

## Steganography Of Images Using Hilbert Curve

### **DESAI Hardikkumar V.**

Assistant Professor,  
Naran Lala College of Professional and  
Applied Sciences, Navsari, India.  
[hardik4dreamz@yahoo.com](mailto:hardik4dreamz@yahoo.com)

### **DESAI Apurva A.**

Department of Computer Science,  
Veer Narmad South Gujarat University,  
Surat, India.  
[aadesai@vnsgu.ac.in](mailto:aadesai@vnsgu.ac.in)

### **Abstract**

The development of Information and Communication Technology draws significant attention towards security and integrity of data. ICT leads researchers to develop applications which are used to communicate secretly. Steganography is a very useful information hiding technique. The major advantage of using this technique is that the message which was hidden is not easy to detect. Our research has addressed major aspects of Steganography. We develop new algorithm to achieve steganography using Hilbert Curve. The algorithm is developed by keeping in mind that the message which was hidden is not easy to detect by naked eye. We have generated gray scale and RGB histogram for different images to check the distribution of data. Also we checked standard deviation and mean of the images to check the intensity of pixel. The paper also focuses on various steganographic techniques like HIDE and SEEKS, JSteg, OutGuess 0.1, OutGuess 0.2, F3, F4, and F5.

**Keywords:** - *Steganography, Hide&Seek, JSteg, OutGuess0.1, OutGuess0.2, F3, F4, F5.*

### **1. Introduction**

Internet is an open resource for all, so this technology is very much useful to transmit data from one end to other very easily and speedily. Therefore information security draws attention of researchers, government agencies; law makers, military, intelligence agencies as well as criminals who require uninterrupted communications. They are interested in

---

---

---

understanding these technologies and their weaknesses, so as to detect and monitor hidden messages.

### 1.1 Steganography

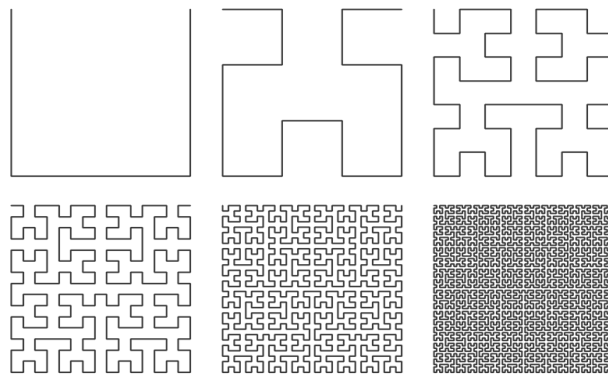
The term steganography refers to the art of covert communications. The message is embedded within another object known as a cover work, by tweaking its properties. The resulting output is known as stegogramme.

One of the oldest examples of Steganography dates back to around 440 BC in Greek History. Herodotus, a Greek historian from the 5th century BC, revealed .Some examples of its use in his work entitled “The Histories of Herodotus”. One elaborate example suggests that Histaeus, ruler of Miletus, tattooed a secret message on the shaven head of one of his most trusted slaves. After the hair had grown back, the slave was sent to Aristagorus where his hair was shaved and the message that commanded a revolt against the Persians was revealed [1].

In modern terms, steganography is usually implemented computationally, where cover work such as text files, images, audio files & video files which are tweaked in such a way that a secret message can be embedded within them.

### 1.2 Hilbert Curve

A Hilbert curve (also known as a Hilbert space-filling curve) shown in figure 1(a) is a continuous fractal space-filling curve first described by the German mathematician David Hilbert in 1891, [2] as a variant of the space-filling curves discovered by Giuseppe Peano in 1890. [3] He is recognized as one of the most influential and universal mathematicians of the 19th and early 20th centuries. Hilbert discovered and developed a broad range of fundamental ideas in many areas, including invariant theory of geometry.



(a)

Figure 1 (a): Hilbert Curves with ever increasing density

## 2. Literature Review

We review different Steganographic techniques like Hide and Seek , JSteg, OutGuess 0.1, Out Guess 0.2, F3, F4 and F5and other related works regarding steganography are presented. We also presented analysis of various steganography techniques.

---

## 2.1 Hide and Seek

Steganography is applicable to all data objects that contain redundancy. People often transmit digital pictures over email and other Internet communication, and JPEG is one of the most common formats for images. Moreover, steganographic systems for the JPEG format seem more interesting because the systems operate in a transform space and are not affected by visual attacks [4]. Visual attacks mean that you can see steganographic messages on the low bit planes of an image because they overwrite visual structures; this usually happens in BMP images. Neil F. Johnson and Sushil Jajodia [5] showed that steganographic systems for palette-based images leave easily detected distortions.

## 2.2 JSteg

The JSteg algorithm was developed by Derek Upham and is essentially as same as a copy of the Hide & Seek algorithm, because it employs sequential least significant bit embedding. In fact, the JSteg algorithm only differs from the Hide & Seek algorithm because it embeds the message data within the LSBs of the DCT coefficients, rather than its pixel values [6].

