g'j + b'k
m' ← ( r' - α R ) / γ
x' ← ( g' - α G ) / γ
// construct a quaternion array
Q_f ← m' + x' i + x' j + x' k
// get the inverse quaternion fast Fourier transform
Qc' ← IQFFT ( Q_f )
Q_c' (will be in the form) ≡ S' w + 0 i + 0 j + 0 k
The extracted text message = S'
```

5. Implementation and Experimental Results

A new methodology is proposed for hiding secret text message inside image. The same methodology can be applied to hide audio or image inside cover image. The proposed system is simulated using Matlab simulator. In terms of development, the proposed steganography system is comprised of two algorithms, one for embedding the textual message and one for extracting it. The embedding process is concerned with hiding a secret textual message within a cover image. The extracting process leads to revealing the secret message at the end. The mathematical quaternion functions of Matlab have been employed for representing both the image and the secret message in quaternion arrays form. Both quaternion fast Fourier transform (QFFT) and inverse quaternion fast Fourier transform (IQFFT) functions have been used for converting from spatial domain to frequency domain and inversely as well. Both of these functions yields quaternion numbers with real values. Consequently, images of type Tiff have been used in the proposed methodology because it is the unique type of images that can be represented and exchanged in the real numbers form.

Several images have been used in the test bed, to embed text messages utilizing the maximum capacity of the image. Various values for α and γ ratios have been used comparing both the embedded and extracted messages. Besides, the original cover image is compared to the transmitted one to determine to how much the difference between them is noticeable. This difference indication can be considered as a similarity metric and it 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 the message hidden within it.

The proposed algorithm is performed for the image shown in Fig.3 (Tif type, with dimensions 1419 x 1001 pixels) and text of length 125952 characters. As shown in Table-1, the ratio α is changed gradually from 0.000001 to 0.5, and consequently γ is changed from 0.999999 to 0.5. The mean squared error (MSE) is measured between the original image and the transmitted image. The relation between α and MSE is shown in Fig.4. It is clear that the difference between the original image and the transmitted one increases as α increases. The formula for MSE between two equal-in-size two images is as in Eq.25.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (24)$$

PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. PSNR (Fig.5) is most easily defined via the mean squared error.

$$PSNR = 10.log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20.log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \quad (25)$$

Where, MAX_I is the maximum possible pixel value of the image. The noise her is the embedded data.

It is found that, the transmitted image begins to be distorted with high values of α as shown in Fig.6.

Figure .3: Original image

Table-1: α, PSNR and MSE yielded results.

α	PSNR	MSE
0.000001	83.6913	4.3E-08
0.000005	69.7119	1.07E-07
0.00001	63.6913	4.27E-07
0.00005	49.7119	1.07E-05
0.0001	43.6913	4.27E-05
0.0005	29.7119	0.0011
0.001	23.6913	0.0043
0.005	9.7119	0.1069
0.01	3.6913	0.4274
0.05	-10.2881	10.6858
0.1	-16.3087	42.743
0.2	-22.3293	170.972
0.3	-25.8511	384.6871
0.4	-28.3499	683.8881
0.5	-30.2881	1068.6

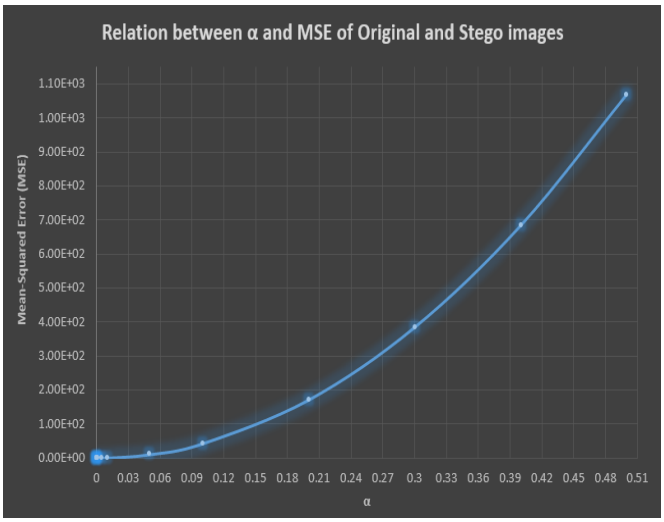

Fig.4: Relation between α and Mean Squared Error (MSE) between Original and Stego images

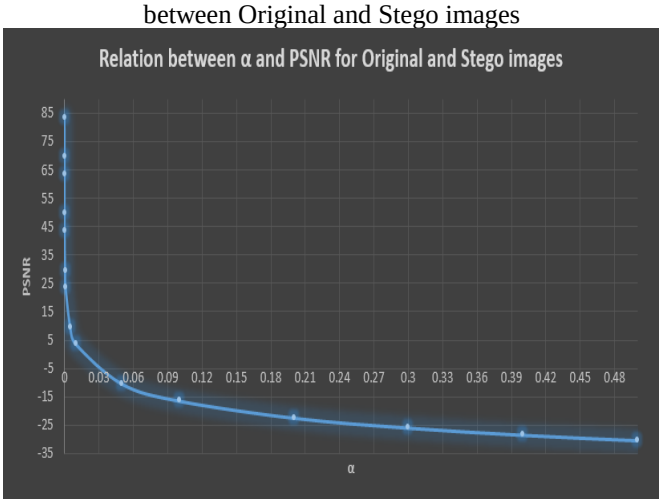

Fig.5: Relation between α and Peak Signal to Noise Ratio (PSNR) of Stego images refereed to the Original image

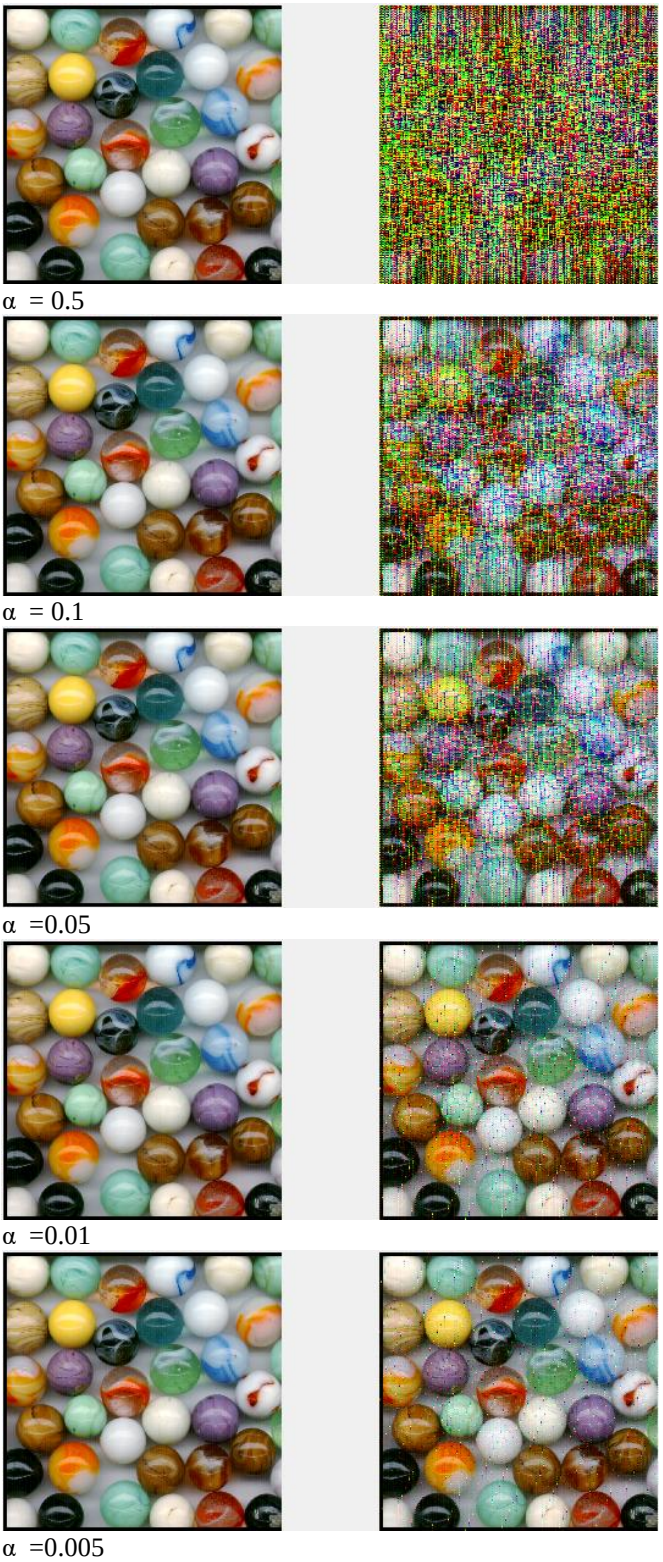

Figure .6: The transmitted images for different values of α

6. Conclusion

In the current paper, a new a steganography methodology has been introduced. Hereby, a textual message has been hidden within a cover image. The cover image is transferred to the quaternion domain space while the secret message is represented in the quaternion Fourier frequency domain before embedding it within the cover image. To be consistent with steganography demands, the stego-image is transmitted in its traditional form in such way that no one, other than the intended recipient, suspects the existence of

the message. The method is implanted and simulated using Matlab simulator. The method has been tested by applying it to various Tiff images and text files. The performance of the system is estimated by measuring both MSE and PSNR metrics. The obtained experimental results showed that cover image can be transmitted without noticeable variation. Moreover, the experimental measurements showed the possibility of embedding text messages with big size utilizing the maximum capacity of the image. When the stego-image is received, the secret message is revealed and it is found to be identical with the secret message.

