Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 14 (2019) pp. 040-047

High Capacity Image Steganography Based on Prime Series Representation and Payload Redundancy Removal

Muhammad Zaheer[1], Ijaz Mansoor Qureshi[1], Kiran Sultan[2], Atta-ur-Rahman[3], Muhammad Zeeshan Muzaffar[4] and Reem Alnanih[5]

[1]Department of Electrical Engineering, Air University,
Islamabad, Pakistan,
{mzaheer, imqureshi}@mail.au.edu.pk

[2]Dept. of Computer & Information Technology (CIT), JCC, King Abdulaziz University,
Jeddah, Saudi Arabia
kkhan2@kau.edu.sa

[3]Dept. of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University,
P.O. Box 1982, 31442, Dammam, Saudi Arabia
aaurahman@iau.edu.sa

[4]Barani Institute of Information Technology (BIIT), PMAS-AA University,
Rawalpindi, Pakistan
zeeshan@biit.edu.pk

[5]Dept. of Computer Science, FCIT, King Abdulaziz University,
Jeddah, Saudi Arabia
ralnanih@kau.edu.sa

Abstract: **Least significant bit (LSB) steganography is the most widely employed technique, as it promises imperceptibility at low computational complexity while hiding the message in LSBs of cover image pixels. Recent research is focused on its capacity improvement by extending the embedding into second and third binary layers of cover image. This paper is focused to improve both capacity and imperceptibility. Considering the cover image, an advance technique for embedding is introduced based on representing cover image pixels using a new 13-bit prime series representation which increases the embedding capacity 3-times as compared to conventional LSB embedding. Moreover, an adaptive algorithm has also been proposed which automatically adjusts the chaotic key used to select the locations of embedding pixels based on the dimensions of cover and secret image. It ensures that the entire secret image is randomly spread and covered in the cover image. Furthermore, redundancy of the secret image has been reduced significantly by applying two dimensional DCT and thresholding for the coefficients. The 2-bit Reed Solomon error correction code applied to the secret information enhances security and reliability against attacks. Consequently, the simulation results illustrate minimum visual distortion effects in the proposed model along with correct recovery of secret data.**

Keywords: Image Steganography, LSB Embedding, DCT, Prime Series, Payload

I. Introduction

Steganography is widely adopted technique for invisible data communication by hiding message into a carrier file like image [1]. Steganography is categorized into four types depending on the cover that are image, audio, video and text [2]-[3]. Moreover, the image steganography is categorized into spatial and transform domain image steganography as depicted in Fig.1.The spatial domain techniques are based on directly manipulating over the pixels of the cover image, whereas in transform domain the secret message is hidden in the transformed cover image [4]. There are various categories of techniques that are widely used in spatial domain such as Least Significant Bit (LSB) substitution, Pixel Value Differencing (PVD), Exploiting Modification Direction (EMD), etc [5]-[6]. The transform domain techniques are categorized based on some defined transforms like DCT, DWT and FFT.

One of the most popular and relatively less computationally complex technique is the LSB embedding method which is applicable in both spatial and transform domain in all digital format [7]-[9]. It involves the manipulation of the LSB of pixel value in spatial domain and manipulation of the LSB of transform coefficient in transform domain techniques. Operating within the trade-offs of imperceptibility, capacity and robustness, we present an approach which tries to maximize the capacity, while ensuring less degradation in the cover and making the system robust against attacks. This method equally benefits the image watermarking domains in terms of imperceptibility, however, vulnerable to certain attacks [17-22]. In this paper, we have proposed a novel embedding method that is based on prime series representation of the cover image pixels that are being utilized to embed the secret information. The proposed prime series representation converts the pixel into 13-bit format providing more bit planes to embed information as compared to the conventional 8-bit binary representation.

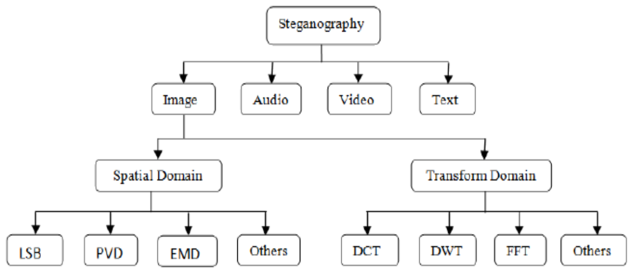

Figure 1. Categories of Steganography

To ensure the complete embed and random spread of the secret information into the whole cover, we have proposed an adaptive chaotic key generation algorithm. The algorithm adjusts the chaotic key that is used to randomly select the embedding pixels based on the cover image and the secret image such that all the secret information is embedded in the cover image and at the same time it is spread all over the cover image. The redundancy in the message image has been removed by applying 2-D DCT and thresholding of the coefficients. After thresholding the new dimensions of the secret image are calculated by locating the row and column that contains the last non-zero coefficient. Only the block information of the calculated reduced size is kept for embedding. Thus, we reduce the size of the payload and need to send the calculated row and column number rather than sending the locations of all the non-zero coefficients. This results in reduction of large overhead information thus enhancing the capacity of the system. The coefficients are given a cover of 2-bit error correction Reed Solomon code to ensure reliable recovery of the information.

