Multimedia Tools and Applications (2020) 79:3893–3911
https://doi.org/10.1007/s11042-019-7471-1

A stegano - visual cryptography technique for multimedia security

K. Gurunathan[1,2] · S. P. Rajagopalan[3]

Received: 31 October 2018 / Revised: 13 February 2019 / Accepted: 7 March 2019 /
Published online: 22 March 2019

Abstract

Owing to the increasing growth in digital communication as well as the multimedia applications, security has now become a very significant problem in the communication as well as storage space of such images. The Visual Cryptography (VC) has been used for hiding the information that are in the images which is a special technique of encryption that is decrypted by a human visual system. In this paper, a technique for embedding a secret message within that of a cover-image to ensure the interceptors will not observe the presence of such hidden data is presented. The method has an essential conception by means of a simple Least Significant Bit (LSB) substitution. Being inspired by the steganography approach, the current work splits the cover images into n blocks of 8X 8 pixels and into a secret message of n partitions in order to improve the image quality and to increase the capacity of secret message along with its security level. For the purpose of improving this stego-image quality and for increasing the capacity of secret message along with its security level, being inspired by the current work that splits cover images into the n blocks of 8X 8 pixels and into a secret message of n partitions. In the proposed method, the Cuckoo Search (CS) is used for searching an approximate and optimal solution of finding any optimal substitution matrix to transform the message in every block as opposed to finding a single optimal matrix for substitution and the entire cover-image is presented. The final quality of its resulting in the stego-image, and its secret message and its capacity with the level of security of this method proposed will be calculated and then comparted to the other different methods. The results of the experiment proved that the proposed method outperformed all the Joint Photographic Experts Group (the JPEG) and the Joint Quantization Table Modification (the JQTM) based method in terms of quality of image, security level and embedding capacity.

Keywords Steganography · Information hiding · Multimedia · Visual cryptography (VC) · Joint photographic experts group (JPEG) · Joint quantization table modification (JQTM) and cuckoo search (CS) algorithm

✉ K. Gurunathan
iamalsoguru01@gmail.com

Extended author information available on the last page of the article

1 Introduction

The Information transmission by the internet includes some sensitive personal data that can also be intercepted. Furthermore, there can be applications and various web sites will need the users to fill some forms with perceptive personal information which are the name, the address, the credit card information and telephone numbers. Therefore, users will require some private as well as secure communications for several reasons for protecting secret information from the hackers that is surpassed over another open channel to ensure privacy along with its data integrity for protecting against the unauthorized access or use. The Cryptography as well as the steganography will be the very common methods for securing communications [25].

The Multimedia content contains images, the videos and the audio files. The images will be the very based on such visual multimedia. The videos will be image streams that are displayed in a sequence of a particular speed. It focuses on the image files for achieving this visual steganography. These images will be visual data that are stored within the picture frame and are made up of different regions that contain pixels. The pixels contain three of the basic colours which are Red (R), Green (G) and Blue (B). These pixel values (the R, G, B values) may be further manipulated for hiding data within these images. There can be a marginal deviation within pixel values which will not modify the images but will have a small shade variation in its changed region which may not be able to be seen in those circumstances that are normal. This image will thereby serve as the cover for information that can achieve stenography. The image that is edited may be transmitted along with that of the original image to the receiver. A receiver further decodes data which is from this image by comparing the pixel based images. The process also includes encoding along with decoding with a blend of the media based cryptography as well as asymmetric and cryptographic algorithms [12].

Cryptography is that science of making use of mathematics for encrypting and decrypting data for keeping the messages secured by means of changing intelligible data form (the plain text) into an unintelligible form (the cipher text). Cryptography originated from “kryptós” a Greek word that stands for “hidden” and the word “gràphin” that stands for the word “writing”. So the right meaning of the term cryptography means “hidden writing”. Such cryptosystem contains the plaintext, the encryption algorithm, the decryption algorithm, the cipher text, along with the key. The Plaintext will further either the message or even the data which are both normal as well as readable. The encryption will be that process that can convert such plaintext to its cipher text using this key. There is a Cipher text that effects from such encryption by the method of applying such an encryption key which is on the plaintext. The decryption is however, the actual procedure of retrieval of that of the plaintext back from its cipher text. There is also a key that is used for controlling its cryptosystem (the cipher system), and this is further known only by either the sender or the receiver. This cryptography will be extremely powerful for the securing of such data; the cryptanalysts may also be able to succeed in breaking ciphers for the purpose of analysing the contents of the cipher to receive plaintext [4].

This current global explosion based upon the utilisation of the internet and the multimedia has been raising the need for the hiding of data. This was able to encourage the professionals of data hiding in increasing the efforts of data safety for any information that make use of electronic media for moving from place to place. Steganography is that science and art that conceals data by means of installing them into the other which are innocuous messages. This comes from a Greek work that denotes “covered writing”. The main aim here for steganography will be the concealing of the message and its existence that produces one secret channel. There are several other issue based on the secrecy of such confidential data more importantly

medical data. Such issues will be answered by means of providing one more secured technique known as steganography [3]. Steganography along with cryptography is in high demand for secured data today because intruders managed in detecting the presence of secret data in a format that is encoded to be able to read the exact message that can be very tedious [13].

Steganography may be further classified into either pure or a secret key steganography. The pure steganography is that system of steganography that does not need any swap to be made of that of the secret key. The Embedding process (E) may be also explained to be a mapping E: C x M → S, in which the C will be the possible cover medium set and M the secret message; S will denote the Stego-medium. The process of extraction contains mapping D: S → M, C; the extracting of a secret message out of a stego-medium. The secret key steganography is that system of steganography needing a prior exchange of a secret key. The Embedding process (E_k) may be described to be mapping E_k: C x M x K → in which C denotes the set of cover-medium and the M the secret message; S denotes the Stego-medium, K being the secret key that is used for embedding this secret message. The course of extraction will contain mapping D_k → C, M; the extorting of a secret message out of its stego-medium [20].

