EFFICIENT METHOD FOR HIDING DATA BY PIXEL INTENSITY

M.Shobana[#1] , R.Manikandan[*2]
[#1]Department School of Computing, SASTRA University, Thanjavur,TamilNadu, India.
[*2]Senior Asst Prof, School of Computing, SASTRA University, Thanjavur,TamilNadu India.
[1] divyashobana.m@gmail.com
[2]manikandan75@core.sastra.edu

***ABSTRACT*- Data communication substructure has become more universal that there is absolutely no favoritism between different types of data in the carry plane of communication with each and every one skilled to carry it through the public data networks. Steganography technique is used to hide or embed data into an image or audio or video. Here the cover object used is an image. In the existing method for hiding and extraction of information from the given image three kinds of algorithm are used, based on its data and index channel of an image. In the proposed system, three kinds of hiding technique are implemented with some modifications in the logic level. Third algorithm is designed using color channels, based on its intensity. This technique would boost up the number of bits embedding in the image. The accomplishment of all the three algorithms are analyzed and the efficient one is taken into consideration while implementing in FPGA.**

Keywords: Steganography, Index planes, data planes.

I.INTRODUCTION

To avoid hacking the data which is transmitted between the two entities we go for secure communication. Secure communication is act of transacting the information without the interruption of the attackers. Other than direct communication with no possible observer, it is possibly safe to say that no communication is definite secure in this sense, although practical hindrance such as regulation, resources, methodical issues (interception and encryption), and the absolute volume of communication serve to limit observation. Some methods used to establish the secure communication is mentioned as (a)Encryption (b)Steganography (c)Identity based network (d) Anonymized networks (e) Anonymous communication devices

In this above specified category, the steganography has many advantages compared to others and it is plausible deniability .The aim of steganography help us to provide a covert communication path between sender and receiver in such a way that nobody can detect its existence; that is hacker should not gain any knowledge about cover object through naked eyes. Phase involved while designing the stego algorithm (i.e.) a undisclosed message is embedded and it is extracted using stego-algorithms. During the embedding progression, by altering some portion of cover medium the unrevealed message is inserted into it. This embedding technique is further classified into *spatial* and *frequency* domains. In the extraction progression the hidden message from the medium is recovered. In steganography many cover mediums are used mostly images. The reason behind it is huge redundancy and ease embedding of data. The effigy used for hiding in the first phase is labeled as cover image. The resulted image with hidden message is defined as stego image .Both cover image and stego image should has high resemblance

II.EXISTING METHOD

In this approach the color image is used as the cover object. Color image is divided into red plane, green plane, blue planes. There are two channels namely data channel and index channel. The data channel will holds the data (i.e. message bits).Based on the two LSB of the index channel, the data channel will be selected, if LSB is ‘00’ then no embedding will take place l, if it is ‘01’ then embedding of data will be in data channel2 and if it is ‘10’ then embedding of data will be in data channel1and if it is ‘11’ embedding will be on both data planes. In this way the data channel is get selected by using embedding process.

In related works they proposed three mechanisms for selecting the above two specified channels. In first method they defined red as the index channel. Green and blue act as the data channel in which data is embedded. In second method, User will define index channel the rest two channel play as the data channel. In third method, the index channel is assigned in a cyclic manner [1].

III.PROPOSED METHOD

The entire cover image will be split into red, green and blue plane. In this paper, we have proposed three new mechanisms for selecting the data and index planes, In order to maximize the embedding bits in the cover medium. There are two plane namely data plane and index plane. The data plane will holds the message in terms of bits. The index plane is used to indicate which plane should used to hold the message bits.

3-bit based random image steganography

In this method, the index channel is selected by using the all combination of three bits. The three bits value is used here is binary equivalent of 0,1,2,3,4,5,6 and 7 . For each pixel, a three bit value is assigned. Here the first bit indicates red plane, the second bit indicates green plane and the third bit indicates blue plane.

In first case, in these three bits, any two of the bits are common and it's different from the remaining one bit then the plane corresponding to the place of that different bit will act as the index plane and the remaining two planes are said to be data planes. In second case, all the values of the three bits are identical here red plane is act as index plane as default.

