Constructive Role of SFC & RGB Fusion versus Destructive Intrusion

R.Amirtharajan
Assistant Professor
ECE/SEEE
SASTRA University

R.John Bosco Balaguru
Professor
ECE/SEEE
SASTRA University

ABSTRACT

Digital Crime is the latest terrorist who can intrude into any domain by breaking any type of firewall or secret code without frittering even a single drop of blood. To fight this terror, a cryptic army was evolved but not good enough to succeed. As a consequence, an effective commando namely steganography has been evolved who can combat any type of destructive intrusion. In this paper, Space Filling Curve (SFC) and RBG colour compound stego action against the threat of digital crime has been proposed. The proposed stego system scans the colour image pixel by pixel along a complex path, not row by row, and hides the variable k bit of the secret data in each pixel visited in the order defined by a Space-Filling Curve (SFC) such as the Hilbert curve and the Moore curve traversing paths. Such curves visit each pixel in the color image which is split into Red, Green and Blue components. The effectiveness of the proposed stego system has been estimated by computing bit error rate (BER), Mean square error(MSE),Peak Signal to Noise Ratio (PSNR) and Mean Structural Similarity index(MSSIM). This paper also illustrates how security has been enhanced using this algorithm.

Categories and Subject Descriptors

D.2.11 Information hiding
D.4.6 Security and Protection

General Terms

Security

Keywords

LSB Steganography, Information hiding, Space Filling Curves Steganography.

1. Introduction

Internet has shrunk the world into a global village. The amount of information being communicated via internet has increased manifold times. No one can ever eradicate the capricious usage of the information that is being shared over the internet. Therefore, data encryption [2, 6, 13] and data hiding[1, 8, 10] are used to protect the sensitive data from disclosure when they are transmitted over an insecure channel. In data encryption, at the sender end data is encrypted with a secret key K_p to form a cipher text. Only the authorized receiver could decrypt the cipher text with the secret key K_p to obtain the secret data. However, the transmitted cipher text is a string of irregular codes. It flags the importance of the transmitted data and attracts the attention of illegal users who either decipher it or destroy it completely. Data hiding provides a good solution to overcome this problem.

The concept of data hiding or steganography was first proposed by Simmons in 1983. According to dictionary, steganography (also known as "steg" or "stego") is the art of writing in cipher, or in characters, which are not intelligible except to persons who have the key. In computer terms, steganography has evolved into the practice of hiding a message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. In contemporary terms, steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file or even a video file [1, 8, 10]. The techniques of data hiding have to exhibit imperceptibility and hiding capacity. Even after hiding the secret message, the stego image must be of high quality. This property could prevent the attackers from detecting the secrets existing in the stego-image. The number of the secret bits (payload) that can be hidden into the cover image should be as large as possible.

Another classification in information hiding [10] called digital watermarks also known as fingerprinting is significant especially in copyrighting materials which are similar to steganography. They are overlaid in files, which appear to be part of the original file and are thus not easily detectable by any average person. Watermarking has been widely used to protect the copyright of digital images. It embeds a trademark of the owner into the protected image. The owner can prove the ownership of the suspected image by retrieving the embedded trademark. Water marking must satisfy the requirements of imperceptibility, security and robustness.

Data secrecy expects the following from watermarking and from information hiding. Initially both hides the data into the cover and only the legal user could exactly extract data from the stego cover. Furthermore, the quality of processed image is very important. The higher image quality makes people more difficult to perceive the existence of sensitive data.

One of the straight solutions of hiding secret data is to directly replace the Least Significant Bit (LSB) of each pixel in the cover image with the bits of secret data. It results in less distortion than directly manipulating the Most Significant Bit (MSB) of each pixel in the cover image. Hence, the method [3] is very simple and the scheme could maintain a good image quality. However, the stego-image creation uses simple raster scan for embedding and extraction so there is a possibility of vulnerability of secret data threat. Therefore, it has been proposed a data hiding scheme to comply with the following requirements.

First, the quality of the embedding image should be acceptable so that the human eye cannot perceive the embedded data from the stego image.