VC is that secret sharing technique which had been suggested by Moni Naor along with Adi Shamir in the year 1994, in which information was encrypted in a manner in which their decryption was carried out using human visual system. Being in contrast to the methods of general security that will tend to hide some information by the applications of the mathematical secret transformation. The Visual Cryptography Scheme (the VCS) will store the top secret to be an image and VC will be to encrypt the Secret Image (SI) within some n shares. This decryption will need the stacking of the n shares on one another. It will be impossible to be able to be retrieved such secret information from the n-1 shares of these images. The pixel positions are p[0, 1] to p[0, 7] in row 0, p[1, 0] to p[20, 25] in row 1, p[2,0] to p[2, 5] in row 2, p[3,0] to p[3, 4], p[4,0] to p[3, 4], p[5,0] to p[12, 13], p[6,0], p[6,1] and p[7,0].

In the VC, reconstructed images after the process of decryption can encounter some major problems. The quality of image of such reconstructed images may not be quite same as their original image owing to the expansion of the pixel [21]. The efficiency of the VCS algorithm is an important factor and it has to be reliable in such a way that the intruders cannot read its original image. An important functional need for a VCS system based on the share size that will be similar to its original image for preventing doubt for an unauthorized user [10].

Both steganography and VC are considered to be a different topic for the image security and using steganography in combination to the VC will be a sturdy model adding many challenges of identifying some hidden and encrypted data. Finally, at the time these encrypted shares get reassembled or also decrypted for redesigning their genuine images it may be possible to have an exposed image that can contain some confidential type of data. These types of these algorithms may not persist without possessing some suitable characteristics within this VC procedure. The main ground for such a method of rebuilding that will change in accordance with the encrypted information will make a system feasible to extract encrypted data from an exposed image [9].

The Multimedia steganography is a recent as well as a secure form of stenography. This had actually began in the year 1985 which was after the advent of that of the personal computer which is adapted to all such classical issues in stenography. The Visual steganography had been widely practised and also done with some image files. It also began with the secret messages that are in the lowest bits of the noisy images or even that of the sound files. These images that are present in different formats like the jpeg may also have a very extensive colour spectrum not reflecting any type of distortion for the embedding of such data. It further

performs the steganography on all the image files and will also hide the encrypted images within their encrypted format ensuring the achieving of various cryptographic systems. Another most commonly used technique that is present in image steganography will be the bit insertion wherein the LSB of the pixels are modified. The other techniques may also involve this type of a spread spectrum, the patch work, along with the JPEG based compression and so on. As opposed to the traditional and LSB encoding, this makes use of a modified technique of bit encoding for achieving the image steganography where the pixel will only store one byte of the data [6].

The JPEG-JSTEG is one recognized tool for industrial information hiding [26]. This will replace the LSB for the quantized Discrete Cosine Transform (the DCT) coefficients having secret messages. But this message capacity of the JPEG-JSTEG will be much restricted. For increasing the secret capability of message which is proposed there is the Joint Quantization Table Modification (the JQTM) method that is depending upon a variation of the standard type of JPEG quantization table with the secret messages that are embedded within DCT coefficients frequency of every 8 * 8 block. This capacity of hiding of this JQTM will be more on being evaluated to that of the JPEG-JSTEG; but, there are lesser (limited to 6) quantized the DCT coefficients which are for every block for hiding this secret message. One more restriction of the system is that is has a low level of security. For increasing this capability of the JQTM further and for mitigating the shortcomings of the JQTM, a proposal was made by Li et al. in 2007, a JPEG and steganography method based on the CS algorithm. For this approach, the table of quantization that was used in the JQTM was modified further for increasing the secret message capacity. The rest of the investigation has been organized thus. The related work in literature is discussed in Section 2. Section 3 explains all methods used for work. Section 4 discusses the final results of that of the experiment and the conclusion is duly made in Section 5.

2 Related works

Rani et al., [23] had proposed another novel approach for that of multimedia data security by means of integrating the steganography as well as the VC aiming to improve efficiency, reliability and security. This technique has two phases. The first for hiding the message in a dynamic manner within a cover image 1 by making a change to the number that was hidden in the RGB channels based upon indicate value. These VC systems will hide a cover image 2 into two and at times even more images known as shared. In the next phase there are two shares created form cover image 2 and a stego image is created for the two shares. These shares will be kept safe as they do not show anything on the content of multimedia. A cover image 2, stego image with a hidden message is recovered form shares with no involvement of complex computation. The results of the experiment proved that this new scheme was simple and can retrieve several contents of multimedia with a high security level.

The rapid growth in the field of E-Commerce market that has been seen in the current times and the increasing demand for online shopping debit or credit card frauds etc. are main distress for the customers and banks more so for Card Not Present (CNP). Roy and Venkateswaran [24] had presented another new approach for the provision of limited information that can safeguard customer data and the increase in the customer confidence and also prevention of identity theft. This method makes use of the combined application of such steganography and also the VC for such a purpose.

Muhammad et al., [17] had further proposed another more secure crystographic framework that had been used for the purpose of authenticity of all these visual contents by means of making use of the image stenography and also by using the transformation colour models, their Three-Level Encryption Algorithm (the TLEA), and finally the Morton Scanning (MS)-directed Least Significant Bit (the LSB) substitution. This particular system makes use of that of the I-plane of the input image within the Hue-Saturation-Intensity (the HSI) for the secret data embedding which was by using the MS-directed LSB substitution method. Moreover, any of the secret data which was encrypted by the TLEA before the actual embedding, thus adding to the additional level of security or also the secure authentication. All the results qualitative as well as quantitative can confirm a great performance of this system and further provided better mechanisms to prove the authenticity of the visual contents of the social network.

Muhammad et al., [18] had proposed another safe image steganographic framework that was based upon the Stego Key-directed Adaptive LSB (SKA-LSB) and the method of substitution using multi-level cryptography. In this scheme the stego key was encrypted by the Two-Level Encryption Algorithm (the TLEA); a secret data will be encrypted by using a Multi-Level Encryption Algorithm (the MLEA), and an encrypted information will be embedded within its host image with an adaptive method of LSB substitution which depends on the MLEA, the sensitive contents, the red channel and secret key. All the quantitative along with the qualitative results of the experiment proved that such a framework could maintain a balance that is better than its proposed framework which can maintain a balance between the quality and security of the image. This achieves a reasonable payload having less complexity confirming its effectiveness on being compared to the other techniques that are state-of-the-art.

