A Data Conceal and Protection in Digital Image using Fuzzy Based Substitution and Affine Based Encryption

Neeraj Yogi1, Prof. Shweta Shrivastava2, Dr. Vineet Richhariya3

1M.Tech Scholar , 2Assistant Professor, 3HOD

Department of Computer Science and Engineering LNCT Bhopal

Abstract - When information travels over unsecured medium, then information security become primary issue. Information security on the internet becomes the major concern where vital information needs to be sent and concealed from the outer world. When information is private, important and vital than it needs secure medium, but internet and other transmission media is not secure enough to carry such type of information so solution to this problem can be Steganography and cryptography. Steganography and cryptography are two main technologies that are used for data security. Steganography to give a way hides information in other media and cryptography converts information into unreadable form. There are several algorithms are developed for data hiding and encryption. In this paper, we present a new method, in which provide two levels of security by image steganography and image encryption. Image steganography uses fuzzy based four-pixel differencing and altered least significant bit (LSB) substitution method and image encryption uses affine encryption. Affine transform gave edge for embedding. Firstly carrier image shuffled by affine method then n number of secret bits is embedded that get by fuzzy function. Embedded image reshuffled. There is readjustment procedure which minimizes the image changes after embedding. Proposed method raises image security as well as image capacity and quality.

Keywords—image steganography, LSB, image cryptography, affine transform, fuzzy.

I. INTRODUCTION

Today internet turned into great media to transfer and share data like audio, video, text, etc. across the globe. Information transmission over the internet is growing at a rapid rate along with some sensible data like as email, message, credit card information and corporate data, however growing data transfer have brought new risks, such as hacking and its misuse makes data security become a major concern. Many techniques developed for providing security to confidential data over the internet. Steganography and cryptography are widely used techniques to provide secure transmission. Steganography is a method for data hiding. It is a way for hiding secret data. Steganography can be divide basis of cover medium such as text, image, audio, and video [2]. Image steganography technique can be divided into two domains: spatial domain and frequency domain. In spatial domain, the secret message hides directly into the image pixels, in frequency domain, first images are transformed to frequency domain and then, the secret message hides in the transform coefficients [13]. In the last decade, many methods for data hiding in images proposed. Some of them, data hiding technique is based on the method of substituting the least significant bits (LSB) of the pixels of the cover image. Several methods have used the pixel-value differencing (PVD) technique [4,13,7]. Some methods have used the pixel-value differencing and substituting LSB [5,8,9]. Some data embedding method is based on the side match for two sided, three sided and four sided in [11].

Lotfi Zadeh has introduced this important idea in a continuous-valued logic that he called “fuzzy set theory” .fuzzy set theory define how to fuzzy logic can use various engineer application [6]. There are two common models for fuzzy inference systems named Mamdani and Sogeno models. It uses Sogeno fuzzy system to hide secret bits in each pixel. It used Four-pixel differencing and modified least significant bit (LSB) substitution with Sogeno fuzzy system [2]

Sometime steganography is not sufficient to protect data from unauthorized person. Cryptography is also another way to protect data.

Cryptography is a method for data transforming. It converts data into unreadable form. Various cryptography techniques are used for text encryption such as DES, AES, RSA and IDEA. Higher security can achieve by DES, AES, RSA and IDEA. All these methods are used for text encryption only not for image and video. Image and text data has their unique features. The available encryption algorithms are good for text data. They may not be suitable for multimedia data Encryption on image needs special requirements and thus requiring different encryption algorithms [12, 14]. Various methods for image encryption such as position permutation based algorithm, value transformation based algorithm and transformation based algorithm [15]. Many encryption methods are based on chaotic system. In this showed a new nonlinear chaotic

algorithm (NCA) which used power function and tangent function place of linear function. In this algorithm in a one-time and one password system is used. Proposed an image encryption algorithm is used it is based on a binary sequence generated from a chaotic system. It disorganized an image according to the generated binary sequence [16,17]. Some methods use position of pixels for image encryption. Shuffling the image pixel by affine transformation it relocates image pixels [1].

Image steganography technique hides data only in other medium but it is not secure enough and cryptography is not sufficient for hiding data alone and cannot protect data efficiently. Encrypted data can be easily suspected. For any eavesdropper can detect easily presence of secret data so he can try many attack on encrypted data to retrieve original information. Further enhancement in data security can use steganography. Combination of Steganography and Cryptography technique can provide higher security.