Second, the scheme provides the ability of high payload so that more data could be embedded with high imperceptibility.

Third, the complexity against an adversary will be increased to many folds by adapting Hilbert or Moore SFC based embedding instead of raster scan method.

Fourth, if random scan applied to stego system key length plays a role which is usually shared between the participants as private keys but in the proposed method no key has been shared between the parties. So that the legal user can more correctly extract the embedded data from the stego-image without keys

In the current process of information hiding an interesting and novel data embedding scheme has been proposed and implemented successfully. Instead of adapting the usual raster scan for data embedding and extracting from the pixels of an image, embedding based on Hilbert, Moore [7, 18] space filling curves in RGB planes has been identified as an innovative and effective technique. The flow of space filling curve will provide the embedding path for stego process which will definitely be a nightmare for hackers. Before embedding the secret data, the cover image considered has been divided into equal number of repeated smaller blocks The level of confidentiality of this proposed scheme has also been tested with four different metrics.

The rest of this paper is organized as follows. Related work will be described in Section 2. The proposed method will be presented in Section 3.Experimental results will be discussed in Section 4. Finally, a brief conclusion will be presented in Section 5.

2. Related works

In the recent past, many steganography methods have been proposed and they are classified into two major types based on the cover image domains namely spatial [1, 3, 19] and frequency [4, 11]. In the spatial domain the encrypted secret data is hidden in the pixels of cover image by employing Least Significant Bit (LSB) [3, 16], pixel value differencing [17,19], mod [14, 17], lossless data hiding [4, 5] and spread spectrum [9] based schemes. These schemes have been adapted by many authors to achieve good imperceptibility with higher pay load [14]. In the frequency domain methods, the secret data is hidden in the transformed coefficients of the cover image where Discrete Cosine Transform (DCT) [4] and Discrete Wavelet Transform (DWT) [11] act as domain converters.

In spatial domain stego methods, LSB embedding scheme has been widely used to hide secret data because of its simplicity and speed of implementation. In addition this technique offers higher hiding capacity and at the same time quality of the stego image can be well-controlled [3]. In LSB embedding process, authors have adapted raster scan [1, 3, 8, 9, 14, 16, 17, 19] as well as random scan [7, 12, 15, 18] to hide the secret data in each pixel. Between these two scans, random is preferred over raster to increase the level of complexity against the eavesdroppers. But the real challenge is on maintaining good imperceptibility of the stego image and sharing the secret key for retrieving the original message.

Tuomas Aura [15] has proposed a stego method by adapting random embedding procedure in which stego key and a secure hash function are used to generate a sequence of unique pixel addresses for embedding. Provos *et.al* [12] has proposed a hide and seek software is a technique for random selection of pixels for embedding secret data and hence generating stego image. In these random approaches all the pixels of the cover image have not been used for hiding secret data which in turn affect the payload besides good imperceptibility.

Recently, a scheme proposed in [20] hide large amount of data in true color image. It uses 8 bits to represent each color component of the color pixel. The secret image can be either grayscale image or colored image. However the secret image extracted was not good in terms of peak signal to noise ratio (PSNR) value and visual observation. Grayscale cover image has limited capacity and the usage is also limited. Only few papers of steganography techniques have been presented on color image [5, 20]. These schemes use the transform domain and the hiding capacity is increased.

From the literature it is obvious that obtaining maximum stego-image quality as well as payload, minimum key length with more complexity against hackers through either random or raster scan based stego technique is found to be rare. Hence in this paper, the authors have proposed and implemented SFC based variable k-bit embedding stego method with an aim of achieving higher imperceptibility, payload, optimized key length and mammoth complexity against hackers.

3. Methodology

In general, random embedding scheme requires a specific key with variable size to retrieve the embedded secret data at the receiving end. In order to overcome this drawback, the concept of space filling curve (SFC) has been adapted for embedding the secret data in image where Hilbert and Moore SFC method can be used for k-bit embedding.

