ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
DOI: 10.17485/ijst/2015/v8iS7/64275
Indian Journal of Science and Technology, *Vol 8(S7), 228–235, April 2015*

A Novel Approach for Color Image, Steganography Using NUBASI and Randomized, Secret Sharing Algorithm

B. Srinivasan[1]*, S. Arunkumar[2] and K. Rajesh[2]

[1]Department of Information Technology, School of Computing, SASTRA University, India;
srinivasan@core.sastra.edu
[2]Department of Computer Science and Engineering, School of Computing, SASTRA University, India;
arunkumar@cse.sastra.edu, rajesh.k@cse.sastra.edu

Abstract

In this paper, we present a new approach for concealing secret message in a digital image by adding three layer securities. In the first layer, the secret image is encrypted by using the famed AES algorithm. In the second layer, we establish a Non-Uniform Block Adaptive Segmentation on Image (NUBASI) algorithm for generating segments of the cover image. This algorithm accept a Key from sender and by using this key, split the cover image into small pieces each with different dimension. In the third layer, a new randomized secret sharing algorithm hide the secret data into the different segments. This algorithm defines 32 different patterns for selecting the segments order to implant the cipher data. This proposed method was implemented and tested for various size cover images and secret messages. The quality of the final stego-image and original image are compared and analyzed through their PSNR values.

Keywords: Cryptography, Image Segmentation, Non-Uniform Block, Randomized Algorithm, Steganography

1. Introduction

Cryptography is used as an information security tool by which the data are encrypted by which the plain meaningful information is converted into the unknown information which contains tousled data. Cryptographic algorithms can be generally classified into two categories of symmetric and asymmetric key algorithms. In the symmetric key algorithms, the same key is used to encrypt and decrypt the information at both sender and receiver end. In Asymmetric algorithm[1] also known as the Public key algorithm, there are two separate keys, private and public keys are used in encryption and decryption. Asymmetric key algorithms require the presence of different key and private key generated for the user has to be kept secretly because once the key is known for an intruder the plain text can easily be retrieved from the cipher text. Many algorithms follow this standard and AES is one of them. The Advanced Encryption Standard (AES)[2] specifies a FIPS (Federal Information Processing Standards) – is a secured cryptographic algorithm which is used in protecting secret information. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information. This new algorithm replaced the old famous encryption algorithm called Data Encryption Standard (DES) in 2001 and now-a-days more and more applications are starting to use AES instead of DES to protect their information security in the past ten years.

Steganography[3–5] and Cryptography[6–10] are equivalent data security techniques and the techniques can be implemented side by side, in fact steganographic system can implement cryptographic data security. Image segmentation[11,12] is used to segment image may be of four types according to different properties of image, i.e., region-based segmentation, boundary- or edge-based segmentation, both region and boundary information,

*Author for correspondence

and thresholding methods[13]. Region based segmentation works on the group of pixel that are related based on some characteristics of an image. Boundary- or edge-based segmentation works on intensity value of the pixel. The boundary or edge can be detected wherever there is an abrupt change in intensity. To exploit the advantages of both the approaches, these two types of algorithms can be integrated to make the new algorithm, third approach. In the fourth thresholding method, the images are segmented based on certain fixed value, threshold.

The present research in the field of information hiding can be generally classified in three sub fields; Spatial domain, Frequency Domain and Adaptive domain methods. In the Spatial domain[9], the way of hiding data is the direct manipulation of the pixel values of a cover medium. In the Frequency Domain techniques, such as DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform), the information is embedded in the transform coefficients of the cover medium. In the Adaptive domain, the model human visual systems are used and exploits assured image characteristics like luminance, corners, edges to embed information in cover medium[14–16]. Least Significant Bit (LSB) substitution[17,18] is most commonly used method that replaces the pixels in the cover image with secret data bits to get stego-image. Here the data to be secured is embedded in the least significant bits of the cover image. The LSB substitution scheme[19] is simple to implement as embedding and extracting processes do not require complex computations.