The rest of the paper is organized as follows. Section 2 formulates the problem. Section 3 presents the proposed model with explanation of each module in detail. Section 4 discusses the extraction and recovery of the secret message. Section 5 demonstrates the simulation results and Section 6 concludes the paper.

II. Problem Formulation

One of the main goals of steganography is to increase the capacity, while maintaining a certain level of imperceptibility [10]-[12], [16]. Keeping this as a target, our proposed model is shown in Figure 2.

The milestones set for this work are:

- Proposing some embedding technique to enhance Embedding Capacity of the cover image, removing redundancy in the message and minimize distortion in cover image
- Proposing an algorithm to randomly spread the message image into the entire cover image and the algorithm adjusts this spreading depending on the cover and the message images and some other factors
- Making the message more secure for error free recovery

We present an innovative prime series representation of the cover image pixels in which we have utilized prime numbers to enhance the capacity by embedding 3 bits of information per pixel thus increasing overall capacity of cover image three times. Our proposed adaptive key generator algorithm gives approximate density spread of the message over the whole cover image. The algorithm calculates the average distance between the cover image pixels which are chosen by the random chaotic key such that the entire message is embedded fully into the cover image. Furthermore, the redundancy in the message is removed using 2D-DCT transform along with thresholding of the coefficients, secured using channel codes to contribute towards improved capacity and security. We discuss the working of overall proposed algorithm in subsequent sections.

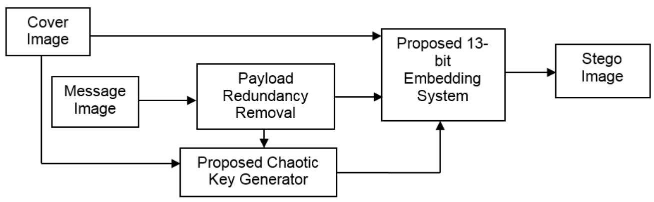

Figure 2. Block Diagram of Proposed Model

III. Proposed System Implementation

The proposed system consists of three stages as explained below.

A. Finding the Adaptive Chaotic Key

The proposed method of key generation is explained below. The key generation has been made dependent on the result of chaotic key generator (CKG) shown in Figure 3, which generates an output depending on these conditions:

a. If $0 \leq \text{rand} < 0.25$ output is Z_1
b. If $0.25 \leq \text{rand} < 0.5$ output is Z_2
c. If $0.5 \leq \text{rand} < 0.75$ output is Z_3
d. If $0.75 \leq \text{rand} < 1$ output is Z_4

where, Z_i are integers ($i = 1, 2, 3, 4$)

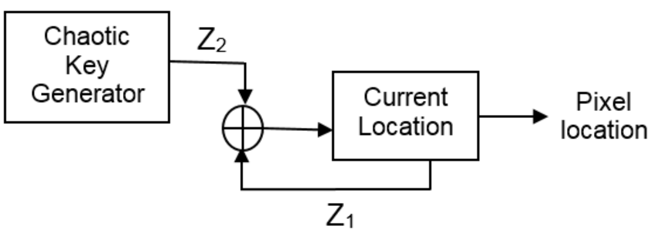

Figure 3: Chaotic Key Generator

Suppose the sequence of output integers from CKG is [Z_1, Z_2, Z_3….]
Location of first pixel = Z_1
Location of second pixel = ($Z_1 + Z_2$)
Location of third pixel = ($Z_1 + Z_2 + Z_3$) and so on.

The average separation between the pixels in this algorithm to embed information is dependent on the value of possible output of chaotic key generator that is given as:
Mean separation between pixels is given as;

$$\sum_{i=1}^{4} \frac{Z_i}{4}$$

The average separation of the key generator is dependent on the size of information to be embedded and size of cover image. The stepwise calculation of average separation of the chaotic key is provided below with the help of Figure 4.

