LSB- Image Steganography Algorithm Based on Evaluation Parameter using Artificial Neural Network

[1]Akansha Vishwakarma, [2]M. P. Parsai

[1]Research Scholar, [2]Professor
Dept. of E&TC Engineering
Jabalpur Engineering College, Gokalpur, Jabalpur, MP, India

***Abstract*: This paper present a literature review on LSB Steganography technique in a spatial domain to highlight their achievement on evolution parameter and their challenges. In this paper compare the embedded method in a spatial domain regarding their embedded capacity, visual quality, imperceptibility and give general procedures to evaluate these parameters.**

Keywords: LSB Steganography, ANN, Payload, Visual Quality, Imperceptibility.

I. INTRODUCTION

Steganography is a method of data hiding or covered writing in a such a way that no one know the communications is going on apart from sender and intended receiver[2] . In Steganography data must remain unchanged, it simply hide the information into file format .The file format maybe text, image ,audio or video file. Steganography is done in many way i.e. images steganography, audio Steganography and video Steganography. Steganography is a common form of hiding the information in which many message bit embedded into image and kept introduce distortions undetectable[1] . Steganography is derived from Greek word which means covered writing and its essential mean "to hide the plain sight"[2]. This technique used for many decades but with the increasing the users demand in digital world, new technologies for information hiding have become required. Steganography is a different from cryptography. In cryptography secret information is encrypted through private or public key and then transfer to the user but in Steganography data hidden through the existing methods and transfers to receiver by which attacker does not recognise that the communication is going on [2]. Image steganography is done in two domain i.e. spatial domain and transform domain. In spatial domain secret data is directly embedded into cover image .In transform domain before embedded the secret data through image first apply for Fourier transform that convert time domain into frequency domain then apply embedding process [1].

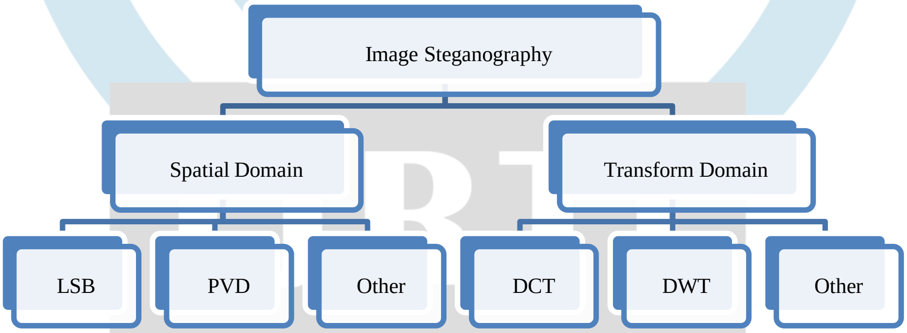

Fig. 1. Classification of Image Steganography

Here terms 'cover image' is the image used to hide the secret data.' Secret data' is the information that used to transfer indirectly. 'Stego key' is the key that must be shared with both the ends. 'Stego image' is the image in which the secret data is hidden[1].Ideally Steganography method must have high un-detectability , high embedded capacity and good visual quality[1] .In literature various type of images steganography method has been proposed to achieve these parameters to applying appropriate approach. In spatial domain image steganography is most prominent method to embedded the data because it is simple and less complex method. Spatial domain is a future classified into LSB substitution, pixels value differencing, exploding modifications directions, grey label modifications and so on but the LSB substitution method is the simplest technique for embedding secret data into cover image .In this method LSB of a cover image replace by secret data.

II. ARTIFICIAL NEURON NETWORK

The artificial neural network (ANN) is the component of artificial intelligence that having artificial neurons called processing unit which are interconnected by nodes [9]. Processing unit made up of input and output unit with back propagation rule. ANN perform two phase i.e. Training phase and Supervise phase. In training phase it recognize pattern in data through visually , textually or aurally and during supervise phase it compare its produced output to actual output by adjusting the weight of its connection between processing unit until it produce lowest possible error [9]. The neural network tress the pattern formed by secret data and selected bits from cover image and create cipher text. This cipher text is embedded into LSB of cover image followed by proposed algorithm and produce stego image [10].

