Performance Analysis of Digital Steganography Technique with Image Mosaic, Least Significant Bit and Wavelet Transform

Vaneeta Sunil Phand[1], Santosh Bandak[2]

[1]M.Tech in Computer Science and Engineering, PDA College of Engineering, Kalaburagi, Karnataka, India

[2]Professor, Department of Computer Science and Engineering, PDA College of Engineering, Kalaburagi, Karnataka, India

Abstract: ***Image steganography is a secret communication method that uses an image as the cover to hide the secret image from potential attackers that there is some secret message hidden in the image that is being transmitted. When we appreciate the astonishing beauty of a world famous art or picture in its digital form on the computer, it is hard to imagine that the picture or the image might actually be working as a messenger, carrying some invisible important secret message with it. In other words, steganography is techniques that provide protection to the secret message by offering it the appearance of an image. The proposed work focuses on analysis of different steganographic techniques for images. In this work we have proposed a unique mosaic based technique which extracts texture block from payload and embeds it in the usual similar texture block of the carrier. it results in visible steganography which looks like a normal mosaic image. The source block to the carrier block mapping is saved in a table this is the partial information required for reconstruction therefore it is not possible by steganolysis tools to predict a steganographic method by analyzing the image. Another reason being that there is no embedding data but rather a substitution of blocks this result is better security for the data and we also show that image mosaic technique is better when compared to that of least significant bit steganography and wavelet transform with respect to mean square error, peak signal to noise ratio and edge similarity.***

Keywords: Steganography, Image Mosaic, least significant bit, Wavelet transform, Hiding Image behind Image, MSE, PSNR, edge similarity.

1. Introduction

Data security is one of the major challenges in the present electronic communication scenario. There is a need for more secure and robust communication so that the communicating parties do not have the fear of terrorism, the publishers of digital images are worried about their works that would be corrupted by illegal copying or redistribution and hence it is of prime importance to protect information

The word "Steganography" is of Greek origin and means "covered or hidden data". The main objective behind using steganography is to hide the very existence of the secret information in the cover image. Steganography and cryptography are counter parts in digital security the obvious advantage of steganography over cryptography is that messages do not draw attention to themselves, to messengers, or to recipients Recently digital images from various sources are more frequently utilized and transmitted through the internet for various applications, such as online personal albums, confidential enterprise archives, document storage systems, medical imaging systems, and military image database sets. These images usually contain private or confidential information so that they need to be protected from leakages during transmissions

In modern Image Stenography which exploits the advantages of the present day digital media such as multimedia objects often have a highly redundant representation, generally permits the addition of large amount of payload by means of simple modifications that preserve the perceptual content of the underlying cover image and hence they have been found to be perfect candidates to carry payload. The cover object could be an audio file, video file or an image file and the message to be hidden called the Payload could be a plain text, audio, video or an image. The carrier or the cover object along with the hidden message is known as the stego-object

1.1 Steganography model

An image Steganography system consists of two modules: the embedding module and the retrieval module. At the sender end the embedding module is used where the payload information is embedded into the cover image to form stego-image using any one of the Steganographic techniques, whereas at the receiver end the retrieval module is made used to extract the payload information from the stego-image by using inverse Steganographic technique as shown in the Figure 1.

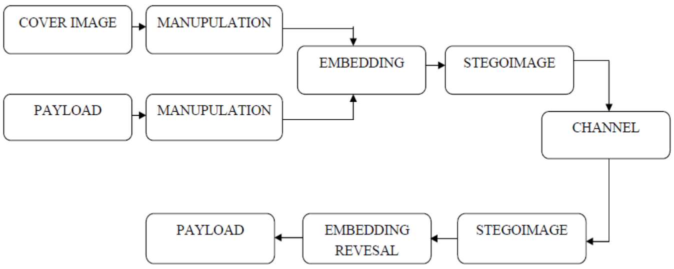

Figure 1: Block diagram of Steganography Model

At the transmitter end, cover image and the payload are applied to the stego-system encoder to form stego image using any one of the steganographic techniques. At the receiver end stego system decoder extracts the payload information by identifying the key which may be used between the transmitter and the receiver to provide security against the attackers

1.2 Design Issues

- Robustness: The embedded data should be as immune as possible to alterations from intelligent attacks.
- Imperceptibility: The cover data should not be significantly degraded by the embedded data.
- Capacity: Ideally we want large capacity but that would affect Imperceptibility and robustness and hence a compromise needs to be made between these three.
- Security: It is the inability of attackers to detect the hidden images, accessible only to the authorized user.

