International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

An Efficient Steganography using ABC Optimization and Image ScramblingScheme

Daparthi Naresh[1], V. Naresh[2]
[1] M.Tech Student, Dept. of ECE, AKRG College of Engineering and Technology,West Godavari, Andhra Pradesh, India
[2] AssistantProfessor, Dept. of ECE, AKRG College of Engineering and Technology,West Godavari, Andhra Pradesh,India

Abstract: With the evolution of Internet Technology, the need for the security of information during its transmission has also increased rapidly. Steganography plays a prominent role in the field of data hiding and providing a means for secret communication. Steganography basically refers to the process of secretly hiding messages into a cover medium in a way that only the receiver can suspect its existence. In this, the data is hidden behind the cover image. The data is hidden character wise behind the pixels of the image. The various algorithms or techniques used for steganography are LSB-Hash, RSA Encryption, and Decryption. In this project, we use DES Encryption to increase the security level, and DWT to preserve the original quality of the cover image, while also keeping the original image intact after extraction. The usage of ABC Optimization increases the embedding capacity and gives improved PSNR and MSE values. Along with this scrambling algorithm to increase the security level of transmission

Keywords-LSB, Steganography, DES, Artificial Bee Colony, Scrambling

I. INTRODUCTION

Security of data to maintain its confidentiality, proper access control, integrity and availability is a major issue in data communication. As soon as a sensitive message was etched on a clay tablet or written on the royal walls, then it must have been foremost in the sender's mind that the information should not get intercepted and read by a rival. Codes, hence, form an important part of our history; starting from the paintings of DaVinci and Michelangelo to the ancient Roman stenographic practices the necessity of data hiding was obvious. Today in the e-age, the need to protect communications from prying eyes is greater than ever before. Cryptography, the science of encryption plays a central role in mobile phone communication, e-commerce, Pay-TV, sending private e-mails, transmitting financial information and touches on many aspects of daily lives. Today's technology can be traced back to earliest ciphers, and have grown as a result of evolution. The initial ciphers were cracked, so new, stronger ciphers emerged. Code breakers set to work on these and eventually found flaws, forcing cryptographers to invent better ciphers and so on. The significance of key is an enduring principle of cryptography. With the advent of the computer age, the mechanical encryption techniques were replaced with computer ciphers .They operated according to the same principles of substitution and transposition (where the order of letters or bits is altered). Again each cipher depended on choosing a key, known only by the sender and the receiver which defined how a particular message would be. This meant that there still was a problem of getting the key to the receiver so that the message could be deciphered. This had to be done in advance, which was an expensive slow and risky process. For years, this key distribution problem haunted code makers i.e. if you want to decipher a scrambled text you have to know the key in advance. But there was revolution in cryptography known as public key cryptography, which destroyed the key distribution problem. This was a technology tailor made for the internet. Customers could send credit card details and send them to retailers on the other side of the planet. It formed the basis of all kinds of modern day communications.

Generally, the file used, in which the data is hidden is refered to as "Cover Object" and "Stego object" is refered to as the file which secret message. General

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

Steganography mechanism is depicted in Fig.1. Among several cover media, image file are best suited due to their high degree of redundancy [2]. When the data is hidden, two characteristics are must essential which are quality and security. The Image steganography technique is broadly used procedure to protected information used for hidden communication. Such as featured tagging, military agencies copy right protection [3].

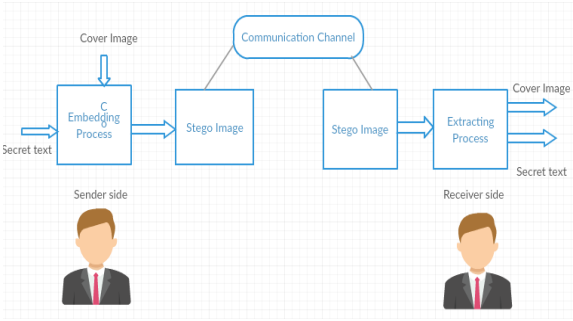


Fig. 1 General Steganography Mechanism

Steganography techniques are classified into two types which are spatial domain and frequency domain techniques. In spatial domain, data is hidden directly on the pixel values of the image and in frequency domain, image is transformed prior to data being hidden on the transformed coefficients [4]. Some of the spatial domain techniques are LSB, PVD, EBE, RPE, PMM and Pixel intensity based etc. and some of the frequency domain techniques are DCT, DWT, DFT, IWT and DCVT [5].

