Improved Steganography Scheme based on Fractal Set

Mohammad Alia[1] and Khaled Suwais[2]
[1]Faculty of Sciences and Information Technology, Al-Zaytoonah University of Jordan, Jordan
[2]Faculty of Computer Studies, Arab Open University, Saudi Arabia

Abstract: *Steganography is the art of hiding secret data inside digital multimedia such as image, audio, text and video. It plays a significant role in current trends for providing secure communication and guarantees accessibility of secret information by authorised parties only. The Least-Significant Bit (LSB) approach is one of the important schemes in steganography. The majority of LSB-based schemes suffer from several problems due to distortion in a limited payload capacity for stego-image. In this paper, we have presented an alternative steganographic scheme that does not rely on cover images as in existing schemes. Instead, the image which includes the secure hidden data is generated as an image of a curve. This curve is resulted froma series of computation that is carried out over the mathematical chaotic fractal sets. The new scheme aims at improvingthe data concealing capacity, since it achieveslimitless concealing capacity and disposes of the likelihood of the attackers to realise any secret information from the resulted stego-image. From the security side, the proposed scheme enhances the level of security as the scheme depends on the exact matching between secret information and the generated fractal (Mandelbrot-Julia) values. Accordingly, a key stream is created based on these matches. The proposed scheme is evaluated and tested successfully from different perspectives.*

Keywords: *Steganography, data hiding, security, julia set, mandelbrot set, and fractal set.*

Received July 10, 2017; accepted December 17, 2017

1. Introduction

For many years, data hiding techniques have been used and have detained the thoughts of the researchers as one of the important fieldsin information security. Steganography is defined as the art of hiding confidential data inside multimedia aspects. Image steganography hasinterrelated common services of protecting the information confidentiality and integrity; meanwhile it scrambles the data into meaningless form. Unlike cryptography [5], steganography is implemented using cover medium which may include an image, audio or video. Cover-medium (also known ashost-medium or stego-medium) is the carrier wherein the secret information is embedded.

In general, steganography system involves embedding process and extracting process for the sender and receiver parties. At the sender side, the embedding process produces the cover image which hides the secret data. Typically, hiding data inside image pixels indeed requires choosing the pixels secretly using a secret key. Meanwhile, secret key is commonly known as a stego-key. Whereby, receiver party should then extract the hidden secret data from the received stego-image. The general steganographic scheme is illustrated in Figure 1.

The security of steganographic techniques is predominantly affected by three major components [4, 5]; Imperceptibility, capacity (payload) and robustness. Imperceptibility refers to the statistical matches between the cover file and stego-file. Identical statistics will always bestowbetter imperceptibility. On the other hand, capacity refers to the maximum amount of secret information that can be embedded in the cover file. Generally, steganographic primitives aim at maximisingthe capacity and minimisingthe perception of hidden messages in the stego-file. From the robustness perspective, steganographic developers aimatdesigning steganographic schemes that can show robustness against visual and statistical attacks, as well as against image manipulation.

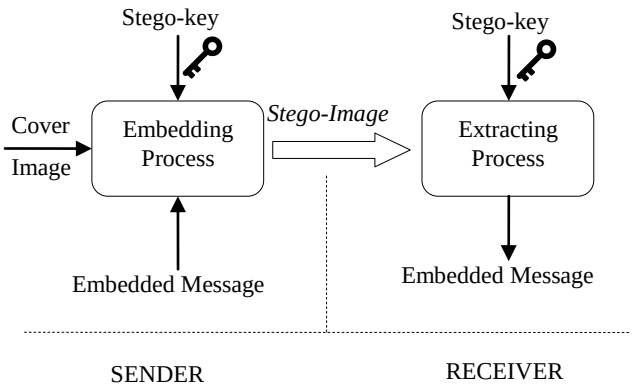

Figure 1. general steganographic scheme.

One of the simplest techniques used for hiding a significant amount of information in a multimedia file is the Least Significant Bit (LSB) technique [7]. In modern computer systems, 24-bit Bitmap Image

(BMP) or 32-bit Cyan Magenta Yellow and Black (CMYK) image files are used to store digital image files. LSB typically uses 24-bit image to hide the secret information. However, LSB process actually needs stego-key to control the steganographic process such as the selection of pixels which are later used to embed the secret binary information. Figure 2 representsimpact of embedding the letter "A" in a given 3 pixels-24 BMP image file.

Original pixel values before embedding

	Blue	Green	Red
Pixel no.1	00100111	11101001	11001000
Pixel no.2	00100111	11001000	11101001
Pixel no.3	11001000	00100111	11101001

The new values of the pixels after embedding letter "A"

	Blue	Green	Red
Pixel no.1	00100111	11101001	11001000
Pixel no.2	00100111	11001000	11101001
Pixel no.3	11001000	00100111	11101001

Figure 2. illustrative example on embedding the letter "A" in three pixels - 24 BMP image file.

However, in this paper, we are presenting an improved steganographic scheme based on fractal set. In particular, we will rely on the integration between Mandelbrot and Julia fractal sets to embed secret information by generating key-dependent data to achieve higher levels of security. In the proposed method, the stego-key is generated using key dependent data protocol that is based on matching the secret data and Julia set value.

The remainder of the paper is organised as follows. Sections 2 provides an overview offractals. Section 3 discusses the related works. The proposed scheme is introduced in section 4. A number of performance and security tests are performed and the results are presented in section 5. A concluding remark is given in section 6.