2. Organization

The paper is organized as: section 1 discusses Introduction, section 3 discusses the Related Work, section 4 discusses Proposed Work, section 5 discusses Results & Performance Comparison and section 6 discusses Conclusion.

3. Related work

In [1] author has done a survey of the existing Steganographic techniques and discussed the requirements of stego systems, in variety of available image formats like gray scale, JPEG, binary and Pallet images. They have summarized various spatial- domain hiding techniques like LSB, PVD and MBNS and a comparison is made of the systems. Some suggestions regarding future research and development are made. The author [2] here has proposed a model of steganography based on information theory by interpreting the adversary's task of analyzing the differences among the cover text and stego text as hypothesis testing problem. Relative entropy is made used in order to measure to the stego systems security. The universal stego system that needs no knowledge of cover text distribution, except for the one that it been generated from independently repeated experiments is discussed. In [3] they have discussed most of the steganalysis technique. The properties of information hiding techniques can help the steganalyst to infer the presence of hidden secret message and where to look for such hidden messages in the medium. Author in [4] have presented a steganalysis technique for images, which are used for embedding by Steganographic algorithms. They have used the seventh and eighth bit planes of the image for the evaluation of several binary similarity measures. The interrelationship between the bit planes and also the binary texture characteristics within the bit planes is used to form a classifier that can differentiate between stego and cover images. The scheme is found to have complementary performance with other steganalysis schemes. Author here [5] has discussed a Steganographic method based on keyword shift by borrowing the ideas from cryptographic algorithm of low key authentic degree. Switching of sensitive keywords in the text is the master key of the method. In [6] author has proposed a novel image based steganography technique for communicating secret information more securely between two locations by making use of the idea of secret key for authentication at both ends in order to achieve high level of security. Author here in [7] has proposed a high capacity technique for transform domain image steganography and the algorithm works on the wavelet transform coefficients of the original image in order to embed the secret data by retaining integrity of the wavelet coefficients at high capacity embedding. Author in [8] has presented the application of Wavelet Transform and Genetic Algorithm in a steganography scheme by making use of a genetic algorithm based mapping function to embed data in Discrete Wavelet Transform coefficients in 4x4 blocks of the cover image. The optimal pixel adjustment process is applied after embedding the message and the frequency domain is used to improve the robustness of steganography. In [9] author has proposed an adaptive steganographic technique in which the bits of the payload image are hidden in the integer wavelet coefficients of the cover image adaptively along with optimum pixel adjustment algorithm. In [10] the author has proposed Difference Expansion Based Reversible Data Hiding Using Two Embedding Directions the existing difference-expansion (DE) embedding techniques perform one layer embedding in a difference image. They do not turn to the next difference image for further layer embedding unless the current difference image has no expandable differences left. The major disadvantage of these techniques is that image quality may have been severely degraded even before the next layer embedding begins because the previous layer embedding has used up all expandable differences, including those with large magnitude. In [11]author proposes Reversible Image Watermarking Using Adaptive Prediction Error Expansion & Pixel Selection Reversible image watermarking which enables the embedding of copyright or useful information in a host image without any loss of information. Here author proposes a novel technique to improve the embedding capacity i.e. reversible watermarking with an adaptive prediction error expansion & pixel selection. Hiding data in images by simple LSB substitution [12] Author here proposes, a data hiding scheme by simple LSB substitution. By applying an optimal pixel adjustment method to the stego-image obtained by the simple LSB substitution method, the image quality of the stego-image can be greatly improved with low and extra computational complexity. The worst case mean-square-error between the stego-image and the cover-image is measured. In [13] proposes Image Quality Assessment: From Error Visibility to Structural Similarity Author here proposes objective methods for assessing perceptual image quality which are attempted to evaluate the visibility of errors between a distorted image and a referred image with the various known properties of the human visual system. Author here assumes that the human visual perception is been highly adapted and extracts the structural information from a scene, he has introduced an alternative framework for quality assessment which is based on the amount of structural information degraded. In [14] an Analysis and Improvement of Encryption Algorithm Based on Blocked and Chaotic Image Scrambling is done .Based on blocked image scrambling encryption, author presents a new image encryption algorithm by proposing the chaos theory. This algorithm firstly makes spatial scrambling based on image blocking so as to interrupt pixel position, then furthering this interruption through Arnold Mapping in the chaos and then transforming the pixel RGB color space with optimized Arnold Mapping. Author [15] here explores the problem of reconstructing an image from a bag of square which are non-overlapping image patches, the jigsaw puzzle problem. Completing jigsaw puzzles is much tedious and requires expertise even for humans, and is known to be NP-complete. Author here departs from previous methods and develops a graphical model to solve it. Author [16] here has proposed a chaotic map based on cryptography technique, in this technique confusion and diffusion is applied on spectral domain (DCT) hence the encryption can be achieved quickly without applying more number of confusion and diffusion cycle as it was needed in spatial domain