1. Two dimensional DCT is applied on the $M \times N$ message image.
2. Resultant DCT equivalent is passed through a thresholding block to eliminate the small magnitude DCT coefficients which are not required for reconstruction. Reduced dimensions of the image after thresholding are calculated by locating the row and column index containing the last non-zero entry. These are named as $M' \times N'$.
3. Total number of bits in the reduced block of information is calculated by using relation: $B = M' \times N' \times 8$ considering 8-bit format.
4. Information bits are passed through (n, k) Reed Solomon encoder. We have used $(15,7)$ 2-bit error correction code. So total number of bits becomes
   $B_c = B.\left(\frac{n}{k}\right)$
5. Number of pixels in the cover image is $P = A \times B$; where A and B are width and height of cover image respectively.
6. Since 3 bits are being embedded per randomly chosen pixel, so number of pixels required for embedding all bits is given as:
   $R = \frac{B_c}{3}$
7. The average separation required between the pixels of the cover image to embed information is calculated as:
   $$S = \frac{P}{R}$$
8. The selected average is used to find the values zi, (i=1, 2, 3, 4), to be used for key generation.

Example:
A small example of the whole process is provided below for better understanding.
If S = 5, the possible values are,
$Z_1 = 2$, $Z_2 = 4$, $Z_3 = 6$ and $Z_4 = 8$, such that, $\sum_{i=1}^{4} \frac{Z_i}{4} = 5$

Similarly, we could have $Z_1 = 1$, $Z_2 = 4$, $Z_3 = 6$ and $Z_4 = 9$, such that $\sum_{i=1}^{4} \frac{Z_i}{4} = 5$

We can choose any set of $\{Z_i\}_{i=1}^{4}$ satisfying the condition.

B. Proposed 13-bit representation

As explained earlier, the focus of our research is to enhance the available region for embedding information. In this section, we present a new representation of the cover image to enhance the capacity for embedding more information. If we consider the normal bit representation used to represent a pixel value of cover image that lies in the range 0-255, we use 8-bit binary representation. For example, the value 51 in decimal is represented in 8-bit format as 00110011.
In LSB embedding schemes, the LSB that has weight = 1 is used for embedding, which does not affect the pixel value significantly, that is maximum by addition or subtraction by a value 1. Therefore, we need a representation system which provides more least significant levels to embed more information.

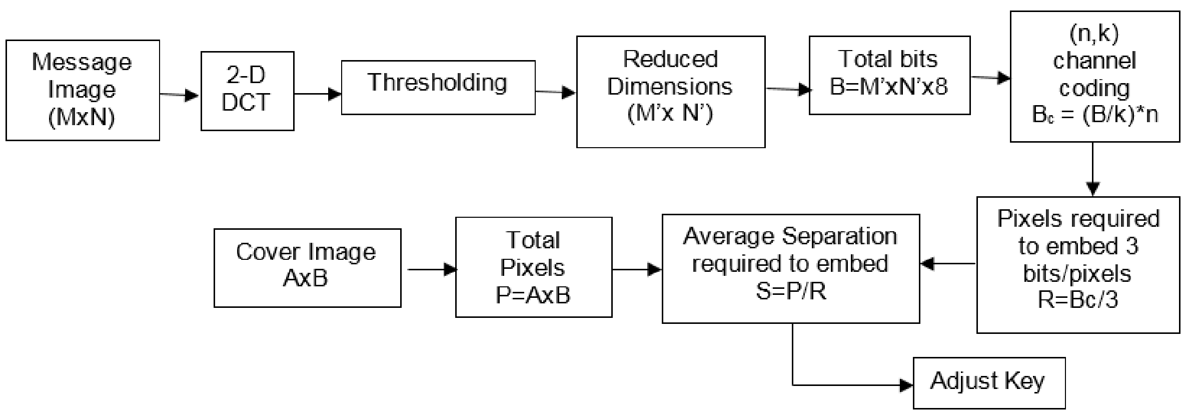

Figure 4: Adaptive Key Generation

For the above stated reason, we have proposed a new representation system that is based on prime number series, for which we have extended the 8-bit representation to 13-bit representation in order to add more bit planes that can be used to embed more information. In this case, the basis is a set of prime numbers from 1 to 41 that are: (1, 3. 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41). The scheme is explained to represent 51 in terms of these new basis in Table I below.

Decimal value is represented in these new prime number basis as given above so 51 = 1 + 13 + 37. We can represent any gray scale pixel value between 0 - 255 using this representation. Thus, the pixel values of cover image, if represented using this proposed representation, have more bit planes to offer for embedding which is basically the aim of this research to improve capacity. Furthermore, it is difficult for an attacker to judge which representation has been used for embedding. Therefore, as compared to simple LSB embedding, this scheme works better in terms of capacity and security as well. We have used last 3 significant bits for data embedding which increases the capacity of the proposed embedding scheme three times as compared to LSB embedding. To reduce the computational load, only those pixels of the cover image have been converted that have been randomly chosen for embedding information.

A. Embedding system

The overall implementation of the proposed embedding system is presented in Figure 5.

The inputs to this module are the key from the chaotic key generator, the encoded information bits and the cover image. The embedding is done as follows:

1. The generated key is used to locate the pixels to be used for embedding.
2. The chaotically located pixels are converted into 13-bit format using prime number representation.
3. 3-bits of encoded information is embedded in last 3 bits of each converted pixel of cover image.
4. The converted pixels are converted back to 8-bit format in order to generate stego image.