In this paper the original image without the embedded secret data is named cover image. Image with secret data embedding is named stego image. We use image encryption and image steganography. Here Fuzzy based four-pixel differencing least significant bit (LSB) substitution method for secret bit embedding and image encryption is based on Affine transformation algorithm which shuffled blocks of pixels [1].

S-shaped membership function is used to get number of bits that change in each pixel. S-shaped membership function gets four pixels difference value and generates fuzzy value that help to choose numbers of bits to be hide. The remainder of this paper is organized as follows. S-Shaped fuzzy membership function is introduced in section 2. Our proposed method is shown in section 3 and 4 section present experimental results of proposed method and comparison. Lastly conclusions are given.

II. S-SHAPED MEMBERSHIP FUNCTION

The Fuzzy Logic has eleven built-in membership function types. These eleven membership function are, built from several basic functions: piecewise linear functions, the sigmoid curve, the Gaussian distribution function and quadratic and cubic polynomial curves. In Fuzzy logic three related membership functions are the Pi, S, and Z curves, all these named because of their shape. The function smf (Fig 1) is the mirror-image function of the Z function that opens to the right.

The S-shaped membership function has two parameters t1 and t2. The shape of S-shaped membership is shown in figure 2. The membership value lies between 0 and 1. The membership value is 0 when points below t1, 1 for points above t2, and 0.5 for the midpoint between t1 and t2.

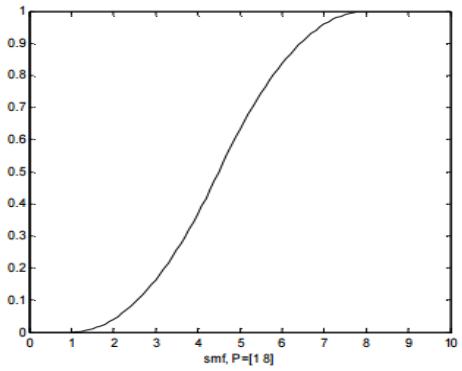

Figure 1 S-shaped membership function

This spline-based curve is a mapping on the vector d. The parameters *t1* and *t2* locate the extremes of the sloped portion of the curve, as given by [9]:

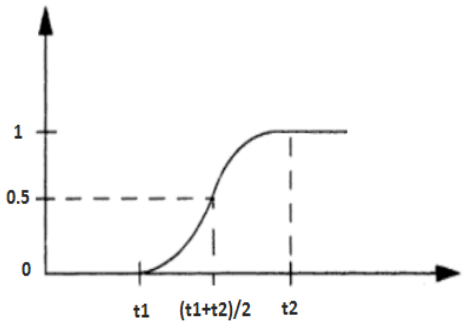

Figure 2. S-shaped membership function

Polynomial function can take be one, two, or many input and generates single output Such as function z = f(x) is a single input and single output function. Here x is input, z is output and f(x) is the function. Fuzzy function is similar function but generates fuzzy value that lies between (0, 1).

III. PROPOSED METHOD

The pixels in edge areas can endure much more changes without detectable alteration compare than the pixels in smooth areas. S-shaped membership function contains two parameters t1, and t2.

$$f(\mathrm{d};\mathrm{t1},\mathrm{t2}) = \begin{cases} 0, & \mathrm{d} \le \mathrm{t1} \\ 2\left(\frac{x-\mathrm{t1}}{\mathrm{t2}-\mathrm{t1}}\right)^2, & \mathrm{t1} \le \mathrm{d} \le \frac{\mathrm{t1}+\mathrm{t2}}{2} \\ 1-2\left(\frac{x-\mathrm{t1}}{\mathrm{t2}-\mathrm{t1}}\right)^2, & \frac{\mathrm{t1}+\mathrm{t2}}{2} \le \mathrm{d} \le \mathrm{t2} \\ 1, & \mathrm{d} \ge \mathrm{t2} \end{cases}$$

Equation 1 S-shaped membership function

Parameter t1 and t2 decides range of function here t1 and t2 are threshold value. S-shaped membership function

takes difference of four pixels d and generates fuzzy output (0, 0.5, 1).