4. Proposed Work

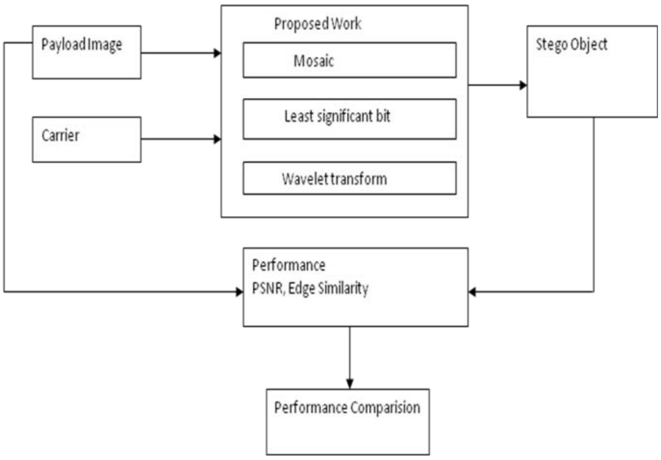

Figure 2: Proposed Block Diagram

The block diagram for the proposed work is as shown above in figure 2. The payload image and the carrier images are taken and then the payload image is hidden into the carrier using the three different techniques the stego-object obtained is compared with the the payload image with respect to the mean square error, peak signal to noise ratio and edge similarity for checking how different is the stego-object from the payload image so that the intruder does not easily recognize that there is some hidden information into it and then the payload image is recovered from the stego-object nearly losslessly

4.1 Image Mosaic Steganography Model

The mosaic technique works in two phases as explained in below. The Figure 3 proposes the steps how the mosaic technique works and compute the Mean Square Error(MSE), Peak Signal to Noise Ratio(PSNR) and Edge Similarity at the results of this technique

In the first phase, a mosaic image is formed, which consists of the fragments of an input secret image with color corrections according to a similarity criterion based on colour variations. The phase includes four stages: 1) fitting the tile images of the secret image into the target blocks of a preselected target image; 2) transforming the colour characteristic of each tile image in the secret image to become that of the corresponding target block in the target image; 3) rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block; and 4) embedding relevant information into the created mosaic image for future recovery of the secret image.