IV. Extraction and Recovery of Message

The algorithm for extraction of the information is shown in Figure 6.

The algorithm uses the chaotic key generated at encoder and the stego image as inputs and works as follows.

Table I: Representation of 51 in terms of basis

Bit Weight	1	3	5	7	11	13	17	19	23	29	31	37	41
Bit Value	1	0	0	0	0	1	0	0	0	0	0	1	0

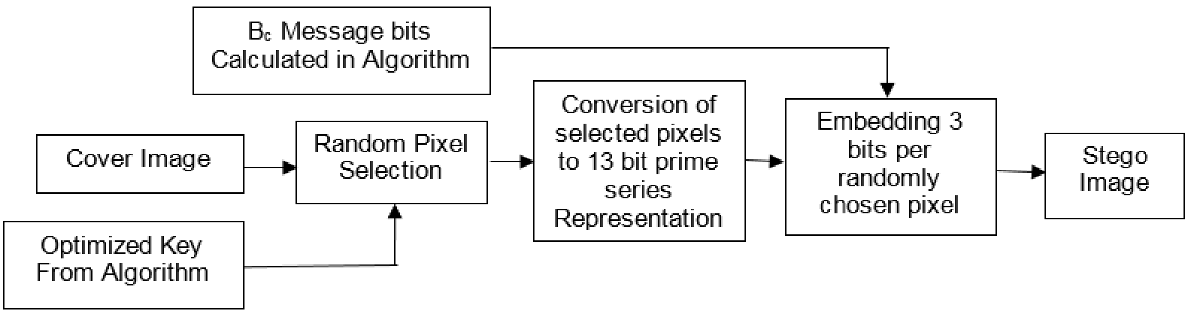

Figure 5: Embedding System

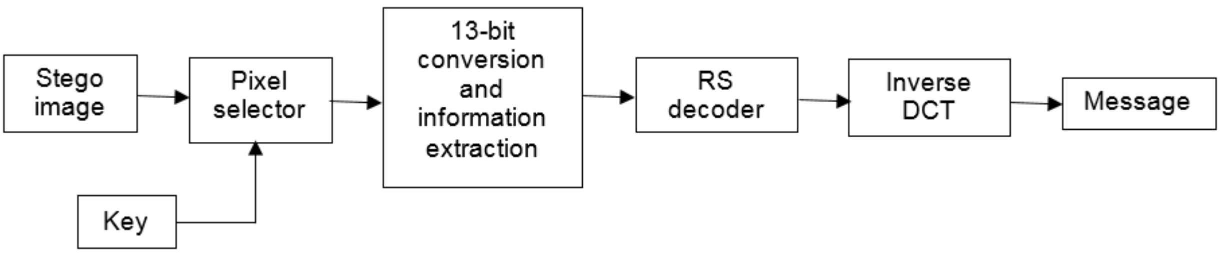

Figure 6: Extraction and Message Recovery

1. The chaotic key is used to locate the pixels of the cover image that are carrying the information.
2. The selected pixels are converted to 13-bit format and information is extracted from the last three bits of each selected pixel.
3. The extracted information is channel coded, So RS decoder is applied to decode the information.
4. The decoded information is passed through inverse DCT transform to recover the message image.

V. Simulation Results

The performance of the proposed algorithm will be illustrated in this section with the help of simulation results. Two images of size 256 x 256 shown in Figure 7 are selected as message images for embedding. The two different images that are being used as cover images are shown in Figure 8, both of size 512 x 512. As already discussed, we have applied DCT in combination with thresholding to the message image in order to remove the redundancy in payload. 2-bit error correction Reed Solomon code has been used to make the message recovery error free. Table II demonstrates the significant payload reduction for message image “Eagle” due to DCT and thresholding being applied on message image at different values of thresholding parameter. The results show significantly less payload than the original message even after adding redundancy for the correction code. The reduced block of DCT coefficients is selected for embedding, thus, we only need to know the size of this block at the receiver side instead of knowing the location of each non-zero coefficient.