Wang[20] designed an image hiding technique using optimal LSB substitution and genetic algorithm. In this scheme, the secret data are scrambled by using a one-to-one and onto function to scramble the secret data. This method has one additional advantage, i.e., the quality of the stego-image is satisfactory for a fair degree of payload. However, the scheme suffers from the disadvantage that it requires complex computations. In 2001, Chen[21] has used the greedy algorithm in the data hiding technique. This algorithm uses complex data structures such as weight matrix, cost matrix etc., which makes the system more complex in nature. So this algorithm was having more computational overhead and less stego-image quality.

Wang and Moulin[22] designed a data hiding algorithm through which the messages are embedded into the cover-text in a secure manner. EL-Emam[23] suggested a method to conceal a huge amount of secret information into the RGB color image which protects the well-known statistical and visual attacks and works in efficient way. Munuera[24] related the error correcting codes with the steganographic algorithms which is then used to build the efficient steganographic protocols.

Sajedi and Jamzad[25] proposed a new method called BSS (Boosted Steganography Scheme) which use a preprocessing stage before using steganography algorithms. Qian and Zhang[26] introduced a secure steganography method which is lossless in nature. The secret messages are concealed into the JPEG bitstream by Huffman's code mapping. Qu[27] used the quantum secure direct communication by entanglement swapping of Bell's states in the data hiding method by which he released a new quantum steganography protocol. Lee and Chen[28] suggested a new secure steganography method which uses a special function to deal with the four performance measures i.e., the embedding capacity, the visual quality, the security, and the complexity of the data-embedding algorithm. Lee[29] combines the prediction of difference expansion and the data hiding algorithms by which he presents an adaptive reversible data scheme to improve the embedding capacity.

Wu[30] used a method to obtain the optimal pixel adjustment for enhancing the quality of the stego-image and by which he introduced a secret image sharing algorithm. Phadikar and Maity[31] combine the data-hiding technique with the data modulation to provide the purpose of quality access control of image using Quantization Index Modulation (QIM). El-Emam and Abdul-Shaheed[32] introduce a novel data hiding algorithm by applying the various components such as fuzzy logic, rough sets, genetic algorithms, adaptive neural networks, ant colony, support vector machines etc., of soft computing to the steganography methods to obtain robust, low cost, optimal and adaptive solutions in data hiding problems.

Nameer N. El-Emam and Rasheed Abdul Shaheed AL-Zubidy[33] introduced a new steganography algorithm with the concept of image segmentation to conceal the secret information into the color images. A new segmentation algorithm named Non-uniform Adaptive Image Segmentation (NUAIS) is introduced for splitting the image into various numbers of sub-images. An adaptive neural network with genetic algorithm using uniform adaptive relaxation ANN AGAUAR are used in this method to increase the speed of the training process and to achieve high concealing rate. And this algorithm works against visual and statistical attacks. In order to improve the security of the secret data, with these added security layers, the proposed paper introduce the concept of randomization. The randomization is used in both segmentation and data hiding technique.

2. Proposed Work

The proposed system describes three layer securities for hiding secret message into the cover image. In the first layer, a cipher messages are produced by encrypting the secret message by the eminent encryption standard, Advanced Encryption Standard (AES) by accepting a 128-bit secret key (SEC_KEY). The digital cover image is segmented by using our NUBASI algorithm.

NUBASI, Non-Uniform Block Adaptive Segmentation on Image is an algorithm which produces the number of segments with different dimensions of an input cover image by accepting the same secret key, SEC_KEY. The number and size of segments are fully depends on the input secret key. In the third level, RSS, Randomized Secret Sharing algorithm uses the same key, SEC_KEY for embedding the secret message into the segmented images. The inverse-NUBASI algorithm finally produces the stego-image by merging all the stego-segments. The block diagram for this procedure is shown in Figure 1.