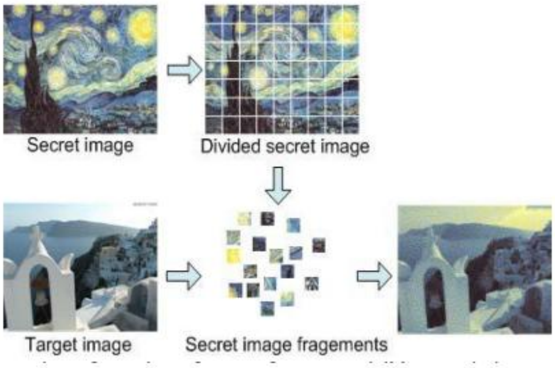

Figure 3: Image Mosaic Generation

In the second phase, the embedded information is extracted to recover nearly losslessly the secret image from the generated mosaic image. The phase includes two stages: 1) extracting the embedded information for secret image recovery from the mosaic image, and 2) recovering the secret image using the extracted information. And at the two stages we compute the mse, psnr and edge similarity for both the mosaic created and the recovered secret and compare this with the other techniques that we have proposed

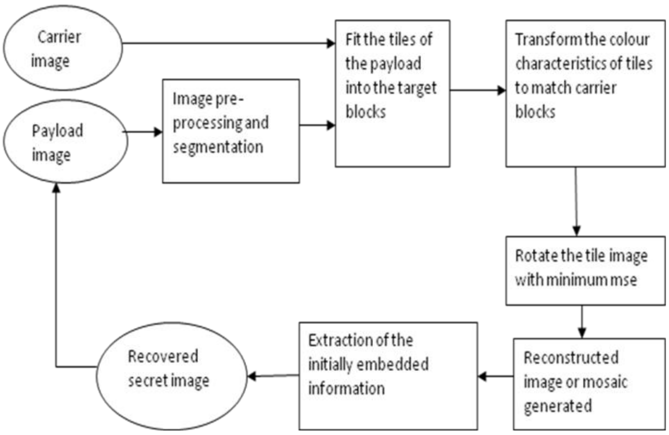
Carrier image
Payload image
Image pre-processing and segmentation
Fit the tiles of the payload into the target blocks
Transform the colour characteristics of tiles to match carrier blocks
Rotate the tile image with minimum mse
Reconstructed image or mosaic generated
Extraction of the initially embedded information
Recovered secret image

Figure 4: Proposed Model For Image Mosaic Steganography

4.2 Least Significant Bit Steganography (LSB)

The two block diagrams for the least significant bit are shown below one is for the encoding (Figure 5) and the other is the decoding (Figure 6) first the secret or the payload image is taken then partitioned into k bits per pixel then with the least significant bit the the encryption is performed k bits per pixel by using block mapping and optimal substitution algorithm on the other hand the cover image with n bits per pixel is taken the extraction of the least bit is performed after the extraction the cover image is made into k blocks which has k bits per pixel the encrypted secret image with k bits per pixel is replaced with the carrier of k bits per pixel and the stego object is formed which has the secret or the payload image hidden into it at the receiver end by knowing the k value one can recover the payload or the secret image hidden into the carrier

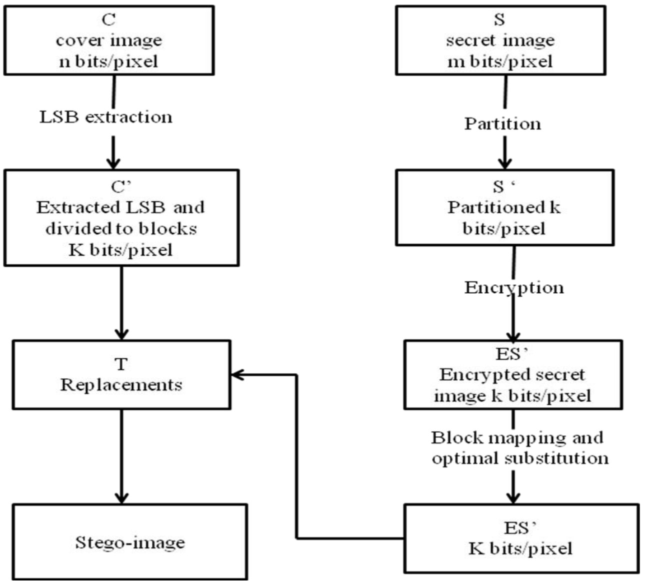

Figure 5: Encoding with Least Significant Bit steganography

The decoding block diagram Figure 6 is as shown below at the receiver end secret image needs to be recovered from the stego object the number of bits embedded in each pixel is taken each of the pixel of the stego image is converted to binary. The first n bits of the stego key is used for first pixel extract the embedded bits that are embedded into the carrier starting from the least significant bit from the stego object check for whether the bits are completely extracted if done end the step else go for the next pixel of the stego image and convert it to binary then get the next bit of the stego key used for next pixel and extract the remaining bits from the stego key