## 2.3 OutGuess 0.1

In much the same way that embedding the message data sequentially using the Hide & Seek method was not considered very secure, neither was the fact that the JSteg algorithm embedded in the same fashion. The first version of Outguess, designed by Neils Provos [7], improved the JSteg algorithm by scattering the embedding locations over the entire image according to a PRNG on image.

## 2.4 OutGuess 0.2

Neils Provos [8] created a revised version of the OutGuess 0.1 algorithm, called OutGuess 0.2. It was ensure that the statistical properties of the cover image were maintained after embedding, such that stegogrammes looks statistically similar to a clean image. This would make it harder for steganalysts to calculate the likelihood that their suspect image is a stegogramme. The algorithm is exactly the same for OutGuess 0.2 as it was for OutGuess 0.1. The difference lies in what happens after the information has been embedded. In OutGuess 0.2, corrections are made to the coefficients such that they appear similar to that of a clean image in terms of frequencies of the values. This is known as statistics aware steganography.

## 2.5 F3

As an alternative to the OutGuess 0.2 algorithm, AndreasWestfeld designed an algorithm called F3 [9]. It was considered even more secure. The reason for this is that it did not instantiate the same embedding process as the JSteg and OutGuess algorithms. Instead of avoiding embedding in DCT coefficients equal to 1, the F3 algorithm permitted embedding in these regions, at the same time as it would still avoid embedding in zeros and the DCT coefficients. The algorithm still embedded the message data sequentially. Another change with this algorithm was that it did not embed directly in the least significant bits of the DCT coefficients, but instead took the absolute value of the coefficients first, before comparing

---

them to the message bits. If both the absolute value of the coefficient, and the message bit were the same, then no changes are made. If they are different, then the absolute value of the DCT coefficient is reduced by 1. An implication of this however, is that zero values are often created which the decoding algorithm will not be programmed to extract data from. The F5 algorithm worked around this by reembedding  $m_i$  when the result is that a zero DCT coefficient is created.

## 2.6 F4

The main drawback with F3 was the reality that it effectively embedded more zeros than ones as a result of the shrinkage mechanism. This meant that when the statistical properties of the stegogrammes are examined through its some object of embedding became visible. This is much the same as what happened in the JSteg implementation except a slightly different pattern is derived. In addition to this, steganalysts also found that more odd coefficients existed in F3 stegogrammes than even coefficients. This now meant that there were two weaknesses that could be examined when viewing the histogram of a suspect image. F4 was developed to remove these properties such that the histogram would appear similar to that of a clean image.

## 2.7 F5

The F5 algorithm [10] is predominantly the same as the F4 algorithm, at least in terms of its strategy for encoding the message data. However, the F5 algorithm was designed in an attempt to improve on the F4 algorithm by minimizing the disturbance caused when embedding the message data.

The earliest work was done by Davern and Scott (1996) [11], who divide the domain blocks of the image into two sets. They then use standard fractal image compression techniques to select a domain block that matches the range block, however they choose a block from one of the two domain sets depending on whether the data bit they are embedding is a one or a zero.

A. Jacquin (1995) [12], most fractal coding schemes are based on representation by Partition Iterated Function System (PIFS), a solution to inverse problem which was first published by Jacquin. A PIFS differs from IFS in the Individual mappings operating on a subset of image, rather than the entire image.

Pauate et al, Saupe et al, Wotilberg et al, (1997, 1994, 1999) [13, 14, 15], Theoretical background referred to in fractals to generate fractals considers an IFS consisting of a collection of contractive affine transformations. The iteration procedure of applying a number of transforms is terminated when convergence is met i.e. an attractor.

Bas et al, Li C Wang, Liao P et al (1998, 2000, 2006) suggested that a great variety of steganographic methods on fractal compression principles [16, 17, 18] are good, but greatest robustness is ensured by means of the methods [17, 18] since they directly manipulate the code of compressed image. Building in secrecy increase the given approaches will provide high level of protection.

---

Lokesh Kumar (2012) [19], in his proposed system cryptographic and steganographic security is combined to give two tier securities to secret data. In proposed scheme secret message is encrypted before hiding it into the cover image which gives high security to secret data. Advanced encryption standard (AES) is used to encrypt secret message and alteration component technique is used to hide encrypted secret message into cover image. Since the resulting perceptual quality of the mixed images is good, it is hardly attracted from eavesdropper by naked eye. Finally we can conclude that the proposed technique is effective for secret data communication.

Rosziati Ibrahim et al (2010) [20], in his proposed a new steganography algorithm with 2 layers of security. A system named SIS (Steganography Imaging System) has been developed using the proposed algorithm. They tested few images with various sizes of data to be hidden. With the proposed algorithm, they found that the stego image does not have a noticeable distortion on it (as seen by the naked eyes). SIS can be used by various users who want to hide the data inside the image without revealing the data to other parties. SIS maintains privacy, confidentiality and accuracy of the data.

Wojciech Frączek et al (2010) [21] , suggested that Stream Control Transmission Protocol (SCTP) is a new transport layer protocol that is due to replace TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocols in future IP networks. Currently, it is implemented in such operating systems like BSD, Linux, HPUX or Sun Solaris. It is also supported in Cisco network devices operating system (Cisco IOS) and may be used in Windows. This paper describes potential steganographic methods that may be applied to SCTP and may pose a threat to network security. Proposed methods utilize new, characteristic SCTP features like multi-homing and multistreaming. Identified new threats and suggested countermeasures may be used as a supplement to RFC 5062, which describes security attacks in SCTP protocol and can induce further standard modifications.