LFSR based image steganography

In this method, 3-bit LFSR will generate random bits for every pixel in the cover object. In the first case any of one bit is differ then its corresponding plane act as index plane and the other two same bits will act as the data plane. In second case all three bits are same then red plane act as the index plane.

Pixel intensity based image steganography

In this method, all the three color planes will be converted in to binary values. For each pixel in the image, the plane which has the minimum number of ones in its MSB will act as index plane and the other two color planes are considered as data planes. Compared to method 1 and method 2 in the existing work, this method will help us to embed more number of message bits in the cover medium.

After determining the index and data channel using any of the method which is specified above then follow these steps :For each index plane its two LSB is considered .If the value of the LSB is 00 or 11 then the embedding process will be on both data plane or if the value is 01 then data will hide in data plane2 alone or if the value is 10 then data will hide in data plane1 alone. The number of bits gets embed in the data plane is equal to the number of ones in its MSB of the data plane. These above steps are similar for all the three methods.

IV. PSEUDO CODE

A. 3-BIT BASED RANDOM IMAGE STEGANOGRAPHY

1) EMBEDDING METHOD

Parameters used: Covert Message (D), Cover Object(C) as inputs **,** Stego-image(I) with covert message embedded in it as output.

1. Convert secret message into binary

2. Isolate the cover object into Red, Green and Blue planes.

3. When every bit traversed in D perform the steps given below

3.1 For each bit in D, assign an three bits value of (0…7),starts from 0 increment the value by 1 until it reaches 7 ,if it reach again go back to 0 and repeat increment

3.1.1 If one of the three bits is 1 and the other two bits is 0 then according to the position of the bit one index plane and two data plane is selected

-if 1 is in first bit position then Red plane act as the index plane

-if 1 is in second bit position then Green plane act as the index plane

-if 1 is in third bit position then Blue plane act as the index plane

3 .2 .2 If one of the three bits is 0 and the other two bits is 1 then according to position of the bit one index plane and two data plane is selected

-if 0 is in first bit position then Red plane act as the index plane

-if 0 is in second bit position then Green plane act as the index plane

-if 0 is in third bit position then Blue plane act as the index plane

3.2 If it is 000 or 111 value then Red plane is selected as the default index plane

4. For every pixel traversed in Index plane perform the steps given below

-let a[0] = present pixel's LSB in Index plane

-let a[1] = present pixel's next LSB in Index plane

4.1 if a=01 then

g=1's count in dataplane2 (MSB)

Hide g-bits of message in the dataplane2

Else if a=10 then

g= 1's count in dataplane1 (MSB)

Hide g-bits of message in the dataplane1
Else
Let g1=1's count in dataplane1 (MSB)
g2= 1's count in dataplane2 (MSB)
Hide g1 bits and g2 bits of message in data plane1 and data plane 2 respectively
-If all secret data is embedded then
Go to step 5
Else
Go to step 4
5. Save the resulting stego Image

2) EXTRACTION METHOD

Parameters used: Stego Image (I), key (k) as input and Covert Message (D) as output.
1. Stego image I is splitted into Red, Green and Blue Planes.
2. Message size is given as the key (k)
3. Perform the step 3 which is given in the embedding side for k times to get index and data planes
4. For every pixel traversed in Index plane perform the steps given below
-let a[0] = present pixel's LSB in Index plane
-let a[1] = present pixel's next LSB in Index plane
4.1. If a = 01 then
Let g =1's count in dataplane2 (MSB)
Extract g-bits from present pixel of data plane2
Else if a = 10 then
Let g = 1's count in dataplane1 (MSB)
Extract g-bits from present pixel of data plane1
Else
Let g1 = 1's count in dataplane1 (MSB)
g2= 1's count in dataplane2 (MSB)
Extract g1-bits and g2-bits from current pixel of data plane1 and dataplane2 respectively
5. Save the result as Secret Data (D)

