EasyChair Preprint

№ 5110

Augmentation of Novel Algorithm for Secured Information Hiding with Pixel Mapping

N Shyla, K Kalimuthu and N Shylaashok

March 9, 2021

AUGMENTATION OF NOVEL ALGORITHM FOR SECURED INFORMATION HIDING WITH PIXEL MAPPING

Shyla N, Assistant Professor, FET-Jain University, Bangalore, Dr. Kalimuthu, Associate Professor SRMIST,Kattankalathur, Chennai .

***Abstract*:** Information Hiding is one of the difficult issues in the field of Network Security. In contrast to cryptography, Steganography is utilized to shroud the presence of mystery message by installing the message behind any spread item like picture, text, sound, video documents. Different creators proposed, different techniques for concealing mystery data behind dark scale pictures, for example, least noteworthy strategy, dim level adjustment, pixel esteem differencing, pixel planning strategy and pixel planning technique with BPCS, yet all these technique are not up to the imprints that implies expanding the installing limit of StegoImage and to furnish Stego-Image with a subtle quality are still difficulties. To improve indistinct quality, we proposed an upgraded procedure "An Enhanced Data Hiding Approach Using Pixel Mapping Method (PMM) With Optimal Pixel Substitution Approach " that gives a superior Peak Signal to commotion ratio(PSNR) between Cover-Image and Stego-Image with great implanting limit. The proposed approach depends on four modules – planning rules, set classifier technique, pixel choice strategy, and least differencing capacity to shroud information inside a picture. This strategy works by choosing a lot of pixels; map mystery information into these chose pixels as indicated by planning rules and creates new Stego pixel esteem in the wake of planning mystery message as per Minimum Pixel Difference work. This coordinated proposed approach gives greater security to mystery information as without realizing the planning rules and areas of pixels nobody could remove the mystery information. This proposed approach gives bigger inserting limit as well as produces a worthy Stego picture quality that can be seen by natural eyes.

Keywords- Steganography, Information Hiding, Pixel Mapping, Pixel Value Differencing, Gray Scale Image, Cover Image, Method, Optimal Substitution, Stego Image**.**

I. INTRODUCTION

To shield mystery message from being taken during transmission, there are two different ways to tackle this issue when all is said in done. One way is encryption, which alludes to the way toward encoding mystery data so that solitary the privilege individual with a correct key can interpret and recoup the first data effectively. Another way is steganography and this is a strategy which shrouds mystery data into a spread media or transporter so it becomes unnoticed and less alluring. Limit and imperceptibility are the benchmarks required for information concealing procedures of steganography. An acclaimed outline of steganography is Simmons' Prisoners' Problem [19]. A supposition can be made dependent on this model is that on the off chance that both the sender and collector share some normal mystery data, at that point the relating steganography convention is known as then the mystery key steganography where as unadulterated steganography implies that there is none earlier data shared by sender and beneficiary. On the off chance that the open key of the collector is known to the sender, the steganographic convention is called open key steganography [1], [2] and [9]. For a more exhaustive information on steganography system the peruser may see [17], [21].Some Steganographic model with high security highlights has been introduced in [3], [4] and [5]. Practically all advanced document organizations can be utilized for steganography, yet the picture and sound records are more reasonable due to their serious extent of excess [21]. Fig. 1 underneath shows the various classes of steganography strategies.

Fig 1. Steganography Kinds

A block diagram of image steganographic system is given in Fig. 2.

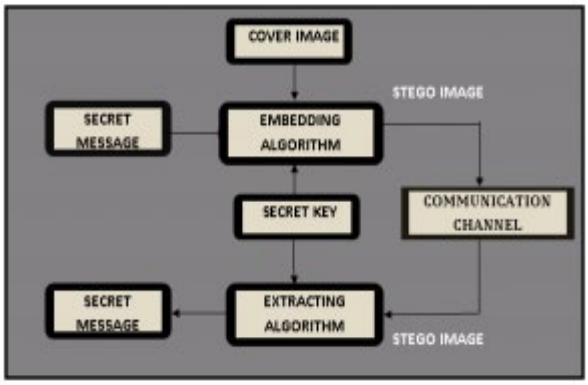

Fig 2. Image Steganographic System

A message is implanted in an advanced picture (spread picture) through an implanting calculation, with the assistance of a mystery key.