Hemalatha S (2013) [22], Observes that two secret images can be hidden in one color image and they can be regenerated without actually storing the image. This approach results in high quality of the stegoimage having high PSNR values compared to other methods. However the disadvantage of the approach is that it is susceptible to noise if spatial domain techniques are used to hide the key. This can be improved if transform domain techniques are used to hide the key. The approach is very simple and the security level can be increased by using standard encryption techniques to encrypt the keys.

Sharon Rose Govada et al (2012) [23], he suggested a method is a combination of Word shifting, Text Steganography and Synonym Text Steganography. So we called this as “Three Phase Shielding Text Steganography” This method overcomes various limitations faced by the existing Steganographic algorithms.

Gowtham dhanarasi (2012) [24], suggested a novel method for image steganography using block complexity analysis in wavelet domain. Many researchers have been reported different techniques but all the methods suffer with image quality problem. So in order to achieve good quality,

### **3. Proposed Algorithm & Flow Chart**

We present algorithm to hide the image within image, we develop a new algorithm with the use of Hilbert Curve. The algorithm is developed by keeping in the mind that no one can easily detect the hidden image.

---

### 3.1 Embedding algorithm

In this approach, we take three images for the purpose of steganography of images using Hilbert Curve. Manaal image 2(a) is an original image which refers to as cover or carrier image. Tree image 2 (b) is an image to embed within cover image and image 2(c) is an image of Hilbert Curve which is used to identify location on Manaal image 2(a).

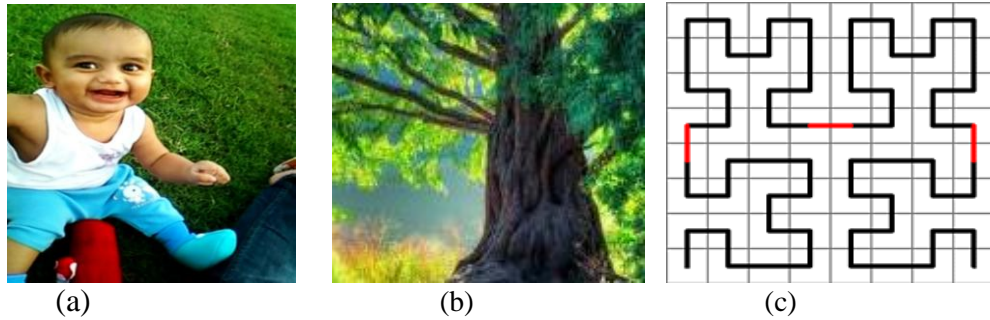


Figure 2 (a): Manaal Image (Cover/Carrier) (b): Tree Image (Image to Hide) (c): Hilbert Curve Image

Hilbert Curve image 2(c) is generated on Manaal image 2(a) to identify locations in Manaal image 2(a) after that, all pixel values of Manaal image 2(a) are changed to 8 bit value 11111111 using bit manipulation technique and last four bit values are changed to 0 using bitor and bitand operations and make the value 11110000.

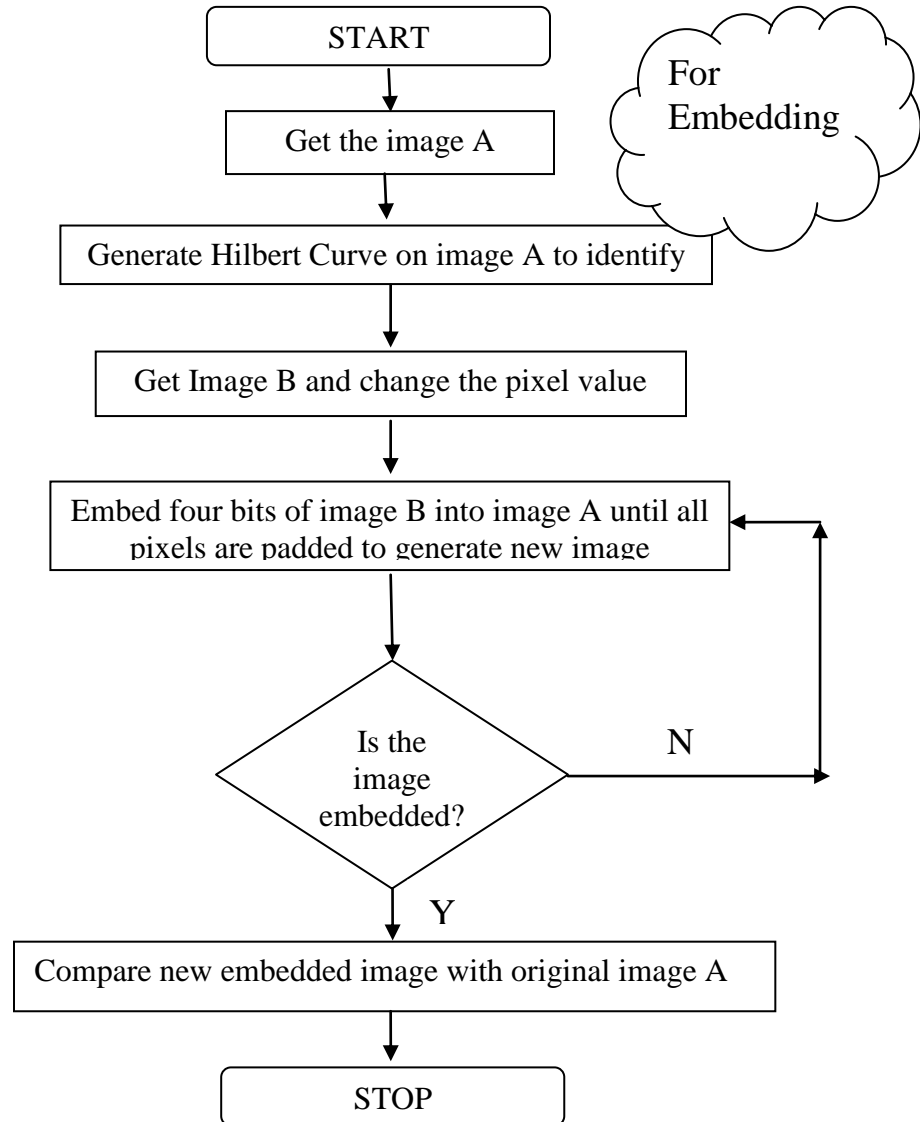
Now, image 2(b) bit value is changed to 8 bit value 11111111 using bit manipulation technique. Then embed first four bits of image 2(b) to last four bits of Manaal image 2(a) to generate new image 3(a) containing stegogramme which is looks like Manaal image 2(a).