SFC is a one dimensional curve which traverses through each and every point within a two dimensional space or image. SFC scans a pixel array which has a size of M x N pixels and while scanning, it will not retain the same direction but will turn around to embrace all the pixels at least and at most once. Hence the unpredictable traversing path of SFC through the image has been chosen to hide the secret message in the cover. In this scheme, both the sender and receiver can adapt a particular SFC so that there is no need to communicate the key and also providing a complicated traversing path for k-bit embedding which does not require any key.

Before considering the entire cover image for secret bit embedding, block of 4 × 4 pixels has been taken to implement Hilbert SFC and Moore SFC traversing path based stego technique by adapting a common traversing path for both the sender and receiver. After performing this process for a single 4 × 4 block, it has been extended to the full image by considering it as multiple of 4x4 blocks to cover up the entire $2^8 \times 2^8 \times 3$ pixels.

The traversing paths to embed secret data, based on Hilbert SFC and Moore SFC in gray scale are shown in Figures 1 and 2 and Hilbert scan and Moore SFC in RGB in Figure 3 and 4.

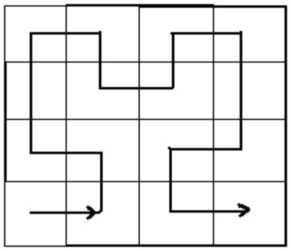

Figure 1. Hilbert Scan

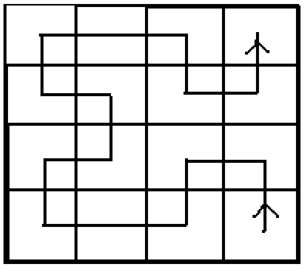

Figure 2 Moore Curve

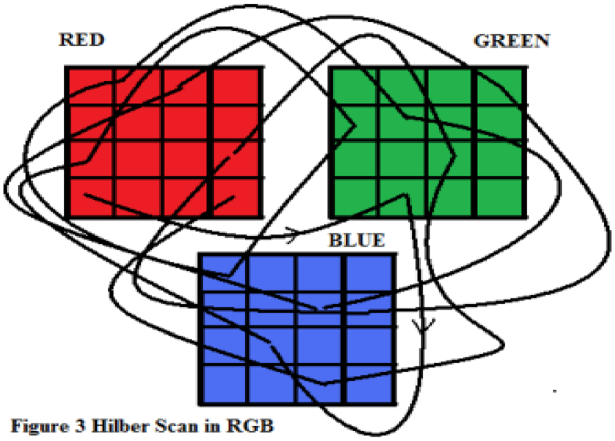

Figure 3 Hilber Scan in RGB

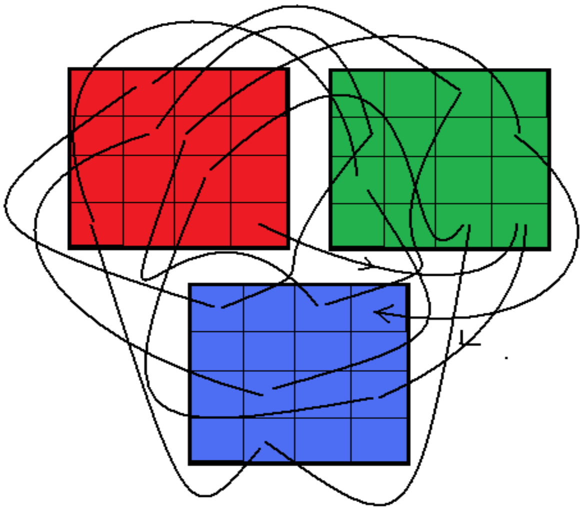

Figure 4 Moore Curve in RGB

3.1 Embedding module

Algorithm for secret data embedding process:

Input : Color cover Image (Ic) and Secret message (S)
Output : Stego Cover

Step 1 : Read the Colour cover image (Ic) and the secret data to
be embedded
Step 2 : Scramble the secret data using DES
Step 3 : Convert the secret data into binary row matrix
Step 4 : Split the cover into RGB planes
Step 4 : Divide the image into 4×4×3 blocks
Step 5 : Call Hilbert or Moore traversing module on step 4
Step 6 : Implement variable k-bit LSB embedding module
as specified by the user
Step 7 : Combine the RGB plane to form stego cover

3.2 Retrieval module

Algorithm for secret data recovery process:

Input : Stego Cover Image (Is)
Output : Secret message (S)

Step 1 : Read the stego image (Is) and split to RGB planes
Step 2 : Divide the image into 4×4×3 blocks
Step 3 : Call Hilbert or Moore traverse module
Step 4 : Implement variable k bit LSB retrieval module
Step 5 : Decrypt the scrambled data
Step 6 : Save the secret data (S)

3.3 Error metrics

The effectiveness of the stego process proposed has been studied by estimating the following four metrics for both cover images.

