IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

Bit Plane Based Image Authentication in Spatial Domain

Sujit Das[1], Jyotsna Kumar Mandal[2*], Arundhati Bhowal[3]

[1,2,3]University of Kalyani, Kalyani, Nadia-741234, West Bengal, India

[*]*Corresponding Author: jkm.cse@gmail.com*

Available online at: www.ijcseonline.org

Abstract: In this paper a corelated bit plane based steganographic technique has been proposed. The image is sliced into bit planes. A weighted matrix is created corresponding to each bit plane. The entries in the weighted matrix is made based on the position of bit plane and the values are $2^{bit-plane\ position}$ corresponding to ones in bit plane matrix. The correlation of original image and all the weighted matrices corresponding to all bit planes are calculated and bit planes corresponding to two minimum correlation coefficients are selected for embedding. The secret image is converted into binary string. A $2x2$ window is swept over the selected bit planes in row major non-overlapping fashion and secret bits are embedded into these windows in diagonal fashion. The proposed method achieved better image quality on embedding

Keywords: Steganography, Correlation

I. INTRODUCTION

The security in terms of digital content is an important issue. There are variant urges of security in different domains. The data when transferred through networks is not safe if sent without any protection. There are various approaches for protection starting from channel security to content security. The issues of content security deal with mainly two major approaches, Cryptography and Steganography. Cryptography aims at encrypting the content information producing unintelligible data and anyone can realise the presence of some valuable information into the scramble data. A different approach is taken for methods of Steganography, where one secret content is hidden into another content which is called cover media and it is very difficult to sense the presence of the visually.

There are so many literatures based on steganography aims at achieving the higher imperceptibility while hiding higher information into cover media. There variant methods have been used to achieve this objective. In this article the method of correlation is used for selecting the embedding position. The correlation is a statistical method for finding relation between two random variables and correlation coefficient provides the measure that how two variables are related. The values for correlation coefficient ranges over -1 to 1, -1 indicates variables are inversely related and 1 indicates variables are related same way, a zero value indicates two variables are uncorrelated. The expression to find the correlation coefficient is given in formula 1

$$r = \frac{n\sum(xy)-(\sum x)(\sum y)}{\sqrt{[n\sum x^2-(\sum x)^2][n\sum y^2-(\sum y)^2]}} \quad (1)$$

The layout of this article is as follows, literature is presented in section 2. The proposed method of the article is given in section 3. The results and simulations are represented in section 4. The comparison is presented in section 5 and the conclusion is represented in section 6, following this reference are provided.

II. LITERATURE REVIEW

There is deluge of paper based on Steganography, contributed over decades by various researchers. In Varendar et al[7], a transform domain steganography method has been used. Integer wavelet transform along with chaotic map has been used to increase the security level in colour images. This method can be used to text, graphics and images as secret information candidates.

Maniriho et al [8] used a difference expansion and modulus function in embedding process. In this method difference values for both negative and positive have been used for selection for embedding candidates.

Kanan and Nazeri[9] have proposed the data lossless method and tenable visual image quality in spatial domain along with the method of Genetic Algorithm. The paper searched and analysed the critically optimisation problem in steganography.

Lio et al[10] used JPEG Steganography scheme where messages are embedded by modifying Discrete Cosine Transform(DCT) coefficients and dependencies of inter

block coefficients are used to make the performance better. The method uses medical images as cover images.

Gaurav and Ghanekar [1] proposed an innovative Steganography scheme based on local reference edge detection method and exclusive disjunction property. The method achieved better imperceptibility and robustness along the line of same strategy followed by other authors.

Ghosal and Mandal[2] used Starling Transform to convert the cover image into transform coefficients and secret image is scrambled to add more security in concealing scheme.
Kumar et al[3] proposed an innovative and adaptive steganography scheme based on fuzzy edge detection scheme to have improve edge detection process and to have better imperceptibility.

Lee et al[4] proposed an image steganography method with an adaptive embedding scheme that collaborate the methods of edge detection and hybrid Hamming codes to hide a secret information into a cover image. In this method for edge detection, the popular canny edge detection algorithm is used.

From the literature survey it is clear that most of the methods based on edge detection schemes which involves huge computational burden even before the embedding process is started. In proposed method a very simple process has been used to only identify the embedding location which does not involve any complex process to do that.