2. Fractals

The word fractal is derived from the complex number that consists of real and imaginary number components. It is defined as a point on the complex plane such that the point Z is defined in Equation (1):

$$Z = (x + yi) \tag{1}$$

where x is the corresponding point over the horizontal real axis and y is the corresponding point over the vertical imaginary axis. The unit of imaginary number$i$ is defined in Equation (2) [8, 11]:

$$i = \sqrt{-1} \tag{2}$$

Fractal is also viewed as fragmental geometric shape that is a never-ending complex pattern. Driven by recursion, fractal is an image of dynamic systems created interactively from almost similar smaller components by repeating a simple process over and over in an on-going feedback loop [5]. Recently, fractals are presenting an example of a chaotic system, where a totally new image can be generated by only changing the initial parameters of the system [8, 11]. Among the available fractal sets, we are mainly interested in Mandelbrot as well as Julia fractal sets [6, 9]. Example on image generated by Mandelbrot and Julia fractal sets is shown by Figure 3.

Julia fractal set is the set of repeated points over complex plane generated by Equation (3):

$$Z_n = Z_{n-1}^2 + C \mid \; |n \text{ enumber of iterations } (0 - \infty) \tag{3}$$

where Z_n, C are complex numbers. Similarly, Mandelbrot fractal set is the set of points on a complex plane that are generated by Equation (4):

$$Z_n = Z_{n-1}^2 + C \mid \; |n \text{ enumber of iterations } (0 - \infty) \tag{4}$$

where $Z_0 = 0$ and C is a complex number. Typically, the fractal image is generated by applying Equations (1) and (2) recursively.

Unlike Mandelbrot, Julia set iterates Equation 1 for fixed complex C iteration and with a non-zero value of Z. On the other hand, Mandelbrot set iterates Equation 1 with Z stating at 0 and varying C as a complex number. Even though Mandelbrot and Julia are technically deferent, all Z_n points must respectively reside on the Mandelbrot set or the Julia set [13, 2].

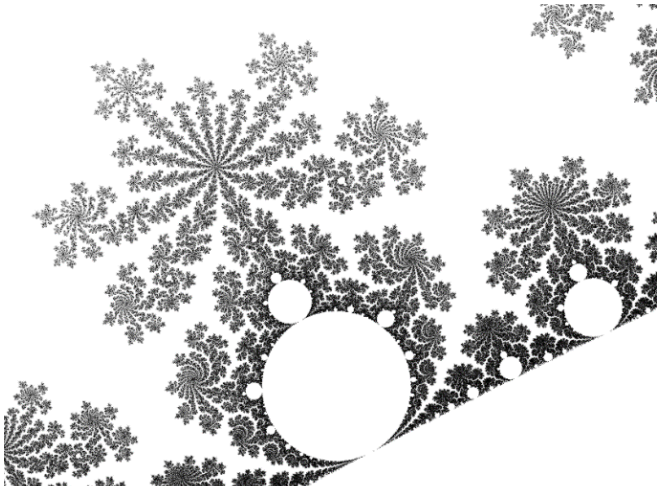

Figure 3. Mandelbrot and Julia sets in the region of -0.4 + 0.6*i*.

3. Literature Review

Several schemes were presented to enhance the quality and security of steganographic primitives. In [5, 3], a steganographic technique is proposed based on Exact Matches algorithm (EM) between the values of image pixels and the secret information as shown in Figure 4. This technique creates a Random Key-Dependent Data (RKDD) to be utilised as a part of the separating procedure. However, this steganographic technique

overcomes the limitation of LSB capacity and low robustness. We found that proper statistical analysis was not conducted.

In [10], a high capacity image steganography technique based on LSB substitution method is proposed. The method divides the image into two parts. The first part is used for data embedding, where pixels values are changed based on the secret message using LSB substitution technique. The second part is used to show the changes applied to the first part (output). The embedding process starts by dividing the cover image into two segments. The size of the image $N=H\times W$ and the secret data is divided into K blocks. The number of hidden bits at each pixel is fixed for the whole image. Now the embedding process hidesbit by bit using optimal LSB technique. The second part of the image indicates the changes made in the first part. Starting from the end of the second part, modify the LSB to indicate the modified pixels in the first part. At the end, cover image is combined back again to get the stego-image. At the receiver side, the extraction process comparesthe original image with the stego-image and findsthe modified pixels. Hence, the original image must be known to the receiver side. The main limitation of this method I that the receiver must know is the original image and the stego-image, making the stego-image suspected by hackers. In addition, this method works only on gray scale images.

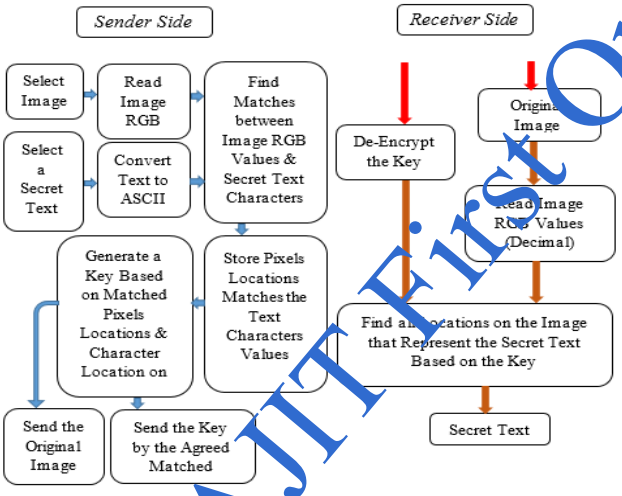

Figure 4. Steganographic based on RKDD [5].

The work proposed in [1] is known by the Zero-Order Hold method (ZOH) for embedding a secret message inside another image. The average of the adjacent pixels in the cover image istaken and checked against the secret message bits. Pixels are kept unchanged if they match the secret message bit value. In the case they don't match, they will be modified to match the secret image values. Test results have shown that ZOH has higher Peak Signal-to-Noise Ratio (PSNR) values than the traditional LSB method.

Five Modulus Method (FMM) and LSB Substitution is an alternative steganographic approach presented in [12]. Around 75% of the size of the secret message is hidden inside the cover image using Five Modulus Method, while the rest of secret message is hidden inside the cover image using LSB Substitution method. However, the test results show a good image quality and low computational complexity.