III. LSB SUSTITUTION METHOD

LSB substitution method is one of the most simple and prominent method of a data heading in spatial domain. LSB substitution method replace LSB of a pixel in the cover image to the secret data and particular section of the pixels in determine by stego key[1]. In any information hiding method depend on a payload ,visual quality and security .Payload is dependant on number of the pixels in an image, if number of the pixels are more than payload is mode so we can embedded the more information into the cover image .And based on the different LSB algorithm we increased payload of an image ,visual quality and undetectability of cover image. If we increase payload by substitutions two or more LSB into pixel than the security also increase. It increase more difficulty to attack to crack the embedded information[3]. Some algorithm also used for a random embed information into pixels rather than sequentially embed information. These random pixels are scattered on everywhere throughout the cover image from a centre to edge in special domain[3] .It is easy to embedded the information without using any transform so the spatial domain LSB technique is used to embedded the data into the image and this method follow certain steps:

- Convert the secret information into binary code .
- Replace each LSBpixel of cover image into binary bit.

The reason behind to replace only LSB rather than other bit of the secret information is that the LSB contain very less or minimum information of the text data and replacing with this to cover image pixels the embedded or the stego image does create a more difficulties in compare to original image By detecting through HVS system but particular software can determine the pattern in image is being irregular[3].After applying these operations into image its visuals quality gets affected in some small quantity that is based on evaluation parameter. Many literature give a different algorithms to achieve stego-parameters based on this here we are discussing some general and easy algorithm that satisfy used demands in increasing the parameter aspect

A. ±1 LSB based algorithm

In this method the probability of a changing per pixels is reduced to ${}^{1}/_{3}{}^{rd}$ without reducing the embedded capacity [3]. Embedded capacity of information is 1bpp as result to reducing the embedded probability of a changing per pixels in some capacity of stego image corresponding to cover image. In ±1 LSB algorithm simple LSB replace with each pixels of a cover image to two message bit. In the embedded process each pixel value increased or decreased by 1, if the pixel value is even then it is incremented by one or remain unchanged and if the pixel value is odd then it is decremented by one or remain unchanged [3]. As a result every two consecutive values in histogram of a pixels value convert to same value and histogram of image will be the pair wise format i.e. POV and it is also known as ‘pair of value’ .This can be detected by chi -square stego analysis[3] .When the LSB of a cover image and secret data bit are not matched ,the pixel value is increased or decreased by one randomly that is called LSB matching.For LSB matching instead of embedding LSB sequentially, randomly LSB substitutions is performed which started from centre of cover images to edge[3] .The secret information is encrypted into bit and embedded into cover image randomly hence each bit may match to LSB of a pixel value with ⅓ probability . It reduce the probability of a changing per pixel and it offer capacity of a bit is 1bpp which is exactly same and it is considered the improvement versions of LSBMR rewards version of LSB matching .In this method stego image same as cover image that increase resistance against Stego analysis. The expansions of pixel group from 2 pixels in LSBMR to 3 LSB pixels in ⅓ probability embedding reducing probability of a changing per pixel so therefore the expenses of this probability of a changing per pixels for any level k extensions of generalised algorithms [3].It is proved that three is optimum value for the number of pixels in group.
Embedded Process:

- Cover images divided in three group of the pixels and these called embedded unit and give a secret key.
- For each embedded unit has to fetch secret bit and pixels value.
- Pixel from all three list are integrated and located in there original stego image.

This method provide high imperceptibility but it depend on secret key and having low embedded capacity.

B. Adoptive LSB substitution algorithm

Adaptive LSB substitutions method is used to obtain high payload and good visual quality of stego image. This method is based on this concept that edge area having less tolerance to change pixels value rather than the smoothen areas[4] .Many literature use edge area for embedding more information which create a minimum differences compare to original image. To avoid these degradation in image edge area as well as to achieve the better quality and high payload of a cover image, the adapter LSB substitutions method is proposed[4].

The prominent edge areas having greater variance value compare to smoothen areas so the maximum variance is in the block having maximum mean square value cause high PSNR which directly proposal to embedded capacity of Stego image [4].

The proposed method is based on a concept that this edge area can tolerate a smaller number of changes then the higher textures area and not give more change then the smoothen areas so embedded more secret data into noise non-sensitive area rather than this noise sensitive area and calculate data hiding capacity of each pixel is based on highest bit of each pixel in cover image then this adoptive number K of LSB of east pixels should remain unchanged before and after data hiding [4].
Embedded process:

- Consider cover gray scale image and secret data.
- Find highest bit of cover image to make residual image.
- Calculate adopted number K of LSB of each pixels in cover image based on residual image.
- Generate pseudo random sequence with 0 and 1 by secret key .
- Perform of elemental wise xor operation with the secret data and pseudo random sequence .

- last bit of a pixels of a cover image and K^{th} binary secret data bit read to transform a secret data one by one as denoted binary data and convert into decimal value .
- Hide K binary secret data into cover image replace came LSB of a pixels value with integer.
- Embedding into cover image .