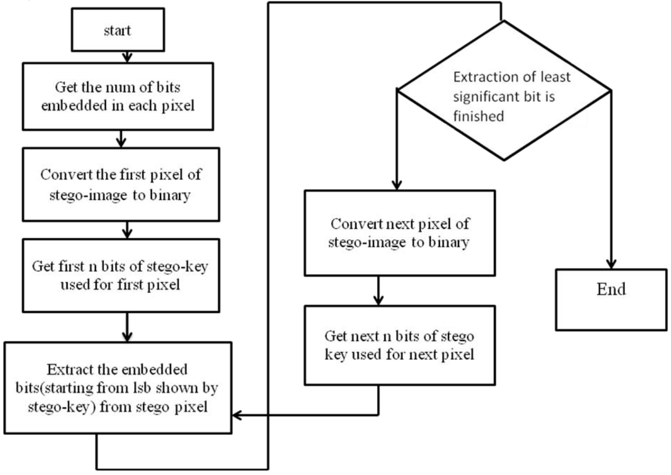
start
Get the num of bits embedded in each pixel
Convert the first pixel of stego-image to binary
Get first n bits of stego-key used for first pixel
Extract the embedded bits(starting from lsb shown by stego-key) from stego pixel
Extraction of least significant bit is finished
Convert next pixel of stego-image to binary
Get next n bits of stego key used for next pixel
End

Figure 6: Decoding with Least Significant Bit Stegonography

4.3 Discrete Wavelet Transform Stegonography (DWT)

The encoding and decoding block diagrams using the discrete wavelet transform as shown below for encoding Figure 5.the payload and the cover images are taken and perform a 2-D wavelet decomposition through **Haar wavelet** of the cover image and then computes the approximation coefficients matrix CA and detail coefficients matrices CH, CV, and CD. which is decomposition in horizontal, vertical and diagonal manner respectively then the redundant values of the pixel in the carrier image are made to zero then it is normalized and stored as the decomposed values in the database and is used to encode the secret by storing the decomposed values in cH1 and cV1 to this the inverse discrete transform is applied and the reconstructed image is saved

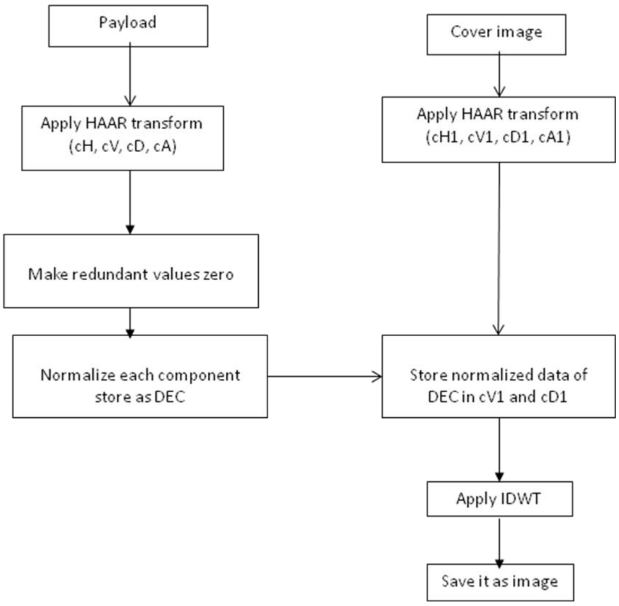

Figure 7: Encoding model for Discrete Wavelet Transform

For decoding as in Figure 7 read the stego image to S1 and then perform the Extraction with the normalization size m from first pixel of the obtained stego image Set the first pixel value as second pixel for compensating for the losses that will incur then Convert S1from unit16 scale to original scale. Further apply wavelet transform of variable S1 and call the sub image or the components as cA1, cV1, cH1, cD1 respectively extract the data from cH1 then perform the Denormalization of the values. Extract the decomposed values from combined data of cD1 and cH1. And then denormalize the dec .Take IDWT of set {cA, cD, cV, cH} and this is the recovered image

