ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

Enhanced Steganography Using Improved Adaptive Block Truncation Coding

Karthikayini.A [1], Vivetha.M [2], Poornima.M [3], Dr.B.Muthukumar [4]

Assistant Professor, Department of Commerce with Computer Applications, Jayaraj Annapackiam College for Women's Autonomous, Theni, Tamilnadu, India[1][2][3]

Professor, Department of CSE, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India [4]

ABSTRACT: Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word Steganography combines the Greek words Steganos, meaning "covered, concealed or protected", and graphein meaning "writing". In this research work, it has been proposed to use images to hide the secret data. Using images to hide and transmit secret data leads to additional overhead of increased cost associated with storage and transmission cost, as the image requires more space for storage. However, hiding data inevitably destroys the host image, even though the distortions is imperceptible. To overcome such drawbacks, image compression techniques are used to both hide the secret data and to reduce the storage and transmission cost. To enhance the hiding capacity and maintain the quality of the host image after embedding hidden data, we present a high payload reversible data hiding scheme that is based on the Absolute Moment Block Truncation Coding (AMBTC) compression domain. It explore the feature of inter pixel redundancy in an AMBTC compressed image to improve the coding efficiency of compressed images. Normally, AMBTC transforms an input image into a set of blocks and for each block, a bit-plane and a set of two quantizers is generated. These blocks are categorized into Shade and Edge blocks based on the magnitude of amplitude values. For a Shade block, the mean is treated as one quantizer and the secret data is stored as second quantizer. For Edge blocks, high mean and low mean act as two quantizers and a respective Bitplane is generated. The secret data will be stored as Bitplane and second quantizer for shade blocks and creates an illusion of secret data being the Bitplane and second quantizer. The proposed method enables to have higher embedding capacity and increases the complexity of identifying the existence of secret data. It also compresses the stego-image without much degradation in the visibility of stego image.

KEYWORDS: steganography, BTC, AMBTC, image, compression, stegoimage, secret data, embedding capacity.

I. INTRODUCTION

Steganography is a branch of Information Hiding method to hide secret data in media such as audio, video and images [1]. Steganography aims at security of information to be passed. The transmission media must be robust enough to carry the secret information. Components of Steganography include components such as Cover Image, Message and Key. Steganography is of many types such as Text- based, Audio, Image and Video Steganography. Steganography is applied in fields such as Copyright Protection, Feature Tagging, Secret Communication, Digital Watermark, and even used by terrorist to hide their secret [2]. Absolute Moment Block Truncation Coding (AMBTC) technique is one of the lossy image compression techniques. In this paper, AMBTC technique is used to hide the information as port of compressed image.

1.1 A Brief History of Steganography

The earliest recordings of steganography were by the Greek historian Herodotus in his chronicles known as "Histories" and date back to around 440 BC. Herodotus recorded two stories of Steganographic techniques during this

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

time in Greece. The first stated that King Darius of Susa shaved the head of one of his prisoners and wrote a secret message on his scalp. When the prisoner's hair grew back, he was sent to the Kings son in law Aristogoras in Miletus undetected. The second story also came from Herodotus, which claims that a soldier named Demeratus needed to send a message to Sparta that Xerxes intended to invade Greece. Back then, the writing medium was text written on wax-covered tablets. Demeratus removed the wax from the tablet, wrote the secret message on the underlying wood, recovered the tablet with wax to make it appear as a blank tablet and finally sent the document without being detected. Romans used invisible inks, which were based on natural substances such as fruit juices and milk. This was accomplished by heating the hidden text, thus revealing its contents. Invisible inks have become much more advanced and are still in limited use today. During the 15th and 16th centuries, many writers including Johannes Trithemius (author of Steganographia) and Gaspari schotti (author of Steganographica) wrote on Steganagraphic techniques such as coding techniques for text, invisible inks, and incorporating hidden 2 messages in music. Between 1883 and 1907, further development can be attributed to the publications of Auguste Kerckhoff (author of Cryptographic Militaire) and Charles Briquet (author of Les Filigranes). These books were mostly about Cryptography, but both can be attributed to the foundation of some Steganographic systems and more significantly to watermarking techniques. During the times of WWI and WWII, significant advances in steganography took place. Concepts such as null ciphers (taking the 3rd letter from each word in a harmless message to create a hidden message, etc), image substitution and microdot (taking data such as pictures and reducing it to the size of a large period on a piece of paper) were introduced and embraced as great Steganography[3]. In digital world of today, namely 1992 to present, steganography is being used all over the world on computer systems. Many tools and technologies have been created that take advantage of old Steganographic techniques such as null ciphers, coding in images, audio, video and microdot. With the research this topic is now getting we will see a lot of great application for Steganogra phy in the near future. Steganography is a technique of hiding information in an image. The overhead in terms of increased transmission time is reduced by compressing the image. The term Steganography originates from the Greek word stegano meaning "covered or protected" and graphein eaning "to write". Steganography means is not to alter the structure of the secret message, but hides it inside a cover-object (carrier object) [4]. After hiding process cover object and stego-object (carrying hidden information object) are similar.