(a)  
Figure 3 (a): Manaal Image (extracted)

[Algorithm 1 – Embedding algorithm to hide image using Hilbert Curve]

- |  |
|--|
| <p><b>Step 1:</b> Get the image “A”.</p> <p><b>Step 2:</b> Generate Hilbert Curve to identify targeted region in an Image</p> <p><b>Step 3:</b> Change the Pixel value of Targeted Region in an Image.</p> <p><b>Step 4:</b> Get the image ‘B’ to embed.</p> <p><b>Step 5:</b> Change the pixel value of image ‘B’ using bit manipulation.</p> <p><b>Step 6:</b> Pad the pixel of image ‘B’ to image ‘A’ till all the pixels are embedded to generate stegogramme ‘A<sub>1</sub>’</p> <p><b>Step 7:</b> End.</p> |
|--|



### 3.3 Extracting Algorithm

In the extraction process, we take the embedded image 4(a) and recognize targeted region by generating Hilbert Curve image 4(b) and extract last four bits 1 1 1 1 (5678) of on image.

After getting all the values from embedded image 4 (a), join them together so values are changed to 11111111 to extract the hidden tree image 5(a) from main image 4(a) and compare original, embedded and extracted image.



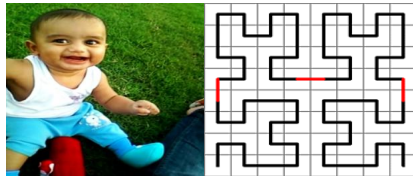


Figure 4 (a): Man Image (With Stegogramme) (b): Hilbert Curve

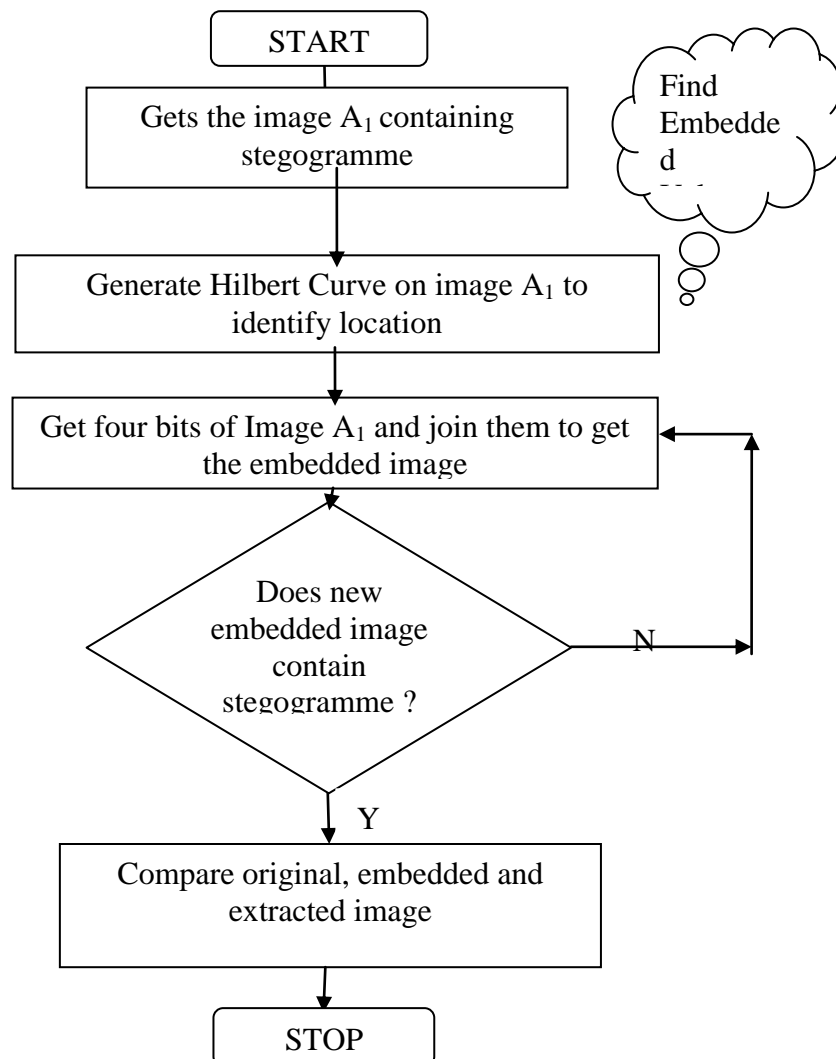


Figure 5 : Tree Image (extracted)

- Step 1:** Get the embedded image ' $A_1$ ' containing Stegogramme..  