The LSB and the Set Partitioning in Hierarchical Trees (SPIHT)-based compression is another method presented in [14]. The SPIHT is wavelet based technique whichis computationally very fast and is among the best image compression based transmission algorithm. The technique first compresses the message image using the SPIHT algorithm. Consequently, the compressed data is embedded into the cover image using LSB technique. The compressions are made by the wavelet transform and then using the SPIHT coding. In the repossess side, the data is firstly decoded using the LSB method and then decompressed using the SPIHT algorithm. Consequently, inverse wavelet transform is applied to recover the original secret image.

The proposed public steganography in [4] allocatestwo phases for hiding the secret information. The first phase is to find the shared stego-key between the two communication parties (Alice and Bob) using Diffie-Hellman protocol. The second phase is responsible for selecting pixels which will be used to find the matches between the secret data block and image pixel using the secret stego-key. Eight bits binary information will be hidden in the selected pixel that dependson the matching method. These eight bits will be compared respectively with the selected RGB pixel's bytes, red, green and blue values to produce one dimensional array with 2 bit binary values as 00, 01, 10 and 11.

Upon studying the existing steganographic schemes, we found that they follow the traditional concept which relies on hiding data inside a cover image using different techniques. We also found that these schemes might be subjected to several statistical attacks and limited data to hide.

4. Steganographic Scheme based on Fractals

In this paper, we proposedan alternative scheme that aims at producingunchanged image which satisfies the robustness and boundless capacity criteria of secure steganography. The proposed scheme operates by locating all exact matches between the values of the secret information and the Mandelbrot-Julia Fractal sets. Our scheme is designed to overcome the drawback of existing steganographic schemes which suffer from limited hiding capacity and low robustness.

The proposed steganographic scheme is composed of three major phases. The first phase is responsible for applying Mandelbrot-Julia Fractal set-based public

key exchange protocol to generate shared secret stego-key. The second phase supports hiding secret information to generate the key stream by collecting the matched values between the secret value and Mandelbrot-Julia set items, whereas the third phase supports data extraction. Figure 5 presents the overall structure of the proposed steganographic scheme.

Our scheme generates an image that represents a Mandelbrot-Julia curve with a set of points. Each point represents a character of 8-bits. Sender and receiver share a secret key that specifiesthe iteration numbers. In turn, the iteration number is responsible for generating specific points on the curve. Accordingly, the receiver can easily extract back the hidden data by re-iterating the Mandelbrot-Julia equations using the shared secret values.

- *Phase*1: Public-Key exchange protocol based With reference to Figure 5, the sender (Alice) and the receiver (Bob) share the secret stego-key over insecure medium. In this regard, we are adopting the Fractal key exchange protocol proposed in [8] in order to achieve this objective.

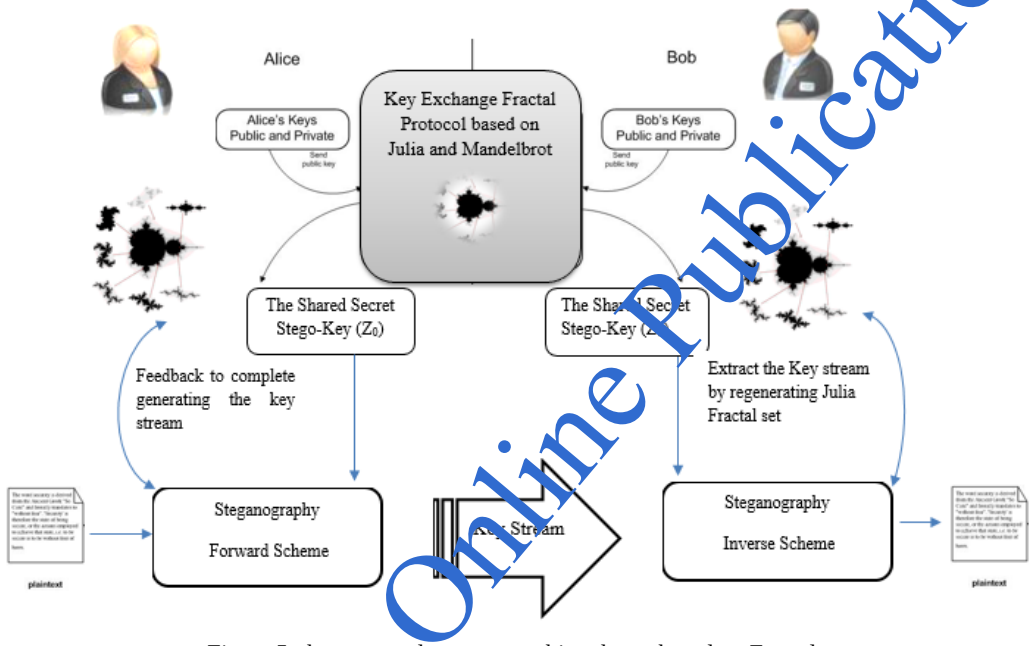

Figure 5. the proposed steganographic scheme based on Fractal.

The fractal-based key exchange protocol relies on implementing the following set of Equations (5), (6), (7):

$$Z_k\ e = Z_{k-1} \times C^2 \times e \mid \quad |Z, C, e \tag{5}$$

$$Z_n\ d = Z_{n-1} \times C^2 \times d \mid \quad |Z_i, C, d \tag{6}$$

$$C^{k-x} \times (Z_n\ d)\ _k e = C^{n-x} \times (Z_k\ e)\ _n d| \quad |Z\ , C, e, d \tag{7}$$

where Z_i, C, e, d are complex numbers and k, n are the number of iterations. Note that the global value C is known to the public.

On the other hand, the variables d and n are defined as Alice's private values, while the variables k and e are defined as Bob's private values. Alice and Bob private values are then used in Mandelbrot function to produce Alice and Bob public keys, such as $(Z_k\ e)$ and$(Z_n\ d)$,respectively. The public values are then exchanged such that the secret key is shared in the form of key$(Z_k\ e)_n d = (Z_n\ d)_k e$between the two communicating parties. In our model, the stego-key is denoted by (Z_0). The architecture of the fractal-based key exchange protocol is illustrated in Figure 6.