II. LITERATURE SURVEY

2.1 AMBTC Algorithm

Absolute Moment Block Truncation Coding (AMBTC) is one of the lossy image compression techniques. The computational complexity involved is less and quality of the reconstructed images is appreciable and improves the efficiency. In AMBTC, the high mean and low mean values are stored or transmitted along with the bit plane. AMBTC has several advantages over BTC [27]. One advantage is in the case that the quantized is used to transmit an image from transmitter to a receiver, it is necessary to compute the transmitter into two quantities, the sample mean and the sample standard deviation for BTC and sample first absolute central moment for AMBTC. When we compare the necessary computation for deviation information, we will see that in case of standard BTC it is necessary to compute a sum of m values and each of these will be squared, while in case of AMBTC, it is only necessary to compute the sum of these m value. Since the multiplication time is several times greater than the addition time in most AMBTC digital processors, thus using AMBTC the coding and decoding processes are very fast for AMBTC because the square root calculation and multiplications are omitted. Lema and Mitchell presented a simple and fast variant of BTC, named Absolute Moment BTC (AMBTC) that preserves the higher mean and lower mean of a block. The AMBTC algorithm involves the following steps:

Step 1: An image is divided into non-overlapping blocks. The size of a block could be (4 x 4) or (8 x 8), etc.

Step 2: Calculate the average gray level of the block (4x4) as equation 2.1.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

Step 3: Pixels in the image block are then classified into two ranges of values. The upper range is those gray levels which are greater than the block average gray level (x) and the remaining brought into the lower range. The mean of higher range XH and the lower range XL are calculated.

2.2 Li et al's scheme [28]

Li et al.'s scheme does not require extra data to be included in the stego -code stream. Li et al. 's scheme can enhance the security of the embedded conventional data. Before the embedding process, suppose that the high mean table H, low mean table L and Bitplanesequence BM are obtained after the BTC scheme. The detailed steps of the embedding process are listed as follows:

Step 1: Perform the Bitplane flipping technique on H, L and BM to embed the first Secret Bit stream:

Step 1.1: For each block with Li < Hi, if the secret bit is '1', then swap the element Hi in H and the element Li in L. Otherwise, no operation is required.

Step 1.2: For each block with Li=Hi, the whole Bitplane BMi in BM can be replaced with k × k secret bits.

Step 2: Obtain the modified mean tables H′ and L′ and the Bitplane sequence BM′, respectively.

Step 3: Perform the histogram shifting technique on H′ and L′ to embed the second secret Bit stream.

Step 3.1: Find a zero point v and a peak point u in the histogram. Assume that u<v.

Step 3.2: Increment the pixel values that are between u and v by 1.

Step 3.3: Scan the whole mean table; once a pixel with the value of u is encountered, check the secret bit. If the bit is '1', then increment the pixel value by 1. Otherwise, the pixel value remains intact.

Step 4: Obtain the final marked high mean table H″, low mean table L″ and Bitplane sequence BM′ to reconstruct the stego BTC-compression image. Without extra data in the stego-code stream, Li et al.'s scheme achieves very low image Distortion after data embedding and enhances the security of embedded conventional data successfully. However, as a data hiding scheme, the hiding capacity of Li et al.'s scheme is Unacceptable.

III. PROPOSED METHOD

The proposed algorithm consists of three stages; i. the AMBTC compression stage, ii. The data hiding stage and iii. the data recovery stage.

The AMBTC Compression Stage

This stage is a preprocessing stage before data hiding. The aim of this stage is to obtain HMean, LMean and Bitplane sequence. Given an M x N sized grayscale original image X, the following are the steps followed to transform the image into a compressed form based on

AMBTC.

Step 1: The original gray scale image of size M x N is divided into non-overlapping blocks.