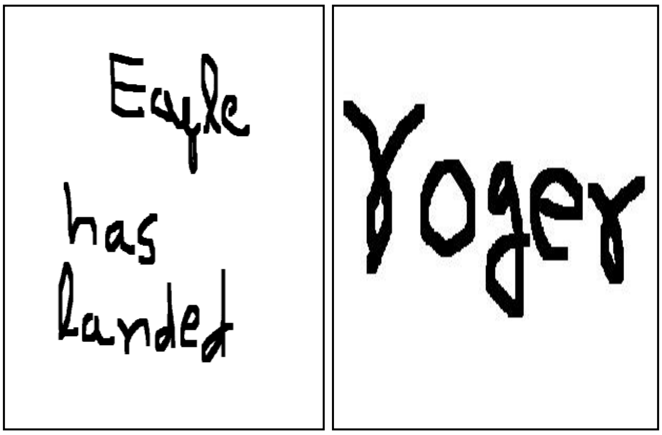

Figure 7: (a) Message Image Eagle, (b): Message Image Roger

Figure 8: Cover Images, (a), Baboon, (b) Lena

The value of average separation required between the pixels of cover image to embed information is also shown against each value of thresholding, that has been calculated by our proposed algorithm and the chaotic key has been adjusted accordingly. Table III demonstrates the similar results for message image 2, i.e. “roger”.

Table II: Payload and Average Separation Calculation for Message Image “Eagle”

Threshold Value (Th)	Reduced Image Dimension $M' \times N'$	Total bits to be Embedded B_c	Average Separation
1	160 x 167	213760	2
1.5	71 x 74	90068	9
2	59 x 70	70800	12
2.5	57 x 63	61560	13

We have selected two different performance parameters to demonstrate the results which are:

1. Peak Signal-to-Noise Ratio (PSNR)
2. Structural Similarity Index (SSIM)

1. Peak Signal-to-Noise Ratio (PSNR):

PSNR is most commonly preferred metric to verify the perceptual quality of stego image [13-14] and [24-25]. Here the signal is original cover image and the noise is the error introduced due to embedding. It is given by:

$$PSNR = 20 \log_{10} \frac{255}{RMSE} \qquad (1)$$

Table III: Payload and Average Separation Calculation for Message Image “roger”

Threshold Value (Th)	Reduced Image Dimensions $M' \times N'$	Total bits to be Embedded B_c	Average Separation
1	56 x 74	71040	12
1.5	53 x 60	54515	15
2	39 x 60	40115	20
2.5	38 x 50	32572	25

2. Mean Structural Similarity Index (MSSIM):
MSSIM is a method for measuring the similarity between two images. The MSSIM index is a full reference metric; in other words, the measuring of image quality based on an initial uncompressed or distortion-free image as reference. SSIM is designed to improve on traditional methods like PSNR and mean squared error (MSE), which have proven to be inconsistent with human eye perception [15]. The MSSIM metric has been calculated on various windows of an image. The measure between two windows x and y of common size $N \times M$ is computed as:

$$MSSIM\left(X,Y\right)=\frac{1}{M}\sum_{j=1}^{M} SSIM\left(x_j,y_j\right) \qquad (2)$$

Where X and Y are the cover and the stego images respectively, x_j and y_j are the image contents at the j^{th} local window, and M is the number of windows of the image. SSIM is computed as,

$$SSIM\left(x,y\right)=\frac{\left(2\mu_x\mu_y+C_1\right)\left(2\sigma_{xy}+C_2\right)}{\left(\mu_x^2+\mu_y^2+C_1\right)\left(\sigma_x^2+\sigma_y^2+C_2\right)} \qquad (3)$$

where σ_x is the mean intensity of x, σ_y is the mean intensity of y, σ_x^2 is the variance of x, σ_y^2 is the variance of y, σ_{xy} is the variance of x and y, $C_1=\left(K_1L\right)^2, C_2=\left(K_2L\right)^2$ are the two variables to stabilize the division with weak denominator, L is the dynamic range of the pixel values (255 for 8-bit grayscale image), $K_1=0.01$ and $K_2=0.03$ by default. The value of MSSIM should be closer to 1 to indicate the maximum similarity between cover and stego image. This maximum similarity indicator makes it more difficult to predict a clue of data embedding.
Table IV demonstrates the values of the two performance parameters mentioned above for both the cover images when the message image embedded is "Eagle".

Results are presented against the different values of thresholding applied on message image Eagle. In addition to it, we have also presented the PSNR of the recovered message image against each value of the thresholding parameter. The observed values of PSNR and MSSIM clearly depict that our proposed algorithm results in a high capacity and the imperceptibility of the cover image is also high. In addition to it, the recovered message image is also shown in Fig.9 for each value of thresholding parameter which was embedded after thresholding resulting into improved capacity due to payload reduction.

Table V presents the similar results for message image "roger" as presented in Table 3. Fig.10 shows the recovered message image "Roger" for different values of thresholding being applied.
Results presented in Table IV and V along with recovered images shown in Figure 9 and 10 respectively clearly portray that as we increase the value of thresholding parameter, the size of payload reduces, which results in an improvement in the PSNR and MSSIM of stego image. But the PSNR of recovered image falls off because of more information content being reduced. The recovered image with lowest PSNR is also still clearly readable, which highlights the reliability of the proposed system.