The subsequent stego picture is communicated over a channel to the beneficiary where it is handled by the extraction calculation utilizing a similar key. During transmission the stego picture, it very well may be checked by unauthenticated watchers who will just notification the transmission of a picture without finding the presence of the concealed message. In this work a particular picture based steganographic technique for dim level picture has proposed. In this strategy as opposed to inserting the mystery message into the spread picture a planning procedure has been fused to create the stego picture. This technique is equipped for removing the mystery message without the nearness of the spread picture.

II. LITERATURE SURVEY

2.1. Information Hiding by LSB

Different procedures about information covering up have been proposed in writings. One of the normal procedures depends on controlling the least-huge piece (LSB) [7], [8] and [15], [18]planes by legitimately supplanting the LSBs of the spread picture with the message bits. LSB techniques regularly accomplish high limit however lamentably LSB addition is powerless against slight picture control, for example, editing and pressure.

2.2. Information Hiding by PVD

The pixel-esteem differencing (PVD) technique proposed by Wu and Tsai [22] can effectively give both high installing limit and remarkable impalpability for the stegoimage. The pixel-esteem differencing (PVD) strategy fragments the spread picture into non covering squares containing two associating pixels and changes the pixel contrast in each square (pair) for information inserting. A bigger contrast in the first pixel esteems permits a more noteworthy adjustment. In the extraction stage, the first range table is vital. It is utilized to segment the stego-picture by a similar strategy as used to the spread picture. In view of PVD strategy, different methodologies have likewise been proposed. Among them Chang et al. [14]. proposes another strategy utilizing tri-way pixel-esteem differencing which is better than unique PVD technique as for the inserting limit and PSNR.

2.3. Information Hiding by GLM

In 2004, Potdar et al.[10] proposes GLM (Gray level alteration) strategy which is utilized to plan information by adjusting the dim degree of the picture pixels. Dim level change Steganography is a method to plan information (not implant or shroud it) by adjusting the dim level estimations of the picture pixels GLM strategy utilizes the idea of odd and even numbers to plan information inside a picture. It is a coordinated planning between the paired information and the chose pixels in a picture. From a given picture a lot of pixels are chosen dependent on a numerical capacity. The dim level estimations of those pixels are analyzed and contrasted and the bit stream that will be planned in the picture.

2.4 BPCS Steganography

BPCS (Bit-Plane Complexity Segmentation) steganography was presented by Eiji Kawaguchi and Richard O. Eason [11] ,to defeat the deficiencies of conventional steganographic strategies like Least Significant Bit (LSB) method, Transform area implanting strategy. The significant part of BPCS-Steganography contrasted with those philosophy is that the implanting limit is very large.BPCS steganography utilizes significant trademark that of human vision. In BPCS, the vessel picture is partitioned into enlightening locale and commotion like area and the mystery information is covered up in clamor squares of vessel picture without corrupting picture quality [11], [16]. In LSB method, information is covered up in last four pieces for example as it were in the 4 LSB bits[13]. Be that as it may, in BPCS procedure, information can likewise be covered up in MSB planes alongside the LSB planes gave mystery information is covered up in complex area [11].

2.5. Essential Principle of BPCS Steganography

In BPCS, a multi-esteemed picture (P) comprising of n-bit pixels can be decayed into set of n twofold pictures. Model: P is a n-bit dark picture say n=8. Consequently P = [P7 P6 P5 P4 P3 P2 P1 P0] where P7 is the MSB bit plane and P0 is the LSB bit plane. Each piece plane can be fragmented into enlightening and commotion district. An enlightening district comprises of basic example while commotion like district comprises of complex design. In BPCS, each clamor looking area is supplanted with another clamor looking example without changing the by and large picture quality.Thus, BPCS steganography utilizes this nature of human vision framework [16], [12].

