Binary in Binary for Secret Writing – A Cryptic's Cousin Approach

R. Amirtharajan
Assistant Professor
School of Electrical & Electronics Engineering
SASTRA University, INDIA

Venkata Abhiram Murarisetty
Project Engineer
C-wing, 4th floor, S-6, CDC-5
WIPRO technologies

Dr. R.John Bosco Balaguru
Associate Dean Research
School of Electrical & Electronics Engineering
SASTRA University, INDIA

ABSTRACT

Binary images, like cartoons, text documents, signatures captured by signing pads and/or 2-color images are very commonly used in our daily life. The JPEG compression method which was designed to efficiently compress color images do not do a good job on a monochromatic (binary) image. Changing the pixel values in these images for hiding the data, may produce a noticeable change in the cover media. Embedding capacity and preservation of visible artifacts are the potential problems of this technique. This paper proposes several methods for hiding data in binary images (including fax). The proposed algorithms alter pixels of the embeddable blocks of cover image depending on the characteristic values of the block. In addition, the new algorithm deals with statistical embedding for each block, which enhances the security of embedded data and the capacity of the embedding method. The performances of the algorithms are tested over various sizes of binary cover images by embedding various sizes of secured data. The effectiveness of the stego process proposed has been studied by estimating the number of errors, Bit error rate and Relative entropy.

General Terms

Data Security.

Keywords

Image steganography. Block based embedding.

1. INTRODUCTION

With the catastrophic growth of digital media, its security-related issues are also becoming a greater concern. One central issue is confidentiality, which is typically achieved by encryption[3]. However, as an encrypted message usually flag's the importance of the secret message, it also attracts cryptanalysts'[3] interests. The sometimes confusing terminology Steganography has a different flavor from encryption; its purpose is to embed a piece of critical information in a non-critical host message (e.g., web pages, advertisements, etc.) to distract opponents' attention [8], [9]. One less confusing name for Steganography would be data hiding. It should be understood that Steganography is orthogonal to encryption, and it may be combined with encryption to achieve a higher level of security.

Steganography[1, 2, 6] is the science that deals with the hiding of the secured information in a harmless signal[1, 2]. Binary images are two color (Black & White) images with pixel values (either 1 or 0). Therefore, embedding the secured data can easily distort the cover image. Hence, the amount of data that can be securely embedded into the binary cover image is very low. Several embedding algorithms[4, 5, 7-10] have been developed for binary images using one of the frame work presented below:

- By altering the pixel value i.e. flipping of black pixel to white or vice versa.
- By changing the characteristics of the block in consideration i.e. thickness of strokes, curvature, spacing or relative positions.

For example, K.H. Hwang et.al [5] proposed an embedding algorithm that's embeds in the edge portion of the cover image. The prime factor is that modifications made to edge portions of the cover are more difficult to be recognized. Run length mechanism was introduced to make sure that pixel alterations are carried out in the edge portions only. Min.Wu and Bee Liu [8] proposed an embedding algorithm for binary images. The secured data is embedded into shuffled blocks by manipulating the flipable pixels. The shuffling of the blocks before embedding ensures the equalization of embedding capacity from region to region. H.K. Pan et.al [9] introduced the use of weighted matrix rather than secret key matrix and also altered the logical operation. The distortion in quality of the cover image remains. J. Chen et.al [5] proposed a technique that improves the effectiveness of the PAN's technique [9]. The cover is decomposed into several 4×4 blocks. Each block is again portioned into four 3×3 overlapping blocks. The characteristic value of each sub-block defined by the number of ones in each block is determined for each block.

In this paper, we investigate the following issues

1. How to select pixels for alteration so as to embed information with as little visual changes as possible to the cover.

2. How to maximize the capacity of the proposed technique by employing a statistical embedding rate for each block.

The rest of the paper is organized as follows. Section 2 describes the related works. Section 3, discuss in detail about the proposed scheme for embedding the secret data into a binary cover image. Section 4 explains the simulation results for the proposed algorithm for various images. Section 5 provides the conclusion.