II. RELATED WORK

In this section, a few newly proposed techniques for image encryption, has been introduced.

1) A New Block Image Encryption Algorithm by Fridrich, 1997.

Jiri Fridrich presented an encryption algorithm that adapted certain invertible chaotic two-dimensional maps to create new symmetric block encryption schemes. This scheme is especially useful for encryption of large amount of data, such as digital images.

2) A Technique for Image Encryption using Digital Signatures, 2003.

AlokaSinha and Kehar Singh have proposed a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the encoded version of the original image. Image encoding is done by using an appropriate error control code, such as a Bose-ChaudhuriHochquenghem (BCH) code. At the receiver end, after the decryption of the image, the digital signature has been used to verify the authenticity of the image.

3) A Technique for Image Encryption using multi-level and image dividing technique, 2003.

Chang-Mok Shin, Dong-HoanSeo, Kyu-Bo Chol, Ha-Wmn Lee, andSmJmng Kim[16] proposed image encryption by using binary exclusive OR operation and image dividing technique. They converted binary images to binary phase encoding and then encrypt these images with binary random phase images by binary phase XOR operation. Encrypted gray image was then obtained by combining each binary encrypted images.

4) Image Encryption Using Advanced Hill Cipher Algorithm.

In this paper, we have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption. The objective of this paper is to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption, where we may not be able to decrypt the encrypted message, if the key matrix is not invertible. Divide the image into blocks apply the involutory key matrix to each block and create a temporary block using the ith pixel value of each block again multiply it with involuntary key matrix and find transpose of it transfer it to destination.

5) Image Encryption Using Block-Based Transformation Algorithm, 2006.

In this paper the original image is divided into random number of blocks the original image is divided into a random number of blocks that are then shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm.

6) H-S-X Cryptosystem and Its Application to Image Encryption, 2009.

In this paper, we have proposed a novel technique which is a modified version of Hill cipher algorithm for image encryption named H-S-X (Hill-ShiftXOR) which can be applied to any type of images whether they are colour or gray. First color image is decomposed into (R-G-B) components. Second, encrypt each component (R-G-B) separately by the algorithm. Finally, concatenate the encrypted components together to get the encrypted color image.

7) Image Encryption Using DCT and Stream Cipher, 2009.

The proposed method based on the idea of decomposing the image into 8x8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT. Then, the DCT coefficients correlated to the higher frequencies of the image block are encrypted using Non-Linear Shift Back. The concept behind encrypting only some selective DCT coefficients based on the fact that the image details are situated in the higher frequencies, while the human eye is most sensitive to lower frequencies than to higher frequencies. Encrypt the selected coefficients by XORing the generated bit stream from the NLFSR +Key with the coefficient bits, the sign bit of the selected coefficients will not be encrypted.

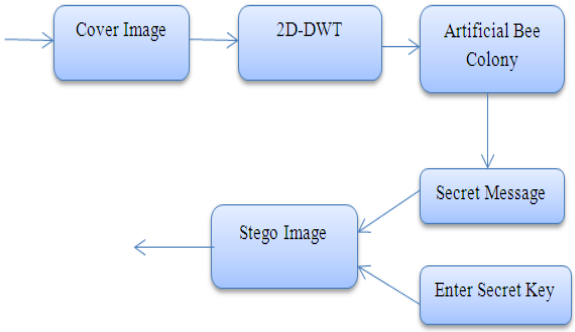
8) Choase Based Image Encryption Using Block-Based Transformation Algorithm.

The proposed algorithm is for image compression and encryption. The proposed algorithm with block size of 8-bit applies wavelet transform for each block for image compression and 256-bit secret key used for image encryption. The key is used to generate a pad that is then merged with the plaintext a byte at a time.