Maximum number of bits can be hide in edge area compare then smooth area Fuzzy function determines smooth area and edge area. Fuzzy function adaptively hides messages using two levels (lower-level and higher-level), and threshold value t1 and t2 is used to partition the range of d into two levels.

1. If S-shaped membership function value (mfv) = 0 than block belongs to ‘‘smooth area” (low level). Two bit can hide in smooth area.
2. If S-shaped membership function value lie between (mfv) 0 and 1 than block belongs to ‘‘error block”.
3. If S-shaped membership function value (mfv) = 1 than block belongs to ‘‘edge area” (high level). Four bit can hide in edge area.

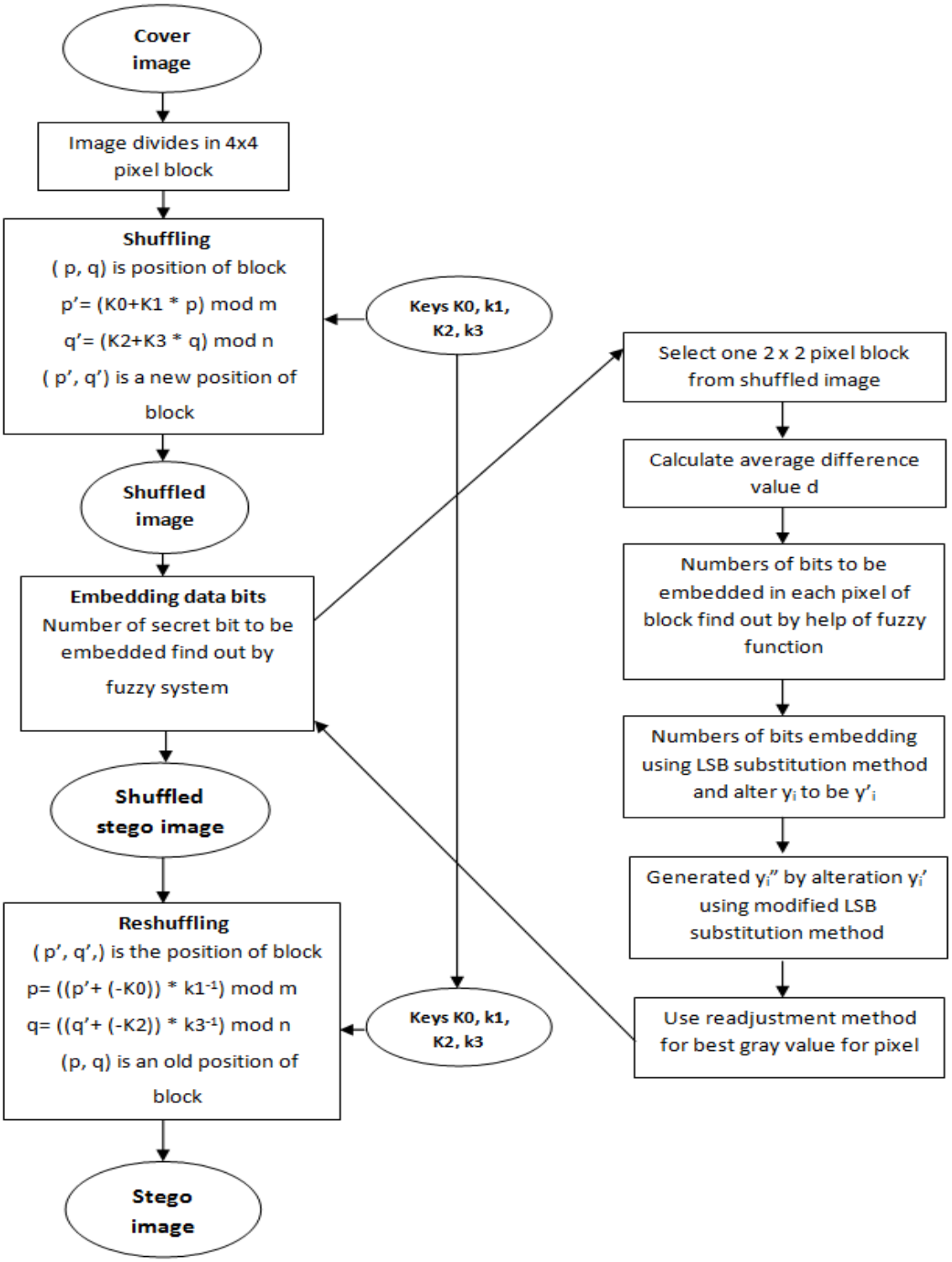

Figure 3 flow chart of proposed method

A. The Data Embedding Algorithm

Proposed method can divide in three phase.