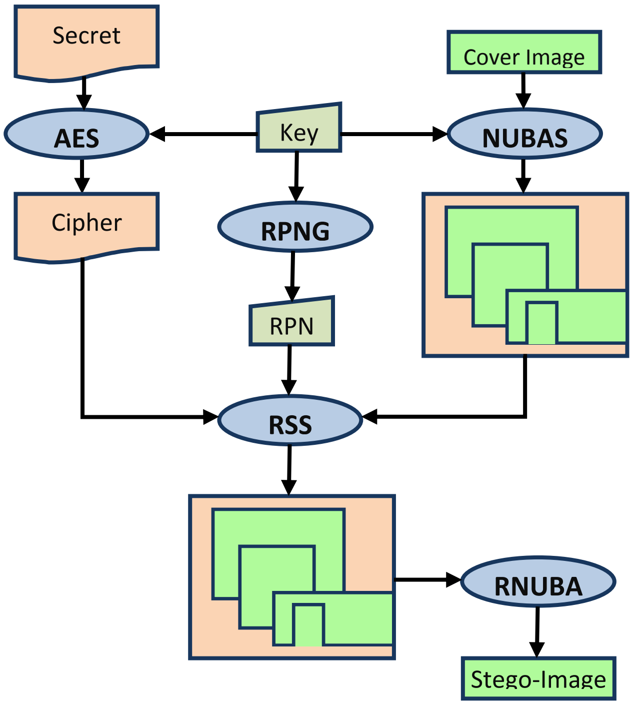


Figure 1. Block diagram for the proposed system.

2.1 NUBASI

Segmentation refers to splitting an image into various numbers of sub images. Based on the size of the sub images, there are two classifications of segmentation, Uniform and Non-Uniform. In uniform segmentation, all the produced segments are having same dimension. But, in the non-uniform segmentation, each and every segment is having different dimension. In this algorithm, a digital cover image with dimension 'M x N' and a 128-bit key are taken as inputs and finally produces T numbers of non-uniform image segments. Here, the key plays a vital role in dividing the image. The algorithm and description are given below. The number T is calculated as T = floor(L/2) * (floor(L/2)+1).

Algorithm NUBASI (Img, SEC_KEY[], Seg[])

***Input:* Img** → A digital cover image with dimension M x N.

SEC_KEY → A list containing sequence of characters with size L.

***Output:* Seg** → A list of segmented images with size T, each with different dimensions, where T is L/2 x L/2.

```
1. Find the Height and Width of the cover image Img, ImgW & ImgH
   ImgW ← Img.Width
   ImgH ← Img.Height
2. Find the Length of the Key, KeyLen
   KeyLen ← Key.Size
3. Split the input Key list into two lists KeyV and KeyH
   splitKey(Key[], KeyV[], KeyH[])
4. Find the Lenth of the KeyV and KeyH, KeyLenH & KeyLenV
   KeyLenH ← KeyV.Size
   KeyLenV ← KeyH.Size
5. Find sum of all the keys in KeyV, SumKeyV
   SumKeyV ← getSum(KeyV[])
6. Find sum of all the keys in KeyH, SumKeyH
   SumKeyH ← getSum(KeyH[])
7. Calculate Partition Percentage, PPV and Pixel Length, PixV for each key in KeyV list
   for i ← 0,1,2,…,LenV-1 do
       $PPV_i = round((KeyV_i / SumKeyV)*100)$
       $PixV_i = round((PPV_i * ImgH) / 100$
   end for
```

```
8. Calculate Partition Percentage, PPH and Pixel Length,
   PixH for each key in KeyH list
   for i ← 0,1,2,…,LenH−1 do
       $PPH_i$ = round(($KeyH_i$ / SumKeyH)*100)
       $PixH_i$ =round(($PPH_i$ * ImgW) / 100
   end for
9. Perform segmentation over the cover image Img as
   $X_1$ ← $X_2$ ← 0
   T ← 0
   for i ← 0,1,2,…, LenH−1 do
       $X_2$ ← $X_1$ + $PixH_i$
       for j ← 0,1,2,…, LenV−1 do
           $Y_2$ ← $Y_1$ + $PixV_j$
           $Seg_T$ ← getSubImage(Img,$X_1$,Y1,$X_2$−$X_1$,
               $Y_2$−$Y_1$)
           T ← T + 1
       end for
       $X_1$ ← $X_2$
       $Y_1$ ← 0
       /*Shift the list PixV left*/
       t ← $PixV_0$
       for k ← 1,2,…,LenV−1 do
           $PixV_{k-1}$ ← $PixV_k$
       end for
       $PixV_{LenV-1}$ ← t
   end for
```

The 16-Byte input key is first divided into two lists, KeyV and KeyH. The KeyV contains the bytes in odd positions of the input key, while the KeyH contains the bytes in even positions of input key.