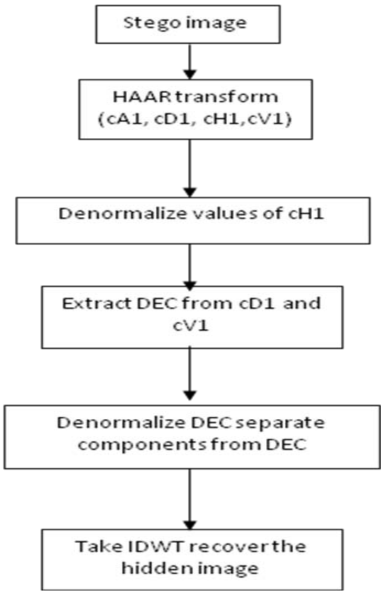
Stego image
HAAR transform
(cA1, cD1, cH1,cV1)
Denormalize values of cH1
Extract DEC from cD1 and cV1
Denormalize DEC separate components from DEC
Take IDWT recover the hidden image

Figure 8: Decoding With Wavelet Transform

5. Results And Performance Comparison

Analysis Of Mean Square Error: The table 1 below shows the Mean Square Error (MSR) values generated with the digital images for the three different technique that is Image Mosaic, Least Significant Bit Steganography and Wavelet Transform techniques

Table 1: Mean Square Error Values

Sl. no	Carrier image	Payload image	MSR for mosaic	MSR for LSB	MSR for wavelet
1	ship .jpg	princess benedikt.jpg	0.01	0.063	0.084
2	System.jpg	Monitor.jpg	0.02	0.062	0.62
3	screenshot1.jpg	screenshot2.jpg	0.07	0.0679	0.011
4	Texture.jpg	Painting.jpg	0.10	0.0624	0.39
5	Ambloyma.jpg	decomposed ambloyma.jpg	0.01	0.0623	0.079

The graphical interpretation of the comparison of mean square error values for 20 set of images is as shown below in Figure 9.

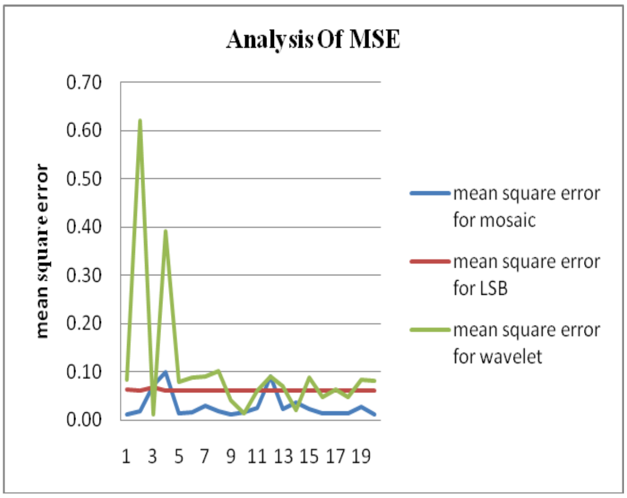

Figure 9: Graphical Analysis of MSE

MSE is a measure of similarity of similarity resulting image with that of the payload

The above graph of Mean Square Error shows that the average Mean Square Error of Image Mosaic is better than the other two methods however the Mean Square Error for Least Significant Bit Steganography was found to be most consistent. We observe that for the texture based technique Mean Square Error for Wavelet transform was higher. Image Mosaic technique peformed better for most number of images including texture images which justifies the usage of the proposed Image Mosaic based technique

Analysis Of Peak Signal To Noise Ratio: The table 2 below shows the value the Peak Signal To Noise Ratio (PSNR) values generated with the digital images for the three different technique that is Image Mosaic, Least Significant Bit Steganography and Wavelet Transform techniques

Table 2: Peak Signal To Noise Ratio Values

sl. no	Carrier image	Payload image	PSNR for mosaic	PSNR for LSB	PSNR for wavelet
1	Ship.jpg	princess benedikt.jpg	58.8	62	27.45
2	System.jpg	Monitor.jpg	50.2	60.16	25.71
3	screenshot1.jpg	Screenshot2.jpg	67.71	59.80	29.54
4	Texture.jpg	Painting.jpg	52.22	64	28.15
5	Ambloyma.jpg	decomposed ambloyma.jpg	59.15	60.18	26.46

The graphical interpretation of the comparison of peak signal to noise ratio values for 20 set of images is as shown below in figure 10.