2. Related works

2.1 THE WU – LEE METHOD

The novel features of this method [7] are the use of a key K for additional security and the use of logical operations. The image is divided into blocks B of m × n pixels each, and the key, which is also an m × n block of bits, is used to embed at most one data bit d in each block. For simplicity, it is assumed that the image size is an integer multiple of the block size. The main advantage of the method is that the data bit is embedded in the block by changing the value of at most one pixel. But this method is not very secure. An attacker who has access to the original image can gain information about the key by comparing the original blocks to the modified ones. A pixel location that hasn't been changed in any block implies a 0-bit in the key. Any pixel location that has changed in any of the blocks implies a 1-bit in the key. The key K must be carefully selected. A key with few 1's will render many blocks invalid. A key with many 1's is easier to compromise. Similarly, a cover image with many zeros may produce many zero blocks that are invalid.

3. Information hiding in Two color Images

3.1. Direct 9:1 pixel embedding Scheme (PES 9:1 scheme)

When we consider two color images, data can be embedded by changing the pixel values of the binary image. In basic steganographic implementation of two color images we change every 9th pixel of the binary image with the secret message bits. The secret data is first converted into binary format, now it is rearranged into single row of bits (0's and 1's). Now every 9th pixel of the binary image is replaced with bits from the row matrix. This is a basic substitution approach of steganography.

3.1.1 Methodology:

Encryption:

Step 1: Read the binary cover image and the secret data to be embedded.
Step 2: Convert the secret data into binary row matrix.
Step 3: Replace every 9th pixel in the binary cover image with the secret data bit.
Step 4: Hence our required steg cover is formed.

Decryption:

Step 1: Read the stego image.
Step 2: Collect the every 9th pixel value and form a row matrix.
Step 3: Now convert each 8 bits into a character.
Step 4: Hence our required secret message is recovered.

Statistical approach of steganography means that the number of black and white pixels in the image will not change after embedding the secret data. In this approach first we will find the statistics of the image. To achieve this we are considering the WU-LEE method. According to this method we will divide every image into blocks of size 3×3.

3.2 Block Based 3×3 Pixels Odd Parity (BOP Scheme):

As we can notice from the results of PES 9:1 that it has high data capacity, but the changes in the cover image are visible in stego image. So in order to increase the invisibility we will go for statistical approach of Steganography as mentioned above.

Now count the number of white pixels in each block. Identify the blocks with odd parity i.e. the blocks having 1, 3, 5, 7, 9 white pixels. As we are going for the statistical embedding the statistics of the block shouldn't change. We shall embed the secret data bits at the center of each identified blocks. The following cases arise when we go for embedding,

Case 1: Center pixel is white and the secret data bit is also white, then there is no change in the statistics of the block.

Case 2: Center pixel is white and the secret data bit is black, then we will swap one black pixel of the block with center pixel of the block. Hence there is no change in the statistics of the block.

Case 3: Center pixel is black and the secret data bit is white, then we will swap one white pixel of the block with center pixel of the block. Hence there is no change in the statistics of the block.

Case 4: Center pixel is black and the secret data bit is also black, then there is no change in the statistics of the block.

3.2.1 Methodology:

Encryption:

Step 1: Read the binary cover image and the secret data to be embedded.

Step 2: Convert the secret data into binary row matrix.

Step 3: Divide the image into 3×3 blocks, and find the number white pixels in each block.

Step 4: Consider blocks having only odd number of white pixels.

Step 5: Change the center pixel of the block with the secret data without changing the statistics of the block.

Step 6: Hence our required stego cover is formed.

Decryption:

Step 1: Read the stego image.

Step 2: Divide the image into 3×3 blocks, and find the number white pixels in each block.

Step 3: Consider blocks having only odd number of white pixels.

Step 4: Collect the center pixel value from each identified block and form a row matrix.

Step 5: Now convert each 8 bits into a character.

Step 6: Hence our required secret message is recovered.

3.3 Block Based 3×3 Pixels Even Parity (BEP Scheme)

In the BOP Scheme we can notice that we have attained a certain amount of invisibility compared to PES 9:1. Consider the case where we have 9 white pixels and we have to embed a black pixel; there we change another white pixel to black in order to maintain block statistics. This in turn decreases the invisibility as a plain white image will have black dots on it, in order to avoid that condition we go for Even Parity.