The partition percentages, for splitting image in horizontal direction (PPH) and vertical direction (PPV) are calculated based on the values stored in KeyH and KeyV. Then, the PPH and PPV values are used to calculate the pixel length in horizontal and vertical directions, PixH and PixV. For the successive columns, the order for the vertical keys is shifted by one value in upward direction. For example, if the vertical keys order for the first column is $\{K_0, K_2, K_4, K_6, K_8, K_{10}\}$, then the order for the second column is $\{K_{10}, K_0, K_2, K_4, K_6, K_8\}$. Finally the T numbers of segmented sub images are generated based on the calculated pixel length. The segmentation on image is shown in Figure 2.

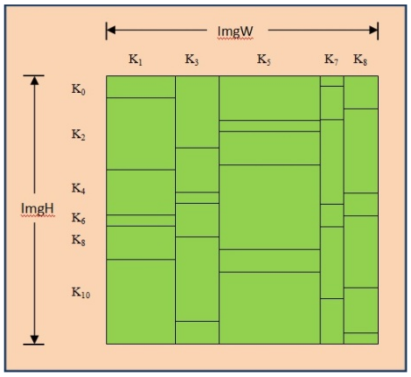


Figure 2. Cover Image Segmentation based on SEC_KEY.

2.2 Randomized Secret Sharing

The non-uniform image segments which are produced by the NUBASI algorithm are numbered as Seg_0, Seg_1, and so on., up to $Seg_{T-1.}$ The cipher message which is generated by the AES algorithm is divided into T-1 numbers of blocks B_0, B_1, B_2, and so on., B_{T-2} with equal size. The segments for each block of message are selected by a random number, RPN. The RPN, Random Pattern Number is a number between 0 to 31 and which is generated by an algorithm Random Pattern Number Generator (RPNG). The same 16-Byte secrete key, SEC_KEY is used in generating the random pattern number. The order in which the segments are selected for embedding cipher message blocks is selected from 32 defined patterns. The order of segments in the row-by-row pattern and the entire 32 patterns are shown in Figure 3 and Figure 4.

The pattern number is first embedded into the first segment, Seg_0. The cipher message blocks B_0 to B_{T-2} are embedded into the remaining image segments by using following randomized secret sharing algorithm, where a random number, RPN is used in selecting the segment order.

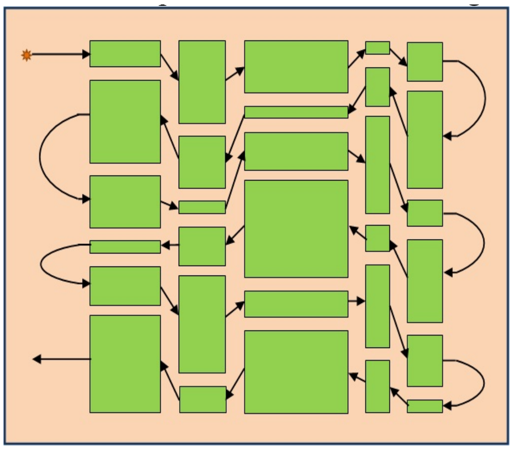


Figure 3. The row-by-row pattern for selecting segments for hiding cipher message blocks.