VI. Conclusion

The proposed system explored a new representation of cover image pixels to exploit 3-bit planes for embedding the information to improve capacity. The improvement in capacity is further aided by the reduction in the payload done by using DCT and thresholding on the message image. The message image has been given a cover of 2-bit error code to make it robust against errors. The system is able to automatically adjust the chaotic key depending on the cover image and the message image. The simulation results demonstrate better capacity and imperceptibility using two different performance evaluation parameters. The message image recovered is of good quality and is clearly readable depicting error free recovery.

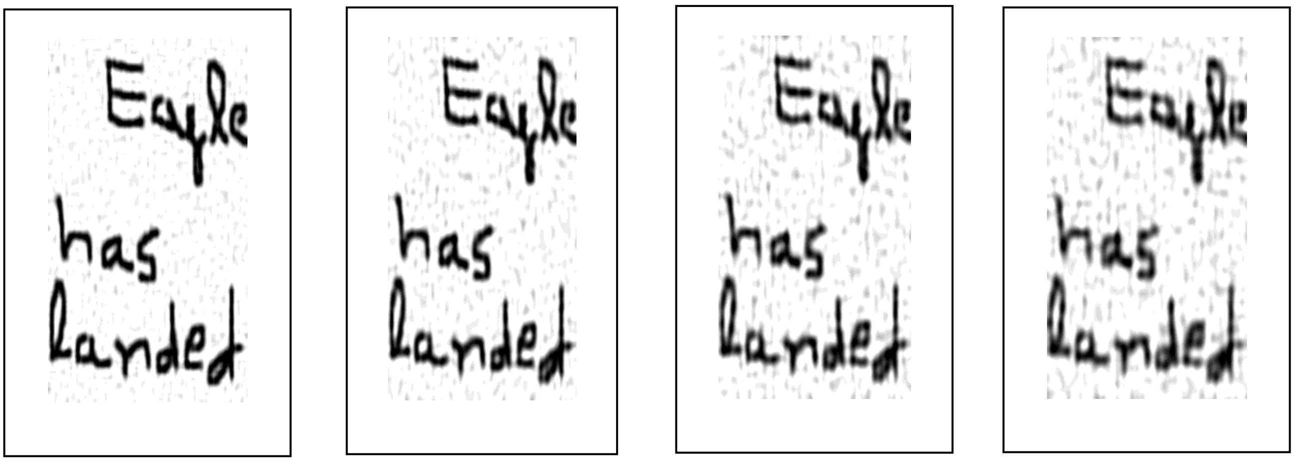

Figure 9: Recovered Message Image "Eagle" for Different Values of Thresholding Parameter (a) Th = 1 (b) Th = 1.5 (c) Th = 2 (d) Th = 2.5

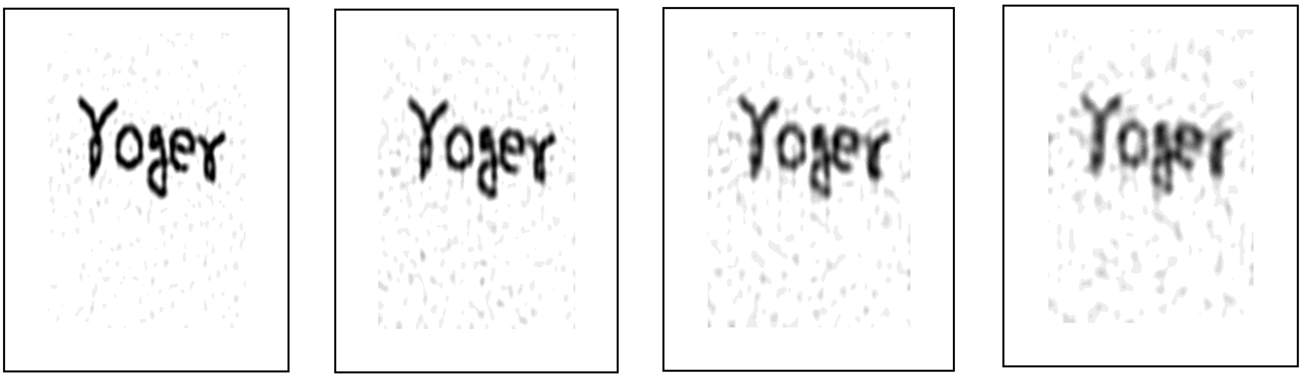

Figure 10: Recovered Message Image “roger” for Different Values of Thresholding Parameter (a) Th = 1 (b) Th = 1.5 (c) Th = 2 (d) Th = 2.5

Table IV: Simulation Results for Message Image “Eagle”

Threshold Parameter (Th)	PSNR of Baboon (dB)	PSNR of Lena (dB)	MSSIM of Baboon	MSSIM of Lena	PSNR of Recovered Image (dB)
1	60.34	60.13	0.9877	0.9859	58
1.5	61.78	61.22	0.9921	0.9908	57.2
2	63.05	62.96	0.9958	0.9940	56.8
2.5	63.78	63.41	0.9970	0.9961	56.56