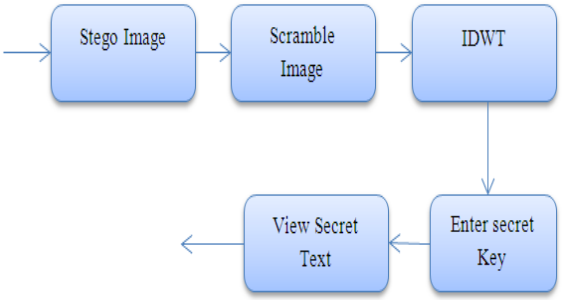
III. PROPOSED WORK

The proposed methodology is divided into different subsequent sections like DWT, ABC Optimization to find optimal pixel location for embedding, and DES for encryption. The image is first converted into grayscale if it is a colored image and DWT is applied to divide the image into four subsequent sections which contain one band with low-frequency coefficients and three bands with high-frequency coefficients. Further ABC is applied on the obtained or segmented region to optimize the values for the process of embedding. The message to be embedded is first encrypted using DES and then inserted into the appropriate bits of the image, using the LSB insertion method.

Proposed concept uses DES algorithm for encryption and decryption techniques. An N-level decomposition of the cover image and the secret images are done, and frequency components, DES factor of the same are combined. Secret Messages are extracted from the stego image at the receiver side.



(a) Encryption Process



(b) Decryption Process

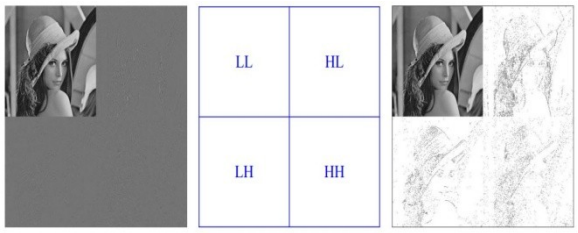
Fig. 2 Proposed Methodology

A. Discrete Wavelet Transformation

The wavelet transform decomposes a typical image data to a few coefficients with large magnitude and

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

many coefficients with small magnitude. In wavelet transform first step decomposes a signal into constituent parts in the time-frequency domain on a basis function localized in both time and frequency domains. The image or signal is decomposed into four different frequencies: approximation, vertical detail, horizontal detail and diagonal detail.Up to a level, the decompositions are repeated on the approximation coefficients. As details are not decomposed at the high levels and can be described by the small scale wavelet coefficients, the wavelet transform is not suitable for images having rapid variations.

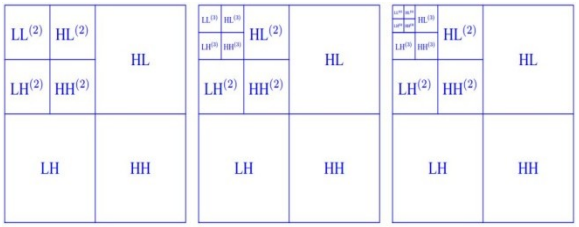


(a) CDF(2,2) wavelet applied as tensor product to the rows and columns of the image *lena*

(b) the different frequency blocks

(c) set all coefficients v in LH, HL, HH with $-20 < v < 20$ to white color

Fig. 3 Discrete Wavelet Transformation



(a) two levels of 2D-DWT

(b) three levels of 2D-DWT

(c) four levels of 2D-DWT

Fig.4 Process of 2D-DWT

B. Artificial Bee Colony Optimization

The ABC algorithm is developed by inspecting the behaviors of the bees on finding a food source, called as nectar, and the information of food sources to the bees in the nest is shared. The different phases of ABC are classified into three types, namely, the employed bee, onlooker bee, and the scout bee. In the employed bee phase, the employed bee stays on a food source and provides the neighborhood of the source in its memory. In the onlooker phase, the onlooker receives the information of food sources from the employed bees in the hive and to gather the nectar one of the food source is selected; and for finding new food, the new nectar, sources the scout is responsible. The process of the ABC algorithm is presented as follows:

Step 1. Initialization: In a solution space randomly Spray ne percentage of the populations, and then their fitness values calculated, called as nectar amounts, where the ratio of employed bees to the total population is represented by ne. The populations positioned into the solution space, are called as employed bees.

Step 2. Move the Onlookers: The probability of selecting a food source is calculated, select a food source to move by roulette wheel selection for each onlooker bees and then determine the nectar amounts of them.

Step 3. Move the Scouts: By a continuous predetermined number of iterations, if the fitness values of the employed bees do not improve, which is called" Limit", such food sources are abandoned, and these employed bees become the scouts. The movement of scouts takes place.

Step 4. Update the Best Food Source Found So Far: Memorize the position and the best fitness value, which are found by the bees.