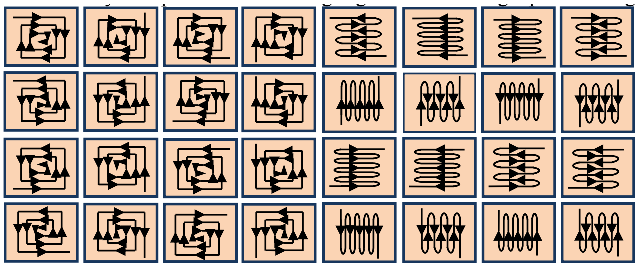


Figure 4. List of all patterns with pattern number 0, 1, 2, . . . , 31.

```
Algorithm RSS ( Seg[], CMsg[], RPN, StegImg )

Input: Seg → A List of cover image segments, $Seg_0$, $Seg_1$,
            $Seg_2$, . . . , $Seg_{T-1}$
      CMsg → Cipher Message with size M
      RPN → A random pattern number from 0 to 31
Output: StegImg → A stego-image embedded with the
secret message.

1. Split the CMsg into 'T-1' numbers of blocks, $B_0$, $B_1$, $B_2$,
   . . . , $B_{T-2}$
2. Embed the RPN into $Seg_0$
      Embed ( RPN, $Seg_0$ )
3. Embed the CMsg blocks into different image
   segments
      for each Blk in $B_0$, $B_1$, $B_2$, . . . , $B_{T-1}$ do
            Choose a segment $Seg_i$ based on RPN
            Embed ( Blk, $Seg_i$ )
      end for
4. Merge all the cover image segments into a single
   image
End RSS
```

```
Algorithm Embed ( Msg[], Img )

Input: Msg → A list containing sequence of bytes
      Img → A cover image with dimension R x C
Output: Img → A image embedded with Msg
Convert the Msg into sequence of bits, $MBit_0$, $MBit_1$,
$MBit_2$, . . . , $MBit_N$
i ← 0
j ← 1
Repeat while i < N
      For r in 0, 1, 2, . . ., R
            For c in 0, 1, 2, . . . C
                  getPixel ( Img, r, c, P )
                  getRGB ( P, R, G, B)
                  storeBit(B, 8-j, MBiti)
                  storeBit(G, 8-j, MBiti+1)
                  storeBit(R, 8-j, MBiti+2)
                  setRGB(P, R, G, B)
                  setPixel ( Img, r, c, P)