B. LFSR BASED IMAGE STEGANOGRAPHY

1) EMBEDDING METHOD

Parameters used: Covert Message (D), Cover Object(C) as inputs **,** Stego image(I) with covert message embedded in it as output.
1. Convert secret message into binary
2. Isolate the cover object into Red, Green and Blue planes.
3. Initialize the 3bit LFSR
4. Generate 3-bit value of LFSR for the pixels present in cover image
5. On the basis of LFSR value index and data plane is selected
6. For every pixel traversed in Index plane perform the steps given below
-let a[0] = present pixel's LSB in Index plane
-let a[1] = present pixel's next LSB in Index plane
6.1 if a=01 then
g= 1's count in dataplane 2(MSB)
Hide g - bits of message in the dataplane2
Else if a=10 then
g= 1's count in dataplane1(MSB)
Hide g-bits of message in the dataplane1
Else

Let g1=no of 1 in MSB of dataplane1
g2= no of 1 in MSB of dataplane2
Embed g1 bits and g2 bits of message in data plane1 and data plane 2 respectively
-If all secret data is embedded then
Goto step 7
Else
Goto step 4
7. Save the resulting stego Image

2) EXTRACTION METHOD

Parameters used : Stego Image(I), key (k) as input and Covert Message (D) as output.

1. Stego image I is splitted into Red, Green and Blue Planes.
2. Message size is given as the key (k)
3. Perform the step 3 and step 4 which is given in the embedding side for g times to get index and data planes
4. For every pixel traversed in Index plane perform the steps given below
-let a[0] = present pixel's LSB in Index plane
-let a[1] = present pixel's next LSB in Index plane

4.1. If a = 01 then
Let g =1's count in dataplane2(MSB)
Extract g-bits from present pixel of data plane2
Else if a = 10 then
Let g = 1's count in dataplane1(MSB)
Extract g-bits from present pixel of data plane1
Else
Let g1 = 1's count in dataplane1(MSB)
g2= 1's count in dataplane2(MSB)
Extract g1-bits and g2-bits from current pixel of dataplane1 and dataplane2 respectively
5. Save the result as Secret Data (D)

C. PIXEL INTENSITY BASED IMAGE STEGANOGRAPHY

1.EMBEDDING METHOD

Parameters used: Covert Message (D), Cover Object(C) as inputs **,** Stego image(I) with covert message embedded in it as output.

1. The secret message is converted into binary
2. The cover image is splitted into Red, Green and Blue
3. Consider the plane which has minimum number of 1 in the MSB as index plane
4.For every pixel traversed in Index plane perform the steps given below
-let a[0] = present pixel's LSB in Index plane
-let a[1] = present pixel's next LSB in Index plane

4.1 if a=01 then
g=1's count in dataplane2(MSB)
Hide g-bits of message in the dataplane2
Else if a=10 then
g= 1's count in dataplane1(MSB)
Hide g-bits of message in the dataplane1
Else
Let g1=1's count in dataplane1(MSB)
g2= 1's count in dataplane2(MSB)
Hide g1 bits and g2 bits of message in data plane1 and data plane 2 respectively
-If all covert message is embedded then

Goto step 5

Else

Goto step 4

5.Save the resulting stego Image

2) EXTRACTION METHOD

Parameters used: Stego Image(I) as input and Covert Message (D) as output

1. Stego image I is splitted into Red, Green and Blue Planes.
2. Message size is given as the key (k)
3. Perform the step 3 which is given in the embedding side for k times to get index and data planes
4. For every pixel traversed in Index plane perform the steps given below

-let a[0] = present pixel's LSB in Index plane

-let a[1] = present pixel's next LSB in Index plane

4.1. If a = 01 then

Let g =1's count in dataplane2(MSB)

Extract g-bits from present pixel of data plane2

Else if a = 10 then

Let g = 1's count in dataplane1(MSB)

Extract g-bits from present pixel of data plane1

Else

Let g1 = 1's count in dataplane1(MSB)

g2= 1's count in dataplane2(MSB)

Extract g1-bits and g2-bits from current pixel of data plane1 and dataplane2 respectively

5. Save the result as Secret Data (D)

V.RESULTS AND DISCUSSION

Here we took 256x256 images as cover medium and the PSNR and MSE values are calculated to evaluate the efficiency of the above three algorithms. The value of PSNR and MSE is calculated using the following equations

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

Where R is the maximum fluctuation in the stegoimage

TABLE I
3-BIT BASED RANDOM IMAGE STEGANOGRAPHY (METHOD 1)