Step 2: Divide the image into blocks, each of size K x K where value of K can be 4,8,16 and so are. Each block TS is represented as

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

$$TS=\begin{bmatrix} x1 & x2 & \ldots\ldots & x_k \\ . & . & & . \\ . & . & & x_k^2 \end{bmatrix}$$

Step 3: Calculate the mean of the block using the equation (3.1).

$$\text{Mean}=\frac{1}{16}\sum_{i=1}^{16} x_i \tag{3.1}$$

Step 4: Find the High mean and Low mean values the equation (3.2) and (3.3).

$$\text{HMean}=\frac{1}{q}\sum_{x_{i\geq Mean}}^{16} x_i \tag{3.2}$$

$$\text{LMean}=\frac{1}{q}\sum_{x_{i<Mean}}^{16} x_i \tag{3.3}$$

Step 5: Set the threshold (TH).

Step 6: Find difference between High Mean and Low Mean using equation (3.4).

$$D = \text{HMean} - \text{LMean} \tag{3.4}$$

Step 7: if D<= TH, the block is shade block, and only the mean value is stored.

Step 8: if D> TH, the block is edge block. The HMean, LMean and Bitplane are computed.

Step 9: Repeat the steps 3 to 8 for each block.

The Data Hiding Stage

The proposed method is a reversible data hiding algorithm. Assume the secret bit sequence to be embedded is S= {s1, s2, …..}. Before embedding, the secret data undergoes permutation operation in order to enhance the security. In AMBTC, all input blocks are treated equally and for each block, a set of two quantizers and a Bitplane of size 16 bits

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

are generated. In the proposed method, an Indicator bit (1/0) is used to represent a Shade block (0) and an Edge block (1).

For a shade block, the Mean is stored as the first quantizer and the 8– bit secret data is stored as second quantiz er. As a Bitplane is not necessary for a shade block, a 32 bit secret data is stored as Bitplane which increases the embedding capacity. Hence in a shade block, a secret data of 40 bits is stored.For an Edge block, HMean & LMean and a 32- bit Bitplane are generated. HMean and LMean are blocks specific. In the Bitplane, out of 2 bits, the first bit indicates the nature of the input pixel value and the second bit represents the secret data.

Second Level of Compression

To reduce the Bit rate, LMean value is subtracted from HMean. For example, HMean = 106, LMean=101.We need to store a high and low mean value.

$$D = 106 – 101= 5$$

As the difference is stored as LMean, it requires only less number of bits. This leads to further reduction in image dat a.

In case of a Shade block, only the mean of the block is stored as first quantizer. The gaps with respect to second quantizer and Bitplane are filled with the secret data. Size of two quantizers and Bitplane is 32 i.e. 8+8+16, out of which 8 bits are use d for compressed image data and the remaining 24 bits are used for embedding the secret data.

Data Extraction and Recovery Stage

An indicator bit is used to identify, whether the block is an Edge or Shade block. If indicator bit is ‘0’, the current block is Shade block. Then the secret data is retrieved from the second quantizer and Bitplane. The compressed image block is reconstructed is replaced with the Mean value for pixel values. If indicator bit is ‘1’, the current block is an Edge block. The StegoBitplane is divided into original Bitplane and secret data. The secret data is retrieved from Bitplane. The current block is rep laced with HMean and LMean, based on original Bitplane.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