Divide the image into blocks of size 3×3 pixels. Now count the number of white pixels in each block. Identify the blocks with even parity i.e. the blocks having 2, 4, 6, 8 white pixels. As we are going for the statistical embedding the statistics of the block shouldn't change. We shall embed the secret data bits at the center of each identified blocks. The following cases arise when we go for embedding,

Case 1: Center pixel is white and the secret data bit is also white, then there is no change in the statistics of the block.

Case 2: Center pixel is white and the secret data bit is black, then we will swap one black pixel of the block with center pixel of the block. Hence there is no change in the statistics of the block.

Case 3: Center pixel is black and the secret data bit is white, then we will swap one white pixel of the block with center pixel of the block. Hence there is no change in the statistics of the block.

Case 4: Center pixel is black and the secret data bit is also black, then there is no change in the statistics of the block.

3.3.1 Methodology:

Encryption:

Step 1: Read the binary cover image and the secret data to be embedded.

Step 2: Convert the secret data into binary row matrix.

Step 3: Divide the image into 3×3 blocks, and find the number white pixels in each block.

Step 4: Consider blocks having only even number of white pixels.

Step 5: Change the center pixel of the block with the secret data without changing the statistics of the block.

Step 6: Hence our required stego cover is formed.

Decryption:

Step 1: Read the stego image.

Step 2: Divide the image into 3×3 blocks, and find the number white pixels in each block.

Step 3: Consider blocks having only even number of white pixels.

Step 4: Collect the center pixel value from each identified block and form a row matrix.

Step 5: Now convert each 8 bits of the row matrix into a character.

Step 6: Hence our required secret message is recovered.

Any mechanism using odd and even parity combination plays a vital role and motivates the next scheme called BFFW scheme.

3.4 Block Based 3 × 3 Pixels 4-5 or 5-4 Black And White Statistics (BFFW Scheme):

The BEP Scheme has attained a greater amount of invisibility compared to its previous schemes but in the cases where the 3 X 3 block has 2 white pixels or 8 white pixels the block is almost entirely block or white, in such a situation if we try to embed the opposite color pixels that particular block has low invisibility making the data less secure, in order to avoid that we go for BFFW Scheme.

In this method after dividing the image into blocks, we will find the statistics of each block i.e. the number of black and white pixels present in each block. We will consider only blocks having 4 white and 5 black pixels or 4 black and 5 white pixels. As we are going for the statistical embedding the statistics of the block shouldn’t change. We shall embed the secret data bits at the center of each identified blocks. The following cases arise when we go for embedding,

Case 1: The block has 5 white and 4 black pixels, center pixel of the block is white and the secret data bit is also white, then there is no change in the statistics of the block.

Case 2: The block has 5 white and 4 black pixels, center pixel of the block is white and the secret data bit is black. Now we have 4 white and 5 black pixels in the block which can be detected while retrieving the data.

Case 3: The block has 5 white and 4 black pixels, center pixel of the block is black and the secret data bit is also black, then there is no change in the statistics of the block.

Case 4: The block has 5 white and 4 black pixels, center pixel of the block is black and the secret data bit is white, then we will swap one white pixel of the block with center pixel of the block. Hence there is no change in the statistics of the block.

Case 5: The block has 4 white and 5 black pixels, center pixel of the block is black and the secret data bit is also black, then there is no change in the statistics of the block.

Case 6: The block has 4 white and 5 black pixels, center pixel of the block is black and the secret data bit is white. Now we have 5 white and 4 black pixels in the block which can be detected while retrieving the data.

Case 7: The block has 4 white and 5 black pixels, center pixel of the block is white and the secret data bit is also white, then there is no change in the statistics of the block.

Case 8: The block has 4 white and 5 black pixels, center pixel of the block is white and the secret data bit is black, then we will swap one black pixel of the block with center pixel of the block. Hence there is no change in the statistics of the block.

3.4.1 Methodology:

Encryption:

Step 1: Read the binary cover image and the secret data to be embedded.

Step 2: Convert the secret data into binary row matrix.

Step 3: Divide the image into 3×3 blocks, and find the number white and black pixels in each block.

Step 4: Consider blocks having only either 5 white pixels or 5 black pixels.

Step 5: Change the center pixel of the block with the secret data without changing the statistics of the block.