- *Phase* 2: Hiding secret information The process of hiding secret information is carried out at the sender side using the secret stego-key. This key is used in Julia Fractal set iterations to produce the key stream. Meanwhile, Julia equation is iterated with Z_0 staring at stego-key value. Consequently, the key steam is computed by gathering the matched values between the secret information and the Julia set items. The area of Mandelbrot set is identified by four different points on the complex number plane and bordered by a circle of radius r = 2, which is cantered at (0, 0i); the origin of the complex number plane. The top and bottom are at approximately y = ± 1.12 respectively. The left and right side point of the set ends with x = -2 (left side) and x = 0.47 (right side). Algorithm (1) shows the pseudo code of the proposed forward scheme for selecting the matches between the secret text and the Julia set items.

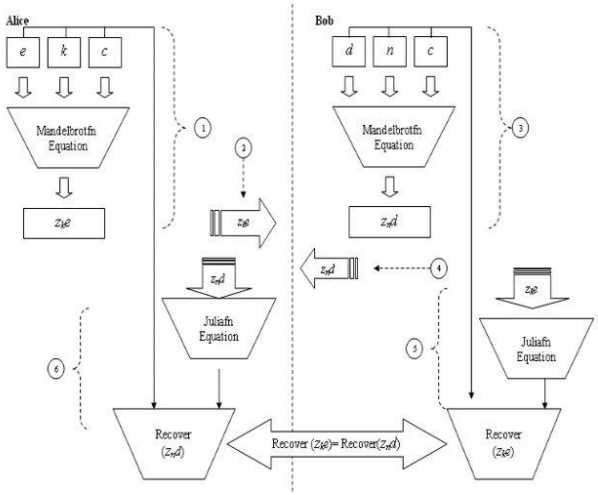

Figure 6. key exchanging protocol based on fractal [8].

- *Phase* 3: Data Extraction In data extraction phase, the receiver aims atrecovering the original secret message from the Julia fractal set. To achieve this, the stego-key value is used as Z_0 to start Julia's equation Equation (3). Consequently, the key stream is isolated from the Julia set to recover the secret data as shown in Algorithm (2).The exact matching between the secret data and pixels' values is considered while processing the given image. The sender and the receiver should iterate the fractal equations initialised by the shared secret key to match the secret information values.

Algorithm 1:Data_hiding Phase

For each run
Initialize julia_set, stego_key, secret_data
End
Do
Start iterating
Use stego_key as Z_0 to start iterating Julia set
Collect exact matches(secret_data, Julia_set)
Store the matched value
Collect iteration number in the keystream
End
Produce keystream
End

Algorithm 2:Data_extraction Phase
For each run
Initialize julia_set, stego_key, keystream
End
Do
Start iterating
Use stego_key as Z_0 to start iterating Julia set
Extract iteration number from keystream
Recover Julia_set (secret_data)
End
Produce secret_data
End

5. Results and Discussion

Testing the proposed scheme in this paper is mainly based on statistical and performance analysis. The core of the scheme relies on generating key values that should be statistically secure against statistical attacks. In termsof the performance analysis, the execution time of the related processes is presented. Unlike traditional steganographic schemes, imperceptibility is not tested since our stego-image is generated during the data hiding process without the need of using cover images. In addition, the hiding capacity is unlimited since it is not bounded of any cover image as in traditional schemes.

Statistical analysis demonstrates the strength of steganographic scheme against possible statistical attacks, which depends on detecting levels of correlations between the generated complex numbers from Mandelbrot iterations. The analysis starts by introducing the correlation test to examine the correlation properties between all the points distributed over the Mandelbrot-Julia curve.

Each point on Mandelbrot-Julia curve is represented by x and y value, where x is the real number and y is the imaginary number on the plane. The combination of both x and y represents a point in the Mandelbrot-Julia curve. The purpose of this test is to show that small changes in the initial value of the variable C, which is used in Equations 3 and 4, results into a completely uncorrelated set of points on the Mandelbrot-Julia curves. We have tested the correlation properties of huge data sets which includes 10000 points on the curve using the initial C values in our experiment that is represented in Table 2.The distribution of the generated values over the Mandelbrot-Julia curve is illustrated in Figure 7.

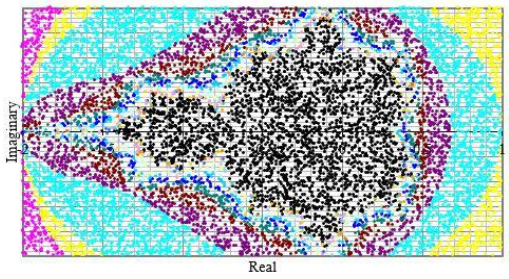

Figure 7. Distribution of points over Mandelbrot-Julia curve.

With reference to the results presented in Table 1, one can clearly show that all the correlations values between different generated points over the Mandelbrot curves are very close to zero, therefore the generated points from the Mandelbrot iterations are uncorrelated. Note that minor changes made in the initial value of C could result into totally uncorrelated values.

From the other perspective, the statistical analysis showed that the mean and standard deviation of all generated real numbers of the complex number are drawn from the same distribution. Similarly, all imaginary numbers are drawn from the same distribution. However, the results show that both real numbers and imaginary numbers are drawn from two different distributionsas illustrated in Figures 8 and 9.

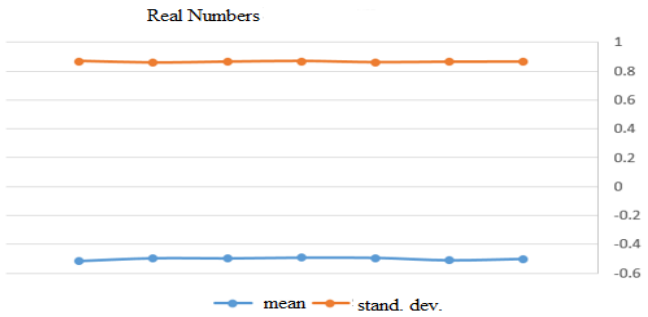

Figure 8. the mean and SD values of all real numbers generated from all data sets.