Bit Error Rate (BER) and Bit Error

BER evaluates the actual number of bit positions which are replaced in the stego image in comparsion with cover image. It has to be computed to estimate excatly how many bits of the original cover image(I_c) are being affected by stego process. The BER for the Stego image (I_s) is the percentage of bits that have errors relative to the total number of bits considered in I_c.

Let I_{cbin} and I_{sbin} are the binary representations of the cover image and stego cover then,

The total number of bit errors, $T_e = \sum_{i=1}^{n} \left| I_{cbin} - I_{sbin} \right|$

And the bit error rate BER = T_e / T_n

T_n is the total number of bits considered for the gray image of size M × N pixels. T_n will be M × N × 8.

Peak Signal to Noise Ratio (PSNR)

The PSNR is calculated using the equation,

$$PSNR = 10\log_{10}\left(\frac{I_{\max}^2}{MSE}\right)dB$$

where I_{max} is the intensity value of each pixel which is equal to 255 for 8 bit gray scale images. Higher the value of PSNR better the image quality

Mean Square Error (MSE)

The MSE is calculated by using the equation,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{i,j} - Y_{i,j}\right)^2$$

where *M* and *N* denote the total number of pixels in the horizontal and the vertical dimensions of the image *Xi*, *j* represents the pixels in the original image and *Yi*, *j*, represents the pixels of the stego-image.

Mean Structural SIMilarity Index (MSSIM) (Zhou Wang et al 2004)[22]

We use a mean SSIM (MSSIM) index to evaluate the overall image quality using the equation,

$$MSSIM(X,Y) = \frac{1}{M}\sum_{j=1}^{M} SSIM\left(X_j, Y_j\right)$$

$$SSIM(X,Y) = \frac{\left(2\mu_x\mu_y + C_1\right)\left(2\sigma_{xy} + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)} \quad (5)$$

where $C_1 = (K_1L)^2$ L=255

$K_1 = .01$

$C_2 = (K_2L)^2$ L=255

$K_2 = .03$

$$\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i$$

where μ_x is the estimate of the mean intensity of the cover image for N= 255, which is representing the total number of pixels, σ_x is the standard deviation (the square root of variance) as an estimate of the signal contrast.

$$\sigma_x = \left(\frac{1}{N-1}\sum_{i=1}^{N}\left(x_i - \mu_i\right)^2\right)^{\frac{1}{2}}$$

Geometrically, the correlation coefficient σ_{xy} is computed using σ_x and μ_x is given by

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}\left(x_i - \mu_x\right)\left(y_i - \mu_y\right)$$

The value of MSSIM is in the interval [1, 0]. The value 1 means that the two images are exactly the same and 0 means totally unrelated.

4. Results and Discussion

In this present implementation Lena and baboon 256 × 256 digital images has been taken as cover images for the Hilbert SFC and Moore SFC traversing path based stego method are shown in

Table 1. Estimation Parameters of Hilbert 4×4 Block Embedding Scheme in RGB planes

Cover image	RGB Plane	K bit	BER	MSE	PSNR	MSSIM
Lena	R	3	0.1883	7.9889	39.1059	0.9644
	G	2	0.1249	2.4587	44.2237	0.9886
	B	3	0.1873	11.570	37.4974	0.9370
Baboon	R	3	0.1876	7.9285	39.1388	0.9900
	G	2	0.1243	2.4520	44.2354	0.9970
	B	3	0.1872	11.621	37.4783	0.9856
Lena	R	3	0.1667	9.4400	38.3810	0.9479
	G	3	0.1663	9.3421	38.4263	0.9513
	B	3	0.1665	9.4111	38.3943	0.9460
Baboon	R	3	0.1668	9.4348	38.3834	0.9860