**Step 2:** Generate Hilbert Curve to define the locations of Stegogramme.  
**Step 3:** Extract the embedded Pixels by changing the value using bit manipulation.  
**Step 4:** Extract the actual Image and cover image  $A_2$ .  
**Step 5:** End

### 3.4 Flowchart for Extraction

Flowchart 2: Extraction flowchart to hide image using Hilbert Curve





#### 4. Experimental Results

The results are based on comparison of images, histogram of images in gray scale and in RGB. We examine different images for steganography. Over here, we analyze the mean and standard deviation of images to check the intensity of pixel.

Firstly, we hide image (b) within image (a) and new image (c) is generated containing stegogramme. Then we compare cover (carrier/cover) image (a) with image (c) to check whether it is embedded successfully or not. We compare histogram in grey scale and in RGB to check the data distribution and analyze mean and standard deviation of cover image, embedded image and post extracted image to check the intensity of pixels. Results are as follows.

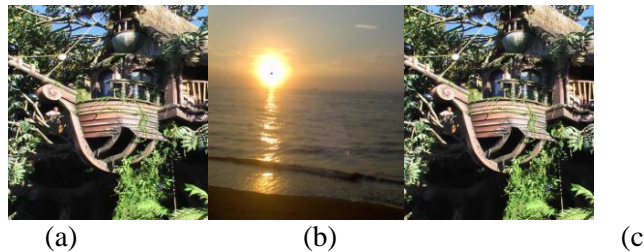
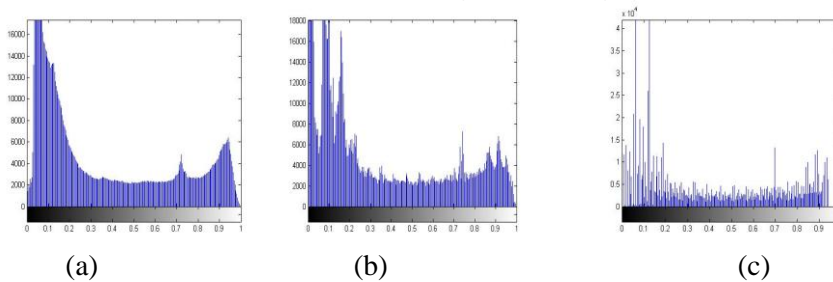
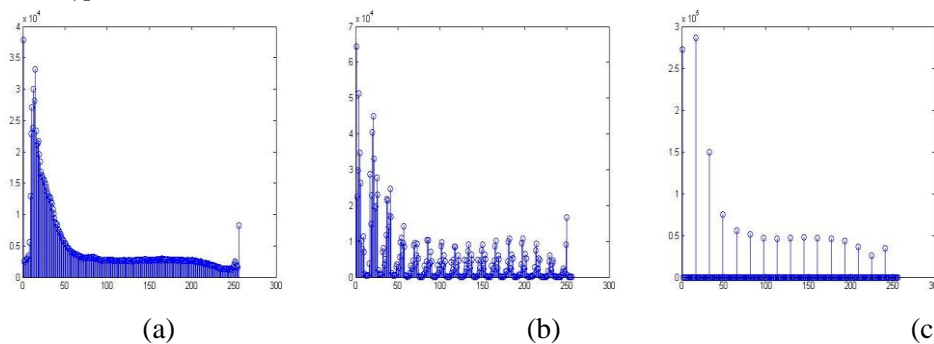


Figure.6 (a): Tree House Image (Carrier/Cover) (b): Sunset (Image to Hide) (c): Tree House-em Image (With Stegogramme)



[Histogram 1 (a): Tree House Image gray scale (Carrier/Cover) (b): Tree House-em Image gray scale (With Stegogramme) (c): Tree House-em Image gray scale (Cover Image Post-Extraction)]



Histogram 2 (a): Tree House Image RGB (Carrier/Cover) (b): Tree House-em Image RGB (With Stegogramme) (c): Tree House-em Image RGB (Cover Image Post-Extraction)