1. Shuffling (Encryption)
2. Substitution (Steganography)
3. Reshuffling (Decryption)

Shuffling (Encryption)

1. Image is divided into 4x4 pixel blocks.
2. Generate new position of pixels. (p, q) is current position of block.

p'= (K0+K1 * p) mod m

q'= (K2+K3 * q) mod n

(p', q') is a new position of block (Where K0, K1, K2, K3 are the keys of 8 bits.)

Substitution (Steganography)

Embedding algorithm:

Every one of pixels of the cover image can have value between 0 to 255 ranges. The cover image is split into non-overlapping blocks of 2x2 pixels block. In each block contains four neighboring pixels Pi,j, Pi,j+1, Pi+1,j, and Pi+1,j+1 pixels and each pixels have gray values of y1, y2, y3 and y4 respectively. The procedure for embedding in cover image is as follows.

1: Calculate the average difference value d of four pixels, where y_{min} is given by.

$$y_{min} = (y1, y2, y3, y4) \quad (1)$$

$$d = \frac{1}{3} \sum_{i=1}^{4} (y_i - y_{min}) \quad (2)$$

2: Find the number of bits to be hidden in the pixels of block using S-shaped membership function.

3: Change the value *yi* to *ýi* by the n bit standard LSB (least signifcant bit) substitution method ($1 \le i \le 4$).

4: Generate *y"i* by changing y'_i using the *n* bit modified LSB

(least significant bit) substitution method ($1 \le i \le 4$).

5: Readjustment procedure for minimizes the perceptual alterations.

Reshuffling (Decryption)

1. Image is divided into 4x4 pixels blocks.

2. (p', q') is position of block

$p = ((p' + (-K0)) * k1^{-1}) \bmod m$

$q = ((q' + (-K2)) * k3^{-1}) \bmod n$

(p, q) is the old location block.

A. The data Extracting Algorithm

Extracting method can divide in two phase.

1. Shuffling (Encryption)
2. Extracting (Steganography)

Shuffling (Encryption)

1. Image is divided into 4x4 pixels blocks.

(p, q) is position of block

p'= (K0+K1 * p) mod m

q'= (K2+K3 * q) mod n

(p', q') is a new position of block.

Where K0, K1, K2, K3 are the keys of 8 bits.

Extracting (Steganography)

Extracting algorithm:

Extraction process does not need original image to extract hidden data from stego image. Extraction algorithm is similar like embedding algorithm. In extraction algorithm stego image divided to 2x2 pixels block which like as embedding process. In each block contains four neighboring pixels Pi,j, Pi,j+1, Pi+1,j, and Pi+1,j+1 pixels and each pixels have gray values of y1, y2, y3 and y4 respectively.

1: Calculated the average difference value d using (2).

2: By using fuzzy system to find out number bit to be extract.

3: Extract *n*-bit of secret data from the *n*-bit LSB of *ŷi* ($1 \le i \le 4$) .

Readjustment procedure:

Readjustment procedure [5] helps to reduce changes that occur after modification of bit. When number of bits embedded in pixel then some bit of its pixel change due to modification. So Readjustment procedure helps to minimize the perceptual alteration.

$\hat{y}_i = y_i'' + l \times 2^k \quad (3)$

($1 \le i \le 4$), $l \in \{0, 1, -1\}$, and search gray value of pixels ($\hat{y}1, \hat{y}2, \hat{y}3, \hat{y}4$) such that

1. d' and d belong to same level, where d'

$$d' = \frac{1}{3}\sum_{i=1}^{4}(\hat{y}_i - \hat{y}_{min}) \quad (4)$$

where $\hat{y}_{min}$= min ($\hat{y}1$, $\hat{y}2$, $\hat{y}3$, $\hat{y}4$) (5)

2. Stego image pixels block ($\hat{y}1$, $\hat{y}2$, $\hat{y}3$, $\hat{y}4$) should not belong to error block.
3. Best value of $\hat{y}i$ such like that it should be similar before and after embedding secret bit.

