

A New Technique of Image Cryptography using Spread Spectrum Watermarking with Improved AES

Rashmi Jha¹ Paramdeep Singh² Yogendra Kumar Jain³

^{1,2,3}Department of Computer Science & Engineering

^{1,2,3}Samrat Ashok Technological Institute, Vidisha (M.P.), India

Abstract— Image Cryptography is technique of hiding some meaningful information inside the image so that the security of Secrete Information can't be accessed by the external users. The Existing Haar Wavelet based Image Cryptography provides efficient Hiding of Secrete Information, but the methodology proposed is not efficient in terms of Security and Correlation Coefficients. Hence a new and efficient technique for the Image Cryptography is proposed which provides efficient results as compared to the existing Haar Wavelet based Image Cryptography. The Untried consequences are performing on various images of different sizes and categories. The Methodology adopted here is based on the combinatorial method of applying Improved Advanced Encryption Scheme based Encryption with Spread Spectrum Technique of secrete information thrashing and applying an effective cryptography algorithm.

Key words: Cryptography, Symmetric Key, Haar Wavelet, Spread Spectrum, AES

I. INTRODUCTION

A copy of a digital image is the same to the original. This has in many illustrations, led to the exploit of digital substance with malicious purpose. Steganography is the discipline and skill of defeating secret data in a host multimedia data like (e.g. manuscript, image, acoustic, video, etc.) [1]. The reason of a steganography algorithm is beating a huge number of covert data into a significant host media such that the entrenched secret data are hides to prevent the attack of unauthorized persons. One method to keep multimedia data alongside illegal confirmation and retransmission is to set in a signal, called digital signature or exclusive rights label or watermark that validate the information proprietor of the data. Data hiding, methods to implant resultant information in numerical media have made significant development in modern years and concerned consideration from both academe and industry. Systems have been recommended for a selection of requests, counting ownership protection, authentication, and admission organize Imperceptibility, and strength besides reasonable processing such as firmness, and the capability to conceal many bits are the essential but to a certain extent inconsistent requirements for many data hiding applications. Steganography is fixed in creation an enhanced steganography scheme with enough and efficient Steganography methods. In steganography, there are three most important objectives counting rising hiding capability, strength to confident attacks and growing security stage [1]. The skill of encrypting confidential message by an enclosed standard as audio, picture, video files, or text is known as Steganography. Modern Steganography is conceding by joining of cryptography and Steganography methods for protected transmission of digital data. Steganography relies on investigating the subsisting Steganography algorithm and its challenges. Steganography is based on improving

protected communication of information. The earlier effort in Steganography makes available an essential conception of Steganography to novel researchers. Excellent information has been position in to defend personal data. The authoritative Steganography plans for hiding MP4 or quick time multimedia data files are true crypt.

A copy of a digital image is impossible to tell apart to the original. This has in many occurrences, led to the exploit of digital substance with malicious objective. One method to save from harm multimedia information alongside prohibited video recording and retransmission is to insert a signal, called digital signature or exclusive rights label or watermark that validate the data proprietor of the particular data. Data hiding, methods to insert resultant information in digital media, have made substantial development in current years and involved concentration from both academia and industry. Existing method have been plan for a selection of applications, including ownership protection, authentication and admission organize. Imperceptibility, strength aligned with reasonable processing such as solidity and the competence to conceal many bits are the fundamental but rather conflicting requirements for many data hiding applications. In [2], a Steganography system based on GA is presented which is secure against RS attacks. This technique in first step drive ins secret bits into swarm image just like simple LSB and in subsequent step alters pixel values to make stego image RS parameters sit in secure area.

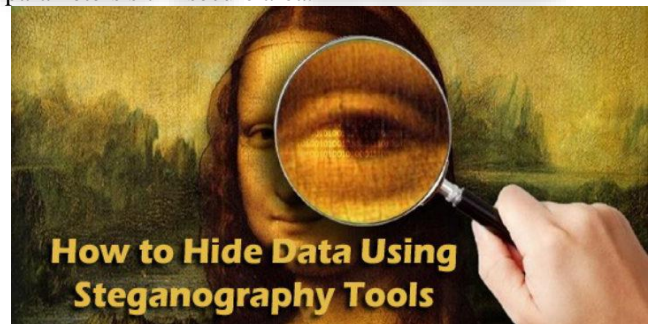


Fig. 1: Type of data hiding by steganography tool

A. Visual Cryptography

Since the augment of the Internet technology one of the most noteworthy issues of in sequence knowledge and communication has been the safety measures of information. Cryptography was formed as a method for protected the confidentiality of communiqué and many dissimilar systems have been prolonged to encode and decode information with the purpose of maintain the message secret. Unfortunately it is a short time not adequate to maintain the substances of a message secret, it may also be essential to keep the way of life of the message secret. In Graphic Cryptography the double is separated into shares called shares which are then dispersed to the contributors. . Visual cryptography is a new type of cryptographic design which can decode covered

images without any cryptographic computation. The scheme is perfectly secure and very easy to implement.