Table 1: Mean and standard deviation of Tree House image in gray scale and in RGB

|            | Mean $\bar{X}$ |                 |                                    | Standard Deviation $\sigma$ |                 |                                    |
|------------|----------------|-----------------|------------------------------------|-----------------------------|-----------------|------------------------------------|
|            | <i>Cover</i>   | <i>Embedded</i> | <i>Cover image Post-Extraction</i> | <i>Cover</i>                | <i>Embedded</i> | <i>Cover Image Post-Extraction</i> |
| Grey Scale | 0.8778         | 0.8747          | 0.9335                             | 0.2928                      | 0.2957          | 0.2197                             |
| RGB        | 241.74         | 243.84          | 248.44                             | 52.85                       | 47.74           | 37.25                              |

Moreover, we find mean and standard deviation of twenty five images to check the intensity of pixels for both gray scale and in RGB as shown in table (2&3).

Table 2: Analysis of images for steganography using Hilbert Curve (grey scale)

| <i>No</i> | Mean $\bar{X}$ |                 |                                    | Standard Deviation $\sigma$ |                 |                                    |
|-----------|----------------|-----------------|------------------------------------|-----------------------------|-----------------|------------------------------------|
|           | <i>Cover</i>   | <i>Embedded</i> | <i>Cover image Post-Extraction</i> | <i>Cover</i>                | <i>Embedded</i> | <i>Cover Image Post-Extraction</i> |
| 1         | 0.8874         | 0.8836          | 0.9052                             | 0.3159                      | 0.3069          | 0.2489                             |
| 2         | 0.8563         | 0.8569          | 0.8763                             | 0.3169                      | 0.3149          | 0.3067                             |
| 3         | 0.8579         | 0.9039          | 0.9076                             | 0.2088                      | 0.2266          | 0.2063                             |
| 4         | 0.8812         | 0.9156          | 0.9107                             | 0.2938                      | 0.2472          | 0.2413                             |
| 5         | 0.9237         | 0.8905          | 0.8934                             | 0.3111                      | 0.3051          | 0.3009                             |
| 6         | 0.8563         | 0.9408          | 0.9432                             | 0.2031                      | 0.2183          | 0.2041                             |
| 7         | 0.8556         | 0.8452          | 0.9421                             | 0.3044                      | 0.2878          | 0.2588                             |
| 8         | 0.8547         | 0.933           | 0.9005                             | 0.3156                      | 0.3047          | 0.2933                             |
| 9         | 0.8596         | 0.8963          | 0.7643                             | 0.3245                      | 0.2256          | 0.2169                             |
| 10        | 0.9389         | 0.9256          | 0.9121                             | 0.3342                      | 0.1914          | 0.1945                             |
| 11        | 0.9458         | 0.8578          | 0.9302                             | 0.2741                      | 0.2278          | 0.2857                             |
| 12        | 0.8612         | 0.9641          | 0.9662                             | 0.2278                      | 0.1946          | 0.1989                             |
| 13        | 0.8878         | 0.9785          | 0.8841                             | 0.2705                      | 0.1932          | 0.1949                             |
| 14        | 0.9128         | 0.9382          | 0.8956                             | 0.1926                      | 0.3175          | 0.2956                             |
| 15        | 0.9378         | 0.9621          | 0.9445                             | 0.2745                      | 0.3068          | 0.2728                             |
| 16        | 0.9378         | 0.8426          | 0.8845                             | 0.2771                      | 0.2938          | 0.2878                             |
| 17        | 0.8659         | 0.9299          | 0.8889                             | 0.3255                      | 0.2869          | 0.2873                             |
| 18        | 0.8759         | 0.9065          | 0.8679                             | 0.2731                      | 0.2836          | 0.2803                             |
| 19        | 0.9378         | 0.9746          | 0.9345                             | 0.1986                      | 0.1986          | 0.1986                             |
| 20        | 0.9426         | 0.9049          | 0.9489                             | 0.3206                      | 0.2972          | 0.2925                             |
| 21        | 0.9412         | 0.9146          | 0.8726                             | 0.2753                      | 0.2675          | 0.2638                             |
| 22        | 0.8569         | 0.8565          | 0.8879                             | 0.2878                      | 0.3075          | 0.2736                             |
| 23        | 0.8579         | 0.8591          | 0.8596                             | 0.2047                      | 0.3095          | 0.3012                             |

|                |          |          |         |          |          |          |
|----------------|----------|----------|---------|----------|----------|----------|
| 24             | 0.8659   | 0.9325   | 0.8793  | 0.2715   | 0.3068   | 0.2976   |
| 25             | 0.8879   | 0.8873   | 0.8879  | 0.2787   | 0.3046   | 0.2983   |
| <b>Average</b> | 0.891472 | 0.908024 | 0.89952 | 0.275228 | 0.268976 | 0.260024 |

We analyze the mean and standard deviation of images with cover image, embedded image and cover image (post extraction) to find the variance between them .After analysis we find that average mean of cover images is 0.8914 ,average mean of embedded images is 0.9080 and average mean of cover image (post extraction) is 0.8995 . Average standard deviation of cover images is 0.2752, average standard deviation of embedded images is 0.2689 and average standard deviation of cover image (post extraction) is 0.2600.It is calculated that, the mean difference between original image and embedded image is 0.0166, mean difference between embedded and cover image (post extraction) is 0.0085 and mean difference between original image and cover image (post extraction) is 0.0081.Further standard deviation difference between original image and embedded image is 0.0063, standard deviation difference between embedded and cover image (post extraction) is 0.0089 and standard deviation difference between original image and cover image (post extraction) is 0.0152.