III. ARCHITECTURE

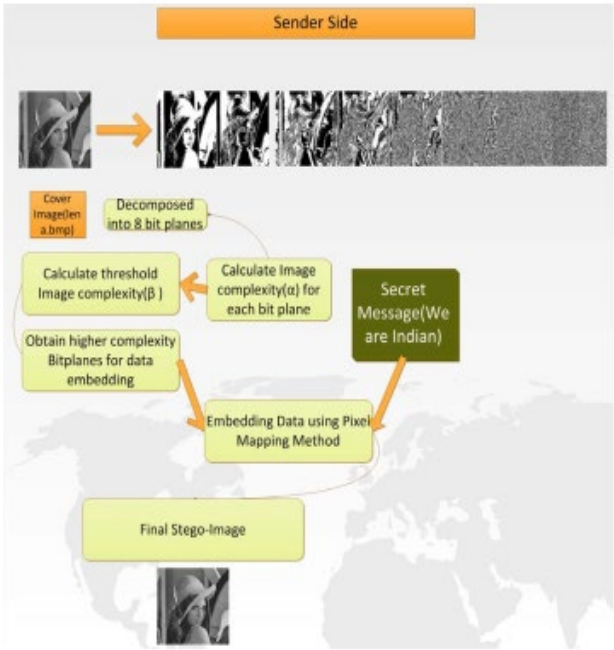

Fig. 3. Sender Side System Architecture

Information Embedding measure: (As appeared in Fig 3)

• Slice Cover Image into 8-piece planes of [b1,b2,b3,b4,b5,b6,b7,b8] where b1 speaks to the most elevated piece plane and b8 speaking to the least piece plane.

• Compute the unpredictability (alpha) of each piece plane from b1 to b8.

• Compute the limit unpredictability for the planes.

• Fetch the higher multifaceted nature planes(that is bit planes with multifaceted nature more prominent than limit intricacy).

• Convert the whole mystery instant message into 8-piece parallel structure and partition the whole double message into an arrangement 2-piece paired stream.

• Divide the a high multifaceted nature bit plane into 32X32 squares which again apportioned into 8X8 double squares. Along these lines apportioning the whole picture into 8X8 parallel squares

• Each of the 2-piece parallel piece stream is installed into each 1X8 double picture information squares of higher complex plane utilizing 2-piece implanting technique for Pixel Mapping Method(PMM).

• Merge all the 8X8 changed and unaltered parallel squares to get the altered piece plane.

• Repeat stages 7 - 9 until all the mystery message characters have been implanted.

• Merge all the bit planes [b1,b2,b3,b4,b5,b6,b7,b8] to get the stego-picture.**I**

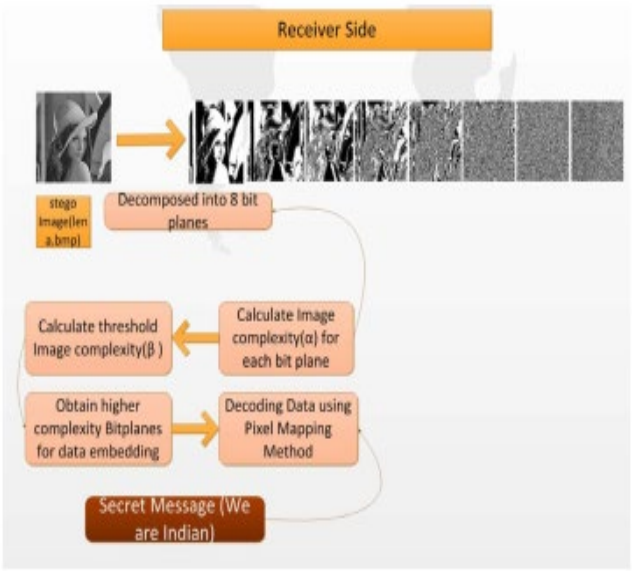

Fig. 4. Receiver Side System Architecture

Information Extraction Method: (As appeared in fig 4)

• Slice the stego picture into 8-piece planes of [b1,b2,b3,b4,b5,b6,b7,b8] where b1 speaks to the most elevated piece plane and b8 speaking to the least piece plane.