Muhammad et al., [15] further proposed another novel Magic LSB Substitution Method (the M-LSB-SM) for the RGB images. This system that was proposed has been based upon the achromatic component (I-plane) of its HSI colour model along with the Multi-Level Encryption (the MLE) which was in a spatial domain. Its I-plane had been partitioned into about four different sub-images of an equal size that can rotate each sub-image having another diverse angle by means of making use of its secret key. All secret information had been divided into four of the blocks that were encrypted by means of using the MLEA. Each such sub-block which was embedded within a rotated sub-image based upon a pattern that had a magic LSB substitution. These results of this experiment could validate the method being able to improve the visual excellence of their stego images that provided some imperceptibility that had several levels of security while being compared to all the other methods.

Muhammad et al., [14] had also further presented one more proficient system for their RGB images that had been based on a Grey Level Modification (the GLM) and the MLE. One secret key with secret data had been encrypted by an MLEA prior to mapping of it to the grey-levels of cover images.

After this, there was a function of transposition which is applied on that of the cover image ahead of data hiding. Using transpose, MLE, GLM and secret key will add some security to this algorithm thus making it challenging for any malicious user for extracting any original secret information. This method had been evaluated both quantitatively as well as qualitatively and the results on comparison proved that it enhances the stego image quality and provided multiple security levels as well.

Muhammad et al., [16] further proposed another adaptive LSB substitution based method that used uncorrelated colour space, which increased the imperceptibility property minimizing changes of detection using the system of human vision. In this scheme, an input image had been passed through the image scrambler, which resulted in the encrypted image that can

preserve privacy of image contents converting them to the HSV colour space to be processed. These secret contents will be encrypted by using Iterative Magic Matrix Encryption Algorithm (the IMMEA) giving better security and producing cipher contents. The adaptive LSB method of substitution was used for embedding this encrypted data within the V plane of the model of HSV colour that was based upon the mechanism of secret key-directed block magic LSB.

Owing to the expansion of the resolution of such decrypted image will diminish. Rani and Mary [22] had presented a visual perception of decrypted images that are improved by subjecting the VC based allocates which are to the Particle Swarm Optimization (the PSO) based technique of image and his improvement. This can improve the sharpness and quality of the image to a considerable extent. A fitness function that is suitable may be applied for optimizing problems with a large dimension that can produce some excellence solutions. The consequences of this intended method had been evaluated to the other techniques of image enhancement to prove both qualitative and quantitative effectiveness. This algorithm will guarantee a highly safe, very quick and also secure transmission of quality of the secret image without any mathematical operations. Shankar and Lakshmanaprabu [27] had utilized this Homomorphic Encryption (HE) having an optimal key selection used for image security. In this the equalization of the histogram was introduced for the purpose of altering all the image intensities and to improve its contrast. For increasing its security level inspired the Ant Lion Optimization (the ALO) in which the function of fitness to be the max entropy of the best one among the encrypted images shown as the image that has an astounding entropy which is among the adjacent pixels. The analysis of the outcomes form all the outcomes of experiments can accomplish an abnormal state with great amount of strength compared to the other strategies.

Prema and Natarajan [19] further proposed an ideal approach for the LSB based steganography that made use of Genetic Algorithm (the GA) with VC. This original message will be converted as a cipher text by means of a secret key and then that is hidden into this LSB of the original image. The GA and VC were used for security enhancement and the GA for modifying pixel location and detection of a message which is difficult. The VC further is used for encrypting its visual information. This was achieved breaking images into two of the shares that are based upon this threshold. This system that is proposed which is tested by the making of steganalysis and the performing of the benchmarking test which is for an analysis of parameters like the Mean Squared Error (the MSE) and the Peak Signal to Noise Ratio (the PSNR). The intend of the work will be to design an enhanced as well as secure algorithm using steganography with the GA and the VC for ensuring an improved security as well as reliability.

Geetha et al., [8] proposed a VC which had 3 phases: Separation of color bands, Generation of numerous shares and Optimal encryption and decryption. Oppositional Gray Wolf Optimization (OGWO) based Elliptic Curve Cryptographic (ECC) approach were used for optimizing the technique. Input color image is separated into R, G and B band and then multiple image shares is obtained using pixel measures. These are partitioned into blocks and decrypt the original image using the optimal key generated by the OGWO algorithm.

Walia et al., [28] introduced a novel stego-key using LSB substitution scheme which offered high embedding capacity and robust against distortion. LUDO scan technique is used improving embedding capacity.

3 Methodology

For this work, increasing the capacity or message of this JQTM it proposed the steganographic method. And this method was inspired by an optimal LSB substitution that transformed secret

messages having an optimal matrix of substitution later embedding the transformed results within its cover image. The method of spatial domain is opted because it improves the quality of the image whereas using frequency domain improves the robustness of the stego-image. As opposed to investigate for an optimal substitution matrix using GA the work employs a CS algorithm.

3.1 Jpeg-Jsteg and JQTM method

Jpeg-Jsteg is that distinctive type of a steganographic algorithm that uses a JPEG file as its cover-image. It has an embedding a scheme that is described briefly as below. Firstly, the Jpeg-Jsteg partitions will be the cover-image into some blocks that are non-overlapping of about 8 * 8 pixels, using the DCT for transforming every block into the DCT coefficients [2]. These DCT coefficients will be scaled in accordance with a standard quantization table of the JPEG that is shown in fig. 1. Secondly, the Jpeg-Jsteg that encrypts these messages and will embed this encrypted messages within the LSBs of all the quantized DCTs based coefficients that do not have values that are not 0, 1, or − 1. This embedding sequence which is utilized in the Jpeg-Jsteg will be in the scan of zigzag based order as listed in Fig. 2 [11].