III. PROPOSED METHOD

The proposed method is manly concentrated on "correlation management" on embedding a hidden image into a cover/carrier image. First, cover image is taken and it's bit-plane slicing is done. The weights of each bit-plane have been calculated. Suppose, 4th bit-plane's weight has to be calculated, then considering (i,j)th position of 4th bit-plane, if there is '0' at (i,j)th position it will be considered as '0'.And if in the (i,j)th position ,there is 1, it will be considered as $2^{bit-plane\ no}$, for example 2^4 for 4th bit-plane.

On calculation of weights of each bit-plane, correlation has been calculated for (1-4th)bit-plane with cover image and these values are sorted in increasing manner. Two bit planes are selected based upon the correlation coefficient values with minimum values. A $2x2$ window is swept over the two bit plane matrices in row major non overlapping fashion. The secret image is converted into binary string. The bits are taken two at a time from the bit string and two $2x2$ blocks of bits from two chosen bit planes are read. The first bit of the two bits is embedded into (1,1) position of $2x2$ block of first bit plane second bit into $2x2$ block of second bit plane. Next time the position is flipped, that is (2,2) position of first block and (1,1) position of second block is chosen. This operation is repeated until all the bit of bit string is embedded. The bit planes are merged after embedding and stego image is generated. A key has been generated to ensure successful extraction secret bits. The selected two bit plane numbers chosen during the embedding process is transformed into binary string of length four. These bits are embedded at the fixed location of first and second bit plane. Again two $2x2$ blocks are chosen from first and second bit plane at the top left position of bit plane matrix. The first two bits are embedded at locations (1,2) & (2,1) of first bit plane block and next two bits are embedded at locations at locations (1,2) & (2,1) of second bit plane block. The chances of overriding with secret bits is zero as because in this respect the opposite diagonal .

The extractions process is done at the receiver end. The stego image is sliced into bit planes. The locations of required bit planes are read from the first and second bit plane top left $2x2$ block. The obtained bit planes are read by $2x2$ block in same way as employed in embedding process. The obtained bit string then converted to secret image. The block diagram of proposed method is given in figure 1.

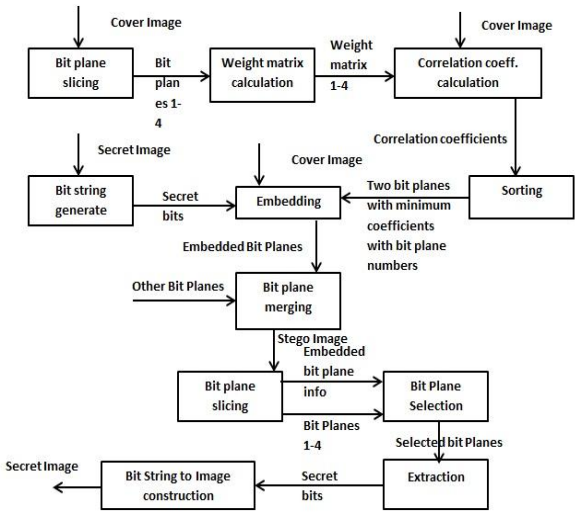

Figure 1 Block Diagram of proposed Method

The algorithms for embedding and extractions is given in Algorithn 1 and Algorithm 2

Algorthim1: Embedding

Input:Cover image(N×N),Secret image(M×M)

Output:Stego Image

Method: Cover image is sliced into bit planes. Weight matrices are created for bit planes 1-4. Correlation coefficient is calculated between weight matrices and cover image and two bit planes are selected

with minimum Correlation coefficient value. Secret image is transferred in binary string. Bits are embedded in selected two bit planes.

Step1:-Select a cover image(N×N)

Step2:-Select a secret image(M×M)

Step3:-Slice the cover image into bit-planes
Step4:-Weights of the bit-planes are calculated

Step5:-Correlation calculation has been done on the weighted bit-planes (1^{st} to 4^{th}) with cover image..

Step6:-Two Bit-planes, BP1 & BP2 , having lowest correlation values has been taken for embedding.

Step7:- convert the secret image into bit string BITS.

Step8:-Two windows, W1 for BP1 & W2 for BP2 of size 2 x 2 , is swept over the two selected bit planes ,BP1 & BP2, in row major non overlapping fashion
Step9:-set W1[I,J]=BITS[K] & W2[I+1,J+1]=BITS[K+1]. In the next iteration the positions are flipped i.e. W2[I,J]=BITS[K] & W1[I+1,J+1]=BITS[K+1]. Here I,J, K are the index variable
Step 10: Repeat step 9 until all bits of BITS are embedded.