Step 6: Hence our required stego cover is formed.

Decryption:

Step 1: Read the stego image.

Step 2: Divide the image into 3×3 blocks, and find the number white and black pixels in each block.

Step 3: Consider blocks having only either 5 white pixels or 5 black pixels.

Step 4: Collect the center pixel value from each identified block and form a row matrix.

Step 5: Now convert each 8 bits of the row matrix into a character.

Step 6: Hence our required secret message is recovered.

If there exist, any mechanism using odd and even parity and their combination then take the advantage of BFFW, BOP, BEP and acquire payload from PEP 9:1 scheme which also plays a vital role in steganography and motivates the next scheme called BTSW scheme.

3.5 Block Based 3 × 3 Pixels 3-6 or 6-3 Black And White Statistics (BTSW scheme):

As we can notice from the results of BFFW Scheme that it has high data security, but very less amount of data can be hidden in the cover image. So in order to increase the data hiding capacity we will go for the next scheme.

In this method after dividing the image into blocks, we will find the statistics of each block i.e. the number of black and white pixels present in each block. And we will consider only blocks having 4 white and 5 black pixels (or) 4 black and 5 white pixels (or)3 white and 6 black pixels (or) 3 black and 6 white pixels. As we are going for the statistical embedding the statistics of the block shouldn't change. We shall embed the secret data bits at the center of each identified blocks. The following cases arise when we go for embedding,

Case 1: All the cases which have 4 white and 5 black (or) 5 white and 4 black pixels can be ignored because, in these cases even after embedding the secret data bit (may be black or white) in the block the characteristics can be 4 white and 5 black pixels (or) 4 black and 5 white pixels (or) 3 white and 6 black pixels (or) 3 black and 6 white pixels, which can be detected when go for retrieval of the data.

Case 2: The block has 6 white and 3 black pixels, center pixel of the block is white and the secret data bit is also white, then there is no change in the statistics of the block.

Case 3: The block has 6 white and 3 black pixels, center

pixel of the block is white and the secret data bit is black. Now we have 5 white and 4 black pixels in the block which can be detected while retrieving the data.

Case 4: The block has 6 white and 3 black pixels, center pixel of the block is black and the secret data bit is also black, then there is no change in the statistics of the block.

Case 5: The block has 6 white and 3 black pixels, center pixel of the block is black and the secret data bit is white, then we will swap one white pixel of the block with center pixel of the block. Hence there is no change in the statistics of the block.

Case 6: The block has 3 white and 6 black pixels, center pixel of the block is black and the secret data bit is also black, then there is no change in the statistics of the block.

Case 7: The block has 3 white and 6 black pixels, center pixel of the block is black and the secret data bit is white. Now we have 4 white and 5 black pixels in the block which can be detected while retrieving the data.

Case 8: The block has 3 white and 6 black pixels, center pixel of the block is white and the secret data bit is also white, then there is no change in the statistics of the block.

Case 9: The block has 3 white and 6 black pixels, center pixel of the block is white and the secret data bit is black, then we will swap one black pixel of the block with center pixel of the block. Hence there is no change in the statistics of the block.

3.5.1 Methodology:

Encryption:

Step 1: Read the binary cover image and the secret data to be embedded.

Step 2: Convert the secret data into binary row matrix.

Step 3: Divide the image into 3×3 blocks, and find the number white and black pixels in each block.

Step 4: Consider blocks having only 3,4,5,6 white pixels.

Step 5: Change the center pixel of the block with the secret data without changing the statistics of the block.

Step 6: Hence our required stego cover is formed.

Decryption:

Step 1: Read the stego image.

Step 2: Divide the image into 3×3 blocks, and find the number white and black pixels in each block.

Step 3: Consider blocks having only 3,4,5,6 white pixels.

Step 4: Collect the center pixel value from each identified block and form a row matrix.

Step 5: Now convert each 8 bits of the row matrix into a character.

Step 6: Hence our required secret message is recovered.

4. RESULTS AND DISUSSION

For implementing the above discussed process, 4 different cover images of 256 × 256 pixels of binary level have been selected. The effectiveness of the stego process proposed has been studied by estimating the following three different metrics for all stego images.