In the Jpeg-Jsteg, a quantized DCT based coefficients are generally zero and for addressing this capacity based problem, Chang et al. [5] had suggested another steganographic system that was based upon JPEG and the JQTM. This JQTM method will modify this standard JPEG based quantization table. In which the 26 coefficients that are placed in its middle-frequency that are set to be equal to 1. These secret messages will be later embedded in the least two-significant bits of a quantized middle-frequency of the DCT coefficients for every block [5].

3.2 Proposed cuckoo search (CS) algorithm

In this, the proposed CS algorithm will contain some procedure as depicted below:

3.2.1 The embedding procedure

In cases of a frequency-domain, a JPEG will be a very popular image standard in the Internet. In case it is applied to a JPEG based image for data hiding to ensure that a stego image is not

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Fig. 1 JPEG standard quantization table

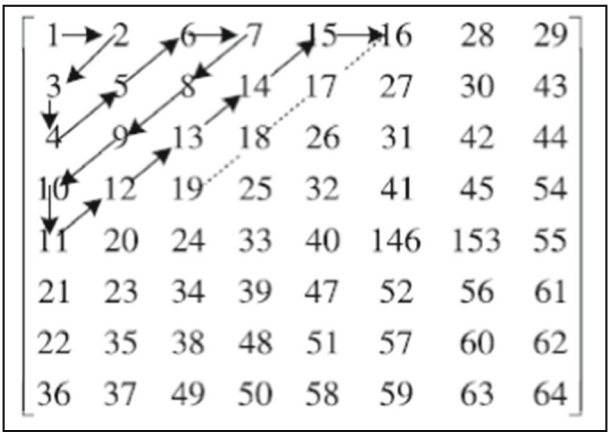

Fig. 2 Zigzag scan order

expected and the Fig. 3 depicts the procedure of embedding for this method. This procedure contains five different phases. They are the message encryption, the image pre-processing, the secret message and its embedding, the JPEG entropy coding, and the stego-image generation of the JPEG [29].

In its first phase, it will develop a CS algorithm for selecting this matrix of optimal substitution, M and this will use this matrix for transforming such secret messages.

In its second phase, this proposed method makes use of the JPEG image and its pre-processing method on the cover image. It will partition the cover image O within the non-overlapping various blocks of about 8 * 8 pixels, and after this it is uses the DCT for transforming every block within the DCT coefficients. The table is found to be notably very different from a quantization table belonging to the JPEG. This is owing to the fact that the secret message that is embedded within the middle-frequency which is a part of such quantized DCT coefficients. In case it has been used for the same table of quantization as per Fig. 1 for quantizing and de-quantizing the DCT coefficients, the quantized DCT coefficients are

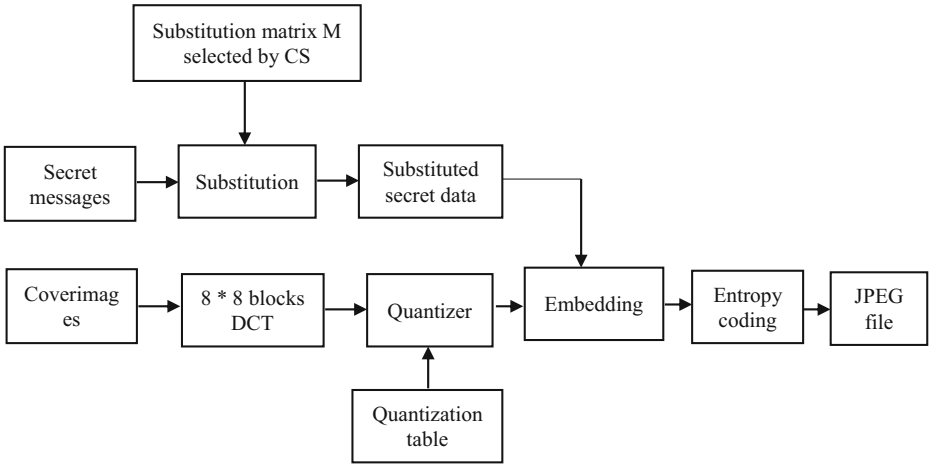

Fig. 3 The diagram of embedding procedure

amplified and its reconstructed new image goes through plenty of distortion. On the basis of this table, these secret messages are reserved and may not be distorted.

In its third phase, it will embed these messages that are substituted from that of the first phase into consequent quantized DCT coefficients for each block. The embedding order of every block and in each one of the block secret messages are embedded within 36 coefficients in the DC-to-middle ranges of frequency. It will embed k secret bits within the least k significant bits for every such coefficient in which k depends on the dimension of the secret messages and here it is set as $k = 2$.

In its fourth phase, once there is a secret message has been embedded into every block, it will employ a JPEG entropy coding (containing the Huffman coding, the Run-Length coding, and the DPCM) for compressing every block. For every such block once entropy coding is done a JPEG file containing the table of quantization with a few compressed data. These are the stego-image which satisfies a JPEG and its standard.

In its fifth phase, this JPEG file and its substitution matrix known as M will be transferred over to their receivers.

3.2.2 The extracting procedure

The process of extraction for this method from the side of the receiver is shown in Fig. 4 [1].

Here in this method the process of extraction has three different phases. The first being JPEG entropy and decoding, second phase being the extracting of secret message, its last and final phase being the decryption of its secret message.

Step 1: Once the JPEG file is received and M the substitution matrix, a receiver will use the decoding of entropy to decode a JPEG file and every 8 * 8 block may be so recuperated.

Step 2: Extraction of their secret bits from that of the 36 different coefficients of every block. This extorting order will be the similar as that of their embedding process.

Step 3: Using a transpose of the M for substituting these extracted messages for obtaining an original secret message with the stego-image.