4. The value difference that evaluated by (6) is minimized.

$$\sum_{i=1}^{4}(\hat{y}_i - y_i)^2 \quad (6)$$

IV. EXPERIMENT RESULT

In our experiment ten gray scale images [20] is used with size 512 × 512 as cover images. Four images shown in fig .4 these images are taken from ten gray images. A sequence of secret bit is embedded into shuffled image. In our experiment cover image is shuffled with the help of following keys (k1=11, k2=13, k3=17, k4=19) and then embeds secret bits. Peak signal to noise ratio (PSNR) and capacity are evaluated. PSNR is used for the quality of the stego image. For a m x n gray scale image, the PSNR value is calculated by (7) and MSE is calculate d by (8).

$$PSNR=10\times\log_{10}\frac{255^2}{MSE} \quad (7)$$

$$MSE=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(c_{i,j}-s_{i,j})^2}{m\ x\ n} \quad (8)$$

$S_{i,j}$ and $c_{i,j}$ are the pixels of stego image and cover image, (i,j) are the coordinate of respective image.

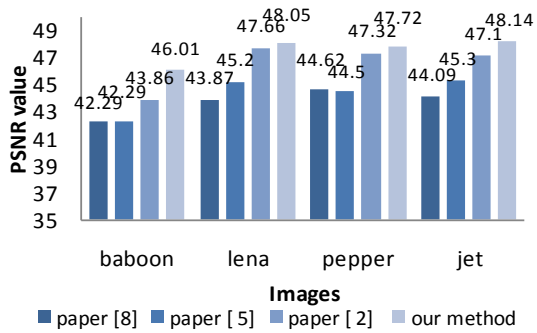

Figure 4 compression of proposed method PSNR values with other methods

The embedding capacity and PSNR values of our method are given in TABLE 1 that shown proposed method has embedding capacity and PSNR value. Proposed method has increased capacity with extra security got by affine method. Affine transform create edge area that increase embedding capacity. It detected edge area better way. We have more embedding capacity and better image quality.

Table 1 Values of the capacity for embedding data and PSNR of stego images by our method.

Cover image	Capacity/ Byte our method	PSNR/dB our method
Baboon	97,046	45.16
House	84,168	46.15
Jet	69,465	47.12
Lake	71,681	46.96
Lena	57,432	47.74
couple	70,368	46.7
Peppers	59,425	47.47
Elaine	72,111	46.53
Girl	69,622	46.79
Cameraman	62,218	47.55
average	71,353	46.81

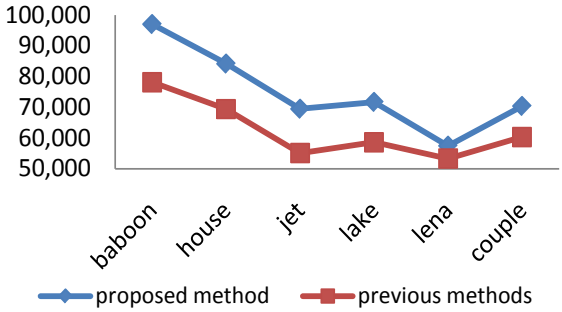

Figure 5 Capacity of proposed methods at various images with other methods

TABLE 2 compares the capacity and the PSNR values of the proposed method with three other methods. All these comparisons are shown that our method have good image quality. In this table shown that our method have good image image quality compare than three methods Yang et al. [8], Liao [5] and Majid [2] with similar capacity, our method is improved image quality.

