Image Steganography Built on Pixel Value Difference in Spatial Domain using Range Table

B. Reddaiah, B. J. Job Karuna Sagar, B. Susheel Kumar, G. Sarvani, A. Sneha sai

Abstract: ***With the increase of digital transactions, providing security for the network and its devices is a big challenge today. Sensitive information that has more value in the network is to be protected from unauthorized users in accessing it. Various algorithms are being developed to provide security services for the data. In this paper security is provided by using pixel value differencing technique. Valuable data is embedded in each of the component of color like red, blue and green of a pixel in a color image. In addition to that in providing additional security pixel value has been updated conditionally, that would be more complex to trace the incremented or decremented bits in a pixel of the stegoimage. From this experiment the proposed method provides better visual quality of stego image. This proposed algorithm is suitable for small business applications where small size data is important and threats are more common.***

Keywords: Security services, pixel, image, pixel value difference, Encryption, Decryption.

I. INTRODUCTION

Techniques to provide security for information started increasing in many applications with digital transactions. The outcome is that people can purchase books, watch movies, contact other places very easily, purchase goods, etc [10].This increase is with the innovation and wide spread of internet technology and it has turned into the most significant event in current world history [5]. With this connectivity one can get the related information that belongs to their filed with less difficulty [9]. As data is in digital form that helps to exchange easily through internet and duplication of data is very much possible protecting the rights of the owner is becoming difficult. The corresponding owners of the data are with thought that they require new technologies that are promising to safe guard their rights [6], [7], [8]. In earlier days security was provided by encrypting the traffic and that is not sufficient to protect the network and data. In the recent past with the rapid growth in software programming on internet technologies a lot of work is going on to hide information in different information [11].

Since then various techniques were developed in protecting the data from unauthorized access from accessing information without the owner permission [18], [19]. The most widely used and strong techniques are cryptography and steganography [12] [13]. Cryptography is the one that encrypts the secret information and transforms into other form by using secret key that can be decrypted with the same secret only. Even though unauthorized persons can access the encrypted form, the information cannot be understood or it is difficult to read it [14], [15], [16] [12]. Steganography is another science in providing security that hides the information and that cannot appear to users [17].

A. Steganography

Cryptography hides with the help of certain algorithms that scrambles the secret message that is to be transmitted whereas steganography hides the secret message and that cannot be seen. Every steganography algorithms that is to be developed has to satisfy three goals like security, capacity and robustness. Figure 1 illustrates the general seganograhic system that hides the data in a cover image and the resultant image is called as stego image. This type of communication is a secret communication that provides more security and gained significance in several different areas.

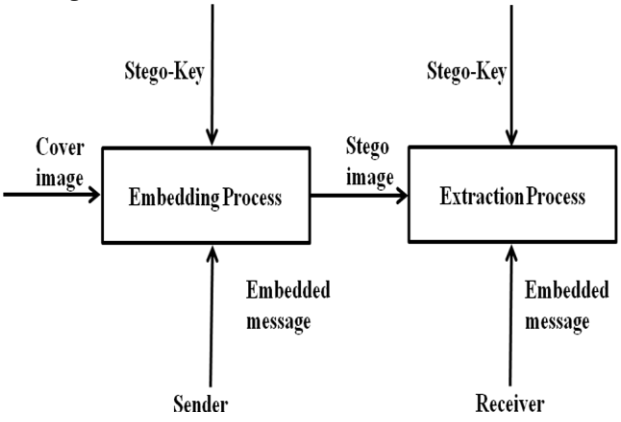

Fig. 1. General framework of steganography

The basic concept of steganographic system is that the presence of data cannot be intercepted unless its existence is exposed. Steganography concentrates on making alterations to host file in a way that is both unseen and unnoticeable. With a success ratio about more than 50 percent in steganographic algorithms, it indicates that the persons cannot conclude about presence of data within the image. As human eye cannot notice the presence of data withinthe image then it is up to the computer to find the variations and authenticate the presence of data embedded.

Revised Manuscript Received on February 05, 2020.