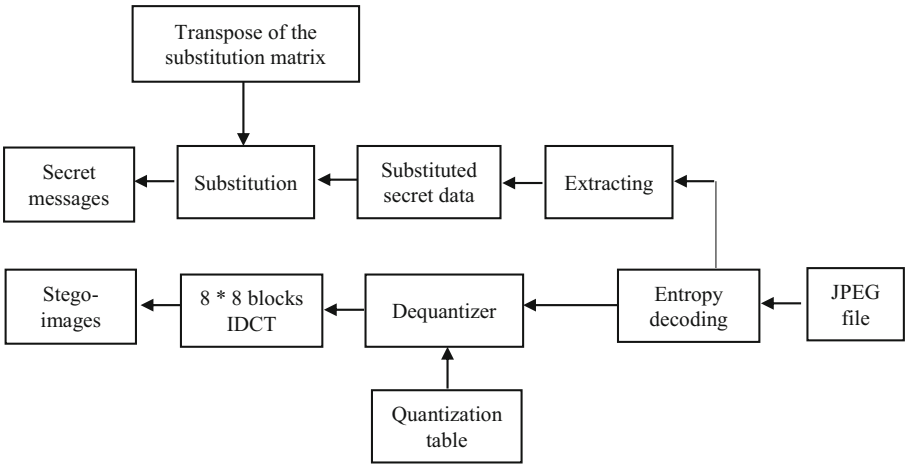

Fig. 4 The diagram of extracting procedure

From the procedures of embedding as well as extracting using the CS algorithm to identify an optimal substitution matrix is critical and in the next section it describes a principle of this CS algorithm and the manner in which a substitution matrix can be derived.

3.2.3 General principle of cuckoo search (CS) algorithm

The CS is a nature-inspired metaheuristic algorithm which had been extended by Xin-she Yang and Suash Deb in the year 2009 inspired by the behaviour of the cuckoos. This breeding may also be duly demonstrated as the performance of such parasitism, by means of laying the egg in certain random nests of the other host birds. At times these birds will discover an alien egg to throw them way or abandon the nest. The cuckoo can have a characteristic of the size shape and colour. It can take some aggressive kind of action by means of removing the remaining native eggs from its host nest for increasing the probability of hatching their eggs. A cuckoo chick that is hatched can throw the other eggs from nests for improving its share of feeding [5].

The CS will depend on the Lévy flight as a random walk, employed for producing one more new mixture (of cuckoos) from current solutions as per (1).

$$x_i^{(t+1)} = x_i^{(t)} + \alpha \oplus Levy(s, \lambda) \tag{1}$$

In which the $x_i^{(t+1)}$ will be the ith cuckoo that is at the instance t + 1; α will be the step size; λ the Lévy distribution coefficient.

This Lévy flight will basically provide a random walk and a random step length will be drawn from that of a Lévy distribution as per (2).

$$Levy(s, \lambda) \sim s^{-\lambda}, (1 < \lambda \leq 3) \tag{2}$$

This incidental type of walk through the Lévy flight is very proficient to explore the search space, because its stride length will be longer on a long term.

The CS has lesser parameters that which will have to be adjusted when evaluated to the methods and in contrast the PSO will require tuning of three parameters. These are the Inertia weight, the result of its assurance and finally the consequence of social impact), in which the tuning range of the parameters of the PSOs will upset the attributes of such search.

In a GA, its rate of crossover and the rate of mutation will have to be adjusted and different methodologies will have to be chosen. Additionally, Yang and Deb had realized a random-walk based search to be better executed by the Lévy flights as opposed to a simple and random walk [7]. The Cuckoo search has idealised rules that are summarised as below:

- A cuckoo will lay only one egg and will dump it in a nest chosen randomly.
- The nest that has greater value eggs that will leftover to the generations in future.
- The host nests that are available is fixed where the changes of discovery of laid eggs by host birds is computed as $P_a \in [0, 1]$. This fraction pa of the n nests will be substituted by the new nests (having fresh and solutions that are random).

The CS and is pseudo code that is outlined as depicted below.

Begin
Objective function : $f(x), X = (x1, ..., xd)^T$
Generate initial population of
n host nests xi $(i = 1, 2, ..., n)$
While$(t <$ *MaxGeneration*$)$ *or* $($*stop criterion*$)$ *Do*
Get a cuckoo randomly by Levy flights
evaluate its quality/fitness F_i
Choose a nest among n (say, j) *randomly*
if $\left(F_i > F_j\right)$,
Replace *j by the new solution*;
End
A fraction (P_a) *of worse nests*
are abandoned and new ones are built;
Keep the best solutions/nests;
Rank the solutions and find the current best;
end while
Postprocess results and visualization
end

CS has many advantages due to its simplicity and efficiency in solving highly non-linear optimisation problems with real-world engineering applications. CS satisfies the global convergence requirements. CS supports local and global search capabilities. CS uses Lévy flights as a global search strategy.

3.2.4 Searching for substitution matrix through CS algorithm

In this it adopts a CS algorithm for searching for a substitution matrix on information hiding and the cuckoo X of dimension 2^k has been described using this substitution matrix, M, as defined as in (3):

$$X = x_0 x_1 .... x_{2^k - 1}, \tag{3}$$

In which $x_0$will represent a position which is of a row 0 in a matrix being M with a value 1, $x_1$the position of the row 1 in M with a value 1. Therefore, this principle of cuckoo X will be identical to matrix M which transforms its final value i to x_i. It is to be noted that the x_i will be a constant that ranges between 0 and 2^k - 1, and $i \neq j$ will imply the$x_i \neq x_j$. One simple example has been illustrated as per fig. 5, in which M the substitution matrix as well as the X the corresponding cuckoo in k = 2.

It is evident that the cuckoos and their function will be similar to the substitution matrices. So, a good cuckoo will be identical to that of an ideal substitution matrix. The value of the X on every dimension will be an integer that ranges between 0 and 2^k - 1. But generally cuckoo $x_i^{(t+1)}$ in eqs. (1) and (2) is will not be any integer vector the same to any substitution matrix and cannot be transformed to these secret messages. A general CS algorithm may not be occupied for solving the trouble of search and there need to be some changes that are made.

$$M = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \end{array} \qquad X\begin{bmatrix} 1 & 2 & 3 & 0 \end{bmatrix}$$

Fig. 5 An example of substitution matrix M and the corresponding cuckoo X for k = 2