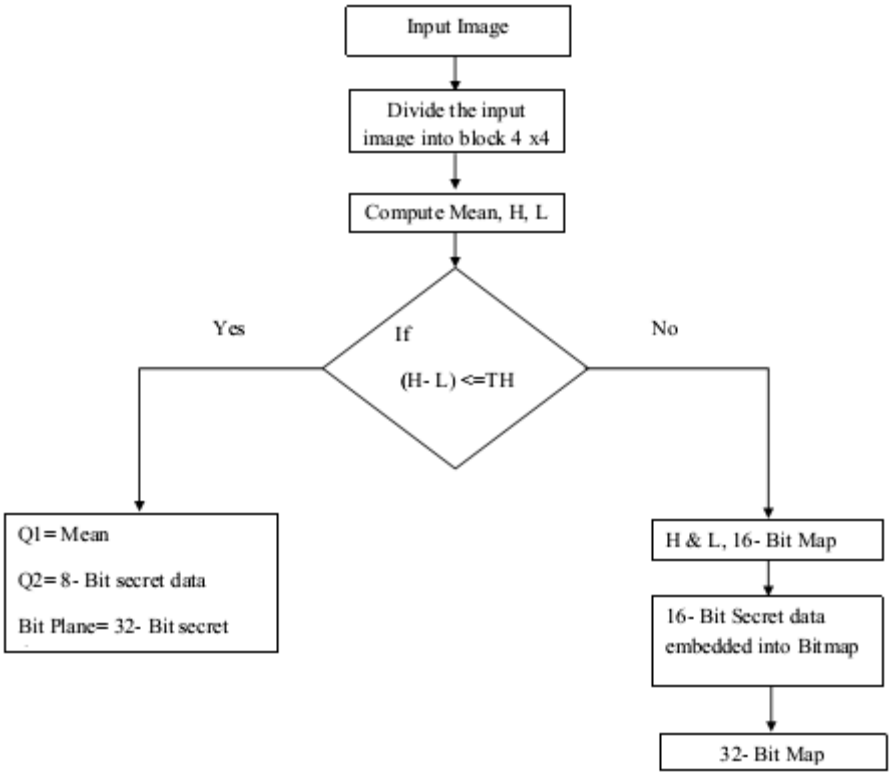

Fig 3.1: Flow chart of Proposed Method

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

The proposed method is tested with a set of benchmark images such as Airplane, Lena, Boats, Peppers, Sailboat, Zelda, Girl, Toys and Gold hill, which are of size 256 x 256 pixels. The input images taken for the experiments are shown in Figure 4.1. The algorithms are implemented using MATLAB R2014b. The Hardware used is, the Intel® Core (TM) 2.40GHZ processor with 4GB RAM. The proposed method is a combination of AMBTC and Steganography which gives a dual benefit of both hiding secret data in an image and to compress the image to reduce the cost associated with storage and transmission. In Table.4.1,the PSNR and BPP, which are calculated for the proposed method and compared with various threshold values are shown. The PSNR value shows the image is of good quality. The cover file has concealed the secret image and it is compressed.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

Fig: 4.1 Standard Images

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

Quality Measurement

The Peak Signal-to-Noise Ratio (PSNR) is used to measure the image quality. PSNR is defined as:

$$PSNR = 10 \log_{10} \left[\frac{255^2}{MSE} \right]$$

Where, MSE is the Mean Square Error between the original image and compressed image. MSE is defined as:

$$MSE = \frac{1}{MxN} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - I'(i,j))^2$$

Where, M is number of rows and N is number of columns. I(i, j) and I'(i, j) denote the pixel values of Original image and Compressed-image respectively.

$$bitrate = \frac{C}{MxN}(bpp)$$

The Bitrate is used to analyze the coding efficiency of any Compression algorithm. The Bitrate is computed using the equation (4.3), where C represents the length of compression code, M x N is the size of the original image. The B itrate measured is represented in terms of bits per pixel (bpp). The lower the Bitrate, higher the coding efficiency is

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

Images	Payload & PSNR	Threshold (TH)				
		5	10	15	20	25
Lena	PSNR	37.58	36.96	36.36	35.86	35.48
	BPP	2.90	2.98	3.02	3.03	3.04
	Capacity	417688	518104	560704	584392	599776
Airplane	PSNR	37.33	37.01	36.62	36.23	35.93
	BPP	2.95	3.00	3.02	3.03	3.04
	Capacity	462544	520696	549880	569536	581752
Baboon	PSNR	32.75	32.62	32.32	32.00	31.71
	BPP	2.85	2.89	2.94	2.96	2.98
	Capacity	275224	325216	350560	422368	456760
Boat	PSNR	35.98	35.39	34.77	34.24	33.88
	BPP	2.86	2.96	3.00	3.02	3.03
	Capacity	320440	448192	511984	549520	572032
Bridge	PSNR	33.47	33.35	33.02	32.55	32.09
	BPP	2.85	2.89	2.93	2.96	2.99
	Capacity	278032	322600	374080	426688	472600
Girl	PSNR	38.39	37.87	37.35	36.89	36.50
	BPP	2.93	2.99	3.02	3.03	3.04
	Capacity	482200	548536	577768	596296	609616
Pepper	PSNR	37.90	36.90	36.27	35.87	35.60
	BPP	2.93	2.99	3.03	3.04	3.04
	Capacity	367936	525736	572968	593680	605968
Zelda	PSNR	39.64	38.24	37.48	36.90	36.48
	BPP	2.86	3.00	3.03	3.04	3.05
	Capacity	402232	557128	597064	618352	631360
Man	PSNR	35.49	35.13	34.63	34.05	33.60
	BPP	2.85	2.93	2.97	3.00	3.02
	Capacity	344032	428752	481288	524896	555448
SailBoat	PSNR	35.13	34.68	34.24	33.91	33.62
	BPP	2.85	2.95	2.99	3.01	3.02
	Capacity	334384	445288	499072	528568	551272
Couple	PSNR	35.87	35.39	34.83	34.30	33.86
	BPP	2.86	2.94	2.99	3.00	3.02
	Capacity	321376	429976	487768	524176	550264
Toys	PSNR	37.98	37.63	37.38	37.05	36.63
	BPP	2.95	3.00	3.01	3.02	3.03
	Capacity	487120	541384	556336	568384	581488
Goldhill	PSNR	37.28	36.52	35.62	34.91	34.44
	BPP	2.84	2.94	3.00	3.02	3.04
	Capacity	339856	457120	528496	569392	594160
Crowd	PSNR	35.85	35.53	35.06	34.60	34.18
	BPP	2.89	2.95	2.98	3.00	3.02
	Capacity	380704	444232	488032	519472	544000
Average	PSNR	**42.55**	35.94	35.42	34.95	34.63
	BPP	**2.88**	2.95	2.97	3.01	3.02