Reddaiah Buduri*, Yogi Vemana University, Kadapa, Andhra Pradesh, India. Email: b.reddaiah@yogivemanauniversity .ac.in

Job Karuna Sagar B J, Yogi Vemana University, Kadapa, India. Email: jksagar2003@yahoo.com

Susheel Kumar Bodi, Yogi Vemana University, Kadapa, India. Email: bjayakarunya@gmail.com

G. Sarvani, Sri Vivekananda Degree & P.G College for Women, Kadapa, India. Email: tanu8368@gmail.com

A. Sneha Sai, Sri Vivekananda Degree & P.G College for Women, Kadapa, India. Email: sunnyammuri123@gmail.com

II. BACKGRUND STUDY

To hide data a technique along with genetic algorithm was developed by Wang et al. This technique is to increase the quality of the stego image [2]. Chang et al. developed a well-organized active programming approach to decrease the computational time [3]. Chan and Cheng projected a method that embeds data using simple LSB substitution [4]. This method follows optimal pixel adjustment process. A new scheme was developed to hide huge quantity of data with good quality by Wu and Tsai. Here in this proposal stego-image pixel value-differencing method was used [1].

III. LITERATURE SURVEY

The word steganography is the combination of two Greek words Stegano refers as sealed and Graphy refers to writing and with a meaning of secret writing. This science is extremely old one that embeds secret information in other data. This is carried out by using certain rules and techniques. With this type of embedding unauthorized users cannot see or identify the hidden information. Through in steganography, information can be sent in a secret path but it is invisible. Figure1 demonstrates the practice of embedding data and extracting data. While protection data by means of steganograpy embedded information is not visible to others and this process does not disgrace the quality of original information.

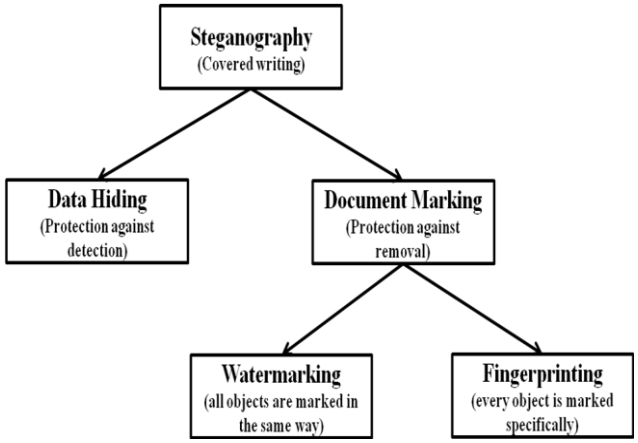

Fig. 2. Taxonomy of steganography

Steganographic algorithms are generally divided into two categories. They are Spatial Domain steganography techniques and Transform Domain steganography techniques. The taxonomy of steganography is shown in figure 2.

A. Spatial Domain Steganography Techniques

This work is based on Spatial Domain Steganography. The spatial technique utilizes the gray level of pixel and their color standards straightly for embedding the secret bits. This technique has simple methods for embedding and extracting in terms of complexity. The main advantage of these techniques is the quantity of preservative noise that sneaks into the image. This reliably have an effect on peak signal to noise ratio and statistical properties of an image. In addition to that these algorithms are mainly useful for lossless image compression methods. Common algorithm that belongs to this category is least significant bit technique. In this substitution technique, least significant bit of binary sign of grey level pixel is used to indicate message bit.

B. Transform Domain Steganography Technique

Transform domain techniques generally encodes the message bits in transform domain coefficients of image. Embedding the content in the transform domain is extensively used for watermarking. These techniques are generally applicable to watermarking aspect of data hiding to its robust property. This technique has high embedding and extraction complexity.

IV. PROPOSED SYSTEM

Each pixel in cover image is by the composition of RGB colors. The value of each pixel is 24 bits, where 8 bits belongs to red, 8 to green and 8 for blue as shown in figure 3. In this work, all the three colors are made useful to hide data within image. Every part of each color from first two adjacent pixel of a block has been separated as shown in figure 3.