Step 5. Termination Checking: Check whether the termination condition is satisfied by the number of iterations. Terminate the program and output the results if the termination condition is satisfied; otherwise go back to the Step 2.

C. Scrambling Process

The main purpose of digital image scrambling, which is used as the preprocessing or post-processing in image information hiding, is to transform a meaningful image into a meaningless or disordered image in order to enhance the power to resist invalid attack and in turn enhance the security. Image watermarking Algorithm based on DWT transform.This algorithm scrambles the watermarking

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

image and puts the watermarking image and original image in three-layer wavelet transform, eventually embeds the watermarking image in the original image to realize the embedding of watermarking. This algorithm scrambles the watermarking image and puts the watermarking image and original image in three-layer wavelet transform, eventually embeds the watermarking image in the original image to realize the embedding of watermarking.

IV. SIMULATION AND RESULTS

For comparing stego image with cover results requires a measure of image quality, commonly used measures Peak Signal-to-Noise Ratio. If SNR and PSNR represent smaller value, then it indicates there is a large difference between the original (without noise) and distorted image. The main advantage of this measure is ease of computation, but it does not reflect perceptual quality. An important property of PSNR is that a slight spatial shift of an image can cause a large numerical distortion but, there would be no visual distortion and conversely, a small average distortion can result in a damaging visual artifact, if all the error is concentrated in a small important region.

$$MSE = \frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2}{M\times N} \quad \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

where,

$$PSNR = 10 \times log10\left[\frac{255^2}{MSE}\right] \quad \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

where$M$ and N are the numbers of rows and columns in the input image, respectively. I_1 is the embedded image and I_2 is the cover image.

The simulation has been conducted in MATLAB environment by taking grayscale cover images of dimension 265X256. The following jpeg cover images have been taken: 1. Pets, 2. Moon, 3. Drop, 4. Plant. The average result evaluated during the experiment is shown in Table 1. The message that has been embedding during our test is "**abhinav.**" The PSNR and MSE values have been calculated using the equations (1) and (2) respectively. A greater value of PSNR represents greater visual quality of the image and minimum distortion between the original image and the embedded image. Hiding capacity represents the amount of data that can be effectively embedded in the image.

Table 1. Comparison results based on Standard DWT Steganography and our proposed method

Name of image	MSE		PSNR in dB	
	Standard Algorithm	Proposed Algorithm	Standard Algorithm	Proposed Algorithm
Pets	0.0321	0.0114	43.6552	48.1392
Moon	0.0058	0.0021	45.5203	50.0043
Drop	0.0331	0.0118	43.5624	48.0463
Plant	0.0195	0.0069	44.3317	48.8157