Cover image	**Plane1**		**Plane2**		**Plane3**		**Bits per pixel(BPP)**			**Maximum embedding capacity**
	MSE	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**	**R**	**G**	**B**	
Lena	1.2968	47.0020	1.0659	47.8538	0.7506	49.3767	2	0.654	0.120	163040
Gandhi	2.0025	45.1151	1.5586	46.2034	1.2027	47.3292	1.83	0.55	0.50	215496
Baboon	1.0533	47.9053	1.0024	48.1205	0.9901	48.1740	1.80	1.600	1.233	197328
Temple	0.6652	49.9011	0.7265	49.5187	0.9093	48.5438	0.75	1	2.25	198768

TABLE II
LFSR BASED IMAGE STEGANOGRAPHY (METHOD 2)

Cover image	Plane1		Plane2		Plane3		Bits per pixel(BPP)			Maximum embedding capacity
	MSE	PSNR	MSE	PSNR	MSE	PSNR	R	G	B	
Lena	1.999	45.1227	1.203	47.3276	0.9592	48.3112	3.20	2.198	2.400	187672
Gandhi	2.0025	44.6091	1.7748	45.6394	1.4875	46.4063	3.56	3.125	2.890	230256
Baboon	1.2928	47.0156	1.1414	47.5566	1.2382	47.2030	2.66	0.666	0.666	205656
Temple	0.7337	49.4756	0.8403	48.8866	1.1987	47.3437	0.72	0.856	1.236	216480

TABLE III
5.3 PIXEL INTENSITY BASED IMAGE STEGANOGRAPHY (METHOD 3)

Cover image	Plane 1		Plane2		Plane3		Bits per pixel(BPP)			Maximum embedding capacity
	MSE	PSNR	MSE	PSNR	MSE	PSNR	R	G	B	
Lena	1.5490	46.2303	0.970	48.2632	0.7024	49.6649	1	0.643	0.637	165656
Gandhi	2.3793	44.3663	1.4753	46.4421	1.1489	47.5279	1.1528	1	1.1428	227304
Baboon	1.1626	44.3663	1.4753	46.4421	1.1489	47.5279	2	1	1	199800
Temple	0.7714	49.2581	0.6909	49.7363	0.8480	48.8467	1.632	0.333	2	200200

Fig1. Original image

Fig2. 3-BIT BASED RANDOM IMAGE STEGANOGRAPHY (Stegoimages)

Fig3. LFSR BASED IMAGE STEGANOGRAPHY (Stegoimages)

Fig4. PIXEL INTENSITY BASED IMAGE STEGANOGRAPHY (Stegoimages)

6. CONCLUSION:

Thus the amount of embedding strength in the cover object is improved when compare to the existing method. Where there is high intensity in a pixel, embedding bits at that particular pixel is more thus if a high pixel intensity image is used as the cover image the embedding of bits is increased. In this way maximum number of hiding capacity is enhanced. In this obscuring algorithm secret key is used thus increase the security of the secret data. Thus this method maintains obscurity of data.

REFERENCES

[1] Amirtharajan R.; Mahalakshmi, V.; Sridharan, N.; Chandrasekar, M.; Rayappan, J.B. "Modulation of hiding intensity by channel intensity - Stego by pixel commando", International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012

[2] Rengarajan Amirtharajan,Rambhatla Rambhatla Subrahmanyam, Pakalapati J S Prabhakar, R Kavitha and John Bosco Balaguru Rayappan, "MSB over hides LSB - A dark communication with integrity" Paper presented at the 20 II 5thIEEE International Conference on Internet Multimedia Services Architecture and Applications, IMSAA20 I 1. Dec 12-13. Banglore

[3] R.Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaaq K and John Bosco Balaguru Rayappan "Colour Guided Colour Image Steganography ", Universal Journal of Computer Science and Engineering Technology 1 (1), 16-23, Oct. 2010. © 2010 UniCSE, ISSN: 2219-2158.

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

[5] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods Signal Processing" 90, 2010,pp. 727752.

[6] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding " IBM Syst. 1. 35 (3&4) ,1996, 313-336.