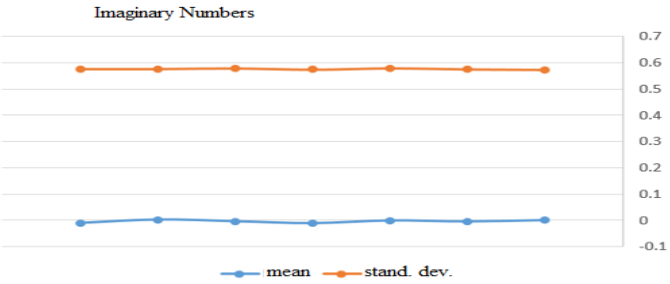

Figure 9. the mean and SD values of all real numbers generated from all data sets.

Specifying the type of distribution is essential to assure that the generated points are not biased to specific region in the distribution. To examine the type of distribution, the histogram analysis is applied. Figure 10 shows the histogram analysis applied on the real and imaginary numbers generated from the seven data sets.

The histogram analysis shows that the real numbers and imaginary numbers of all points on Mandelbrot-Julia curves are symmetric with respect to the mean value. This indicates that the values are drawn from a uniform distribution and they are not biased to specific region. Moreover, the data istested against the uniform distribution using QQ plotting to support our findingsas illustrated in Figure 11.

Table 1. Correlation test on the generated mandelbrot points.

		C=1.3-0.8i		C=1.4-0.8i		C=1.5-0.8i		C=1.6-0.8i		C=1.61-0.8i		C=1.62-0.8i		C=1.62-0.9i	
		Real	**Imag.**	**Real**	**Imag.**	**Real**	**Imag.**	**Real**	**Imag.**	**Real**	**Imag.**	**Real**	**Imag.**	**Real**	**Imag.**
C=1.3-0.8i	**Real**	1	-0.001	0.001	0.011	-0.02	0.019	-0.02	-0.07	-0.07	-0.01	-0.02	-0.01	0.001	0.016
	Imag.	-0.001	1	-0.003	-0.04	0.01	0.015	0.01	-0.08	-0.01	0.009	0.002	-0.01	0.004	0.000
C=1.4-0.8i	**Real**	0.001	-0.003	1	0.007	0.017	0.08	0.003	-0.03	0.015	0.009	0.021	0.010	0.009	0.009
	Imag.	0.011	-0.004	0.0076	1	-0.09	0.013	0.014	-0.01	0.010	-0.02	-0.07	0.013	0.003	0.004
C=1.5-0.8i	**Real**	-0.001	0.012	0.0171	-0.09	1	0.016	-0.05	-0.03	0.008	0.004	-0.01	0.004	0.00	0.000
	Imag.	0.019	0.015	-0.008	0.003	0.16	1	-0.03	0.003	-0.01	-0.04	-0.02	0.00	-0.01	-0.016
C=1.6-0.8i	**Real**	-0.002	-0.010	0.0036	0.01	-0.0	-0.03	1	0.014	-0.09	0.023	0.015	0.010	0.005	0.007
	Imag.	-0.006	-0.007	-0.0029	-0.01	-0.0	0.003	0.014	1	0.004	-0.05	-0.05	0.00	0.002	0.0192
C=1.61-0.8i	**Real**	-0.007	-0.01	0.0157	0.010	0.008	-0.01	-0.09	0.004	1	-0.03	-0.01	0.001	0.001	0.0122
	Imag.	-0.012	0.009	0.0099	0.02	0.004	-0.04	0.023	-0.05	-0.02	1	0.007	0.004	-0.01	0.013
C=1.62-0.8i	**Real**	-0.001	0.00	0.0214	-0.0	-0.02	-0.02	0.015	-0.05	-0.01	0.007	1	-0.01	0.011	0.0191
	Imag.	-0.012	-0.014	0.0101	0.013	0.004	-0.05	0.010	-0.03	0.001	0.004	-0.01	1	0.006	0.0092
C=1.62-0.9i	**Real**	0.001	0.004	0.0053	0.003	0.003	-0.01	0.005	0.002	0.001	-0.01	0.011	0.006	1	0.0076
	Imag.	0.016	0.00	0.0099	0.004	-0.07	-0.01	0.007	0.019	0.012	0.013	0.019	0.009	0.007	1

Table 2. Initial values of c to control mandelbrot-julia sets.

	Initial value of C	**Set Size (no. of points)**
Data Set 1	C=1.3-0.8i	10000
Data Set 2	C=1.4-0.8i	10000
Data Set 3	C=1.5-0.8i	10000
Data Set 4	C=1.6-0.8i	10000
Data Set 5	C=1.61-0.8i	10000
Data Set 6	C=1.62-0.8i	10000
Data Set 7	C=1.62-0.9i	10000

QQ plotting between the actual and theoretical quantiles of the uniform distribution shows a straight line passing through the origin. This shows that the values are drawn from uniform distribution.

The results show that both the real and imaginary values of all points on Mandelbrot-Julia curves are drawn from uniform distributions. Statistical t-test is carried out to examine the statistical relation between real and imaginary values among all sets in terms of the mean values of each data set. This is important as statistical attacks might take advantage of any possible relation between generated values.