• Find the inserted bit planes and gap them into 8X8 paired squares.

• Access each 8X8 square and apply extraction strategy for PMM(2 Bit) to get back the inserted bits.

• Arrange the pieces got in appropriate request to get back the mystery message.

IV. PROPOSED METHOD

Proposed APPROACH WITH Pixel Mapping Method

Pixel Selection Method In our proposed strategy we are consecutively choosing pixels to install message bits into chose pixel. We can likewise utilize an arbitrary capacity 2r+ 5 % width to choose pixels in irregular way where r speaks to column of picture. By utilizing irregular areas we can improve the security of mystery message however it will debase the implanting limit.

During installing the message bits, change the equality of message bit (ASCII Conversion worth) and pixel esteem by planning rules (even to odd transformation)

Moreover increment the security by producing another numbers for both pixel worth and message esteems (Add the two numbers for getting new number as pixel esteem).

In the event that the new pixel esteem is more prominent size, at that point, new number gap by some number to get normal incentive as new pixel esteem)

Pixel Sets Classifier Method

In this we proposed a technique to separate pixels set into subsets of pixels dependent on pixel's force and equality.

For installing information bits set classifier will isolate pixels set into 4 pixels subsets –

PixelEE = {Finite Set Of Those Pixels Having Even Intensity and Even Parity},

PixelEO = {Finite Set Of Those Pixels Having Even Intensity and Odd Parity},

PixelOE = {Finite Set Of Those Pixels Having Odd Intensity and Even Parity}

PixelOO = {Finite Set Of Those Pixels Having Odd Intensity and Odd Parity}

Information Hiding Mapping Rules

In this area some planning rules are characterized based on pixel force and its equality. As we realize that force and equality of a pixel can be even or odd. For inserting 2 pieces information we will keep planning rules given in table 1.

☐Mapping Rule 1 – in the event that information pieces are 00, at that point change the power of chosen pixel into even force and make the equality of chose pixel is even.

☐ Mapping Rule 2 – on the off chance that information pieces are 01, at that point change the force of chosen pixel into even power and make the equality of chose pixel is odd.

☐ Mapping Rule 3 – on the off chance that information pieces are 10, at that point change the force of chosen pixel into odd power and make the equality of chose pixel is even.

☐Mapping Rule 4 – in the event that information pieces are 11, at that point change the force of chosen pixel into odd power and make the equality of chose pixel is odd.

Table 1: Mapping Rules for Hiding 2 Bits per Pixel

Message Bits Pair (0^{th}/1^{st} bits pair)	Pixel Intensity	Parity
00	EVEN	EVEN
01	EVEN	ODD
10	ODD	EVEN
11	ODD	ODD

Table 2: Mapping Rules for Hiding 4 Bits per Pixel

Message Bits Pair (2^{nd} /3^{rd} bits and 0^{th}/1^{st} bits pair)		Pixel Intensity	Parity
00	00	EVEN	EVEN
	01	EVEN	ODD
	10	EVEN	EVEN
	11	EVEN	ODD
01	00	EVEN	EVEN
	01	EVEN	ODD
	10	EVEN	EVEN
	11	EVEN	ODD
10	00	ODD	EVEN
	01	ODD	ODD
	10	ODD	EVEN
	11	ODD	ODD
11	00	ODD	EVEN
	01	ODD	ODD
	10	ODD	EVEN
	11	ODD	ODD

Table 3: Mapping Rules for Hiding 6 Bits per Pixel

Message Bits Pair (4^{th}/5^{th} bits and 2^{nd} /3^{rd} bits and 0^{th} /1^{st} bits pair)		Pixel Intensity	Parity
00	0000	EVEN	EVEN
	0001	EVEN	ODD
	0010	EVEN	EVEN
	0011	EVEN	ODD
01	0100	EVEN	EVEN
	0101	EVEN	ODD
	0110	EVEN	EVEN
	0111	EVEN	ODD
10	1000	ODD	EVEN
	1001	ODD	ODD
	1010	ODD	EVEN
	1011	ODD	ODD
11	1100	ODD	EVEN
	1101	ODD	ODD
	1110	ODD	EVEN
	1111	ODD	ODD