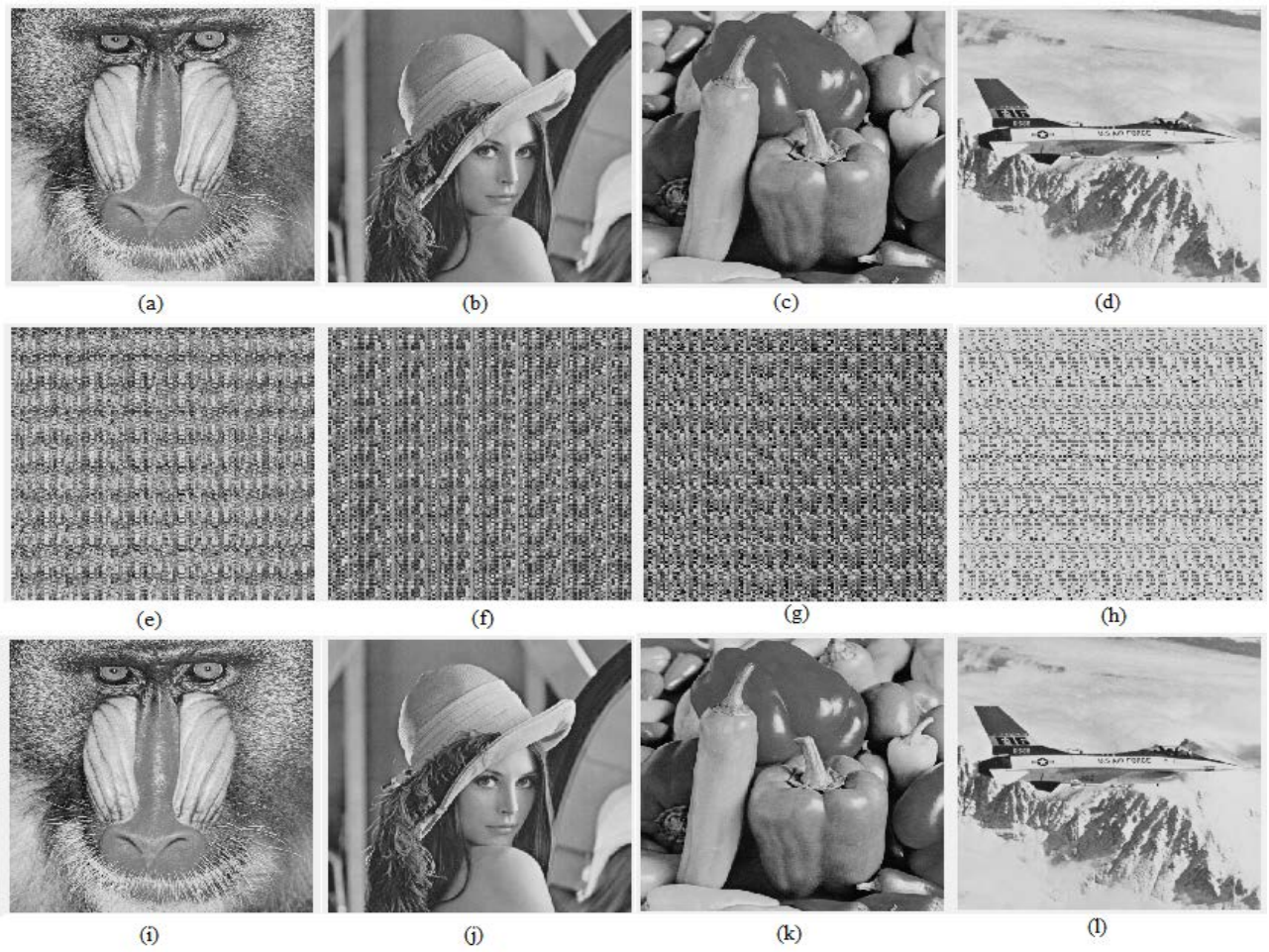

Figure 6 (a), (b), (c) and (d) are the cover images size of 512x512, (e), (f), (g) and (h) are the encrypted images produce by encryption process, and (i), (j), (k) and (l) are the stego images with hidden message.

Table 2 Comparison the PSNR values at same capacity of the proposed method with three other methods

Cover Image	Capacity Yang et al. [8], Liao [5],majid[2] and proposed method	Capacity Of proposed Method Yang et al. [8]	PSNR Of previous Method Liao [5]	PSNR Of previous Method Majid [2]	PSNR proposed method
Baboon	78,132	42.23	42.29	43.86	46.10
House	69,400	42.93	44.99	45.65	46.94
Jet	55,077	44.09	45.30	47.10	48.14
Lake	58,629	42.65	43.98	46.69	47.53
Lena	53,275	43.87	45.20	47.66	48.05
Couple	60,306	43.17	43.83	46.51	47.37
Peppers	56,096	44.62	44.50	47.32	47.72
Elaine	67,213	42.09	44.80	46.28	46.86
Girl	66,562	42.89	43.97	46.73	46.99
Cameraman	52,122	43.91	43.94	47.58	48.33
Average	61.681	43.28	44.31	46.53	47.40