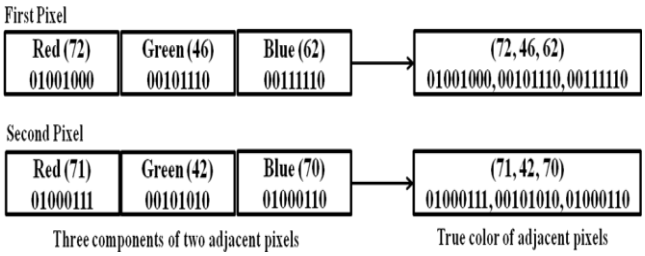

Fig. 3. Components of adjacent pixels

The difference between two pixels of same color is calculated as d_i. For the difference values optimal range for each color is calculated. The optimal range is processed by using range table as shown in figure 4. This is to find out the numbers of secret bits to embed in cover image. Throughout this work Pixel Value Difference (PVD) technique is applied to hide secret message in cover image.

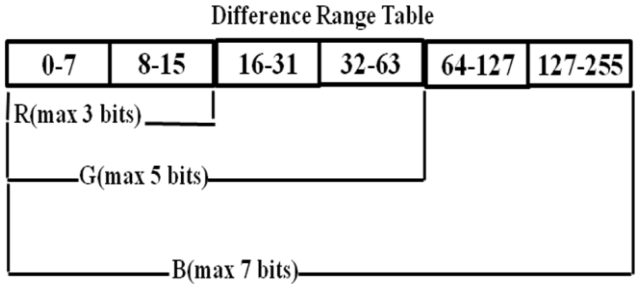

Fig. 4. Components of adjacent pixels

To provide more security to embedded data, LSB value of each color in first pixel of block 1 is considered.

Pixel 1	Pixel 2
R-01000010(66)	R-01000100(68)
G-00101111(47)	G-00100101(42)
B-01000101(69)	B-01001000(72)

If it is 0 then the corresponding decimal value in second pixel of the same block is increment by 1. If it is 1 then it is decremented by 1. The change in pixel 2 values is shown in the example below. The resultant pixels form stego image.

Pixel 2
R-01000101(69)
G-00101001(41)
B-01000111(71)

A. Framework for Encryption

Embedding and extraction of data by using new technique is shown in figure 5 and 6.