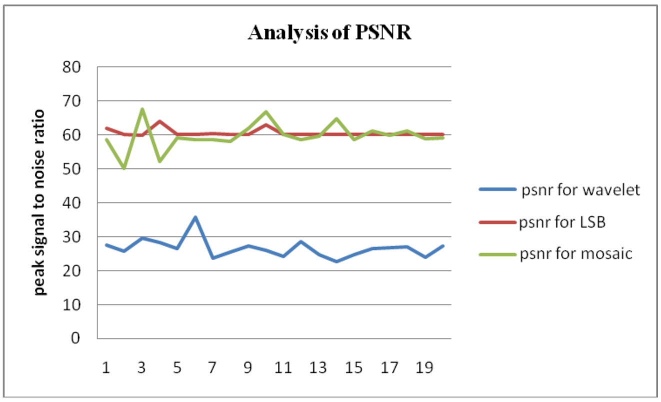

Figure 10: Graphical Analysis of PSNR

The graphical interpretation with respect to Peak signal to noise ratio values is as shown above. In terms of peak signal to noise ratio for image Mosaic based technique was found to be better than the other techniques. Wavelet transform was found to be minimum because it utilizes more volume of data for representing one pixel hence the proposed method is justified.

Analysis Of Edge Similarity: The table 3 below shows the value the Edge Similarity (ED) values generated with the digital images for the three different technique that is Image Mosaic, Least Significant Bit Steganography and Wavelet Transform techniques

Table 3: Edge Similarity Values

sl. no	Carrier image	Payload image	ED for mosaic	ED for LSB	ED for wavelet
1	ship .jpg	princess benedikt.jpg	81.89	99.89	68.86
2	System.jpg	Monitor.jpg	73.28	99.86	85.30
3	screenshot1.jpg	screenshot2.jpg	85.59	99.45	84.33
4	Texture.jpg	Painting.jpg	82.92	99.87	71.57
5	Ambloyma.jpg	decomposed ambloyma.jpg	72.32	99.89	71.48

The graphical interpretation of the comparison of edge similarity values for 20 set of images is as shown below in figure 11.

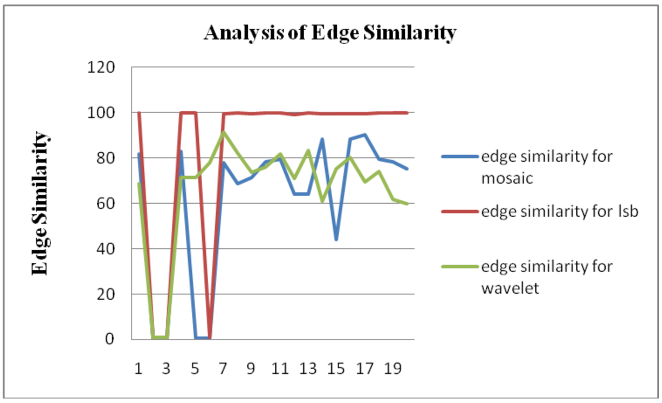

Figure 11: Graphical Analysis of Edge Similarity

Edge Similarity measure represents the edges of the payload and the recovered image

Edge is represented by significant change in neighborhood pixel value as in the LSB method higher bits are not altered. it gives the best edge performance however mosaic based technique performs better than wavelet method and hence all and all is proved better therefore our proposed technique is considered better than the present method