Bit Error Rate (BER) and Bit Error [16]

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(Ic) are being affected by stego process. The BER for the Stego image (Is) is the percentage of bits that have errors relative to the total number of bits considered in Ic.

Let Icbin and Isbin 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 = $\frac{T_e}{T_n}$

Tn is the total number of bits considered for the binary image of size M × N pixels. Then Tn will be M × N.

Relative Entropy [3]

One can detect the presence of data in the stego cover based on the disorder with reference to its original form. Hence the disorderliness otherwise relative entropy has to be computed.

The entropy is a measure of the security for the stego system. Let e1, e2, e3…. em be m possible intensity values (0-255) of the gray image considered for embedding. If P(e1), P(e2), P(e3)….. P(em) are the probabilities of getting particular intensity, then

the entropy of an image is,

H(e) = $\sum_{i=0}^{m-1} P(e_i) \log_2 P(e_i)$

If the probability distribution of the cover and stego image is denoted by Pc and Ps respectively then the relative entropy is,

D(Pc||Ps)= $\sum$ Pc log $\frac{P_c}{P_s}$

The value of relative entropy approaches zero for similar images.

In this present implementation Gandhi, Four Language Text, Pentagon and Blurred Image 256 × 256 digital images has been taken as cover images as shown in Figure 1 a, b, c and d.

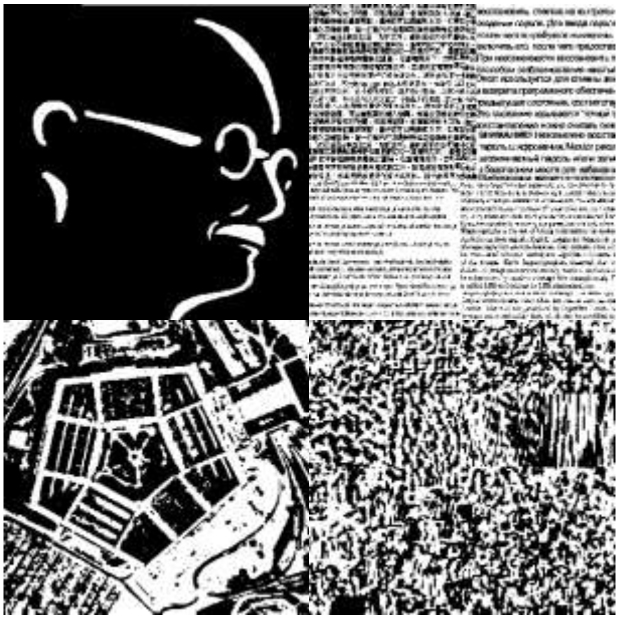

Fig 1: (a), Gandhi (b) Four Language Text ,(c) Pentagon and (d) Blurred Image are the images before hiding and are images after hiding.

4.1 PES 9:1 scheme

This method is relatively easy to implement and it never mind about the uniform disturbances occurred in the cover image. It never tries to hide the presence of the secret message because of the uniform nature of the embedding process. It actually affects utmost 50% on the embedded pixels. If there are m × n pixels present in the cover image than utmost (m × n) / 9 data bit could be accommodated in the binary cover image by replacing every 9th pixel in a row so there is a possibility 50 % error in the embedding operation. Hence there will be (m × n) / 18 erroneous bits. The results are shown in Fig 2. This motivates to go further with statistical approach

4.2 BOP Scheme and BEP Scheme

Advantages:

- Statistically Secure than PES 9:1 scheme.
- Abduct the Stego analysis, Crypt analysis and confuses the hackers.
- Since all the block are not used for embedding sequential extraction is not possible yields more protection for the secret data
- Computational complexity is more hence snatching the secret data is not feasible.

Disadvantages:

- More complex, hence takes slightly more computation time than PES 9:1 scheme.
- Low payload than PES 9:1 scheme, it's quite obvious, since not using all the blocks for embedding.