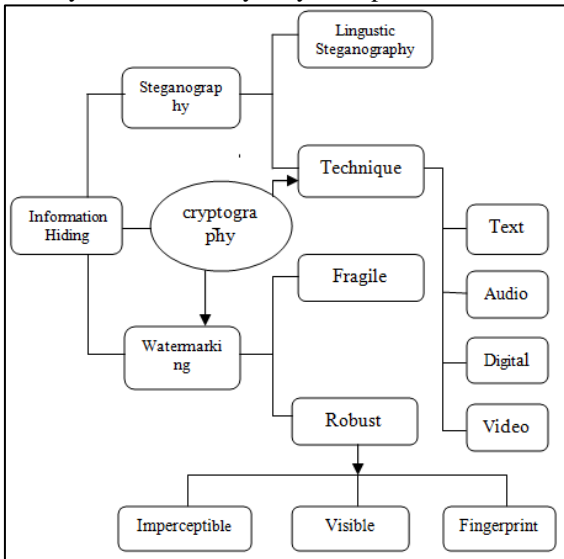


Fig. 2: Cryptography in security domain

B. Steganography

In image steganography the data is concealed entirely in images. The design and perform of hiding data has an extensive times past. In Pasts the Greek historian Herodotus etches of an aristocrat, Histaeus, who required communicating with his son-in-law in Greece. He trims the head of one of his most confidences slaves and tattooed the communication onto the slave's scalp. When the slave's hair grows reverse the slave was posted with the concealed message [4]. In the Second World War the Microdot system was urbanized by the Germans. In sequence, especially photographs, was decreased in volume until it was the size of a typed period. Exceptionally complicated to distinguish, a standard cover message was sent over an unconfident conduit with one of the times on the paper having hidden data [5]. Nowadays steganography is generally applied on computers with digital information organism the carrier and network being the high speed release channels. Steganography be different from cryptography in the intelligence that where cryptography centers on remaining the substances of a message secret, steganography focuses on keeping the presence of a communication secret [6]. Steganography and cryptography are both methods to defend data from redundant parties but neither skill alone is ideal and can be cooperated. Once the attendance of concealed in sequence is exposed or even supposed, the point of steganography is incompletely overcome [6]. There are four categories of file formats that can be used for steganography: text, audio, digital, video. Image and audio files especially comply with this necessity, while research has also uncovered other file pattern that can be used for information hiding.

C. Watermarking

Digital watermarking is the act of protecting a message related to a digital signal (i.e. an image, song, and video) within the signal itself. It is a approach closely related to steganography, in that they both hide a message inside a digital signal. After all, what isolates them is their goal. Watermarking tries to hide a message related to the real

content of the digital signal, while in steganography the digital signal has no relationship to the message, and it is merely used as a conceal to hide its existence. Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and consequently in paper bills.

Watermarking is dividing into fragile and robust. fragile watermarked is destroyed if anybody attempts to temper with the object in which it is embedded, where as a robust watermark is a watermark that is difficult to remove from the object in which it is embedded, Robust are categorized into three group: imperceptible(invisible), visible, fingerprint. An Invisible watermarked is not normally perceptible but can still be use by the rightful owner as evidence of data authenticity in a court law.

A visible watermark is immediately perceptible and clearly identifies then cover object as copyright, secured material much like the copyright symbols. In fingerprint watermarking, it is easy to mix up a digital fingerprint and a digital watermark. A fingerprint image watermarking has been explored to solve the problem of security of data.

II. PROPOSED METHODOLOGY

The planned procedure applied here for material whacking using a hybrid combinatorial method of applying impoved form ogf Advanced Encryption Scheme of the compacted image so that the information hide is made secure from various attacks. Finally the encrypted image is watermarked with the secure image using Spread Spectrum based watermarking.