	G	3	0.1673	9.4328	38.3844	0.9863
	B	3	0.1669	9.4056	38.3969	0.9881
Lena	RGB avg	4 each	0.2492	42.603	31.7984	0.9463
Baboon	RGB avg	4 each	0.2500	42.648	31.8318	0.9511
Lena	RGB avg	2 each	0.1251	2.4012	44.3265	0.9856
Baboon	RGB avg	2 each	0.1251	2.4087	44.3129	0.9965
Lena	RGB avg	1 each	0.0623	0.4990	51.1491	0.9968
Baboon	RGB avg	1 each	0.0626	0.5014	51.1284	0.9992
Lena	R	2	0.1255	2.1821	44.7419	0.9907
	G	3	0.1876	7.8852	39.1626	0.9622
	B	3	0.1873	11.570	37.4973	0.9370
Baboon	R	2	0.1254	2.1735	44.7590	0.9976
	G	3	0.1869	7.8488	39.1827	0.9895
	B	3	0.1872	11.621	37.4783	0.9856
Lena	R	3	0.1883	7.9892	39.1057	0.9644
	G	3	0.1876	10.709	37.8331	0.9550
	B	2	0.1252	2.5730	44.0263	0.9846
Baboon	R	3	0.1876	7.9286	39.1388	0.9900
	G	3	0.1873	10.695	37.8388	0.9874
	B	2	0.1244	2.5690	44.0331	0.9967

Figures 5. Each cover image has been divided into multiple blocks of 4x4x3 pixels. The encrypted secret data has been hidden in each pixel of 4x4x3 block by adapting k-bit LSB technique and in the same way the secret message has been embedded in all the

Table 2. Estimation Parameters of Moore 4×4 Block Embedding Scheme in RGB planes

Cover image	RGB Plane	K bit	BER	MSE	PSNR	MSSIM
Lena	R	3	0.1880	7.9840	39.1085	0.9644
	G	2	0.1254	2.4794	44.1872	0.9884
	B	3	0.1872	11.600	37.4861	0.9369
Baboon	R	3	0.1876	7.9237	39.1415	0.9900
	G	2	0.1249	2.461	44.2191	0.9969
	B	3	0.1871	11.523	37.5149	0.9858
Lena	R	3	0.1877	10.703	37.8357	0.9426
	G	3	0.1871	10.492	37.9220	0.9471
	B	3	0.1877	10.654	37.8556	0.9406
Baboon	R	3	0.1872	10.620	37.8692	0.9842
	G	3	0.1877	10.636	37.8626	0.9848
	B	3	0.1876	10.586	37.8833	0.9867
Lena	RGB avg	4 each	0.2513	44.118	31.6865	0.8464
Baboon	RGB avg	4 each	0.2495	42.536	31.8432	0.9515
Lena	RGB avg	2 each	0.1251	2.4124	44.3062	0.9855
Baboon	RGB avg	2 each	0.1252	2.4086	44.3131	0.9965
Lena	RGB avg	1 each	0.0626	0.5014	51.1283	0.9968
Baboon	RGB avg	1 each	0.0625	0.5002	51.1388	0.9992
Lena	R	2	0.1254	2.1764	44.7533	0.9907
	G	3	0.1883	7.8961	39.1566	0.9622
	B	3	0.1872	11.600	37.4861	0.9369
Baboon	R	2	0.1258	2.1803	44.7455	0.9976
	G	3	0.1877	7.9294	39.1383	0.9893
	B	3	0.1871	11.523	37.5151	0.9858
Lena	R	3	0.1880	7.9840	39.1085	0.9644
	G	3	0.1876	10.759	37.8128	0.9547
	B	2	0.1249	2.5712	44.0292	0.9846
Baboon	R	3	0.1876	7.9239	39.1413	0.9900
	G	3	0.1879	10.761	37.8119	0.9873
	B	2	0.1248	2.5722	44.0276	0.9967

256 x 256x 3 pixels of the cover image. In the current implementation, k=1, 2, 3 and 4 bits LSB embedding [6] have been accomplished to obtain the final stego cover. Figures 6, 7 and 8 show the stego covers for the k=3, 2, 3in RGB plane. Four different metrics have been used to evaluate the quality of the stego covers. The computed metric values of both images employing Hilbert SFC and Moore SFC given in Table I and II respectively.