4.3 BFFW Scheme

Advantages:

- Statistically Secure than PES 9:1 scheme and comparable with BOP scheme and BEP scheme but more comprehensive than BOP and BEP schemes
- Abduct the Stego analysis, Crypt analysis and confuses the hackers as like BOP scheme and BEP scheme better in performance than BOP and BEP.
- Since all the block are not used for embedding sequential extraction is not possible yields more protection for the secret data very similar to BOP scheme and BEP scheme
- Computational complexity is more hence snatching the secret data is not feasible likewise BOP scheme and BEP scheme

Disadvantages:

- More complex, hence takes slightly more computation time than PES 9:1 scheme and comparable with BOP scheme and BEP scheme.
- Low payload than PES 9:1 scheme, it's quite obvious, since not using all the blocks for embedding as similar to BOP scheme and BEP scheme and less than BOP and BEP schemes.
- The Payload depends on than parity hence the statement comparable is not rock-hard or firm as quoted earlier, but little bit sluggish and takes more time to compute.

4.4 BTSW Scheme

Since it get hold of all the advantages from all the schemes and learns lessons from the disadvantages this BTSW schemes supersede the other schemes with respect to the following

- High imperceptibility
- High payload
- Computationally secure
- Comparable computational time for embedding and extraction process
- Abducting hackers.

The BOP Scheme, BEP Scheme, BFFW Scheme and BTSW Scheme results are shown in Fig 3, 4 and 5 respectively.

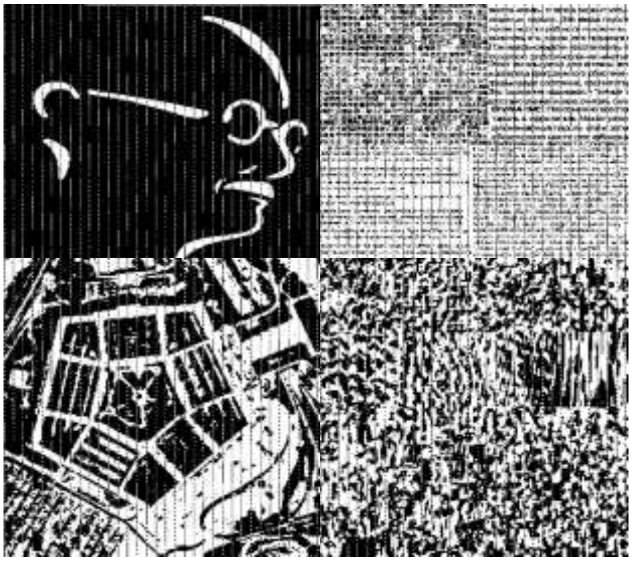

Fig 2: (a), Gandhi (b) Four Language Text ,(c) Pentagon and (d) Blurred Image are the stego images using PES 9:1 scheme.

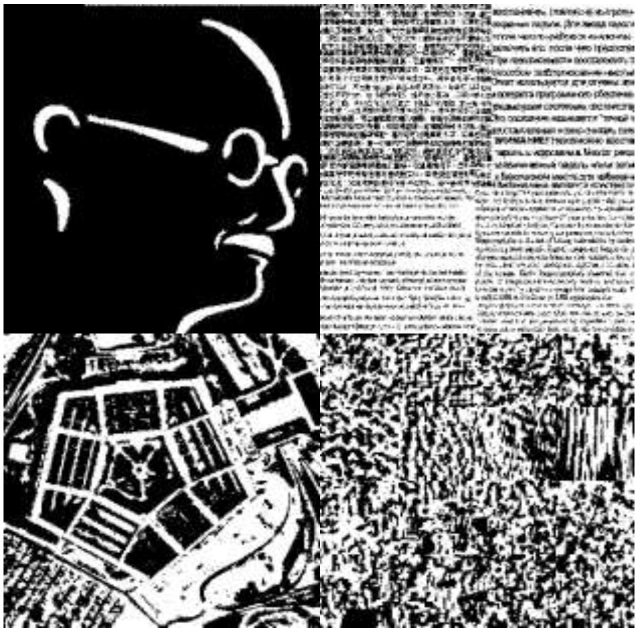

Fig 3: (a), Gandhi (b) Four Language Text ,(c) Pentagon and (d) Blurred Image are the stego images using BOP scheme.