The planned procedure implemented here works in the following stages:

- 1) Take an input image and a secrete image
- 2) Apply Two Different Types of Key Stream Generators such as A5/1 Key Stream Generator on the Original Input Image.
- 3) Apply Advanced Encryption Scheme on the Inventive Image & Key Stream Generator.
- 4) Apply Spread Spectrum Watermarking on the Ciphred Image.

A. Input Image & Secret Image

For the testing of the projected procedure several Grey scale and Colour images are taken from various sources of various types. The images include high dynamic images as well as Grey level images and Colour images so that the proper working of the methodology is computed.

B. A 5/1 Key Stream Generator

The Key Stream Generator consists of 3 different types of Linear Feedback Sift Registers; let us say for example Re1, Re2, Re3 of varying lengths of 19 and 22 and 23 bits correspondingly. Here Each of the Linear Feedback Sift Registers uses Clock Cycles for the Majority functions. The Improved Majority Function contains three bits C1, C2 and C3. The 64 bits of the key Map to the Linear Feedback Sift Registers initial States as Re1 (19bits), Re2 (22 bits) and Re3 (23 bits). At each Regulator Cycle after the initialization point, the last bits of each of the Linear Feedback Sift Registers are XORed to generate one output bit.

C. Spread spectrum Watermarking

- 1) Take an original image (ciphered image) and a secret image.
- 2) Choose alpha worth which signified watermark indication asset feature in spread spectrum algorithm, here in our work we assume alpha=5;
- 3) Calculate DWT of the unique image, which used for the transformation of the image to be embedded.
- 4) Calculate total number of pixels of the original image and watermark image.
- 5) Calculate $a_j = b_j$ where $ir <= j < (i+1)r$.
- 6) Calculate watermark signal as $w_j = \alpha * a_j * p_j$, where $p_j = \{+1, -1\}$.
- 7) Now we will find the kernel of the image by taking kernel size 31 and by taking the level of the kernel size as 3 we will find the kernel image of the inventive image by calculating kernel image = $(1/(2 * \pi * s^2)) * \exp(-((X-m)^2 + (Y-m)^2)/(2 * s^2))$;
- 8) This watermark signal is then embed with the kernel image to get the final watermark image.

The implanting procedure is accept out by first making the watermark signal W by using watermark material bits, chip rate and PN sequence. As shown in Fig 4.3 flowchart the watermark evidence bits $b = \{b_i\}$, where $b_i = \{1, -1\}$ are spread by r, which gives

$$a_j = b_i, \quad ir \leq j < (i+1)r$$

The sequence a_j is then multiplied by $\alpha > 0$ and P. The watermark signal $W = \{w_j\}$, where

Where, $p_j = \{1, -1\}$ the watermark indication produced is extra to the encrypted signal, to give the watermarked signal C_w .

$$C_w = C + W = c_{wi} = c_i + w_i, \quad \forall i = 0, 1, \dots, L-1$$

The encrypted value of M2 denoted by C2 is

$$c_{2i} = (m_{2i} + k_{2i}) \bmod 255 \quad \forall i = 0, 1, \dots, L-1$$

The figure shown below is the flow diagram of spread band based watermarking technique. The watermarking starts with the initialization of parameters.

ΔDq is the initial difference parameter and $K[i]$ is the array matrix containing pixel values.

Here Q is the Quantization parameter used in Spread Spectrum Watermarking.

D. AES Algorithm

The more popular and commonly adopted symmetric encryption algorithm likely to be encounter nowadays is the Advanced Encryption Standard (AES). It is finding at least six times faster than triple DES.

A replacement for DES was need as its key size was too modest. With growing computing power, it was consider vulnerable against exhaustive key search attack. Triple DES was design to overcome this drawback but it was find slow.

The features of AES are as pursue

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and quicker than Triple-DES
- Provide full details and design details
- Software implementable in C and Java

1) Operation of AES

- AES is an insistent rather than Feistel cipher. It is based on 'substitution-permutation network'. It contains of a series of linked operations, some of

which require replacing inputs by specific outputs (substitutions) and others requires shuffling bits around (permutations).

- Interestingly, AES performs all its calculation on bytes rather than bits. Hence, AES performs as the 128 bits of a plaintext block as 16 bytes. These 16 bytes are organized in four columns and four rows for processing like that matrix -
- Unlike DES, the number of rounds in AES is variable and based on the length of the key. AES applies 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds applies a different 128-bit round key, which is calculating from the original AES key.