From this implementation it is observed that the number of bit error value increases with increase in the number of k-bit embedding. It is also found that Moore SFC based embedding shows a little higher bit error than the Hilbert SFC case. From the estimated values of MSE one can note that it increases with increase in the number of k-bit embedding and this trend is the result of significant depth of distortion on each pixel due to increasing number of bit embedding. Same type of variations has been observed for both stego covers.

Figure 5 Cover Image Lena and Baboon 256 × 256 Pixels

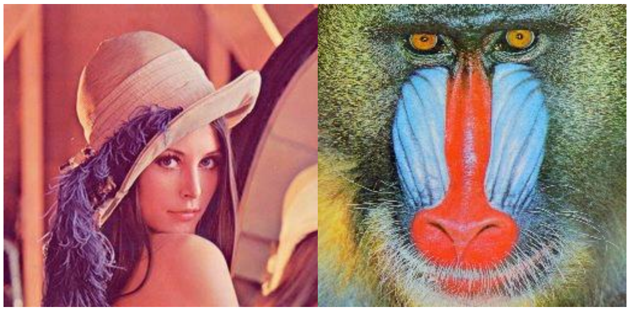

Figure 6 Stego Cover Lena and Baboon through Hilbert SFC for k= 3 in RED, k=2 in GREEN and K=3 in BLUE

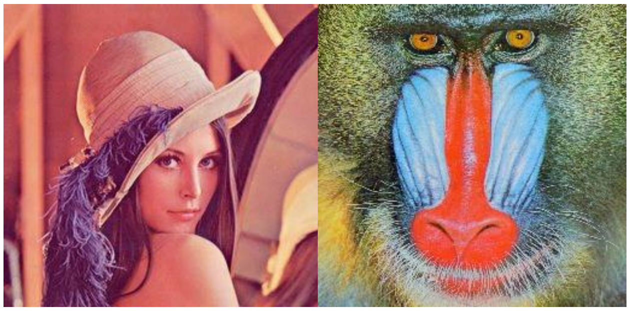

Figure 7 Stego Cover Lena and Baboon through Moore SFC for k= 3 in RED, k=2 in GREEN and K=3 in BLUE

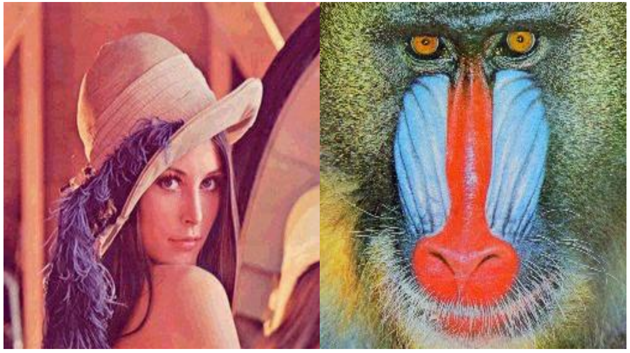

Figure 8 Stego Cover Lena and Baboon through Hilbert SFC for k= 4 in RED, k=4 in GREEN and K=4 in BLUE

Computed values of PSNR prove that, it is better for lower k bit embedding than the higher k bit case. It is a known fact that the PSNR value should be greater than 30 dB for a better stego cover and the present calculated result substantiates the same. In the present case, it is significant that even for the k=4 bit in all planes case this value is around 31 dB which confirms the effectiveness of this SFC based stego technique.

In addition to the PSNR pixel quality estimation, the authors have estimated two types of image quality index based on statistics measures namely universal image quality index and MSSIM [21]. But in the present implementation, the estimated universal quality index is always found to be closer to 1 for k=1 to 4 bit embedding. Hence the latter method has been adapted to evaluate the quality index for all the k-bit cases. From the computed values it has been observed that the MSSIM value decreases with increase in k-bit embedding which validates the deteriorating quality of stego cover.