6. Conclusion

Image steganography and watermarking techniques are commonly been for multimedia data security. Wavelet and LSB are most common steganography methods. These two methods do not require any external information for decoding as the data is hidden in the image it can be interpreted with steganolysis tools. In this work we have proposed a unique mosaic based technique which extracts texture block from payload and embeds it in the usual similar texture block of the carrier. it results in visible steganography which looks like a normal mosaic image. The source block to the carrier block mapping is saved in a table this is the partial information required for reconstruction therefore it is impossible by steganolysis tools to assume a steganographic method by analyzing the image. Another reason being that there is no embedding data but rather a substitution of blocks this result is better security for the data and also the result shows that the proposed system performs better than both LSB and wavelet steganography in terms of visual and quantitative methods. Thus the proposed system is better.

In future this can be further extended or can be modified by combining more than one steganography technique to present hybrid stegenographic methods.

References

[1] Nan-I Wu and Min-Shiang Hwang, “Data Hiding: Current Status and Key Issues,” International Journal of Network Security, vol.4, no.1, pp. 1-9, January 2007.

[2] C Cachin, “An Information-Theoretic Model for Steganography,” Journal Information and Computation, vol.192, no.1, pp.41-56, 2004.

[3] Neil F Johnson and SushilJajodia, “Steganalysis: The Investigation of Hidden Information,” Proceedings of IEEE International Conference on Information Technology, pp. 113-116, September 1998.

[4] İsmail Avcibaş, Mehdi Kharrazi, Nasir Memon and BülentSankur, “Image Steganalysis with Binary Similarity Measures,” EURASIP Journal on Applied Signal Processing, pp. 2794-2757, 2005.

[5] Yong WANG, Qichang HE, Huadeng WANG, Bo YIN and Shaoling DING, “Steganographic Method Based on Keyword Shift,” Information Management and Engineering (ICIME), pp. 454-456, 2010.

[6] Bhattacharyya S Kshitij and A P Sanyal G, “A Novel Approach to Develop a Secure Image Based Steganographic Model using Integer Wavelet Transform,” International Conference on Recent Trends in Information, Telecommunication and Computing, pp.173-178, 2010.

[7] Sarreshtedari S and Ghaemmaghami S, “High Capacity Image Steganography in Wavelet Domain,” International Conference on Consumer Communications and Networking, pp.1-6, 2010.

[8] Elham Ghasemi, Jamshid Shanbehzadeh and Nima Fassihi, “High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm,” International Multi Conference of Engineers and Computer Scientists, vol. 1, 2011.

[9] R O El Safy, H H Zayed and A El Dessouki, “An Adaptive Steganographic Technique Based on Integer Wavelet Transform,” International Conference on Networking and Media Convergence, pp.111-117, March 2009.

[10] Yongjian Hu, Member, IEEE, Heung-Kyu Lee, Kaiying Chen, and Jianwei Li “Difference Expansion Based Reversible Data Hiding Using Two Embedding Directions”, IEEE Transactions On Multimedia, Vol. 10, No. 8, December 2008.

[11] Pramod R Sonawane, K B Chaudhari “Reversible Image Watermarking Using Adaptive Prediction Error Expansion And Pixel Selection “, International Journal Of Engineering Science And Innovative Technology,Volume 2,Issue 2, March 2013.

[12] Chi-KwongChan, L.M.Cheng ” Hiding data in images by simple LSB substitution” Pattern Recognition 37 (2004) 469– 474.

[13] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.

[14] Yunpeng Zhang, Peng Sun, Liang Yi, Yongqiang Ma and Ziyi Guo ”Analysis and Improvement of Encryption Algorithm Based on Blocked and Chaotic Image Scrambling”, Research Journal of Applied Sciences, Engineering and Technology 4(18): 3440-3447, 2012 ISSN: 2040-7467.

[15] Taeg Sang Cho, Shai Avidan, William T. Freeman “A probabilistic image jigsaw puzzle solver”, in Proc. IEEE CVPR, 2010, pp. 183–190.

[16] Shoaib Ansari, Neelesh Gupta, Sudhir Agrawa “An Image Encryption Approach Using Chaotic Map in Frequency Domain”, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 8, August 2012).