Table 3: Analysis of images for steganography using Hilbert Curve (RGB)

| No | Mean $\bar{X}$ |          |                             | Standard Deviation $\sigma$ |          |                             |
|----|----------------|----------|-----------------------------|-----------------------------|----------|-----------------------------|
|    | Cover          | Embedded | Cover image Post-Extraction | Cover                       | Embedded | Cover Image Post-Extraction |
| 1  | 247.88         | 247.52   | 248.12                      | 36.78                       | 36.72    | 36.61                       |
| 2  | 239.72         | 240.62   | 247.66                      | 38.68                       | 38.18    | 37.82                       |
| 3  | 248.86         | 246.88   | 247.93                      | 34.22                       | 39.88    | 35.42                       |
| 4  | 247.69         | 247.19   | 247.22                      | 39.41                       | 36.43    | 36.32                       |
| 5  | 241.04         | 247.66   | 247.67                      | 51.42                       | 39.88    | 37.88                       |
| 6  | 248.73         | 247.69   | 247.87                      | 34.51                       | 36.39    | 36.48                       |
| 7  | 242.87         | 245.41   | 247.51                      | 36.78                       | 36.29    | 37.12                       |
| 8  | 245.46         | 245.56   | 249.32                      | 36.21                       | 36.72    | 38.73                       |
| 9  | 249.56         | 249.78   | 249.68                      | 44.98                       | 44.81    | 44.31                       |
| 10 | 242.78         | 242.62   | 242.65                      | 36.95                       | 36.72    | 36.18                       |
| 11 | 242.32         | 242.18   | 246.37                      | 38.15                       | 46.68    | 46.43                       |
| 12 | 246.78         | 246.68   | 246.65                      | 38.82                       | 35.19    | 35.46                       |
| 13 | 245.78         | 245.68   | 247.88                      | 34.18                       | 34.78    | 34.83                       |
| 14 | 248.78         | 247.89   | 247.78                      | 47.12                       | 48.96    | 48.12                       |
| 15 | 241.56         | 242.86   | 242.96                      | 42.78                       | 34.46    | 34.12                       |
| 16 | 250.78         | 249.88   | 248.76                      | 42.51                       | 34.09    | 33.46                       |
| 17 | 244.81         | 245.71   | 245.81                      | 41.88                       | 49.66    | 48.53                       |
| 18 | 249.52         | 249.69   | 249.86                      | 37.89                       | 37.83    | 35.96                       |

---



---

|                |          |          |          |         |         |         |
|----------------|----------|----------|----------|---------|---------|---------|
| 19             | 244.89   | 245.56   | 245.73   | 36.72   | 37.81   | 37.78   |
| 20             | 248.69   | 248.81   | 246.82   | 43.78   | 43.56   | 42.56   |
| 21             | 244.43   | 244.56   | 245.78   | 41.63   | 41.82   | 40.96   |
| 22             | 248.17   | 248.93   | 249.08   | 44.18   | 44.73   | 43.88   |
| 23             | 243.56   | 243.15   | 243.81   | 48.18   | 49.89   | 48.53   |
| 24             | 244.96   | 244.93   | 243.78   | 39.88   | 34.78   | 34.63   |
| 25             | 244.56   | 244.15   | 244.86   | 48.88   | 48.56   | 48.37   |
| <b>Average</b> | 245.7672 | 246.0636 | 246.8624 | 40.6608 | 40.1928 | 39.6196 |

We analyze the mean, standard deviation of images between cover image, embedded image and cover image (post extraction) to find the variance between them .After analysis of twenty five different images we find that average mean of cover images is 245.76,average mean of embedded images is246.06 and average mean of cover image (post extraction) images is 246.86. Average standard deviation of cover images is 40.66, average standard deviation of embedded images is 40.19 and average standard deviation of cover image (post extraction) is 39.61. It is calculated that, the mean difference between original image and embedded image is 0.2964, mean difference between embedded and cover image (post extraction) is 0.7988 and mean difference between original image and cover image (post extraction) is 1.0952.Further standard deviation difference between original image and embedded image is 0.468, standard deviation difference between embedded and cover image (post extraction) is 0.5732 and standard deviation difference between original image and cover image (post extraction) is 1.0412.

## 5. Conclusions

It was concluded that the image containing stegogramme is not recognized by the naked eye detection, there is not much difference between cover, embedded and cover (post-extraction) image. In the analysis we find mean and standard deviation and concluded that there is negligible difference amongst them and not easy to detect the stegogram.

## 6. Limitations and Future Work

The research provides an opportunity to go ahead in the field of Information Hiding. The research can be extended by using other fractals for the purpose of steganography.

The limitation of our technique is that the size of image to hide should be equal to the size of the fractal used. It may be attempted to overcome.