The simplified of AES structure is given in the following explanation

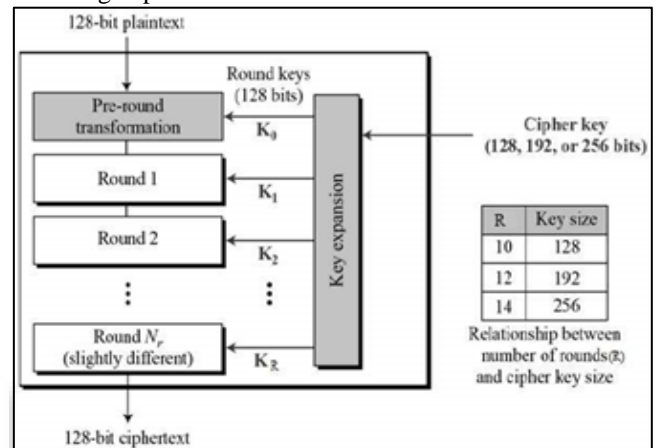


Fig. 3: Basic AES Structure

E. Encryption Process

Here, we modify to description of a typical round of AES encryption. Each round involves of four sub-processes. The first round process is illustrates below:-

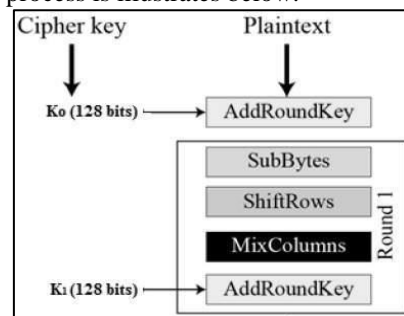


Fig. 4: First Round of Encryption Process

1) Byte Substitution (SubBytes)

The 16 input bytes are changed by finding up a fixed table (S-box) given in design. The result performs in a matrix of four rows and four columns.

2) Shiftrows(move rows)

Each of the four rows of the matrix is moved to the left. Any entries that 'fall off' are restored on the right side of row. Move is carried out as follows -

- First row is not moved.
- Second row is moved one (byte) position to the left.
- Third row is moved two positions to the left.
- Fourth row is moved three positions to the left.
- In a new matrix is result consisting of the same 16 bytes but moved with respect to each other.

3) *Mix Columns*

Each column of four bytes in matrix is now transformed using a special mathematical function. This action takes as input the four bytes of one column and outputs four totally new bytes, which succeed the original column. The result is another new matrix of four row and four column consisting of 16 new bytes. It should be noted that this step is not operated in the last round.

4) *Add round key (XOR with Key)*

The 16 bytes of the matrix are now looked at 128 bits and are XORed perform with the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are translated as 16 bytes and we begin another similar round.

5) *Decryption Process (Decrypt Procedure)*

The procedure of decryption of an AES ciphertext is same to the encryption procedure in the inverse order. Each round subsists of the four steps conducted in the inverse order –

- Add round key(XOR with key)
- Mix columns(shuffling)
- Shift rows(move row)
- Byte substitution(changed byte)

Since sub-steps in each round are in inverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms need to be individually implemented, although they are very exactly related.

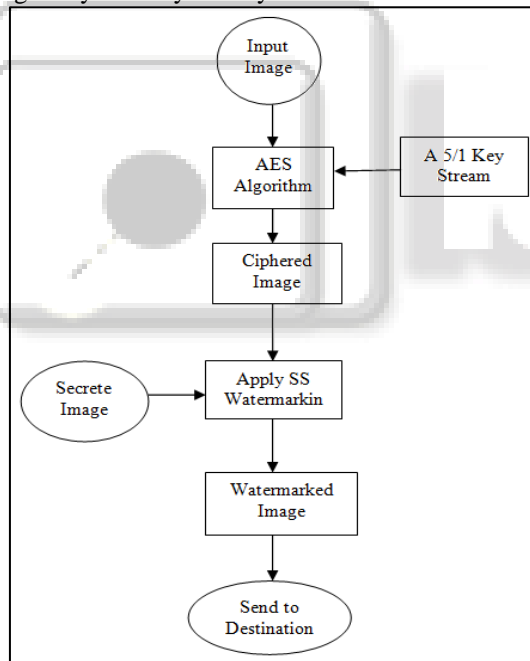


Fig. 5: Flow Chart of the Proposed Methodology

III. RESULT ANALYSIS

The Table Show below is the analysis and Comparison of Existing Haar Wavelet Methodology and the Proposed Methodology implemented for Image Cryptography. The Analysis is done on Various Standard Images and the Original Encryption Peak Signal to Noise is computed.