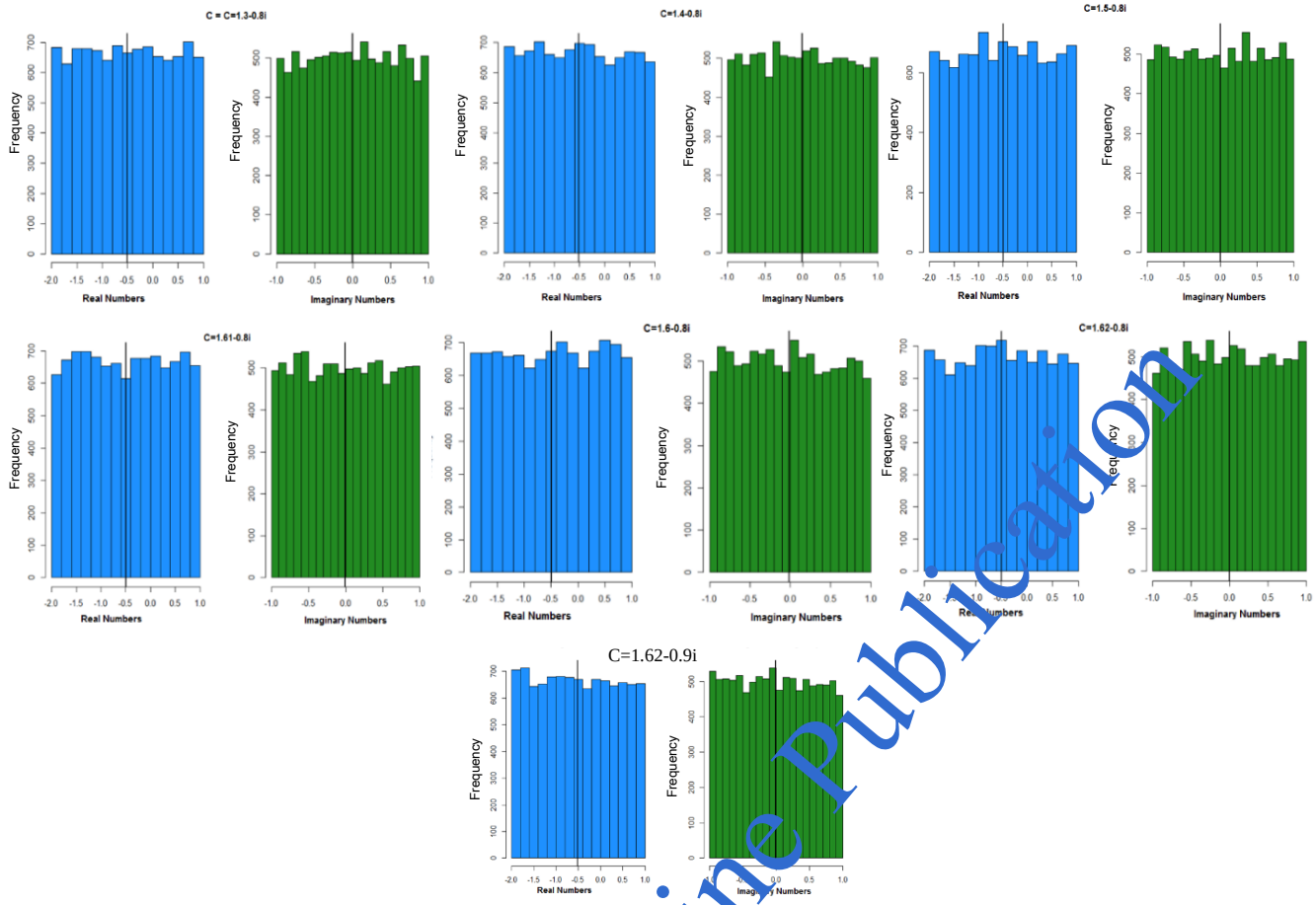

Figure 10. Histogram analysis of real and imaginary numbers generated from the data sets.