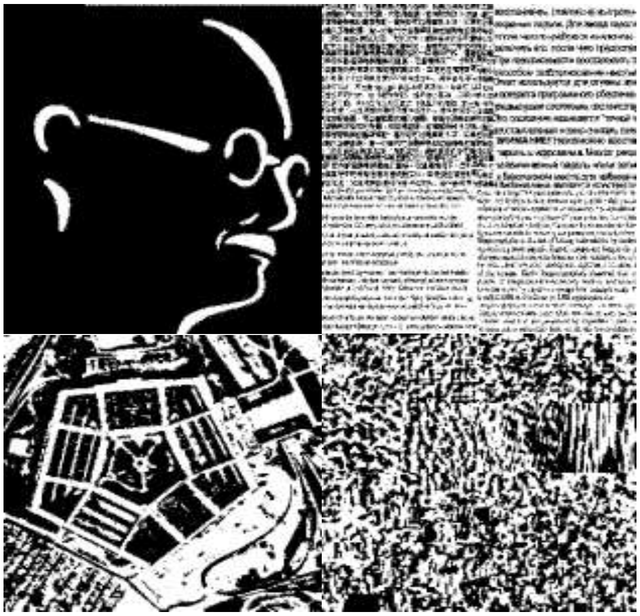

Fig 3: (a), Gandhi (b) Four Language Text ,(c) Pentagon and (d) Blurred Image are the stego images using BFFW scheme.

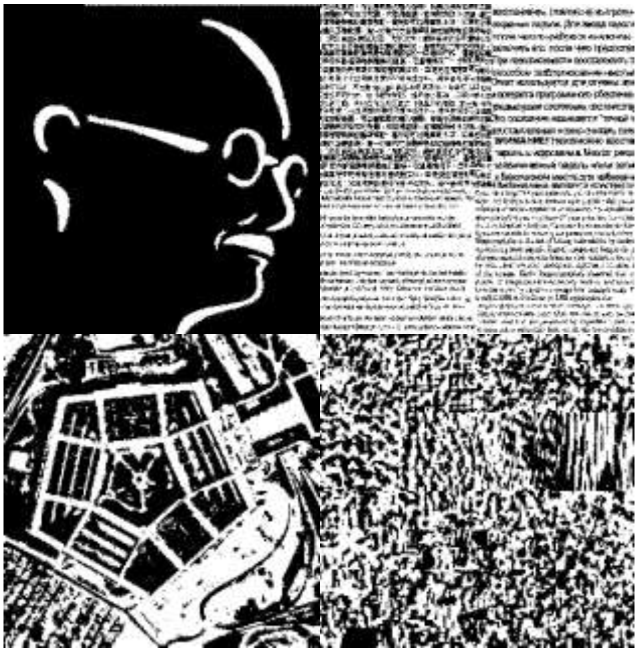

Fig 4: (a), Gandhi (b) Four Language Text ,(c) Pentagon and (d) Blurred Image are the stego images using BFFP scheme.

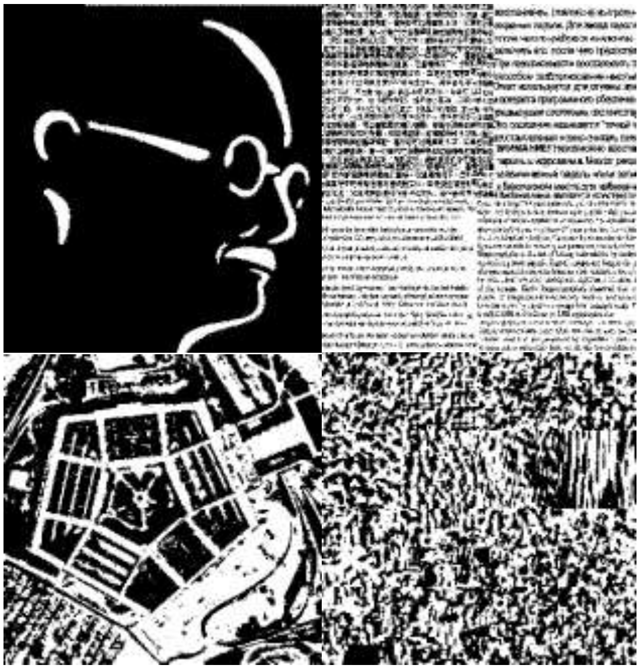

Fig 4: (a), Gandhi (b) Four Language Text ,(c) Pentagon and (d) Blurred Image are the stego images using BTSW scheme.