                  i ← i+3
            end for
      end for
      j ← j + 1
end while
```

The proposed system uses 24-bit cover image for embedding secret message. Each pixel in the segmented image is composed of 3 bytes, each for representing the colors red, blue and green respectively. This algorithm uses one of the most popular steganographic techniques called Least Significant Bit replacement. In each pixel, this algorithm hides minimum 3 bits, each in blue, green and red respectively and maximum of 12 bits. First the LSB of each byte is selected and is replaced by the bit of encrypted secret message. This algorithm allows maximum of 4 bit-changes in each byte of the cover image. When number of bits in the input message block exceeds the number of bytes in the input segmented image block, the bit next to the LSB is continued for the rest of the bits of secret message, as shown in Figure 5. After embedding the message into the image segments, the Reverse Non-Uniform Block Adaptive Segmentation on Image (RNUBASI) algorithm is used in merging all the stego-image segments to produce the final stego-image. This algorithm is absolutely the reverse of NUBASI which is used in segmenting the image.

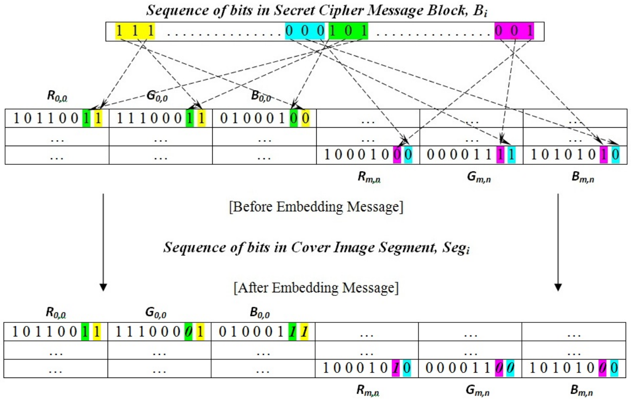
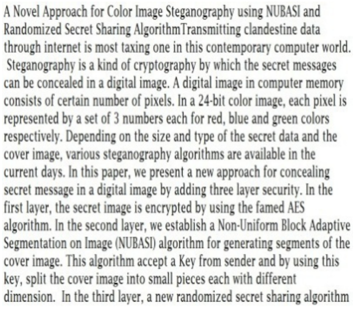
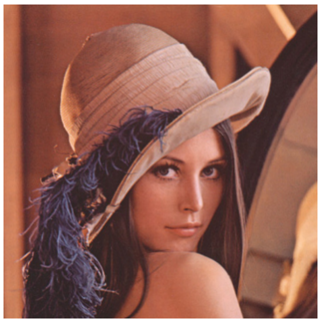
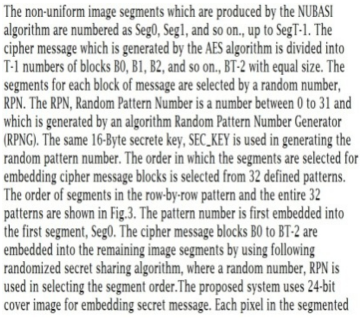
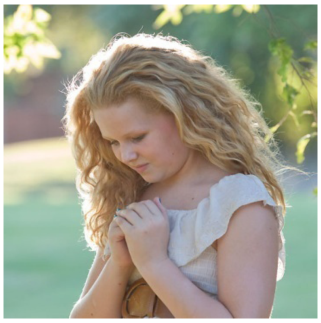
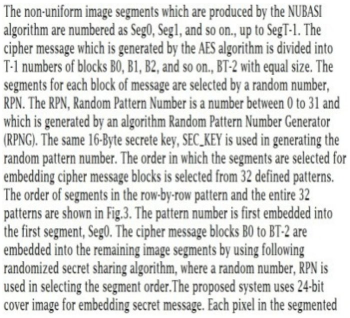
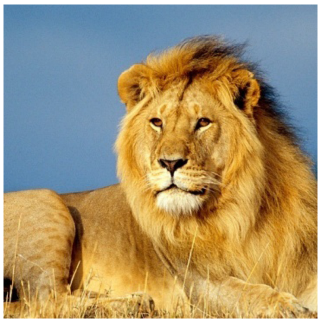