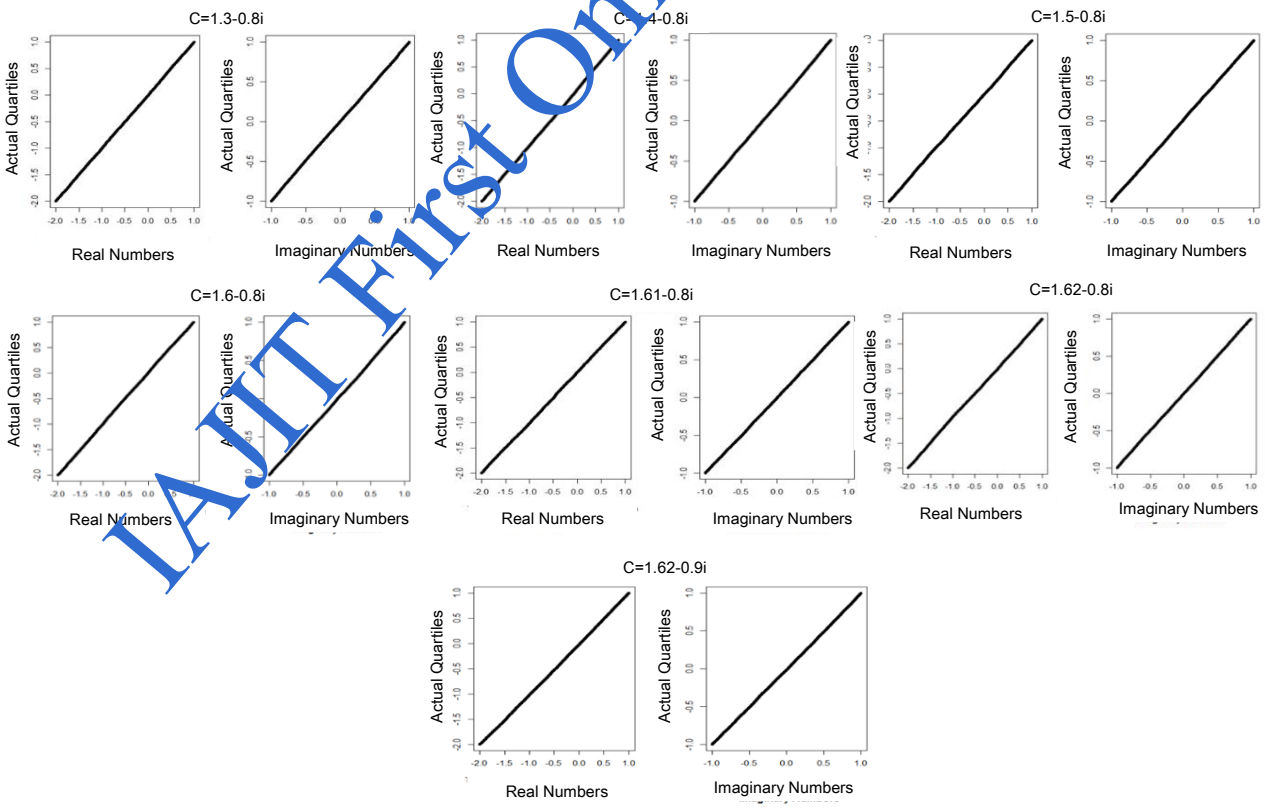

Figure 11. QQ plotting of real and imaginary numbers generated from the data sets against uniform distribution.

Table 3 shows the *t*-test results applied over cross-data sets (inter-relation between different points from different sets). The *t*-test assumes a significance level of 0.05. Accordingly, any *p*-value that is less than 0.05 indicates a negative support to the *null*-hypothesis. The results show that the *p*-values are zero when comparing the mean values of different values across the data sets. This confirms that the uniform distribution of the generated values in each set is totally different from the uniform distribution that generates other values in other sets.

The correlation analysis on the shared secret key values of Fractal key exchange protocol is also examined. We have calculated 256 attempts using Equation (7) to test the correlation properties of the shared key values. The correlation tests are based on changing the sender's private keys values of 128 times on both the key *e* and the private key *n*.

Table 3. Initial values of *C* to control mandelbrot-Julia sets.

Variable	*t*-value	*p*-value
(Real (C=1.3-0.8i), Imagin (C=1.4-0.8i))	-47.8882	0
(Real (C=1.3-0.8i), Imagin (C=1.5-0.8i))	-48.1445	0
(Real (C=1.3-0.8i), Imagin (C=1.3-0.8i))	-47.3178	0
(Real (C=1.3-0.8i), Imagin (C=1.61-0.8i))	-47.8805	0
(Real (C=1.3-0.8i), Imagin (C=1.62-0.8i))	-48.5338	0
(Real (C=1.3-0.8i), Imagin (C=1.62-0.9i))	-47.3506	0
(Real (C=1.4-0.8i), Imagin (C=1.5-0.8i))	-49.1131	0
(Real (C=1.4-0.8i), Imagin (C=1.3-0.8i))	-48.2887	0
(Real (C=1.4-0.8i), Imagin (C=1.61-0.8i))	-48.8491	0
(Real (C=1.4-0.8i), Imagin (C=1.62-0.8i))	-49.5038	0
(Real (C=1.4-0.8i), Imagin (C=1.62-0.9i))	-48.3204	0
(Real (C=1.5-0.8i), Imagin (C=1.3-0.8i))	-46.8086	0
(Real (C=1.5-0.8i), Imagin (C=1.61-0.8i))	-47.3736	0
(Real (C=1.5-0.8i), Imagin (C=1.62-0.8i))	-48.028	0
(Real (C=1.5-0.8i), Imagin (C=1.62-0.9i))	-46.8418	0
(Real (C=1.3-0.8i), Imagin (C=1.61-0.8i))	-46.9672	0
(Real (C=1.3-0.8i), Imagin (C=1.62-0.8i))	-47.6175	0
(Real (C=1.3-0.8i), Imagin (C=1.62-0.9i))	-46.4373	0
(Real (C=1.61-0.8i), Imagin (C=1.62-0.8i))	-48.2549	0
(Real (C=1.61-0.8i), Imagin (C=1.62-0.9i))	-47.3718	0
(Real (C=1.62-0.8i), Imagin (C=1.62-0.9i))	-47.1278	0

The correlation coefficient tests are carried out by changing only one bit of the keys at time t_i. The key *e*is initialised by 1 and then is incremented by 1 at t_{i+1}. Similarly, the key *n* is initialised by 3 and incremented by 1 at t_{i+1}. The average correlation test between two adjacent points of the secret key's values is found to be 0.123898, which indicates that there is no correlation between the distributed points of the secret shared key value. Hence, attacking the secret and shared keys is not possible statistically. Figures 12 and 13 show the distribution of the input key values and the output shared key values respectively.

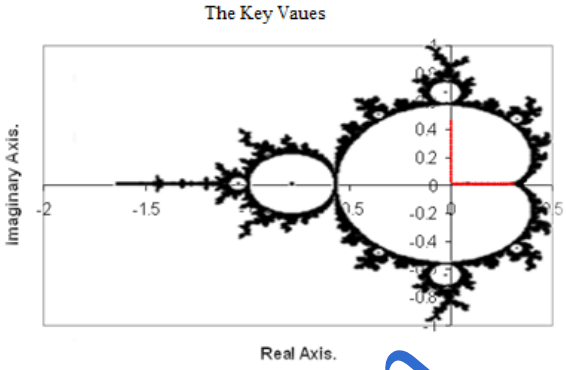

Figure 12. The distribution of the input key values over Mandelbrot-Julia curves.

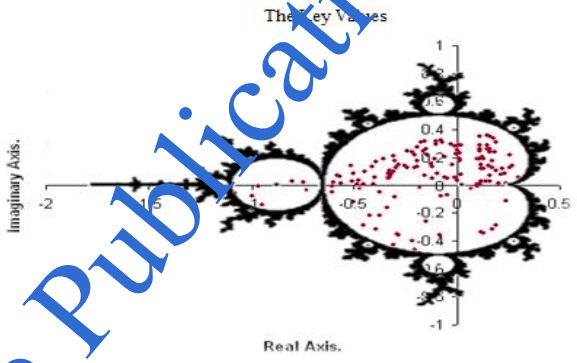

Figure 13. The distribution of the shared key values based over Mandelbrot-Julia curves.