This will map $\left(x_{i0}, x_{i1}, \ldots, x_{i2^k-1}\right)$ to $\{0, 1, 2, \ldots, 2^k - 1\}$ in accordance with the value sequence. This indicates that can be the largest element of $\left(x_{i0}, x_{i1}, \ldots, x_{i2^k-1}\right)$ has been mapped to the 2^k - 1, and the second largest of the elements that will be mapped to the $2^k - 2$. For instance, in case X_i is (−0.2, 2.5, 4.1, 1.3), its equivalent mapped result will be (0, 2, 3, 1). It has to be noted that a mapped result may not be similar to its substitution matrix. Normally, the PSNR will be used for considering the actual quality of stego-image. So here the PSNR is used to be the fitness function that evaluates the act of a cuckoo. The grey level image PSNR has been defined in (4 and 5):

$$PSNR = 10 \times \log_{10}\left(255^2/MSE\right), \tag{4}$$

$$MSE = \frac{1}{WH} \sum_{i=1}^{W} \sum_{j=1}^{H} (S(i,j) - C(i,j))^2, \tag{5}$$

In which the S (i, j) and C (i, j) will represent all the pixel grey values of a stego-image as well as the cover-image for the position (i, j) respectively, also the W and H will represent the number of pixels of a certain width and a certain height of its cover-image. The search for the substation matrix using the CS algorithm has been described as below:

Step 1: Initialization. It will generate K cuckoos randomly as X_i, $i = 1, 2, \ldots, K$ and each such cuckoo will get a random Levy distribution λ. It will set $\text{nest}_i = X_i$ and will calculate PSNR of every cuckoo as detailed above.

Step 2: Updating the Levy flight of every cuckoo by using (2).

Step 3: Calculating the result that is mapped for the X_i after this deduce its corresponding PSNR. In case it is larger than its PSNR that is corresponding to the personal best nest_i, then update nest_i with its new nest X_i.

Step 4: In case its current iteration number n is below iter_{max}, n = n + 1, the go to Step 2; or else stop and further output its best possible result.

3.2.5 Algorithm description

This project work that is proposed contains two different algorithms that are: (i) steganography that uses the CS algorithm and (ii) VC with the Threshold. This application will initiate along with a steganography module in which its cover image is encrypted for generating a stego

image. This stenographic image that is generated within this module acts as the input for any visual and cryptographic module [19].

Algorithm: Steganography

Input: The Cover Image

Output: The Stego Image

Step 1: Read its cover image.

Step 2: Find out all of the pixel values belonging to the cover image.

Step 3: Read every character wise secret data.

Step 4: Convert every such character into that of an equivalent ASCII code.

Step 5: the ASCII code which will have to be converted into binary values.

Step 6: Enter the secret key.

Step 7: All secret data will duly be converted into its cipher data.

Step 8: The stream of 8-bits (the cipher data) will further embedded within the LSB of each and every pixel belonging to the cover image.

Step 9: To apply a CS algorithm within a stego image the pixel location will have to be further modified.

Algorithm: Visual Cryptography

Input: The Stego-Image

Output: The Encrypted Shares

Step 1: Read all the Stego-Image that generated.

Step 2: This stego image is broken into three different layers which are the split-1, the split-2 and the split-3 and these files contain hidden data for which they may be perfectly reconstructed.

Step 3: a re-assembled picture with its extracted data is gained again.

This suggested system has been based upon a standard VC and a visual secret sharing. The algorithm and its implementation will get better results in terms of insignificant shares while the images are within a light contrast. It is also seen that this can give darker shares in case of a grey output where this scheme has been based on a standard VC and a visual secret sharing. The implementation results better where insignificant shares for the stego images will be normally found with less contrast. It is also observed that such types of algorithm can give darker shares within a grey output. And it also gives some results that are better for image quality as well as steganalysis.

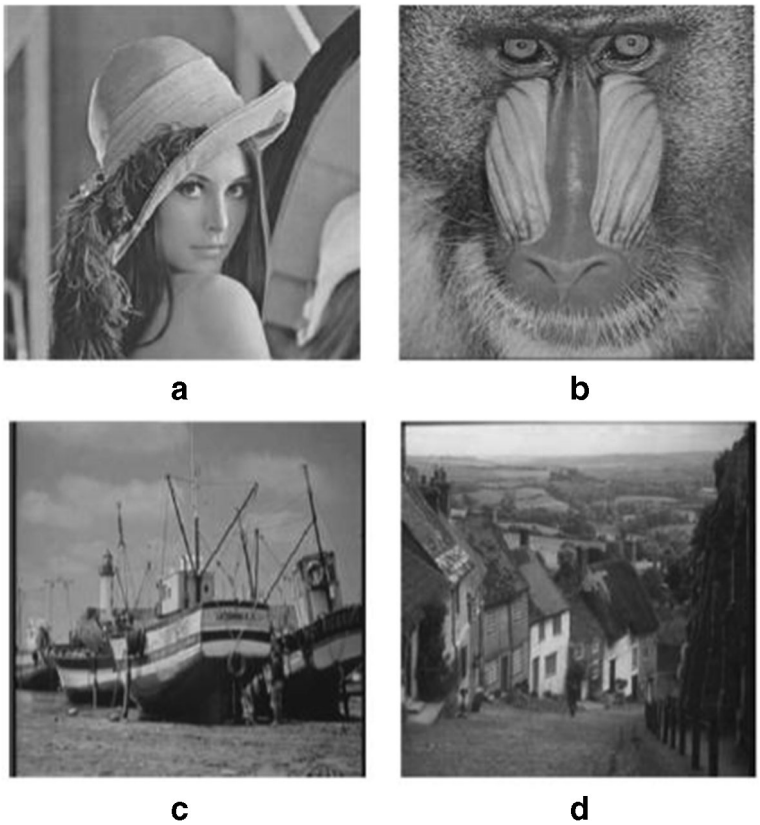

Fig. 6 The cover-images with size 256 * 256: (a) Lena, (b) Baboon, (c) boat and (d) Goldhill

4 Results and discussion

The part portrays all the experimental outcomes of this intended method. It further compares this method with that of the jpeg-jsteg and also the JQTM method in similar conditions. Thus, all the experiments of such comparison will focus upon both criteria. It makes use of the 8-bit grey-level images the Gold hill, the boat, the Baboon and the Lena as per fig. 6 to be the cover images of a size of 256 * 256 pixels and also 256 grey levels.