References

[1] Aruna Varanasi, M. Lakshmi Anjana and Pravallika Pasupulate, "Image Steganography with Cryptography using Multiple Key Patterns," International Journal of Computer Applications (0975 – 8887), Volume 90 – No 15, March 2014.

[2] Amiruddin, Anak Agung Putri Ratna, and Riri Fitri Sari, "New Key Generation and Encryption Algorithms for Privacy Preservation in Mobile Ad Hoc Networks," International Journal of Communication Networks and Information Security (IJCNIS) Vol. 9, No. 3, December 2017.

[3] Umar Mujahid and M. Najam-ul-Islam, "Ultralightweight Cryptography for Passive RFID Systems," International Journal of Communication Networks and Information Security (IJCNIS) Vol. 6, No. 3, December 2014.

[4] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption," International Journal of Database Management Systems, Vol.4, No.6, December 2012.

[5] S.K.Sabnis, R.N.Awale, "Statistical Steganalysis of High Capacity Image Steganography with Cryptography," 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science 79 321 – 327, 2016.

[6] Prashant Kumar Arya, Mahendra Singh Aswal and Vinod Kumar, "Comparative Study of Asymmetric Key Cryptographic Algorithms," International Journal of Computer Science & Communication Networks, vol 5, no. 1, pp.17-21, 2015

[7] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, "Enhanced Least Significant Bit algorithm For Image Steganography", International Journal of Computational Engineering & Management, ISSN (Online): 2230-7893,Vol. 15 Issue 4, July 2012.

[8] Ki-Hyun Jung, Yoo Kee-Young "Steganographic method based on interpolation and LSB substitution of digital images," Computer Standards & Interfaces 31(2):465-470, February 2009

[9] G. Raj Kumar, M. Maruthi Prasada Reddy and T. Lalith Kumar, "An Implementation of LSB Steganography Using DWT Technique," International Journal of Engineering Research and General Science, ISSN 2091-2730, Volume 2, Issue 6, October-November, 2014.

[10] Shilpa Thakar, Monika Aggarwal, "A Review – Steganography," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 12, December 2013

[11] Gurpreet Kaur and Kamaljeet Kaur, "Digital Watermarking and Other Data Hiding Techniques," International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, Volume-2, Issue-5, April 2013.

[12] Chunlin Song, Sud Sudirman, Madjid Merabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images," ISBN: 978-1-902560-22-9,2009PGNet.

[13] Mariusz Dzwonkowski, Michal Papaj and Roman Rykaczewski, "A New Quaternion-Based Encryption Method for DICOM Images", IEEE Transactions on Image Processing, vo. 24, no.11, pp. 4614 – 4622, Nov. 2015.

[14] Anita Pradhan, K. Raja Sekhar, and Gandharba Swain, "Adaptive PVD Steganography Using Horizontal, Vertical, and Diagonal Edges in Six-Pixel Blocks," Security and Communication Networks, vol. 2017, pp. 1–13, 2017.

[15] M.I.Khalil, "Quaternion-based Encryption/Decryption of Audio Signal Using Digital Image as a Variable Key", International Journal of Communication Networks and Information Security (IJCNIS), Vol. 9, No. 2, August 2017.

[16] P. M. Rubesh Anand, , Gaurav Bajpai, and idhyacharan Bhaskar, "Real-Time Symmetric Cryptography using Quaternion Julia Set," IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009.

[17] Eckhard Hitzer, "The Quaternion Domain Fourier Transform and its Properties,", Adv. ppl. Clifford Algebras 26 (2016), 969–984

[18] Bihan, N.L., Sangwine, S.J., "Quaternion principal component analysis of color images," IEEE International Conference on Image Processing, vol, 1, pp. 809–812, 2003.

[19] Ell T.A., "Quaternion-Fourier transforms for analysis of two dimensional linear time-invariant partial differential systems," in Proc. 32nd Con. Decision Contr., pp. 1830-1841, Dec. 1993.