Performance-wise, the experiment shows that each generated image may have around 10000 points on a curve. Each point represents a character of 8-bits. Accordingly, we can store about 80000 bitsin an image havinga dimension of about 500x333. The processing time of each point on the Mandelbrot-Julia curve takes about 2ns on a platform of Intel Core i7® processor and a memory of 4GB.

From the security perspective, the scheme was found secure against brute-force attacks, as this is one of the possible attacks on our scheme. The search space is found to be greater than $(2^{13})^{2^3} = 2^{104}$, for 10000 points on the curve represented by 8 bits.

7. Conclusions

The ultimate objective of this study was to develop an alternative concept for steganographic schemes. Existing schemes are found subjective to several security and statistical attacks as they relyon hiding a text in a cover image. This concept was modified in our proposed scheme to introduce new concept for hiding data.

Our scheme generates an image that represents a Mandelbrot-Julia curve with a set of points. Each point represents a character of 8-bits. Sender and receiver share a secret key that specifiesthe iteration numbers. In turn, the iteration number is responsible for generating specific points on the curve. Accordingly, the receiver can easily extract back the

hidden data by re-iterating the Mandelbrot-Julia equations using the shared secret values.

The experiment results showed that the generated points over the curve are uncorrelated statistically. The results also showed that the generated secret and shared keys are statistically secure. From the security perspective, the scheme was found secure against brute-force attacks.

From the security perspective, the scheme was found secure against brute-force attacks. The search space is found to be $(2^{13})^{2^3} = 2^{104}$.

Acknowledgment

The work presented in this paper was supported and funded by the Arab Open University (AOU), Riyadh, Saudi Arabia. The work is done in collaboration with Al Zaytoonah University of Jordan.

References

[1] Abdelmgeid A., Tarek A., Al-Hussien S., Shaimaa H., (2016), New Image Steganography Method using Zero Order Hold Zooming, *International Journal of Computer Applications* (0975 – 8887), Volume 133 – No.9, January 2016.pp27-38.

[2] Giffin, N., "Fractint," *TRIUMF project at the University of British Columbia Campus in Vancouver B.C. Canada*, 2006.

[3] Johnson, N., Jajodia, S., (1998) "Exploring Steganography: Seeing the Unseen," *IEEE Computer*, pp. 26-34.

[4] Kamel Faraoun. Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption. *The International Arab Journal of Information Technology, Vol. 7, No. 3, July 2010*

[5] Maher A. Alsarayreh, Mohammad A. Alia, Khulood Abu Mariya ,A Novel Image Steganographic System Based on Exact Matching Algorithm and Key-Dependent Data Technique, *Journal of Theoretical and Applied Information Technology*, Vol.95. No 5.p.p 1212-1224

[6] Lazareck, L., Verch, G., Peter, J, "Fractals in Circuits," *IEEE Conference*, pp. 589-594, vol. 1, May 2001.

[7] Mohammad A. Alia, Abdelfatah A. Yahya. Public–Key Steganography Based on Matching Method. *European Journal of Scientific Research* Vol.40 No.2 (2010), pp.223-231

[8] Mohammad A. Alia, Azman Bin Samsudin. New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Sets. *International Journal of Computer Science and Network Security*, VOL.7 No.2, February 2007

[9] Mandelbrot, B., "Fractal Geometry of Nature," *San Francisco: W. H. Freeman*, 1982.

[10] Marghny H., Loay M., (2016), High Capacity Image Steganography Technique based on LSB Substitution Method, *Appl. Math. Inf. Sci.* 10, No. 1, pp 259-266.

[11] Patrzalek, E., "Fractals: Useful Beauty, General Introduction to Fractal Geometry,Stan Ackermans Institute, IPO, *Centre for User-System Interaction*, *Eindhoven University of Technology*, 2006.

[12] Praneeta Dehare, Padma Bonde,(2014), Hiding Image in Image by using FMM with LSB Substitution in Image Steganography, *International Journal of Advance Research in Computer Science and Management Studies*, ISSN: 2321-7782, pp. 455-458.

[13] Taylor, M., Louvet, J., "Sci.fractals FAQ," *Computing Services Mount Allison University Sackville, Canada*, 1998.

[14] Thenmozhi, M., Menakadevi, T., (2016), A New Secure Image Steganography Using Lsb and Spiht Based Compression Method, *International Journal of Engineering Re-search & Science*, vol-2(3), pp80-85.

Mohammad Alia is an Associate professor at the computer information systems department, Faculty of science Computer and information technology, Al Zaytoonah University of Jordan. He received the B.Sc. degree in Science from the Al Zaytoonah University, Jordan, in 1999. He obtained his Ph.D. degree in Computer Science from University Science of Malaysia, in 2008. During 2000 until 2004, he worked at Al-Zaytoonah University of Jordan as an instructor of Computer sciences and Information Technology. Then, he worked as a lecturer at Al-Quds University in Saudi Arabia from 2004 - 2005. Currently he is working as a Faculty Deputy Dean and a Chair of Computer Information Systems Dept. at Al Zaytoonah University of Jordan. His research interests are in the field of Cryptography, and Network security.

Khaled Suwais is an Associate Professor at the Faculty of Computer Studies, Arab Open University. He received his B.Sc in computer science from Al al-Bayt University, Jordan in 2004, M.Sc and PhD in computer science from University Sains Malaysia, Malaysia in 2005 and 2009, respectively. He joined the College of Computer Science and Information at Al-Imam University, Riyadh, Saudi Arabia, in 2009. In 2012,

he joined the Faculty of Computer Studies at the Arab Open University. Dr. Suwais is specialized in the field of information security and cryptography. Currently, he is involved in reviewing several international journals and conferences. His research interest includes: cryptography, information security and operational research.