V. CONCLUSION

In this paper, we proposed new image steganographic method based on fuzzy pixel value differencing and modified LSB substitution with affine transform. Image steganography and image encryption provide higher security to data. Affine transformation is used for scrambling operation that break correlation of neighboring pixels make image unidentifiable and create edge area for to increase data hiding capacity. We embedded n number

of bit to in pixels of image, n number of secret bit generated with help of fuzzy function and with the n-bit modified LSB substitution method. Readjustment procedure helps to increase image quality. Our methods have more embedding capacity and better image quality but for other methods with similar capacity, improve the stego image quality.

REFERENCES

[1] Harshit Somani, Namita Tiwari " Image Encryption using Block Shuffling and Affine Transform: A Review", International Journal of Computer Applications (0975 – 8887) Volume 95– No.19, June 2014

[2] Masume Sabokdast,Majid Mohammadi, "A fuzzy approach for data hiding in images" Fuzzy Systems (IFSC), 2013 13th Iranian confere- -nce on27- 29 Aug. 2013, pp. 1-6

[3] A. Ioannidou, S. T. Halkidis, and G. Stephanides, "A novel technique for image steganography based on high payload method and edge detection," Expert System with Applications, vol. 39, pp. 11517-11524, 2012.

[4] C. H. Yang, C. Y. Weng, H. K. Tso, and S. j. Wang, "A data hiding scheme using the varieties of pixel-value differencing in multimedia," The journal of system and software, vol. 84, pp. 669-678, 2011.

[5] X. Liao, Q. Y. Wen, and J. Zhang, "The steganogeraphic method for digital images with four-pixel differencing and modified LSB substi- -tution," J. Vis. Commun . Image R, vol. 33, pp. 1-8, 2011.

[6] T. J. Ross, fuzzy logic with engineering applications, vol. 3. Wiley, 2010, pp. 1-160

[7] C. M. Wang, N. I. Wu, C. S. Tsai , and M. S. Hwang, "A high quality steganogeraphic method with pixel-value differencing and modulus function," The journal of system and software, vol. 81, pp. 150-158, Apr.2008.

[8] C. H. Yang, C. Y. Weng, S. J. Wang and H. M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems," IEEE Trans. Information forensics and security, vol. 3, pp. 1556- 6013,2008.

[9] John yen, Reza langari "Fuzzy Logic: Intelligence, control and information" person education second edition 2007

[10] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image stegano--geraphic scheme based on pixel-value differencing and replacement LSB methods" Pro. Inst. Elect. Eng., Vis. Image Signal process. vol. 152, pp. 611-615, 2005.

[11] C. C. Chang, and H. W. Tseng, "A steganogeraphic method for digitalimages using side match ," Pattern Recognition Letters, vol. 25, pp.1431-1437, Apr. 2004.

[12] W. Stallings, Cryptography and Network Security principles and practices, 3rd ed., Pearson Education, 2003.

[13] D. C. Wu and W. H. Tsai, "A steganographic method for images By pixel-value differecing" Pattern Recognition Letters, vol. 24, pp. 1613-1626, 2003.

[14] M. V. Droogenbroech, R. Benedett, "Techniques for a selective Encryption of uncompressed and compressed images," in proceeding of Advanced Concepts for Intelligent Vision Systems, 2002, pp 9-1I.

[15] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000.

[16] J. Cheng; J.1. Guo, "A new chaotic key-based design for image encryption and decryption," The 2000 IEEE International symposium on Circuits and Systems, volA, no. 4, pp. 49 - 52, May.2000.

[17] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding – A survey," Proceedings of the IEEE, vol 87 pp. 1062-1078, 1999.

[18] Jui-Cheng Yen and J. I. Guo, "A New Chaotic Image Encryption Algorithm," Proc. 1998 National Symposium on elecommunications, pp.358-362, Dec, 1998.

[19] L. F. Turner, "Digital data security system," Patent IPN WO 89/08915,1989.

[20] "http://www.imageprocessingplace.com"