V. ALGORITHMS

Algorithm of Proposed Method for Embedding Four/Six Bits Data at Sender

Input: Cover Image (Cimg), Secret Message (Data[n]), Count, D[4], D[6];

Initialize count=0, n=length (Data), D [4] = {0, 0, 0, 0}, D [6] = {0,0,0, 0, 0, 0};

Step - 1 Select Cover Image in Which you Want to Hide Data.
Step – 2 Read Message From Text File And Convert Secret Message Into Binary.
Step – 3 Compute Length of Secret Message in Binary
Step – 4 Select Cover Image Pixel (C_Pix) On The Basis Of Pixel Selection Method. If Selected Pixel Is Lies On The Boundary Then Ignore It and Select Another Pixel.
Step – 5 Read First Four Bits or six bits of Message into D0, D1, D2, D3, D4 And D5.
Step – 6 If (D2==0 && D3== 0) Then Find Minimum difference Pixel with C_Pix from Pixel
Set PixelEE, & C_Pix [5] == D0 and C_Pix [6] ==D1
Else
If (D2== 0 && D3== 1) Then
Find Minimum difference Pixel with C_Pix from Pixel Set
PixelEO, & C_Pix [5] == D0 and C_Pix [6] ==D1
Else
If (D2== 1 && D3== 0) Then
Find Minimum difference Pixel with C_Pix from Pixel Set
PixelOE, & C_Pix [5] == D0 and C_Pix [6] ==D1
Else
If (D2== 1 && D3== 1) Then
Find Minimum difference Pixel with C_Pix from Pixel Set
PixelOO, & C_Pix [5] == D0 and C_Pix [6] ==D1
Step – 7 Repeat Steps from 4 To 6 Until Secret Message Is Embedded.
Step – 8 Return Stego Image & End.

Algorithm of Proposed Method For Extraction Four/Six Bits Data at Receiver

Input: Stego Image (Simg), Secret Message (Data[n]), Count, D[4], D[6];

Initialize count=0, n=length (Data), D [4] = {0, 0}, D[6] = { 0, 0};

Step – 1 Select Stego Image from Which you Want to Extract Data.
Step – 2 Select Stego Image Pixel (S_Pix) On The Basis Of Pixel Selection Method. If Selected Pixel Is Lies On The Boundary Then Ignore It and Select Another Pixel.
Step – 3 D0 = S_Pix [5]; D1=S_Pix [6]
Step – 4 If (S_Pix Mod 2 == 0) Then D2 = 0; Else D2 = 1;
Step – 5 If (Parity (S_Pix) Mod 2 == 0) Then D3 = 0; Else D3 = 1;

Step – 6 Repeat Steps from 2 To 4 Until Secret Message Is Extracted.
Step – 7 End.

VI. EXPERIMENTAL RESULTS

Mean Squared error (MSE) is used to measures the average squared difference between Cover-Image and Stego-Image i.e. it measures difference between actual output and desired output. Smaller MSE is better. MSE is calculated by

$$\mathbf{MSE} = \frac{1}{height * width} * \sum_{i=1}^{height} \sum_{j=1}^{width} [C(i,j) - S(i,j)]\text{^}2$$

Where $C(i,j)$, is cover image, S(i,j) is the Stego image, height is maximum no. of rows in image and width is maximum no. of columns in image.

Peak signal to noise ratio (PSNR) is used to measure the quality of Stego-image after embedding secret data in Coverimage i.e. it measures percentage of hidden data to the percentage of image, greater PSNR is better. PSNR is calculated by

$$\mathbf{PSNR} = 20 \log \left(\frac{I_{max}}{\sqrt{MSE}} \right)$$

Where value of I_{max} is 255 for 8 bit gray scale images because maximum value can be defined by using 8 bit is 255.