All the estimating parameters of the two stego covers have been performed using indigenous matlab code in Intel Core2 Duo CPU processor @ 1.60 GHz, 1GB RAM.

5. Conclusion

The present stego system employs several security techniques to protect the clandestine information from being abused. As an initial protection, prior to embedding, the secret information has been scrambled through DES. During the embedding process, the cover image is divided into several blocks in which user has many options to select the size of the basic block. As 30 dB is fixed as the threshold PSNR value for human visual system, the present results possess excellent imperceptibility without noticeable degradation and the same is well supported by the estimated PSNR value for the stego covers. Since the scrambled message has been hidden imperceptibly in the cover image through variable k-bit embedding in a specific traversing scheme through SFC, the effectiveness of stego process has increased appreciably and toughness to crack the secrecy against any serious threat is also improved significantly. In general, all the estimated parameters show the same trend for the images and also for Hilbert and Moore SFC based embedding cases.

References

[1]. W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3&4) (1996) 313–336.

[2]. Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition 2007

[3]. C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) (2004) 469–474.

[4]. Chin-Chen Chang, Chia-Chen Lin, Chun-Sen Tseng and Wei-Liang Tai, “Reversible hiding in DCT-based compressed images,” Information Sciences, Vol. 177, Issue 13, (2007) 2768-2786.

[5]. Chin-Chen Chang, Chih-Yang Lin, Yi-Hsuan Fan, Lossless data hiding for color images based on block truncation coding , Pattern Recognition 41 (7) 2008 2347-2357.

[6]. W. Diffie and M. E. Hellman, “Exhaustive Cryptanalysis of the NBS Data Encryption Standard,” IEEE Computer, Vol. 10, 1977, pp. 74-84.

[7]. Hans Sagan, Space-Filling Curves, Springer-Verlag, New York, (1994). ISBN: 0-387-94265-3.

[8]. S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[9]. L.M. Marvel, C.G. Boncelet Jr., C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process. 8 (8) (1999) 1075-1083.

[10]. F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding—a survey, Proc. IEEE 87 (7) (1999) 1062–1078.

[11]. Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering 4(3) (2006) 275-290.

[12]. Provos, N., Honeyman, P, Hide and seek: An introduction to steganography, IEEE Security & Privacy Magazine 1 (2003) 32-44.

[13]. R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, vol. 21, no. 2, (1978) 120–126.

[14]. C.C. Thien, J.C. Lin, A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function, Pattern Recognition 36 (11) (2003) 2875–2881.

[15]. Tuomas Aura, Practical invisibility in digital communication, in proceedings of the Workshop on Information Hiding, LNCS 1174 (1996) 265-278.

[16]. R.Z. Wang, C.F. Lin, J.C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2000) 671–683.

[17]. C.M. Wang, N.I. Wu, C.S. Tsai, M.S. Hwang, A high quality steganography method with pixel-value differencing and modulus function, J. Syst. Software 81 (1) (2008) 150–158.

[18]. Westfeld Space filling curves in steganalysis in E.J Delp III & P.W. Wong(Eds), Security, steganography and watermarking of multimedia contents VII SPIE 5681, (2005) 28-37

[19]. Young-Ran Park, Hyun-Ho Kang, Sang-Uk Shin, and Ki-Ryong Kwon, An Image Steganography Using Pixel Characteristics Y. Hao et al. (Eds.): CIS 2005, Part II, Springer-Verlag Berlin Heidelberg LNAI 3802, (2005) 581– 588.

[20]. Yuan-Hui Yu , Chin-Chen Chang, Iuon-Chang Lin, A new steganographic method for color and grayscale image hidingComputer Vision and Image Understanding 107 (2007) 183–194

[21]. Zhou Wang, Alan Conrad Bovik, Hamid Rahim Sheikh, Eero P. Simoncelli, Image Quality Assessment: From Error Visibility to Structural Similarity, IEEE Transactions on Image Processing, 13(4) (2004) 600-612.