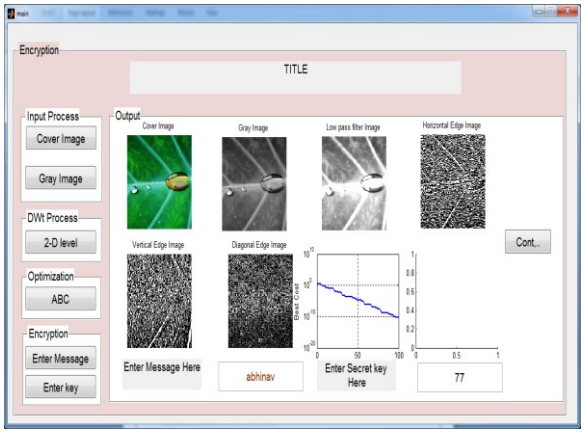


Fig.5 Encryptionresult

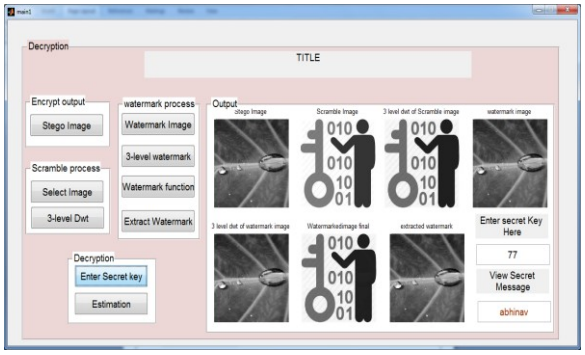


Fig.6Decryption result

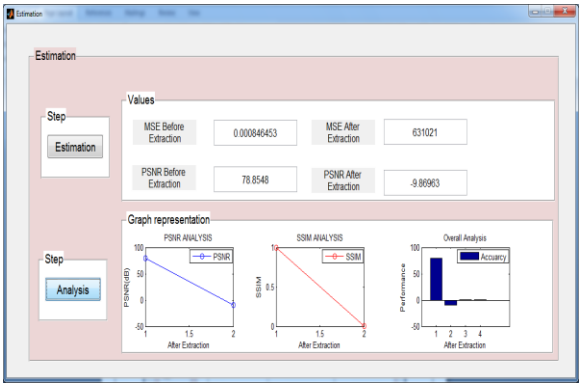


Fig.7Performance metric result

V. CONCLUSION

In this research work demonstrated above, it has been observed to be offering a higher level of security. In steganography, the most important factor is the efficiency with which information is concealed in the cover image. From the obtained MSE and PSNR values, it can be inferred that our proposed algorithm has resulted in a significant improvement, over the traditional DWT based steganography. The mean reduction in MSE is 64.3%. The mean increase in PSNR is 10.13%. The usage of DES serves the purpose of encryption, and ABC algorithm helps in improving the hiding capacity. The advantage of using DWT over other transforms, is that it offers a temporal resolution. The PSNR value is better & MSE value is very less as compared to many of the existing algorithms. This algorithm is also stronger and robust as well as secure compared to other algorithms. No visual defects can be observed from the corresponding stego images. It can also be referred to plannovel algorithms on ways to send diverse language secret texts or images in audio as well as video files with more dynamicity.

REFERENCES

[1] VipulaMadhukarWajgade and Suresh Kumar, "Enhancing Data Security Using Video Steganography", International Journal of

Emerging Technology and Advanced Engineering, Vol.3, No. 4, pp. 549-552, April 2013.

[2] MahwishBano, TasneemM.Shah and Shaheryar Malik, "Improving Embedding Capacity with Minimum Degradation of Stegoimage", International Journal of Basic & Applied Sciences, Vol. 10, No. 06, pp. 30-35, 2010.

[3] Y.K.Lee and L.H.Chen, "High Capacity Image Steganographic Model", Image Signal Process, Vol. 147, No. 3, pp. 288-294, 2000.

[4] Goel, Stuti, Arun Rana, and ManpreetKaur. "A review of comparison techniques of image steganography."Global Journal of Computer Science and Technology 13.4 (2013).

[5] Tiwari, Anjali, Seema Rani Yadav, and N. K. Mittal. "A review on different image steganography techniques." International Journal of Engineering and Innovative Technology (IJEIT) Volume 3 (2014): 19-23.

[6] Christo Ananth, A.S.Senthilkani, Praghash.K, ChakkaRaja.M., Jerrin John, I.Annadurai, "Overlap Wavelet Transform for Image Segmentation", International Journal of Electronics Communication and Computer Technology (IJECCT), Volume 4, Issue 3 (May 2014), pp-656-658

[7] Karaboga, Dervis. An idea based on honey bee swarm for numerical optimization. Vol. 200.Technical report-tr06, ErciyesUniversity, engineering faculty, computer Engineering department, 2005.

[8] Abu-Mouti, Fahad S., and Mohamed E. El-Hawary."Overview of Artificial Bee Colony (ABC) algorithm and its applications."Systems Conference (SysCon), 2012 IEEE International.IEEE, 2012.

[9] Kaur, Amandeep, RupinderKaur, and Navdeep Kumar. "Image steganography using Discrete Wavelet Transformation and Artificial Bee Colony Optimization."Next Generation Computing Technologies (NGCT), 2015 1st International Conference on.IEEE, 2015.

[10] Vinothkumar, N., and T. Vigneswaran. "Steganographic Method Image Security Based on Optimal Pixel Adjustment Process and Integer

Wavelet Transform." International Journal of Advanced Research in Electronics and Communication Engineering 2.3 (2013): pp-261.

[11] Ma, Miao, et al. "SAR image segmentation based on Artificial Bee Colony algorithm." Applied Soft Computing 11.8 (2011): 5205-5214.

[12] Hsu, Ching-Sheng, and Shu-Fen Tu. "Finding optimal LSB substitution using ant colony optimization algorithm." Communication Software and Networks, 2010.ICCSN'10.Second International Conference on.IEEE, 2010.