In case of the JQTM method, one of the quantized DCT coefficients will hide two secret bits, thereby helping each block to hide 26 * 2 = 52-bit secret messages. Here for this system a single DCT coefficient that is quantized can hide k secret bits. In such experiments, for comparing the method proposed with that of the JQTM method under similar circumstances,

Table 1 Capacity for CS

Capacity (Bits)	Jpeg-Jsteg	JQTM	CS
Lena	39.44	53.12	73.67
Baboon	38.17	52.28	71.28
Boat	37.12	51.14	70.67
Goldhill	39.23	52.97	78.88

Table 2 PSNR for CS

PSNR	Jpeg-Jsteg	JQTM	CS
Lena	36.12	36.24	37.92
Baboon	32.21	32.44	33.48
Boat	25.86	36.18	37.54
Goldhill	35.17	35.89	37.12

it will be set k = 2 (one single quantized DCT coefficient that hides two different secret bits). Thus, every block will be able to hide about 36 * 2 = 72-bit messages. The actual capacity as well as the PSNR are as according to Tables 1 and 2 and also figs. 7 and 8.

High message capacity is preferred as the security of the stego-image is high if the quality and message capacity of the stego-image is better. At the same time the quality of the image should be high. The PSNR value should be higher than 30 for a better quality. Hence the quality of the images used for evaluation is acceptable and higher than Jpeg-Jsteg and JQTM method.

From the Fig. 7, it can be observed that the CS has higher capacity by 60.52% & 32.41% for Lena, by 60.5% & 30.75% for baboon, by 62.25% & 32.06% for boat, by 67.14% & 39.3% for goldhill when compared with jpeg-jsteg and JQTM.

From the Fig. 8, it can be observed that the CS has higher PSNR by 4.86% & 4.53% for Lena, by 3.86% & 3.15% for baboon, by 36.84% & 3.68% for boat, by 5.39% & 3.36% for goldhill when compared with jpeg-jsteg and JQTM.

5 Conclusion

Image hiding has a critical role to play in data communication. The security of multimedia will also facilitate information protection in various forms of such digital data like text, video, audio or image. Steganography further gives a method of data hiding which will conceal the presence of secret messages in the media and it also is evident that the security level and the

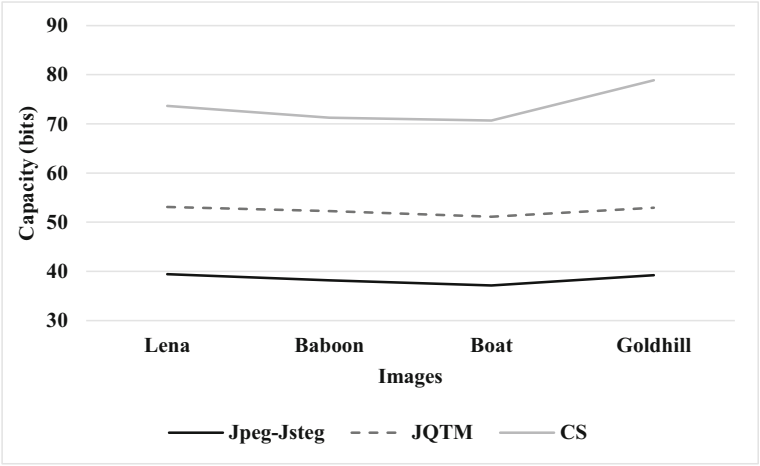

Fig. 7 Capacity for CS

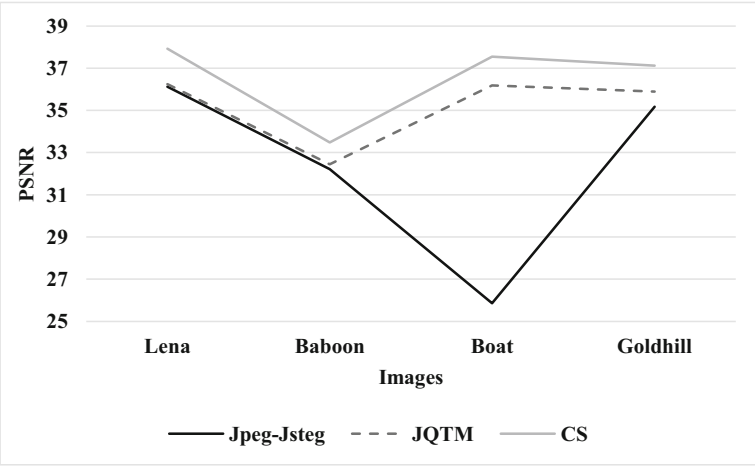

Fig. 8 PSNR for CS

stego image quality have to be researched. For this work, a novel steganographic system, which will conceal huge messages within and acceptable level of quality, was suggested. The method gets an optimal substitution matrix by that of the CS for transforming all secret messages and then hiding them into a cover-image by means the CS which has a higher capacity by about 60.52% and 32.41% for the Lena, by about 60.5% and 30.75% for the baboon, by about 62.25% and 32.06% for the boat, by about 67.14% and 39.3% for the gold hill on being compared to the jpeg-jsteg and the JQTM. The CS also has a higher PSNR by about 4.86% and 4.53% for the Lena, by about 3.86% and 3.15% for the baboon, by about 36.84% and 3.68% for the boat, by about 5.39% and 3.36% for the gold hill on being compared to that of the jpeg-jsteg and the JQTM. Additionally, this method proposed has a higher level of security as one will not be able to improve correctly the secret messages with no being aware of the substitution matrix. In case of the future work, it will also try and improve the method's robustness against certain popular schemes of steganalysis.