Figure 5. Embedding secret cipher message block into cover image segment.

3. Experimental Result and Discussion

For any data hiding system, there are three important requirements to be fulfilled, security, robustness and imperceptibility. In the proposed system, the security is enhanced through three levels of embedding message. First of all, the famous 128-bit Advanced Encryption Standard algorithm encrypt the input secrete message. A new powerful segmentation algorithm, NUBASI, give the non-uniform segmented images with unpredictable size. Finally, a randomized secret sharing algorithm chooses the segments order based on a secret random number. There are totally 32 numbers of patterns (segment order) defined by the proposed scheme. The beauty of this method is for all these three levels, a same 128-bit secret key is used. The cipher text, number of segments, size of each segments and random segment order are entirely depends on this secret key. The security of our proposed method depends on this secret key, which should be shared between the sender and receiver of the stego-image. There are many standard image quality metrics available now a day for comparing the quality of the stego-image with the host image. The efficiency of the proposed scheme has been

Table 1. Experimental result for the proposed system

Cover Image (512 x 512)	Secret Message	Stego-Image	PSNR (dB)
 Lena	 A Novel Approach for Color Image Steganography using NUBASI and Randomized Secret Sharing AlgorithmTransmitting clandestine data through internet is most taxing one in this contemporary computer world. Steganography is a kind of cryptography by which the secret messages can be concealed in a digital image. A digital image in computer memory consists of certain number of pixels. In a 24-bit color image, each pixel is represented by a set of 3 numbers each for red, blue and green colors respectively. Depending on the size and type of the secret data and the cover image, various steganography algorithms are available in the current days. In this paper, we present a new approach for concealing secret message in a digital image by adding three layer security. In the first layer, the secret image is encrypted by using the famed AES algorithm. In the second layer, we establish a Non-Uniform Block Adaptive Segmentation on Image (NUBASI) algorithm for generating segments of the cover image. This algorithm accept a Key from sender and by using this key, split the cover image into small pieces each with different dimension. In the third layer, a new randomized secret sharing algorithm Sec_Msg_1	 Lena_Stego	67.2323
 Baby	 The non-uniform image segments which are produced by the NUBASI algorithm are numbered as Seg0, Seg1, and so on., up to SegT-1. The cipher message which is generated by the AES algorithm is divided into T-1 numbers of blocks B0, B1, B2, and so on., BT-2 with equal size. The segments for each block of message are selected by a random number, RPN. The RPN, Random Pattern Number is a number between 0 to 31 and which is generated by an algorithm Random Pattern Number Generator (RPNG). The same 16-Byte secrete key, SEC_KEY is used in generating the random pattern number. The order in which the segments are selected for embedding cipher message blocks is selected from 32 defined patterns. The order of segments in the row-by-row pattern and the entire 32 patterns are shown in Fig.3. The pattern number is first embedded into the first segment, Seg0. The cipher message blocks B0 to BT-2 are embedded into the remaining image segments by using following randomized secret sharing algorithm, where a random number, RPN is used in selecting the segment order.The proposed system uses 24-bit cover image for embedding secret message. Each pixel in the segmented Sec_Msg_2	 Baby_Stego	63.5600
 Lion	 The non-uniform image segments which are produced by the NUBASI algorithm are numbered as Seg0, Seg1, and so on., up to SegT-1. The cipher message which is generated by the AES algorithm is divided into T-1 numbers of blocks B0, B1, B2, and so on., BT-2 with equal size. The segments for each block of message are selected by a random number, RPN. The RPN, Random Pattern Number is a number between 0 to 31 and which is generated by an algorithm Random Pattern Number Generator (RPNG). The same 16-Byte secrete key, SEC_KEY is used in generating the random pattern number. The order in which the segments are selected for embedding cipher message blocks is selected from 32 defined patterns. The order of segments in the row-by-row pattern and the entire 32 patterns are shown in Fig.3. The pattern number is first embedded into the first segment, Seg0. The cipher message blocks B0 to BT-2 are embedded into the remaining image segments by using following randomized secret sharing algorithm, where a random number, RPN is used in selecting the segment order.The proposed system uses 24-bit cover image for embedding secret message. Each pixel in the segmented Sec_Msg_3	 Lion_Stego	60.2777

evaluated through the PSNR values stego-images. PSNR stands for Peak Signal to Noise Ratio is calculated by

$$PSNR = \frac{10 \times \log_{10}(2^n - 1)^2}{MSE} = \frac{10 \times \log_{10}(255)^2}{MSE}$$

where, MSE is the Mean-Square Error between the original and the stego images. For a host images with mensions are W and H, MSE is defined as:

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} (X_{i,j} - Y_{i,j})^2$$

The proposed system is implemented and tested for the various cover images and secret messages. For the test, we given a 24-bit Lena cover image with dimension 512x512 and a secret text with size 2.5 KB. The result shows that the PSNR for the input cover image and the produced stego-image is above 50 by average. For the Lena image, the PSNR is 67.2323. We got this result by the powerful steganographic algorithm added with three layer security with a single secret key. The proposed system test result for three different images with their PSNR values are shown in Table 1.

4. Conclusion

A new approach for the color image steganography with added 3-layer security has been presented in this paper. A new non-uniform segmentation algorithm has been designed named Non-Uniform Block Adaptive Segmentation on Image (NUBASI) to produce some numbers of segmented images with various dimensions. The Advanced Encryption Standard (AES) algorithm is used in generation of cipher secret message. The security of the algorithm is improved by defining 32 numbers of patterns on segmented images for choosing the order of segments for which the secret message has to be embedded. A random pattern is selected by an algorithm Random Pattern Number Generator (RPNG). The well-known LSB replacement method is used for embedding the secret message. A single 128-bit secret key is used in all the three security level such as encrypting message, segmenting image and choosing the segments order. This algorithm has been implemented and tested for various cover images and secrete messages. The experimental result shows that the proposed method gives very good PSNR values of the original image and the stego-image.