Table 4.1: Comparison of PSNR and BPP of Proposed method with Various Thresholds

V. CONCLUSION

This research work is proposed to hide secret data as part of an image with the intention of increasing the hiding capacity and to enhance the quality of the stego image in which the secret data is hidden. As transmission of image along with the secret data consumes much time, it has been proposed to use a high payload reversible data hiding scheme that is based on the Absolute Moment Block Truncation Coding (AMBTC) compression domain. The feature of inter pixel redundancy is exploited in AMBTC to improve the coding efficiency of compressed images. Normally, AMBTC transforms a n input image into a set of blocks and for each block, a bit-plane and a set of two quantizers is generated. In the proposed method, the blocks are categorized into Shade and Edge blocks based on the magnitude of amplitude values. For a Shade block, the mean is treated as one quantizer and the secret data is stored as second quantizer. For Edge blocks, high mean and low mean act as two quantizers and a respective Bitplane is generated. The secret data will be stored as Bitplane and second quantizer for shad e blocks and creates an illusion of secret data being the Bitplane and second quantizer. The proposed method enables to have higher embedding capacity and increases the

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

complexity of identifying the existence of secret data. It also compresses the stego -image without much degradation in the visibility of stego image. The proposed method has been tested with benchmark images such as Lena, Cameraman, Boats, Bridge, Airplane, Baboon, Kush and Gold hill. With respect to the embedding capacity, the proposed scheme achieves the highest embedding capacity compared with that of the existing technique. The embedding capacity has been increased by 97%. The proposed scheme is more effective method for its high embedding capacity. The proposed method is also applicable for color image and can also try with the video and audio files in future.

REFERENCES

[1] Fariba Ghobany Beram,"Effective Parameter of Image Steganography Techniques", International Journal of Computer Applications Technology and Research, Volume -3, Issue 6, 361-363, 2014, ISSN: 2319-8656.
[2] Rashisingh and Gaurav Chawla, "A Review on Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014, ISSN: 2277 128X.
[3] Bret Dunbar, "A Detailed Look at Steganographic Techniques and their use in an open-systems Environment" ,SANS Institute 2012.
[4] Mehdi Hussain and Murred Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology, Vol.54, May 2013.
[5] Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre, Mr. Pravin and D. Soni, "Comparison of Different Techniques for Steganography in Images", International Journal of Application or Innovation in Engineering and Management (IJAIEM) Volume 3, Issue 2, February 2014.
[6] Jasleen Kour and Deepankar Verma, "Steganography Techniques A Review Paper", International Journal of Emerging Research in Management & Technology, ISSN: 2278-9359 (Volume-3, Issue-5) May-2014.
[7] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, Vol:62, No.1, January 2012, pp.11-18.
[8] Anupam Mondal and Shiladitya pujari, "A Novel Approach of Image Based Steganography Using Psedorandom Sequence Generator Function and DCT coefficients", I,J Computer Network and Information Security, 2015,3, 42-49.
[9] Dr. Nidaa and F. Hassan, "Introduction to Computer Vision and Image Processing", www.uotechnology.edu.i/dep-cs.
[10] Gandharba Swain and Saroj Kumar Lenda, "Classification of Image Steganography Techniques in Spatial Domain: A Study", International Journal of Computer Science and Engineering Technology (IJCSET) ISSN:2229-3354, Vol.5-No. 03 March 2014.