TABLE-1: Simulation results for embedded information and distorted bits along the bit error rate and relative entropy for gandhiji image.

Gandhi	No of bits embedded	No of errors	Bit error rate	Relative entropy
PES 9:1	10200	4453	0.0062	0.0127
BOP scheme	328	280	3.89e-04	0
BEP scheme	232	272	3.78e-04	0
BFFW	80	57	7.92e-05	2.18e-07
BTSW	328	164	2.28e-04	4.65e-08

TABLE-2: Simulation results for embedded information and distorted bits along the bit error rate and relative entropy for Four Language Text image.

Four Language Text	No of bits embedded	No of errors	Bit error rate	Relative entropy
PES 9:1	10200	5528	0.0077	0.0045
BOP scheme	3368	3442	0.0048	0
BEP scheme	3760	4000	0.0056	0
BFFW	1752	1233	0.0017	1.03e-06
BTSW	3680	2182	0.0030	4.39e-05

TABLE-3: Simulation results for embedded information and distorted bits along the bit error rate and relative entropy for Pentagon image.

Pentagon	No of bits embedded	No of errors	Bit error rate	Relative entropy
PES 9:1	10200	4967	0.0069	6.70e-5
BOP scheme	2008	1978	0.0027	0
BEP scheme	1960	2109	0.0029	0
BFFW	736	481	6.60e-04	1.01e-6
BTSW	1880	967	0.0013	5.95e-6

TABLE-4: Simulation results for embedded information and distorted bits along the bit error rate and relative entropy for Blurred Image image.

Blurred Image	No of bits embedded	No of errors	Bit error rate	Relative entropy
PES 9:1	10200	5119	0.0071	3.04e-04
BOP scheme	2888	2746	0.0038	0
BEP scheme	2904	3040	0.0042	0
BFFW	1192	795	0.0011	1.50e-06
BTSW	3128	1634	0.0023	1.45e-05

5. CONCLUSION:

In this paper based on the experimental results of 4 different binary images PES 9:1 has highest data hiding capacity but the changes made to the cover are visible. BOP scheme is better than PES 9:1, but still there are changes in the cover. BOP scheme has another disadvantage as it cannot recover the information from the blocks which has 9 white pixels so the authors use BEP scheme. BFFW will impart least noticeable changes to cover, while BTSW has highest capacity without noticeable changes to the cover. This paper shouts from above results that the BTSW is most reliable over other methods. So as to conclude, for data hiding in binary images it is better to approach statistically for minimum visible changes in the cover image.

6. ACKNOWLEDGEMENT

The first author wishes to thank Prof. R.Varadharajan Professor / ECE School of Electrical & Electronics Engineering, for his valuable guidance and D. Adarsh former ECE Stego group Student /SEEE/ SASTRA University.

7. REFERENCES

[1]. R.Amirtharajan, Krishnendra Nathella and J Harish, "Info Hide – A Cluster Cover Approach" International Journal of Computer Applications 3(5) (2010)11–18.

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

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

[4]. J. Chen; T. S. Chen & M. W Cheng, "A New Data Hiding Method in Binary Image", in proceedings of 5th IEEE international symposium on multimedia software engineering 2003

[5]. K. F. Hwang and C. C. Chang, "A Run Length Mechanism for Hiding Data into Binary Images", In proceedings of pacific rim workshop on digital steganography 2002, 71-74.

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

[7]. M. Wu and J. Lee, "A Novel Data Embedding Method for Two-Color Facsimile Images", International Symposium on Multimedia Information Processing, Taiwan, December 1998.

[8]. Min Wu; Bede Liu; "Data hiding in binary image for authentication and annotation" in proceedings of IEEE Transactions on multimedia, 6(2004)528 – 538.

[9]. H.K. Pan, Y.Y. Chen and Y.C. Tseng, "A Secure Data Hiding Scheme for Two-Color Images", in proceedings of 5th IEEE Symposium on computers and communication, (2000)750-755.

[10]. Yu-Chee Tseng; Hsiang-Kuang Pan, "Secure and invisible data hiding in 2-color images", in proceedings of 20th IEEE Computer and Communications Societies, INFOCOM (2001) 2887 - 896.