5. References

1. Yuan H-D. Secret sharing with multi-cover adaptive steganography. Inform Sci. 2014; 254:197–212.
2. Farashahi RR, Rashidi B, Sayedi SM. FPGA based fast and high-throughput 2-slow retiming 128-bit AES encryption algorithm. Microelectron J. 2014; 45:1014–25.
3. Wu N-I, Hwang M-S. Data hiding: current status and key issues. Int J Netw Secur. 2007; 4:1–9.
4. Qazanfari K, Safabakhsh R. A new steganography method which preserves histogram: Generalization of LSB++. Inform Sci. 2014; 277:90–101.
5. Ramalingam M, Isa NAM. A steganography approach over video images to improve security. Indian Journal of Science and Technology. 2015 Jan; 8(1):79–86.
6. Laskar SA, Hemachandran K. High capacity data hiding using LSB steganography and encryption. IJDMS. 2012; 4:57–68.
7. EL-Emam NN. Hiding a large amount of data with high security using steganography algorithm. J Comput Sci. 2007; 3(4):223–32.
8. Guo Y, Sengür A. A novel image segmentation algorithm based on neutrosophic similarity clustering. Applied Soft Computing. 2014; 25:391–8
9. Peng R, Varshney PK. A human visual system-driven image segmentation algorithm. J Vis Commun Image R. 2015; 26:66–79.
10. Sridhar KP, Saravanan S, Sai RV. Countermeasure against side channel power attacks in cryptography devices. Indian Journal of Science and Technology. 2014 Apr; 7(S4):15–20.
11. Rajanbabu DT, Raj C. Multi level encryption and decryption tool for secure administrator login over the network. Indian Journal of Science and Technology. 2014 Apr; 7(S4):8–14.
12. Sasi SB, Sivanandam N. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015 Feb; 8(3):216–21.
13. Ghebleh M, Kanso A. A robust chaotic algorithm for digital image steganography. Commun Nonlinear Sci Numer Simulat. 2014; 19:1898–907.
14. Parah SA, Sheikh JA, Hafiz AM, Bhat GM. Data hiding in scrambled images: a new double layer security data hiding technique. Comput Electr Eng. 2014; 40:70–82
15. Kanan HR, Nazeri B. A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Syst Appl. 2014; 41:6123–30.
16. Valarmathi, Nawaz GMK. Secure data transfer through audio signal with LSA R. Indian Journal of Science and Technology. 2015 Jan; 8(1):17–22.

17. Digital image steganography using nine-pixel differencing and modified LSB substitution gandharba swain. Indian Journal of Science and Technology. 2014 Sep; 7(9):1444–50.
18. Swain G. Digital image steganography using nine-pixel differencing and modified LSB substitution. Indian Journal of Science and Technology. 2014; 7(9):1444–50.
19. Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. Pattern Recogn. 2004; 37:469–74.
20. Wang RZ, Lin CF, Lin JC. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recogn. 2001; 34:671–83.
21. Chen CC, Min HL, Yu CH. A fast and secure image hiding scheme based on LSB substitution. Int J Pattern Recogn Artif Int. 2002; 16:399–416.
22. Wang Y, Moulin P. Perfectly secure steganography: capacity, error exponents, and code constructions, information theory. IEEE Trans Inform Theor. 2008; 54(6):2706–22.
23. EL-Emam N. Hiding a large amount of data with high security using steganography algorithm. J Comput Sci. 2007; 3(4):223–32.
24. Munuera C. Fast communication steganography and error-correcting codes. Signal Process. 2007; 87(6):1528–33.
25. Sajedi H, Jamzad M. Boosted steganography scheme with cover image preprocessing. Expert Syst Appl. 2010; 37(12):7703–10.
26. Qian Z, Zhang X. Lossless data hiding in JPEG bitstream. J Syst Software. 2012; 85(2):309–13.
27. Qu Z, Chen X, Zhou X, Niu X, Yang Y. Novel quantum steganography with large payload. Optic Comm. 2010; 283(23):4782–6.
28. Lee, C-F. (). A novel data hiding scheme based on modulus function. J Syst Software. 2010; 83(5):832–43.
29. Lee C-F, Tso H-K. Embedding capacity raising in reversible data hiding based on prediction of difference expansion. J Syst Software. 2010; 83(10):1864–72.
30. Wu C, Kao S, Hwang M. A high quality image sharing with steganography and adaptive authentication scheme. J Syst Software. 2011; 84:2196–207.
31. Phadikar A, Maity S. Data hiding based quality access control of digital images using adaptive QIM and lifting. Signal Process Image Comm. 2011; 26:646–61.
32. El-Emam N, Abdul-Shaheed R. Computing an adaptive mesh in fluid problems using neural network and genetic algorithm with adaptive relaxation. Int J Artif Intell Tool. 2008; 17(6):1089–108.
33. El-Emam NN, Abdul Shaheed AL-Zubidy R. New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm. J Syst Software. 2013; 86:1465–81.