This method employ multiple cover with location sensitive secret embedding in 2 LSB plane with less modification per pixels but having limited embedded capacity even employ multi cover image.

C. *Multi -level Encryption algorithm*

To increase more security of the secret information this method is used .In MLEA method instead of embedding secret information into cover image directly , first encrypted a secret data using stego key then embedded into cover image.This increase attacker difficulties to crack secret information .In this algorithm we proposed a secret information framework based on “Stego key directed adoptive LSB substitution(SKA-LSB) method and multi level encryption algorithm (MLEA)”[6] .The secret data is encrypted through MLEA, stego key encrypted through TLEA and encrypted information is the embedded into cover image using adaptive LSB substitutions method [6] .This method based on a 4 sub algorithm :

- TLEA used for encryption of secret key.
- MLEA used for encryption of secret data using TLEA encrypted secret key.
- Embedded MLEA encrypted secret data into cover image using adaptive LSB substitutions technique .
- Extractions algorithms which extract from stego image at the receiver terminal.

MLEA based algorithm used for a colour image steganography using adaptive LSB method to increase the payload and better visuals quality and more resistance against Stego analysis.

a) Two -level encryptions algorithm: The TLEA is a simple algorithms to encrypt a secret key that result better security [6].

b) Multi level encryption algorithms: The MLEA used to encrypt the secret data through a secret key which also encrypted using TLEA algorithm[6] .

Embedded algorithm

First perform TLEA operation which consist of two main step i.e.

- Consider secret key first digit and covert into binary form then perform xor operation with logic 1 [6].
- Apply secret pattern based “ bit shuffling algorithm” shuffling binary bit of each byte in secret key[6] .

Continue this operation on secret key until all secret key is encrypted completely.

Then perform MLEA operation to encrypt secret data. This algorithm consists of 4 step:

- Bit xor operation with secret key and logic 1.
- Encrypted Secret key divide into blocks.
- Shuffling of secret data based on secret key.
- Encrypted the secret information based on adaptive LSB algorithm .

follow this process cause to increase the security of data which cannot easilybreak by attacker.

This method provide light weight encryption algorithm that maintain balance between security and imperceptibility but it has limited embedded capacity .

D. *Cyclic 18 LSB substitution algorithm*

In the social network there are many attacker are available to crack the data and use the information regarding their field .To increase more security of a secret information into colour image the Cyclic-18 substitution method with three-level of encryption algorithm is used that give the dual security of secret data and it is not easy to break security and get information.

This method proposed difficulties for hacker by dividing message bit into block ,TLEA, images scrambling and rotating sub image at various angle[5]. This make information extractions very challenging.

The algorithm is based on a 3 sub algorithms:

- Encryptions of secret data using TLEA algorithm that increase the extra layer of security .
- Before embedding the images scrambling the increasing the complexity of a data extractions .
- Data hiding algorithm called cyclic 18 MLEA substitutions algorithm that produced high quality of stego image and less flexibility for attacker[5].

This method result advancing of a security system maintain the visuals transparency of resultant image an increase security of embedded data hence we introduce some keyword that is used in cyclic 18 LSE substitutions algorithm.

a) *Secret key based images scrambling:* Images scrambling method4 different sub keys used to convert the scrambling process the sub key1 is used to scrambling the eight plane of a red channel, sub key 2 is used to scrambling of eight plane offer blue channel ,sub Key3 is used to scramble the eight plane offer green channel and then sub key 4 is used to combine the three encrypted channels to make scrambled image[5].

b) *Three label encryptions algorithm*: The TLEA used to encrypt the message block of secret information to apply the cyclic 18 LSB algorithm[5] . This algorithm having three the different sub procedure

- Encrypt the stego key by performing bit xor operations with logic 1
- Bits shuffling to create extra level of security.
- Encryptions secret key.

c) *Cyclic 18 LSB substitution algorithm* :The cyclic 18 LSB algorithm used to hide encrypted secret bit in LSB of cover image in randomly manner .To increase security of a secret data this substitutions method having 6 pair .Each pair having three plain so resulting having 18 channel And these channel swapping regarding to the instructions in cyclic manner that's why this algorithm is known as cyclic 18 LSB substitutions method[5].
Colour image consists of a 3intensity i.e. RGB and each colour is made up of 8 bit therefore resulting 24 bit image better 18 planes.
Embedded process:

- Rotate the cover image into 180 degree then based on secret key that is encrypted using TLEA, is scrambled into plane[5].
- Secret key is divided into 3 sub blocks in 4:3:1 (8 bit)
- Encrypted using TLEA then two fold of division key into LSB of plane[5].
- Encrypted blocks are embedded with scrambled image using cyclic 18 LSB substitutions method[5].