References

1. Abbas SA, El Arif TI, Ghaleb FF, Khamis SM (2015) Optimized video steganography using Cuckoo Search algorithm. In Intelligent Computing and Information Systems (ICICIS), 2015 IEEE Seventh International Conf: 572-577. IEEE
2. Almohammad A, Hierons RM, Ghinea G (2008) High capacity steganographic method based upon JPEG. In Availability, Reliability and Security, 2008. ARES 08. Third International Conf: 544–549. IEEE
3. Awad A (2017) A survey of spatial domain techniques in image steganography. J Educ College Wasit Univ 1(26):497–510
4. Bloisi DD, Iocchi L (2007) Image based steganography and cryptography. VISAPP 1:127–134
5. Chang CC, Chen TS, Chung LZ (2002) A steganographic method based upon JPEG and quantization table modification. Inf Sci 141(1-2):123–138
6. Chhabra N (2012) Visual cryptographic steganography in images. Int J Comput Sci Netw Sec (IJCSNS) 12(4):126
7. Fazli S, Kiamini M (2008) A high_performance steganographic method using JPEG and PSO algorithm. In Multitopic Conference, 2008. INMIC 2008. IEEE International (pp. 100-105). IEEE.

8. Geetha P, Jayanthi VS, Jayanthi AN (2018) Optimal visual cryptographic scheme with multiple share creation for multimedia applications. Comput Sec 78:301–320
9. Gupta R, Jain A, Singh G (2012) Combine use of steganography and visual cryptography for secured data hiding in computer forensics. Int J Comput Sci Inform Technol 3(3):4366–4370
10. Kumar RH, Kumar PH, Sudeepa KB, Aithal G (2013) Enhanced security system using symmetric encryption and visual cryptography. Int J Adv Eng Technol 6(3):1211
11. Li X, Wang J (2007) A steganographic method based upon JPEG and particle swarm optimization algorithm. Inf Sci 177(15):3099–3109
12. Marwaha P, Marwaha P (2010) Visual cryptographic steganography in images. Computing communication and networking technologies (ICCCNT), 2010 international conference: 1-6). IEEE
13. Mishra A, Johri P, Mishra A (2017) An approach to secure communication using steganography with cryptography in an audio file using GA. Int J Innov Adv Comput Sci 6 (12)
14. Muhammad K, Ahmad J, Farman H, Jan Z, Sajjad M, Baik SW (2015) A secure method for color image steganography using gray-level modification and multi-level encryption. TIIS 9(5):1938–1962
15. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW (2016) A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. Multimed Tools Appl 75(22):14867–14893
16. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW (2016) Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Futur Gener Comput Syst
17. Muhammad K, Ahmad J, Rho S, Baik SW (2017) Image steganography for authenticity of visual contents in social networks. Multimed Tools Appl 76(18):18985–19004
18. Muhammad K, Ahmad J, Rehman NU, Jan Z, Sajjad M (2017) CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. Multimed Tools Appl 76(6):8597–8626
19. Prema G, Natarajan S (2013) Steganography using genetic algorithm along with visual cryptography for wireless network application. Information communication and embedded systems (ICICES), 2013 international conference: 727-730. IEEE
20. Ramalingam M, Isa NAM (2015) A steganography approach over video images to improve security. Indian J Sci Technol 8(1):79–86
21. Rani MMS, Mary GG (2016) Enhancement of RGB shares of visual cryptography using PSO. Int J Comput Sci Inform Sec 14(9):938
22. Rani MMS, Mary GG (2017). Particle swarm optimization based image enhancement of visual cryptography shares. Artificial intelligence and computer vision (pp. 31-49). Springer, Cham
23. Rani MMS, Mary GG, Euphrasia KR (2016) Multilevel multimedia security by integrating visual cryptography and steganography techniques. In Computational intelligence, cyber security and computational models (pp. 403-412). Springer, Singapore
24. Roy S, Venkateswaran P (2014) Online payment system using steganography and visual cryptography. Electrical, electronics and computer science (SCEECS), 2014 IEEE Students' Conf: 1-5. IEEE.
25. Saleh ME, Aly AA, Omara FA (2016) Data security using cryptography and steganography techniques. IJACSA) Int J Adv Comput Sci Appl, 7(6)
26. Sarmah DK, Kulkarni AJ (2018) JPEG based steganography methods using cohort intelligence with cognitive computing and modified multi random start local search optimization algorithms. Inf Sci 430: 378–396
27. Shankar K, Lakshmanaprabu SK (2018) Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm. Int J Eng Technol 7(1.9):22–27
28. Walia GS, Makhija S, Singh K, Sharma K (2018) Robust stego-key directed LSB substitution scheme based upon cuckoo search and chaotic map. Optik 170:106–124
29. Yang XS, Deb S (2014) Cuckoo search: recent advances and applications. Neural Comput Applic 24(1): 169–174

Mr. K. Gurunathan completed B. E Computer science and Engineering from Pavendhar Bharathidasan College of Engineering and Technology in the year 2005. M. E in Computer Science and Engineering from G K M College of Engineering and Technology, Chennai in the year 2011. Currently working as a Assistant Professor, CSE department Mother Terasa College of Engineering and Technology, Pudukottai. His research interest are Visual Cryptography, Pattern Recognition etc.

Dr. S. P. Rajagopalan was born on 23rd Nov 1943 in Trichy. He has completed his M.Sc.(Applied Mathematics) in 1965-67 in IIT Madras, Chennai. And Joined as faculty in D.G. Vaishnav College on 22nd July 1967 and continued as Principal of the same college from 1996 to 2001. Then he joined as Dean of College Department Council, University of Madras from 2001 to 2005, then he worked as Advisor for Mohammed Sathak Group of Institutions up to 2007. And now he is working as Prof. Emeritus & Dean in Dr.M.G.R. University and also Advisor to Bakthavatchalam College, Chennai. He is having more than 40 years of experience out of 30 years in research. Currently he is working as a professor at GKM college of Engineering and Technology, Chennai. His area of interests are Quantitative Techniques, Data Processing and Project Management, Management Information System, Programming Languages, Simulation Text Generation, Cryptography, Data Mining

Affiliations

K. Gurunathan [1,2] · S. P. Rajagopalan [3]

S. P. Rajagopalan
sasirekaraj@yahoo.co.in

[1] Anna University, Chennai, India

[2] Department of CSE, Mother Therasa College of Engineering and Technology, Pudukottai, Tamilnadu, India

[3] Department of CSE, GKM College of Engineering and Technology, Chennai, Tamilnadu, India