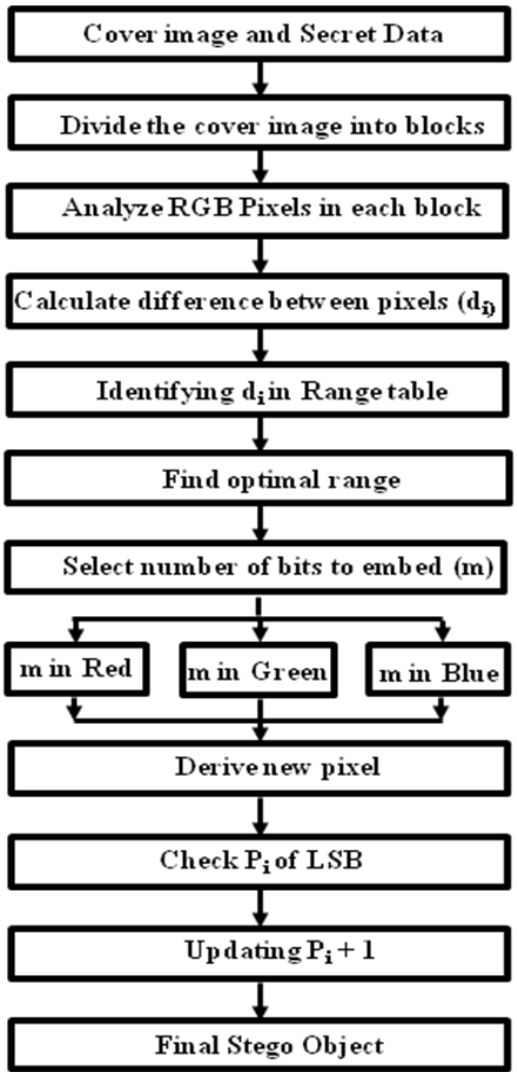

Fig. 5. Block Diagram of Encryption Process

B. Encryption Algorithm

Step 1: Select cover image to hide secret data
Step 2: Select Pain text to hide inside cover image and convert it into binary form
Step 3: In a block consider first two adjacent pixels of cover image for embedding
Step 4: Separate the colors in each pixel into red, green, and blue of each block. Convert each color value into binary form
Step 5: Compute the difference 'd_i' between the pixels of P_i and P_{i+1}
where $d_i = |P_i - P_{i+1}|$
Step 6: Calculate the range 'R_i' for 'd_i' by using range table
Step 7: Find the optimal range for 'R_i'for each color,
where optimal range for $R_i = \min(U_i - d_i)$
Step 8: Compute 'm', the number of bits of plain text to hide in cover image for each color,
where $m = \log_2 (U_i - L_i)$
Step 9: For each color read 'm' bits and embed the bits in the P_i, P_{i+1} of the block
where P_i belongs to first pixel and
P_{i+1} belongs to second pixel of a block
Step 10: Calculate the values of new pixels denoted as p^1_i, p^1_{i+1}
Step 11: If LSB in $P^1_i = 0$ then increment P^1_{i+1} by 1
Or If LSB in $P^1_i = 1$ then decrement P^1_{i+1} by 1
Step 12: Construct image from the pixels P^1_i, P^1_{i+1}…, P^1_{i+n}
Step 13: The resultant image is the stego object with secret text embedded

C. Framework for Decryption

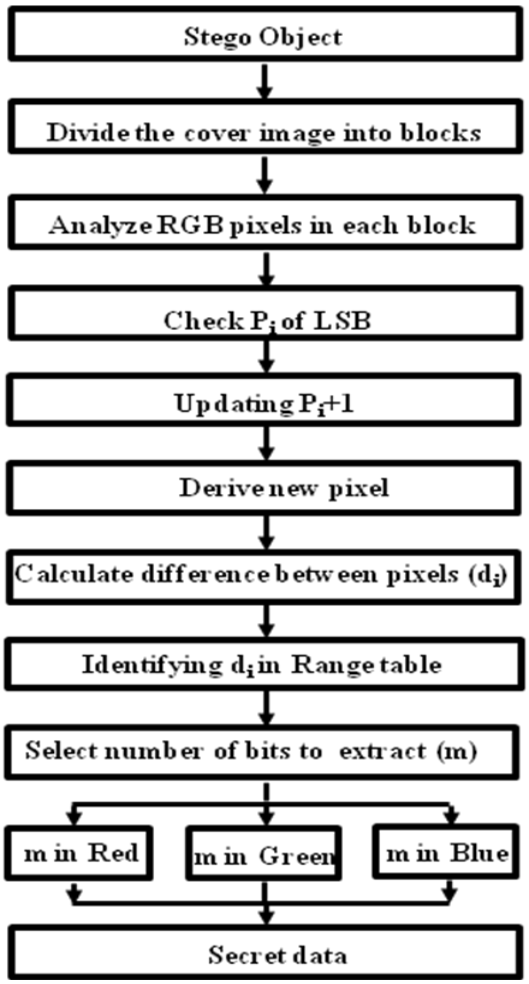

Fig. 6. Block Diagram of Encryption Process

D. Decryption Algorithm

STEP1: Read stego object
STEP2: Construct block considering two adjacent pixels of Stego object
STEP3: Separate the colors red, green, and blue for each pixel in every block
STEP4: Perform reverse operation to the pixels in each block. If LSB in $P^1_i = 0$ then decrement P^1_{i+1} by 1, Or If LSB in $P^1_i = 1$ then increment P^1_{i+1} by 1
STEP5: Calculate the difference 'di'
STEP6: Calculate 'R_i' the appropriate range for the difference 'd_i'
STEP7: Find 'm' the number of bits to be extracted
STEP8: Extract 'm' bits from the image
STEP9: The extracted bits are the bits of secret Data

V. RESULTS

A. Results of Embedding

Results of embedding by using cover image and secret data 'LAST' are tabulated in Table I, II and III. Figure 7 is the cover image that is used in hiding data and figure 8 is the object that contains data in it.