Step11:-A 4 bit key is generated to store the two bit plane numbers in binary representation. The bits are stored in bit plane one and bit plane two at the top left position of bit plane matrices at position (1,2) & (2,1) for bit plane one and next two bits at the location (1,2) & (2,1) for bit plane two.

Step12:- The all bit planes are merged after all process are completed and stego image is generated

Step13:-Stop

Algorithm 2: Extraction

Input: Stego Image

Output: Secret image

Method: Stego image is sliced into bit planes. The required bit plane numbers are extracted from bit plane one and two. The obtained bit planes are read and secret information is obtained
Step 1:-Take the stego image.

Step 2:-Extract the embedded bits from bit plane one and bit plane two from the location top left of the bit plane matrices to get the bit plane number and based on this numbers two bit planes BP1 & BP2 are selected.

Step 3:- create a binary string BITS[1…MxM].
Step 4 Two windows, W1 for BP1 & W2 for BP2 of size 2 x 2 , is swept over the two selected bit planes ,BP1 & BP2, in row major non overlapping fashion.

Step 5:- set BITS[K]= W1[I,J] & BITS[K+1]= W2[I+1,J+1]. In the next iteration the positions are flipped i.e. BITS[K]= W2[I,J] & BITS[K+1]= W1[I+1,J+1]. Here I,J, K are the index variable

Step 6: Repeat step 5 until all secret bits are extracted.
Step 7:- bits of bit string BITS are converted to secret image.

Step 8:-Stop.

IV. RESULT AND SIMULATION

The proposed method is implemented on ten benchmark images [6] is shown in figure of resolution $512x512$ and secret image is shown in figure of resolution $128x128$ for the payload 0.5bpB. Three different parameters, IF, PSNR, SSIM have been computed according to the proposed method to justify the correctness and goodness as well.

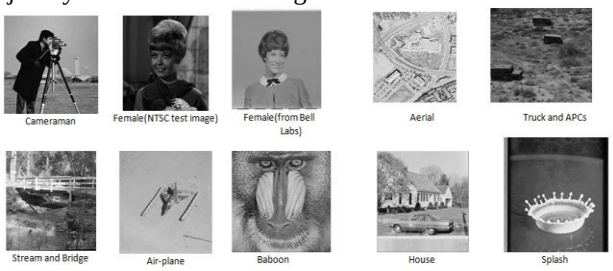

Figure 2 Ten Bench Mark Images Used in proposed Method

Figure 3 Secret Image

The parameter (PSNR, IF, SSIM) values for the benchmark images have been tabulated in the Table 1. The first column represents standard image name. The second column represent size of the images. The third column represents PSNR values, third column for IF , the last column for Structural Similarity Index (SSIM). The last column represents MSE . It can be seen from Table 1 that the maximum PSNR image Airplane which is 86.36 and minimum PSNR for image Female (BellLabs) which is 86.2554. It can be observed that the PSNR for the ten images does not varies in wide range.

Table 1 Performance Parameters (PSNR,IF & SSIM) for Ten Benchmark Images

IMAGE NAME	***SIZE (KB)***	***PSNR***	***IF***	***SSIM***	***MSE***
Cameraman	256	86.3297	0.9995	0.9995	0.0277
Female(NTSC)	256	86.2787	0.9980	0.9980	0.028
Female(BellLabs)	256	86.2554	0.9995	0.9995	0.0282
Aerial	256	86.2645	0.9997	0.9997	0.0281
Truck and APCs	256	86.2676	0.9989	0.9955	0.0281
Stream and Bridge	256	86.2567	0.9994	0.9983	0.0281
Airplane	256	86.3637	0.9997	0.9902	0.0275
Baboon	256	86.2775	0.9995	0.9974	0.028
House	256	86.2979	0.9997	0.9979	0.0279
Splash	256	86.3178	0.9992	0.9983	0.0278

The IF of the is maximum for image Aerial which is 0.9997 and minimum for image Female (NTSC) which is 0.9980. Similarly ,the SSIM is maximum for image Aerial which is 0.9995 and minimum for image Airplane which is 0.9902. It is very noticeable that all the SSIM value is very close to 1, which indicates that structural properties are not hampered with the proposed method. It is also clear from the last column MSE is very less for each of the images.