Table V: Simulation Results for Message Image “roger”

Threshold Parameter Th	PSNR of Baboon (dB)	PSNR of Lena (dB)	MSSIM of Baboon	MSSIM of Lena	PSNR of Recovered Image (dB)
1	61.45	60.96	0.9884	0.9876	59.61
1.5	62.98	62.13	0.9945	0.9923	58.92
2	63.66	62.98	0.9978	0.9965	58.24
2.5	63.97	63.27	0.9991	0.9987	57.83

References

[1] J. Collins, S. Agaian. “High Capacity Image Steganography using Adjunctive Numerical Representations with Multiple Bit-Plane Decomposition Methods”, *Int. J. Cryptography Info. Sec.* , 2016, 6, (1/2), pp. 1-20.

[2] B. Li, J. He, J. Huang, Y. Q. Shi. “A Survey on Image Steganography and Steganalysis”, *Int. J. Info. Hiding Multimedia Sig. Process.*, 2011, 2, (2), pp. 142–172.

[3] G. Swain, S. K. Lenka. “Classification of Spatial Domain Image Steganography Techniques: A Study”, *Int. J. Comp. Sci. Engg. Tech*., 2014, 5, (3), 219-232.

[4] F. Jessica. “Steganography in Digital Media: Principles, Algorithms, and Applications”, ISBN-0521190193, Cambridge University Press, 2010.

[5] C. K. Chen, L. Cheng. “Hiding Data in Images by Simple LSB Substitution”, *Pattern Recognition*, 2004, 37, pp. 469-474.

[6] E. Walia, P. Jain, Navadeep. “An Analysis of LSB & DCT based Steganography”, *Global J.Comp. Sci. Tech.*, 2010, 10, (1).

[7] S. S. Agaian, R. Cherukuri. “Secure and Robust Steganography Algorithm for Binary Images”, *Defence Sec. Symposium. International Society for Optics and Photonics*, 2006.

[8] G. Swain, S. K. Lenka. “A Novel Steganography Technique by Mapping Words with LSB Array”, *Int. J. Sig. Imaging Systems Engg*., 2015, 8, (1), pp. 115-122.

[9] G. Swain, S. K. Lenka. “*LSB Array based Image Steganography Technique by Exploring the Four Least Significant Bits*”, Global Trend in Info. System Software App., Commun. Comp. Info. Sci., 2012, 270, pp. 479-488.

[10] Y. P. Lee, J. C. Lee, W. K. Chen et. al. “*High Payload Image Hiding with Quality Recovery using Tri-way Pixel-value Differencing*”, Info. Sci., 2012, 191, pp. 214-225.

[11] V. Sabeti, S. Samavi, M. Mahdavi, S. Shirani, "Steganalysis and Payload Estimation of Embedding in Pixel Differences using Neural Networks", *Pattern Recognition*, 2010, 43, (1), pp. 405–415.

[12] S. Dey, A. Abraham, S. Sanyal S, "An LSB Data Hiding Technique using Natural Number Decomposition", *In Proceedings of the IEEE Third Int. Conf. IIH-MSP*, Kaohsiung, Taiwan, November 2007.

[13] M. S. Subhedar, V. H. Mankar, "Performance Evaluation of Image Steganography based on Cover Selection and Contourlet Transform", *In Proceedings of the Int. Conf. Cloud Ubiquitous Computing & Emerging Tech.*, Pune, India, 2013.

[14] A. Pradhan, A. K. Sahu, G. Swain, K. R. Sekhar, "Performance Evaluation Parameters of Image Steganography Techniques", *In Proceedings of the Int. Conf. Research Advances in Integrated Navigation Sys. (RAINS)*, Bangalore, India, 2016.

[15] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, "Image Quality Assessment: from Error Visibility to Structural Similarity", *IEEE Trans. Image Process.*, 2004, 13 (4), pp. 600-612.

[16] M. Zaheer, I.M. Qureshi, Atta-ur-Rahman, J. Alhiyafi, M.Z. Muzaffar, "Improved and Secure Differential LSB Embedding Steganography", *Journal of Information Assurance and Security*, vol. 11, pp. 170-178, 2018.

[17] Atta-ur-Rahman, K. Sultan, N. Aldhafferi, A. Alqahtani, M. Mahmud, "Reversible and Fragile Watermarking for Medical Images", *Computational and Mathematical Methods in Medicine*, Article ID 3461382, vol. 2018.

[18] Atta-ur-Rahman, K. Sultan, N. Aldhafferi, A. Alqahtani, D. Abdullah, M. Mahmud, "Robust and Fragile Watermarking for Medical Images: A Joint Venture of Coding and Chaos Theories", *Journal of Healthcare Engineering*, 2018.