Table –I: Results of Embedding process

Cover Image	Block Number	Pixel Number	Color Separation	Pixel value	Binary Form	Secret data	Binary form
Fig. 7 COVER IMAGE	Block-1	P1(P_i)	R	72	01001000	L	01001100
			G	46	00101110		
			B	62	00111110		
		P2(P_{i+1})	R	71	01000111	A	01000001
			G	42	00101010		
			B	70	01000110		
	Block-2	P3(P_i)	R	71	01000111	S	01010011
			G	44	00101100		
			B	67	01000011		
		P4(P_{i+1})	R	70	01000110	T	01010100
			G	43	00101011		
			B	72	01001000		

Table-II: Results of Embedding process continued

Calculate Difference $d_i=\|p_i-p_{i+1}\|$	Identifying 'd_i' in Range table	Ri= min(Ui-di)	Optimal Range	No., of bits to embed $m=\log_2(U_i-L_i)$
R=1	0-7	6	0-7	R=3
G=4	0-7	3	0-7	G=3
B=8	8-15	7	0-7	B=3
R=1	0-7	6	0-7	R=3
G=1	0-7	6	0-7	G=3
B=5	0-7	2	0-7	B=3

Table-III: Results of Embedding process continued

Embedded Pixels			Deriving New pixel	Check LSB of P_i	Updating P_{i+1}	Stego Object		
Pixel Number	Color Separation	Binary form				Color value	Pixel No	Fig. 8
P1(P_i)	R	01001010	74	R = 0 G = 0 B = 0		R=74	P1	STEGO OBJECT
	G	00101100	44			G=44		
	B	00111000	56			B=56		
P2(P_{i+1})	R	01000011	67		67+1=68	R=68	P2	
	G	00101010	42		42+1=43	G=43		
	B	01000101	69		69+1=70	B=70		
P3(P_i)	R	01000010	66	R = 0 G = 1 B = 1		R=66	P3	
	G	00101111	47			G=47		
	B	01000101	69			B=69		
P4(P_{i+1})	R	01000100	68		68+1=69	R=69	P4	
	G	00101010	42		42-1=41	G=41		
	B	01001000	72		72-1=71	B=71		

B. Results of Extraction

Results of extraction are shown in Table IV and in Table V.

Table-IV: Results of Extraction process

Stego Object				Check LSB of P_i	Updating P_{i+1}	Deriving New Pixel	
Pixel Number	Color Separation	Decimal value	Binary form			Color value	Pixel No
P1(P_i)	R	74	01001010	R = 0 G = 0 B = 0		R=74	P1
	G	44	00101100			G=44	
	B	56	00111000			B=56	
P2(P_{i+1})	R	68	01000100		68-1=67	R=67	P2
	G	43	00101011		43-1=42	G=42	
	B	70	01000110		70-1=69	B=69	
P3(P_i)	R	66	01000010	R = 0 G = 1 B = 1		R=66	P3
	G	47	00101111			G=47	
	B	69	01000101			B=69	

$P4(P_{i+1})$	R	69	01000101		69-1=68 41+1=42 71+1=72	R=68	P4
	G	41	00101001			G=42	
	B	71	01000111			B=72	

Table-V: Results of Extraction process continued

Difference calculation $di=\|p_i-p_{i+1}\|$	Identifying d_i in Range table	Select No of Bits to Extract $m=\log_2(U_i-L_i)$	Secret Data			
			Block No	Pixel No	Binary form	Original Data
R=7	0-7	3	Block-1	$P1(P_i)$	01001100 01000001	L
G=2	0-7	3				
B=13	8-15	3		$P2(P_{i+1})$		A
R=2	0-7	3	Block-2	$P3(P_i)$	01010011 01010100	S
G=5	0-7	3				
B=3	0-7	3		$P4(P_{i+1})$		T

Fig. 7. Cover Image

Fig. 8. Stego Object

VI. CONCLUSION

This work started with the discussion of different steganographic method that is used for hiding data by using pixel value differencing in colour images. Here in this work original PVD method is used. The range table is used to find the optimal range and to find the number of bits that are to be embedded. Along with PVD after embedding in pixels the value of next pixel is either incremented or decremented based on condition discussed. This work is on color images and it provides better security than original PVD that is used in grey scale images. This new technique also provides better quality of resultant stego object in terms of visual effect. At other end while extracting the secret data this new technique extracts data efficiently. While extracting original cover image is not used.