Moreover, the research may be extended by using different carriers (covers) like audio and video. One of the methods for audio steganography is to substitute the least significant bit of each sample of the cover speech signal with the secret data. While this method is easy to implement and can be used to hide larger secret messages, it cannot protect the hidden message from small modifications that can happen as a result of format conversion or compression, so further advancement is needed. Moreover, in the video steganography generally video is separated into audio and images .Therefore any of them is selected as cover /carrier and data are embedded within them using LSB or any other technique.The research can be furthered by using cryptography with steganography to enhance the security

---

because by using cryptography, we can convert our plain text message to cipher text by using the secret key and embed the cipher text into any cover medium using steganographic techniques.

## References

- [01] E.H. Blakeney Herodotus, the Histories, chap. 5 book entitled Terpsichore, & chap .7 books entitled Polymnia. London, England: J. M. Dent & Sons, Ltd, 1992.
- [02] D. Hilbert: Uber die stetige Abbildung einer Linie auf ein Flachenstuck. *Mathematische Annalen* 38, 459–460, 1891.
- [03] G.Peano; Sur une courbe, qui remplit toute une aire plane. *Mathematische Annalen* 36, 157–160, 1890.
- [04] A. Westfeld and A. Pfitzmann, “Attacks on Stegano graphic Systems,” *Proc. Information Hiding 3rd Int’l Work- shop*, Springer Verlag, pp. 61–76, 1999.
- [05] N.F. Johnson and S. Jajodia, “Steganalysis of Images Created Using Current Steganographic Software,” *Proc. 2nd Int’l Workshop in Information Hiding*, Springer-Verlag, pp. 273–289, 1998.
- [06] T. Zhang and X. Ping, “A Fast and Effective Steganalytic Technique against JSteg-like Algorithms,” *Proc. 8th ACMSymp. Applied Computing*, ACM Press, 2003.
- [07] N. Provos. "Defending Against Statistical Steganalysis", *Proceedings of the 10th USENIX Security Symposium*, vol. 10, pp. 323-335, 2001.
- [08] N. Provos and P. Honeyman. "Hide and Seek: An Introduction to Steganography", *IEEE: Security & Privacy*, vol. 1, pp. 32-44, 2003.
- [09] A. Westfeld. "F5 - A Steganographic Algorithm: High Capacity Despite Better Steganalysis", *Lecture Notes in Computer Science*, vol. 2137, pp. 289-302, 2001.
- [10] M. Leivaditis. "Statistical Steganalysis", Master’s thesis, Department of Computing, University of Surrey, 2007.
- [11] Davern , P. and Scott, M., “Fractal based image steganography,” *Proc. of the First Intl. Workshop on Information Hiding*, *Lecture Notes in Computer Science* 1174, 279-294 (1996).
- [12] A. Jacquin “A Fractal Theory of iterated Markov operators with Applications to Digital image coding PhD thesis Georgia institute of Technology “, 1995.
- [13] J. Pauate, and F.D. Jordan, “Using Fractal Compression Scheme to Embed a Digital Signature in to an Image,” *Proc. Of SPLE* 2915, 108-118, 1997.
- [14] D. Saupe, and R. Hamzaoui, “A Review of the Fractal Image Compression Literature,” *Computer graphics* 28(4), 268-276, 1994.
- [15] B. Wotilberg and G. De jager, “A Review of the Fractal Image Coding literature,” *IEEE Trans, on image processing* 8(12), pp. 1716-1729, 1999.
- [16] Bas, P., Chassery, J. M., Davoine, F. Using the Fractal Code to Watermark Images // *Proc ICIP’98*, 1998. – № 1. P. 469-473.

- 
- [17] Li, C., Wang, S. Digital Watermarking Using Fractal Image Coding // IEICE Trans. Fund., 2000. – № 6. – P.1286-1288.
- [18] Liao, P., Chen, C., Chen, C., Pan, J. Interlacing Domain Partition for Fractal Watermarking // IJHMSP' 06, 2006. – P. 441-444.
- [19] L. Kumar ,” Novel Security Scheme for Image Steganography using Cryptography Technique”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, 2012.
- [20] R. Ibrahim and T. Suk Kuan,”Steganography Imaging System (SIS): Hiding Secret Message inside an Image”, Proceedings of the World Congress on Engineering and Computer Science 2010 Vol IWCECS 2010, San Francisco, USA, 2010.
- [21] W. Frączek, W. Mazurczyk, K. Szczypiorski,”Stream Control Transmission Protocol Steganography”, Multimedia Information Networking and Security (MINES), International Conference, pp - 829 – 834, 2010.
- [22] S.Hemalatha, D. Acharya, A.Renuka and P. Kamath,” A Secure and High Capacity Image Steganography Technique”, Signal & Image Processing: An International Journal (SIPIJ) Vol.4, No.1, 2013.
- [23] S.R. Govada, B.S. Kumar , M. Devarakonda and M. J. Stephen, “Text Steganography with Multi level Shielding” , IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3,2012.
- [24] G. Dhanarasi and Dr.A. Mallikarjuna Prasad, “Image Steganography Using Block Complexity Analysis”. International Journal of Engineering Science and Technology Vol. 4, pp 34-39, 2012.