This method provide high visual quality with high security.

E. *Improved LSB scheme using Modulo-3 algorithm*

This method is suitable for a ternary number system with high payload and good visual quality. We can embedded larger series of a secret data into cover image without wasting bits. This method is good when embedding capacity is high and give good detections against modern detections SPAM but with the low embedded capacity traditional LSB substitutions method [7] .
Improved LSB substitutions method embedded series of ternary secret data into cover image using modulo-3 operation .This method can hide two ternary number into each gray scale pixel value to only modify the two LSB of a pixel of cover image .In the case of overflow or underflow and carry or borrow simply add 1 to the pixels or subtract 1 to the pixels before embedding [7].
Embedding process:

- Convert the greyscale pixel value into binary bit .
- Divide binary bit into 2 sub segment in 6:2(8 bit)
- Embedded first ternary secret number by adding 1 or subtract 1 to performing modulo operations on 1st 6 bit cause to remove overflow/ underflow and generate stego sub segment .
- Add stego sub segment1 with subsegment2 and perform modulo three operation in case of Carry or borrow then add subtract 1 or add 1 respectively and generate stego pixels value.
- Repeat this operation on next pixel value until all secret data are embedded into cover image.

This method provide high security when embedded capacity is high but it did not give better security when the embedded capacity is low [7] .

IV. COMPARISON OF LSB ALGORITHM BASED ON EVALUATION PARAMETER

Para meter	**±1LSB**	**Adoptive LSB**	**MLEA**	**Cyclic-18**	**Modulo 3**
Payload	1bpp	1bpp	≈1bpp	≈1bpp	3bpp
Visual Quality	52.9 Db	50 Db	>45 dB	>53 dB	37 dB
Stego-analysis	HUF-COM	SPAM 2nd order	Histo-gram	_	SPAM

TABLE I. COMPARISON OF LSB ALGORITHM

V. RESULT

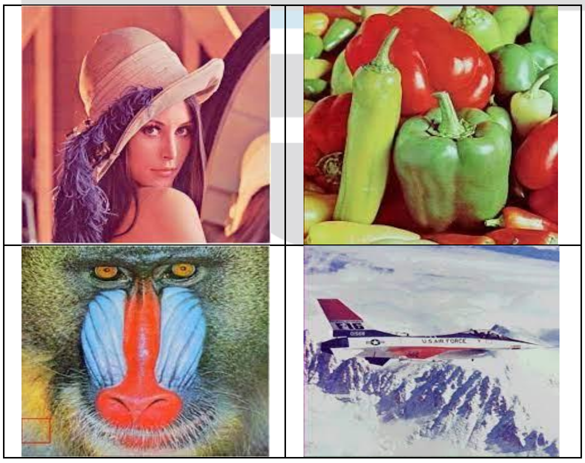

Fig. 2 A set of input cover image of proposed method. The first row show Lena, Peppers and second row show baboon, F61 cover image

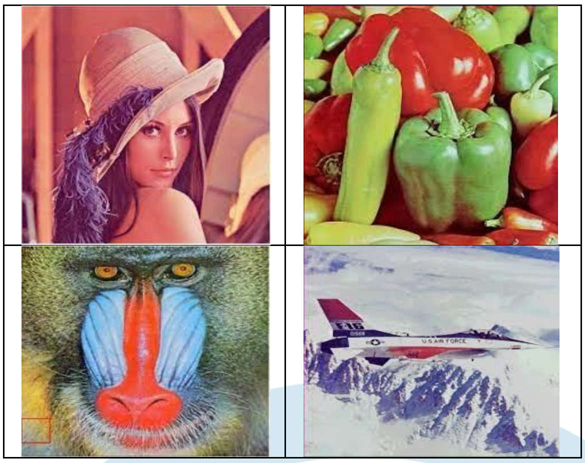

Fig. 3 A set of output stego image of proposed method. The first row show Lena, Peppers and second row show baboon, F61 stego image