VII. CONCLUSION AND FUTURE WORK

This is an effective way to deal with map mystery message into dark scale pictures to give better picture quality and data inserting limit. This upgraded approach can likewise be utilized to insert 8 pieces information by broadening planning rules. Key preferences of this methodology are – unapproved individual can't recover information without the information on planning rules, can give better security by planning information into haphazardly chosen pixels, it has low computational overhead over other Steganography approaches since it doesn't need change of pictures into recurrence area.

Future work of this methodology will think about after changes –

- Relate encryption with this methodology in which message is scrambled by utilizing irregular coarse machine to expand security before inserting information into spread picture.
- Investigating this technique on shading pictures.
- Modifying this methodology by utilizing wavelets.

REFERENCES

[1] Souvik Bhattacharyya and Gautama Sanyal. Study and analysis of quality of service in different image based Steganography using PMM. International journal of applied information system – foundation of computer science, New York, USA 2012

[2] Souvik Bhattacharyya and Gautam Sanyal. PMM (Pixel Steganographic method for gray – level images with four-pixel differencing and LSB Substitution 978-1-61284-7332-0/11/$26 2010 – IEEE

[3] M D medeni and EI M Souidi A novel Steganographic method for gray – level images with four-pixel differencing and LSB Substitution 978-1- 61284-7332-0/11/$26 2010 – IEEE

[4] J.K Mandal and Debashis Color image Steganography based on pixel value differencing in spatial domain – international journal of information science and techniques July 2012.

[5] Wang Yan And Ling-di Ping. A new Steganography algorithm based on spatial domain, 978-0-7695-3991-1/09/$26 2009 – IEEE

[6] Transforming LSB substitution for image based Steganography in matching algorithms. Journal of information science and engineering 26, 1199-1212 2010

[7] Potdar V.and Chang E. Gray level modification Steganography for secret communication. In IEEE International Conference on Industrial Informatics., pages 355–368, Berlin, Germany, 2004.

[8] Chung-Ming Wang, Nan-I Wu ,Chwei-Shyong Tsai and Min-Shiang Hwang A high quality Steganographic method with pixel value differencing and modulus function. The journal of system and software – science direct – 2007

[9] Souvik Bhattacharyya. and Gautam Sanyal. Hiding data in images using pixel mapping method (pmm). In Proceedings of 9th annual Conference on Security and Management (SAM) under The 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing (World Comp 2010), Las Vegas, USA, July 12-15,2010.

[10] Ahmad T. Al-Taani. and Abdullah M. AL-Issa. A novel Steganographic, method for gray-level images. International Journal of Computer, Information, and Systems Science, and Engineering, 3, 2009.

[11] P Huang. K.C. Chang., C.P Chang. and T.M Tu. A novel image Steganography method using tri-way pixel value differencing. Journal of Multimedia, 3, 2008.

[12] Souvik Bhattacharyya, lalan kumar and Gautam Sanyal. A novel approach of data hiding using PMM(Pixel Mapping method). International journal of computer science and information security – vol 8. No. 4 2010.

[13] C.K. Chan. and L. M. Cheng. Hiding data in images by simple lsb substitution. Pattern Recognition, 37:469–474, 2004.

[14] D.C. Wu. and W.H. Tsai. A steganographic method for images by pixel value differencing. Pattern Recognition Letters, 24:1613–1626, 2003.

[15] J.Y. Hsiao. C.C. Chang. and C.-S. Chan. Finding optimal
least significant- bit substitution in image hiding by dynamic programming strategy. Pattern Recognition, 36:1583–1595, 2003.

[16] C.F. Lin. R.Z. Wang. and J.C. Lin. Image hiding by optimal lsb substitution and genetic algorithm. Pattern Recognition, 34:671–683,2001.

[17] Y. K. Lee. and L. H.Chen. High capacity image steganographic model. IEE Proc.-Vision, Image and Signal Processing, 147:288–294, 2000.

[18] Ross J. Anderson. and Fabien A.P.Petitcolas. On the limits of steganography. IEEE Journal on Selected Areas in Communications (J-SAC),Special Issue on Copyright and Privacy Protection, 16:474–481, 1998.