Standard Images	Existing Work	Proposed Work
Lena	0.0017	0.0014
Boat	0.0068	0.0062
Lake	0.0043	0.0038
Barbra	0.0077	0.0069
Living-room	0.0021	0.0018

Fingerprint	0.0065	0.0061
Pirate	0.0026	0.0021
Peppers	0.0102	0.0098
Jet-Plane	0.0099	0.0091
House	0.0131	0.0128
Cameraman	0.0168	0.0162

Table 1: Analysis of Original-Encrypted Image PSNR

The Table Show below is the analysis and Comparison of Existing Haar Wavelet Methodology and the Proposed Methodology implemented for Image Cryptography. The Analysis is done on the Comparison of NPCR and UACI on the Standard Images.

Standard Images	Existing Work		Proposed Work	
	NPCR %	UACI %	NPCR %	UACI %
Lena	99.941	38.981	99.961	39.642
Boat	99.997	46.283	99.998	48.724
Lake	99.953	40.874	99.962	42.844
Barbra	99.961	39.847	99.974	42.485
Living-Room	99.976	38.276	99.979	40.285
Fingerprint	99.996	39.873	99.997	41.284
Pirate	99.974	40.791	99.98	43.285
Pepper	99.998	39.827	99.998	42.496
Jet-Plane	99.91	39.866	99.93	42.642
House	99.989	38.739	99.99	40.184
Cameraman	99.978	39.208	99.983	43.274
Average	99.969	40.233	99.977	42.46

Table 2: NPCR and UACI results performed on standard images

The Table Show below is the analysis and Comparison of Existing Haar Wavelet Methodology and the Proposed Methodology implemented for Image Cryptography. The Analysis is done on the Comparison of Encryption Entropy of Standard Images.

Algorithm	Encryption Image Entropy	
	Lena	Boat
Existing Work	7.998	7.996
Proposed Work	8.2	8.17

Table 3: Analysis and Comparison of Encryption Image Entropy

The Figure Show below is the analysis and Comparison of Existing Haar Wavelet Methodology and the Proposed Methodology implemented for Image Cryptography. The Analysis is done on Various Standard Images and the Original Encryption Peak Signal to Noise is Computed.

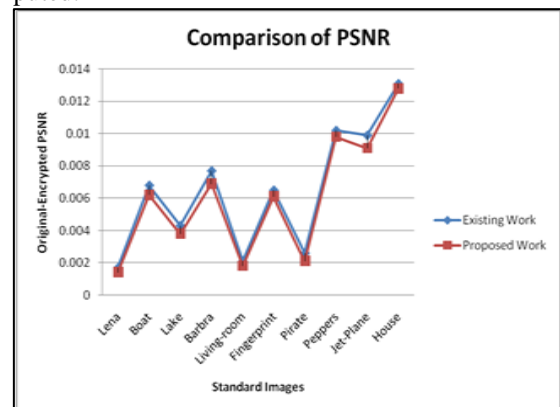


Fig. 6: Analysis & Comparison of Original Encryption PSNR on Standard Images

The Table Show below is the analysis and Comparison of Existing Haar Wavelet Methodology and the Proposed Methodology implemented for Image

Cryptography. The Analysis is done on Correlation Coefficient of Two Adjacent Pixels in Original and Encryption Images.

Encryption Algorithm	Test Image	Horizontal		Vertical		Diagonal	
		Original	Encrypted	Original	Encrypted	Original	Encrypted
Existing Work	Lena	0.919	0.0023	0.927	0.0042	0.962	0.0053
	Boat	0.922	0.0081	0.978	0.0128	0.943	0.0019
	Lake	0.987	0.0025	0.936	0.0015	0.927	0.0105
Proposed Work	Lena	0.024	0.002	0.931	0.0038	0.969	0.0048
	Boat	0.928	0.0078	0.981	0.0124	0.947	0.0014
	Lake	0.991	0.0021	0.939	0.0013	0.931	0.99

Table 4: Correlation coefficients of two adjacent pixels in original and encrypted images

IV. CONCLUSION

The Planned Procedure adopted here for the Image Cryptography using Mosaic Image based Spread Spectrum Watermarking provides results as Cryptography. Various Experimental results are performed on Existing Haar Wavelet based Image Cryptography and the Planned Procedure and the methodology adopted here proves to be more efficient in comparison.