The Parameter values are also shown in graphs which shown in the figure 4, 5,6

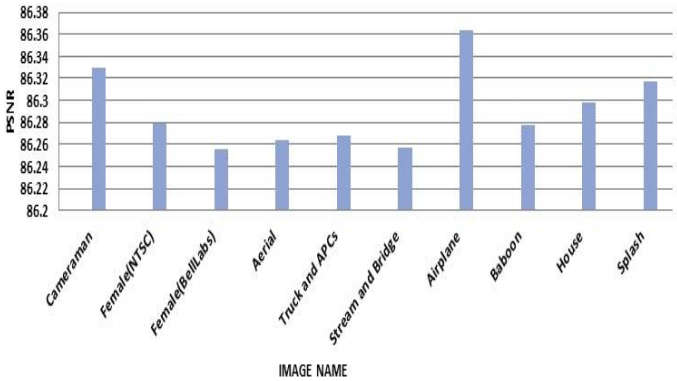

Figure 4 PSNR between Stego Images and Cover Images

The graphical representation of parameter (PSNR) values of ten standard images are presented in Figure 4. The x axis represents the images and y axis represents the corresponding PSNR values. It can be observed from the figure all the value of PSNR remains around 86 dB, only fractional values are changed which does not contribute to degradation. It can be seen that maximum value is for image Airplane and minimum value for image Female (BellLab).

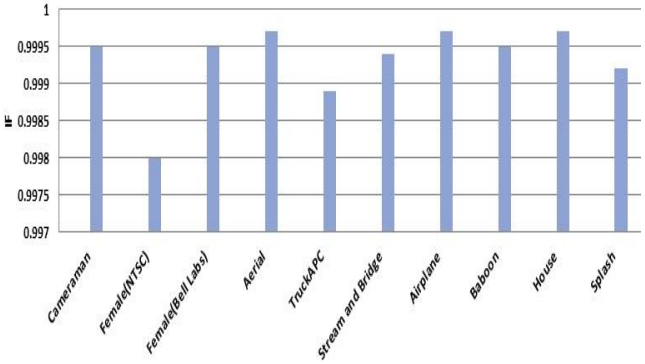

Figure 5 IF between Stego Images and Cover Images

The graphical representation of parameter (IF) values of ten standard images are represented in Figure 5.The x axis represents the images and y axis represents the corresponding PSNR values. It can be noticed from the figure all the value of IF remains very close to 1, which indicates good imperceptibility of the method. It can be seen that maximum value is for image Aerial and minimum value for image Female (NTSC).

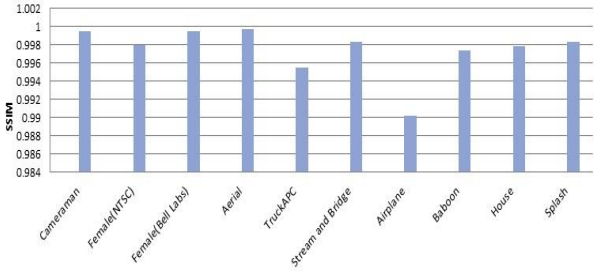

Figure 6 SSIM between Stego Images and Cover Images

The graphical representation of parameter (SSIM) values of ten standard images are presented in Figure 6 .The x axis presents the images and y axis represents the corresponding PSNR values. It can be noticed from the figure all the value of IF remains very close to 1, which indicates that the structural properties are preserved after embedding. It can be seen that maximum value is for image Aerial and minimum value for image Airplane.

V. COMPARISONS

The proposed method is compared with five existing method as given in Table 2. The first column represents abbreviated names of existing methods. Second column represents varying payload for which existing method and proposed methods are tested. The last column presents the PSNR values of existing method and proposed methods corresponding to the payloads.

Table 2 Comparison of Proposed Method with Existing Methods

Method	Payload	PSNR
ISBCDDOHC[1]	0.65	49.5251
STIS[2]	0.5	52.3026
ASBNFEI[3]	0.5	50.03
AHEDHHOC[4]	0.4	47.59
MPBDA[5]	0.4	56.64
Proposed Method	0.5	86.29095

It is noticeable from the Table 2 that methods, AHEDHHOC[4] & MPBDA[5], with payload 0.4bpB have very low PSNR values. The method, STIS[2], with payload 0.5bpB have very low PSNR than proposed method. It is visible that proposed methods performs better in terms of PSNR value than the method, ISBCDDOHC[1] which has payload 0.65bpB.

The comparison between proposed method and existing methods are also depicted in the figure 7. The horizontal axis presents the methods with payloads and vertical axis presents PSNR values. It is also vivid from the graph that the proposed method outperforms existing methods in terms of PSNR quality parameter.