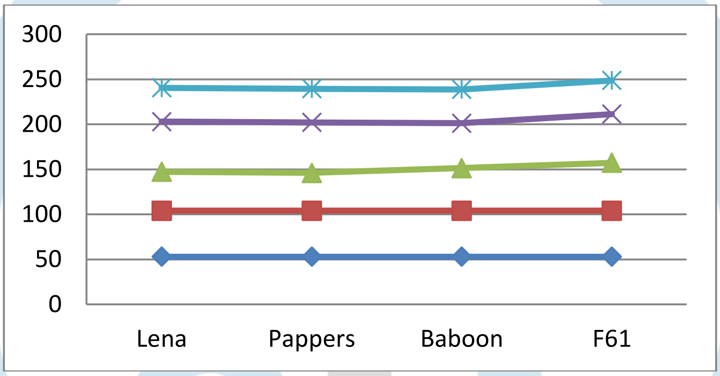

Fig. 4 PSNR for comparison between different algorithm

VI. EVALUATION PARAMETER

A. Payload analysis

Embedded capacity is a quality of a secret data that can successfully hidden into cover image [6]. Payload is the evolutions parameter that based on a number of a secret bit is embedded per pixel [1]. The size of payload is directing proposal to the strength of steganography algorithm [6] and it measure in bit per pixel (bpp).

$$\text{Payload} = \frac{\text{no. of embedding bit}}{\text{H} \times \text{W}}$$

H× Wrepresent the height and width of cover the image.

B. Visual quality analysis

Embedding the secret information into cover image through any stenographic algorithm it is also altered the cover image quality which sometime noticeable by human eye [1] .Based on evolutions parameters visuals quality is calculated before applying any steganography method that avoid this transparency of a secret data.

$$\text{MSE} = \frac{1}{\text{H} \times \text{W}} \sum_{\text{K}=1}^{\text{H}\times\text{W}} (\text{C}_\text{K} - \text{S}_\text{K})^2$$

$$\text{PSNR(dB)} = 10 \times \log_{10}\left(\frac{\text{max}^2}{\text{MSE}}\right)$$

max= maximum pixel intensity value i.e. 255

C_K = cover pixel value, S_K= stego pixel value

H× W represent the height and width of cover the image (Consider lower value for good result).

C. Security analysis

Security parameter is one of the most important parameter of any data hiding method because the hidden information transfer to end user secretly and that is important to hidden by attacker so if a particular algorithms used to hide a certain information with low security than it is easy to crack by attacker. To avoid data transparency the powerful and strong security algorithm use. Stegoanalysis is reverse to steganography ,in which to defeat the steganography method datacan extract [1].

VII. CONCLUSION

This paper is based on thorough survey of LSB substitutions method in spatial domain steganography method based on the evolutions parameter .In general we want to achieve ideal steganography method which has high payload capacity ,good visual quality and high resistance against the stego analysis but if we achieve any such parameters with the these values other parameters like imperceptibility is fall down with the low value or it is limited value .This paper is based on the requirement of a giving parameter to adopt particular algorithms to achieve the evaluation parameter keep the other parameter with their limited value.

REFERENCES

[1] Mehdi Hussain , Ainuddin Wahid Abdul Wahab , Yamani Idna Bin Idris , Anthony T. S. Ho, KiHyun Jung , Image steganography in spatial domain: a survey,ResearchGate, March 2018,pp.1-2710.1016/j.image.2018.03.012

[2] Brij Mohan Kumar, An introduction to steganography techniques in the field of digital image processing, International Journal of Engineering Science ,vol. 7,pp. 13495-13498

[3] S. Sarreshtedari, M.A. Akhaee, One-third probability embedding: A new±1 histogram compensating image least significant bit steganography scheme, IET image processing, 8 (2014) 78-89.

[4] H. Yang, X. Sun, G. Sun, A high-capacity image data hiding scheme using adaptive LSB substitution, Radio engineering, 18 (2009) 509-516

[5] K. Muhammad, M. Sajjad, S.W. Baik, Dual-level security based cyclic18 steganographic method and its application for secure transmission of key frames during wireless capsule endoscopy, Journal of medical systems, 40 (2016) 114.

[6] K. Muhammad, J. Ahmad, N.U. Rehman, Z. Jan, M. Sajjad, CISSKA-LSB: color image steganography using stego keydirected adaptive LSB substitution method, Multimedia Tools and Applications, (2016) 1-30

[7] W.-L. Xu, C.-C. Chang, T.-S. Chen, L.-M. Wang, An improved least-significant-bit substitution method using the modulo three strategy, Displays, 42 (2016) 36-42

[8]Mamta Jain,A survey on digital image processing steganography using RGB channel,3(2017)21-25

[9] https://www.investopedia.com/terms/a/artificial-neural-networks-ann.asp

[10]Kavitha V., Easwarakumar K.S. (2004) Neural Based Steganography. In: Zhang C., W. Guesgen H., Yeap WK. (eds) PRICAI 2004: Trends in Artificial Intelligence. PRICAI 2004. Lecture Notes in Computer Science, vol 3157. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-28633-2_46