REFERENCES

1. J.K. Mandal, Debashis Das, "Steganography Using Adaptive Pixel Value Differencing (APVD) for Gray mages through Exclusion of Underflow/Overfolw", Computer Science & Information Series, ISBN: 978-1-921987-03-8, pp. 93-102, 2012..
2. R.Z. ang, C.F. Lin, J.C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm", Patteren Recognition Vol. 147, No. 3, pp. 288-294, 2001.
3. C.C. Chang, J.Y. Hsiao, C.S. Chan, "Finding optimal least-significant bit substitution in image hiding by dynamic programming stratergy", Pattern Recognition Vol. 36, Issue 7, pp. 1583-1595, 2003.
4. C.K. Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution", pattern recognition Vol. 37, Issue 3, pp. 469-474, 2004.
5. Afrakhteh. M, Ibrahim. S. (2010, 25-27 June 2010). Adaptive steganography Scheme using more surrounding pixels. Paper presented at the Computer Design and Applications (ICCDA), 2010 Intenational Conference.
6. Al-Hunaity, M.F, et al. (2007). Colored digital image watermarking using the wavelet technique. [Article]. American Journal of Applied Sciences, 4(9), 658+.
7. Alturki, F., & Mersereau, R. (2001, Apr 2001). A novel approach for increasing security and data embedding capacity in images for data hiding applications. Paper presented at the Information Technology: Coding and Computing, 2001. Proceedings. International Conference.
8. Awwad, W.F, et al. (2012). A robust method to detec hidden data from digital images. [Report]. Journal of Information Security, 3(2), 91+.
9. Babu, K. S, et al. (2008, 19-21 Nov. 2008). Authentication of secret information in image steganography. Paper presented at the TENCON 2008 – 2008 IEEE Region 10 Conference.
10. Chang, C.-C, et al. (2010). High payload steganography mechanism using hybrid edge detector. [Report]. Expert Systems With Applications, 37(4)m 3292+.
11. Chang, C.-C, et al. (2010). A grayscale image steganography based upon discrete cosine transformation. [Technical report]. Journal of Digital Information Management, 8(2), 88+.
12. Husainy, M. A. F. A. (2009). Image steganography by mapping pixels to letters. [Report]. Journal of Computer Science, 5(1), 33+.
13. Ibrahim, B, et al. (2009). Information hiding: a generic approach. [Technical report]. Journal of Computer Science, 5(12), 933+.
14. El-Emam, N. N. (2007). Hiding a large amount of data with high security using steganography algorithm. [Article]. Journal of Computer Science, 3(4), 233+.
15. Farshchi, S. M. R., & Toosizadeh, S. (2011). High secure communication using chaotic double compression steganography technique. [Report]. International Journal of Research and Reviews in Computer Science, 527+.

16. Hedieh, S., & Jamzad, M. (2008, 8-11 July 2008). Cover selection Method Based on Similarity of Image Blocks. Paper presented at the Computer and Information Technology Workshops, 2008. CIT Workshops 2008. IEEE 8th International Conference.
17. Jin-Suk, K, et al. (2007, 7-9 Nov. 2007). Steganography using block-based adaptive threshold. Paper presented at the Computer and Information Sciences, 2007. ISCIS 2007. 22nd International symposium.
18. Neeta, D, et al. (2007, 6-6 Dec. 2006). Implementation of LSB Steganography and its Evaluation for Various Bits. Paper presented at the Digital Information Management, 2006 1st International Conference.
19. Shaohui, L, et al. (2004, 5-7 April 2004). Stegaanalysis of data hiding techniques in wavelet domain. Paper presented at the Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference.

AUTHORS PROFILE

B. Reddaiah is presently working in Department of Computer Applications, Yogivemana University. Guntur. His research areas of interest are Software Engineering, Security.

B. J. Karuna Sagar has 16 years of experience in teaching and research. His areas of interest are Network security, Hybrid routing protocols. He published papers in various journals. His core research area is Adhoc Sensor Networks.

B. Susheel Kumar 8 years of teaching and research experience. His area of research is Network Security, Image processing and Software Engineering. He published papers in both national and international journals and conferences.

G. Sarvani is pursuing M.Sc Computer Science in Sri Vivekanada Degree and P.G college for Women.

A. Sneha Sai is pursuing M.Sc Computer Science in Sri Vivekanada Degree and P.G college for Women.