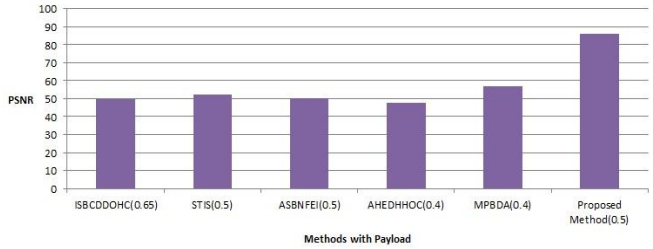

Figure 7 Graphical Comparison of Proposed Method with Existing Methods

VI. Conclusion

In this article simple correlation coefficient has been used to get very high perceptual visibility. It is clear from the simulation results that imperceptibility is very high for varying images used. The proposed method is used for payload 0.5bpB with cover image resolution 512x512 and secret image resolution 128x128. The higher use higher payload following the same method is a matter of future implementation.

REFERENCES

[1]. K. Gaurav, U. Ghanekar," Image steganography based on Canny edge detection",dilation operator and hybrid coding. Journal of Information Security and Applications Volume 41,pp:41-51

[2]. S.K Ghosal, J.K Mandal," On the use of the Stirling Transform in image steganography", Journal of Information Security and Applications,2018,Doi: https://doi.org/10.1016/j.jisa.2018.04.003.

[3]. S Kumar, A. Singh, M. Kumar," Information hiding with adaptive steganography based on novel fuzzy edge identification", Defence Technology,2018, doi: 10.1016/j.dt.2018.08.003

[4]. C-F. Lee, C-C. Chang, X. Xie, K. Mao, R-H. Shi," An Adaptive High-Fidelity Steganographic Scheme Using Edge Detection and Hybrid Hamming Codes", Displays,2018, doi: https://doi.org/ 10.1016/j.displa.2018.06.001

[5]. Nguyen, T.D., Arch-int, S. & Arch-int N., "An adaptive multi bit-plane image steganography using block data-hiding", N. Multimed Tools Appl ,2018, Vol 75 issue 14, pp. 8319–8345.

[6]. Standard Image database, USC University of Southern California, http://sipi.usc.edu/database/, doa:16, October 2018

[7]. M. Y. Valandar, P. Ayubi., M. J Barani. " A new transform domain steganography based on modified logistic chaotic map for color images", Journal of Information Security and Applications, 2017, vol. 34 pp. 142-151.

[8]. P. Maniriho., T. Ahmad," Information Hiding Scheme for Digital Images Using Difference Expansion and Modulus Function", Journal of King Saud University - Computer And Information Sciences.,2018,doi:https://doi.org/10.1016/j.jksuci.2018.01.011

[9]. H.R Kanan,. And B. Nazeri," A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm", Expert Systems with Applications,vol. 41, issue 14,pp. 6123–6130.

[10]. X. Liao, J. Yin ,S. Guo.,X. Li.," Medical JPEG image steganography based on preserving inter-block dependencies", Computers and Electrical Engineering,2018, vol. 67, pp. 320-329.

Authors Profile

Mr. Sujit Das pursed Master of Technology from Dept. of Computer Sc. & Engg.,Univesity of Kalyani in 2016. He has done Master of Applications from Haldia Institute of Technology, West Benagl University of Technology in 2010. He has done his bachelor degree in Computer Sc, from Siliguri College, University of North Bengal. He is currently pursuing Ph.D. from Kalyani University, Dept. of Computer Sc. & Engg. His area of interests are- Network Security, Steganography, Cryptography, Signal Proccessing and Bio-Medical Imaging.

Dr. J..K. Mandal pursed his M.Tech from University of Calcutta. He has done his Ph.D. from Jadavpur University and his reaserch topic was Data Compression and Error Correction Technique. He is Life of Computer Society of India since 1992.He is ex-Dean Faculty of Technology and Management, University of Kalyani. In his more than 30 years of teaching, he has successfully completed 23 PhD students under his supervision and 8 more are pursuing. His area of interest are- Network Security, Steganography, Cryptography, Data Compression, Image Processing, Cloud, Data Science, Mobile Computing, Signal processing, Machine Learning and so on.He has more than three hundreds of publication in total and editors or guest editors in numerous books, Journals, Proceedings etc.

Miss. Arundhati Bhowal pursed her bachelor degree in IT from MCKV Institute of Engineering. She is currently pursuing her Master of Technology ffrom Dept. of Computer Sc. & Engg., University of Kalyani. Her area of interest are- Steganography, Cryptography, Network Security and Image Proccessing.