[19] Atta-ur-Rahman, M. Mahmud, K. Sultan, N. Aldhafferi, A. Alqahtani and D. Abdullah, "Medical Image Watermarking for Fragility and Robustness: A Chaos, ECC and RRNS Based Approach", *Journal of Medical Imaging and Health Informatics*, vol. 8(6), pp. 1192-1200, July 2018.

[20] Atta-ur-Rahman; Naseem M.T., Muzaffar M.Z, "Reversible and Robust Watermarking using Residue Number System and Product Codes", *Journal of Information Assurance and Security*, vol. 7, pp. 156-163, 2012.

[21] M. Z. Muzaffar, I. M. Qureshi, Atta-ur-Rahman, M. T. Naseem, "WPM-LWT based Novel Robust Audio Steganography Technique", *International Journal of Computer Science & Information Security*, vol. 14, no. 8, pp. 161-168, 2016.

[22] M. Z. Muzaffar, I. M. Qureshi, Atta-ur-Rahman, F. A. Alhaidari, M. A. A. Khan, K. Sultan, "Compressed Sensing for Security and Payload Enhancement in Digital Audio Steganography", *Journal of Information Hiding and Multimedia Signal Processing*, 15(6), pp. 1506-1517, 2018.

Author Biographies

Muhammad Zaheer is currently associated with Department of Electrical Engineering, Air University, Islamabad, Pakistan. He received his PhD in EE from department of Electrical Engineering, Air University, Islamabad, Pakistan in 2018 with Digital Communication as his major research area. Previously, he received his Masters and Bachelors from Air University, Islamabad, Pakistan in 2011 and 2008 respectively. His research interests include Digital Communication, Information Security, Cognitive Radio Networks, Evolutionary Algorithms and Embedded Systems.

Ijaz Mansoor Qureshi has received his BE degree in Avionic Engineering from NED University Karachi, Pakistan. First MS degree in Electrical Engineering from Middle East Technical University (METU), Ankara, Turkey and second MS degree in High Energy Physics (HEP) from Syracuse University, USA. He earned his PhD degree in High Energy Physics from University of Toronto, Toronto. He has more than thirty years post PhD experience in teaching and research at different intuitions of good reputation in Pakistan. More than thirty students have completed their PhD in his supervision. Currently he is Professor at Electrical Engineering department, Air University Islamabad, Pakistan. His research interests include digital/wireless communications, digital signal processing, information and coding theory, soft and evolutionary computing.

Kiran Sultan is currently associated with Department of Computer and Information Technology (CIT), JCC, King Abdulaziz University, Jeddah, Saudi Arabia. She did her Ph.D. from Air University, Islamabad, Pakistan in 2013 with major research area Signal Processing in Relay-assisted Cognitive Radio Networks. Previously, she did her Masters and Bachelors from UET Taxila, Pakistan in 2008 and 2003 respectively. Her research interests include Cognitive Radio Networks, Cooperative Communication, Detection and Estimation Techniques, Information Security, Evolutionary Algorithms, Soft Computing and Internet of Things.

Atta-ur-Rahman is currently working at College of Computer Science and Information Technology (CCSIT), Imam Abdulrahman Bin Faisal University (IAU), Dammam, KSA, as Assistant Professor. He has completed his BS degree in Computer Science from University of The Punjab, Lahore, Pakistan; MS degree in EE from International Islamic University, Islamabad, Pakistan and PhD degree in EE from ISRA University, Islamabad Campus, Pakistan in years 2004, 2008 and 2012, respectively. He has been involved in teaching and research since 2003 and authored/co-authored more than 100 publications in conferences, books and journals of good reputation. His research interests include; Digital Communication, DSP, Information & Coding Theory, AI and Applied Soft computing.

Muhammad Zeeshan Muzaffar received the MSc degree in Computer Science from Bahauddin Zakariya University (BZU), Multan, Pakistan in 2005 and MS degrees in Electronic Engineering (EE) from International Islamic University, Islamabad, Pakistan in 2008 and PhD degree in EE from ISRA University Islamabad Campus, Pakistan in 2017. Currently, he is working as Assistant Professor at Barani Institute of Information Technology (BIIT), Rawalpindi, Pakistan. His research interests include digital audio steganography, evolutionary computing, information security and digital/wireless communications.

Reem Alnanih is currently associated with the Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. She holds her Ph.D. in Computer Science from Concordia University, Montreal, Canada, 2015. She obtained her Masters' degree in Computer Science from King Abdulaziz University, Jeddah, Saudi Arabia 2008. Her research interests include Human-Computer Interaction, Software Quality Measurement and Associated Evaluation Techniques, Detection and Estimation Techniques, Soft Computing, and Internet of Things.