Although the Planned Procedure implemented here is feasible for the Steganography but there are future enhancement done in the technique such as image steganography of HDR Imaging, low computational time and less iteration and complexity should be minimized.

REFERENCES

- [1] Cheddad, A. et al. Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 90(3), 727–752, 2010.
- [2] Wang, S., Yang, B., & Niu, X. (2010). A secure steganography method based on genetic algorithm. *Journal of Information Hiding and Multimedia Signal Processing*, 1(1), 28–35.
- [3] Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science.
- [4] Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001
- [5] Jamil, T., “Steganography: The art of hiding information is plain sight”, *IEEE Potentials*, 18:01, 1999
- [6] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, *Communications of the ACM*, 47:10, October 2004
- [7] Masoud Nosrati, Ronak Karimi, Mehdi Hariri. Embedding Stego-Text in Cover Images Using linked List Concepts and LSB Technique. *World Applied Programming*, Vol (1), No (4), October 2011. 264-268.
- [8] Masoud Nosrati, Ronak Karimi, Mehdi Hariri. “An introduction to steganography methods” *World Applied Programming*, Vol (1), No (3), August 2011. 191-195
- [9] Tew, Y., & Wong, K. (2014, Feb). An overview of information hiding in H.264/AVC compressed video. *IEEE Transactions on Circuits and Systems for Video Technology*, 24(2), 305 - 319.
- [10] Elham Ghasemi, Jamshid Shanbehzadeh, and Nima Fassihi, “High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform” S.I. Ao et al. (eds.), *Intelligent Control and Innovative Computing*, Lecture Notes in Electrical Engineering 110, DOI 10.1007/978-1-4614-1695-1 30.
- [11] Hamidreza Rashidy Kanan, Bahram Nazeri, “A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm” *Expert Systems with Applications* 41 (2014) 6123–6130.
- [12] Anant M. Bagade* and Sanjay N. Talbar, “A High Quality Steganographic Method Using Morphing” *J Inf Process Syst*, Vol.10, No.2, pp.256-270, June 2014.
- [13] Jyoti, Md. Sabir, “More Secured Steganography Model with High Concealing Capacity by using Genetic Algorithm, Integer Wavelet Transform and OPAP” *International Journal on Recent and Innovation Trends in Computing and Communication*, ISSN 2321 – 8169 Volume: 1 Issue: 4 MAR 2013.
- [14] Po-Yueh Chen and Hung-Ju Lin, “A DWT Based Approach for Image Steganography”, *International Journal of Applied Science and Engineering* 2006. 4, 3: 275-290.
- [15] Amitav Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, “A novel technique for image steganography based on DWT and Huffman encoding”, *International Journal of Advances in Image Processing*, Vol. 2, Special Issue 1, Part 2, 2011
- [16] Ran-Zan Wang, Chi-Fang Lib, and Ja-Chen Lin, “Image hiding by optimal LSB substitution and Genetic algorithm”, 2001 *Pattern Recognition Society*. Published by Elsevier Science Ltd.
- [17] J. K. Mandal, A. Khamrui. A Data Embedding Technique for Gray scale Image Using Genetic Algorithm (DEGGA). *International Conference on Electronic Systems (ICES-2011)*.
- [18] Samir Kumar Bandyopadhyay, Tuhin Utsab Paul and Avishek Raychoudhury, Genetic Algorithm Based Substitution Technique of Image Steganography, *Journal of Global Research in Computer Science*, Volume 1, No. 5, December 2010.
- [19] H. J. Patel and P. K. Dave, “Least Significant Bits Based Steganography Technique,” in *Proc. IJECCE* 2012, vol. 3, pp. 97-103.
- [20] S. Johri., “An Adaptive Steganography Technique for Gray and Colored Images,” *Journal of Global Research in Computer Science*, vol. 3, pp. 41-45, 2012.
- [21] S. Tiwari, R. P. Mahajan, and N. Shrivastava, “Steganography-an Approach for Data Hiding Based on Encryption and Lsb Insertion,” *IJECCE*, vol. 3, pp. 76-83, 2012.