A NOVEL STEGANOGRAPHIC SCHEME BASED ON HASH FUNCTION COUPLED WITH AES ENCRYPTION

Rinu Tresa M J[1] , Athira M Babu[2] and Sobha T[3]

[1,2]Computer Science and Engineering,Adi Shankara Institute of Engineering and Technology, Kalady
[3]Assistant professor, Computer Science and Engineering,Adi Shankara Institute of Engineering and Technology, Kalady

ABSTRACT

In the present scenario the use of images increased extremely in the cyber world so that we can easily transfer data with the help of these images in a secured way. Image steganography becomes important in this manner. Steganography and cryptography are the two techniques that are often confused with each other. The input and output of steganography looks alike, but for cryptography the output will be in an encrypted form which always draws attraction to the attacker. This paper combines both steganography and cryptography so that attacker doesn't know about the existence of message and the message itself is encrypted to ensure more security. The textual data entered by the user is encrypted using AES algorithm. After encryption, the encrypted data is stored in the colour image by using a hash based algorithm. Most of the steganographic algorithms available today is suitable for a specific image format and these algorithms suffers from poor quality of the embedded image. The proposed work does not corrupt the images quality in any form. The striking feature is that this algorithm is suitable for almost all image formats e.g.: jpeg/jpg, Bitmap, TIFF and GIFF.

KEYWORDS

Steganography, Cryptography, Hashing, Image Format, AES algorithm

1. INTRODUCTION

Steganography is of greater importance in situations where the secret information has to be transferred in a secure manner without the knowledge of a third person. The third person couldn't even get a clue regarding this hidden information. Only the sender as well as the receiver comes to know about this secret hidden message. In steganography there is a cover media in which data hiding takes place. The cover media can be a text, or it can be an image, audio, video etc. This paper focus on image steganography that is the cover media used is image. The applications of image steganography are innumerable especially in this high tech world. Areas include copyright protection to sharing trade secrets, ownership identification, transferring of highly confidential data between governments and much more.

Steganography and cryptography are the two techniques that are often confused with each other. The input and output of steganography looks alike, but for cryptography the case is different. In cryptography the output will be in an encrypted form which always draws attraction to the attacker. While considering the case of steganography this never happens as the attacker is unaware of the hidden message. In cryptography message content is preserved while in

DOI : 10.5121/acij.2014.5103

steganography both the messages as well as people involved in the communication are preserved. This paper combines both steganography and cryptography so that attacker doesn't know about the existence of message and the message itself is encrypted to ensure more security.

Steganography has been used since ancient times. Its history dates back to 440 BC. In ancient Greece the use of wax tablets was common. The other technique used was tattooing on the scalp of the messenger. After the growth of hair the message becomes hidden and the messenger is sent to the intended King. The messengers head is again shaved to view the secret message. But this technique takes a lot of time, mainly the time required for the growth of hair.

In the present scenario the use of images increased extremely in the cyber world so that we can easily transfer data with the help of these images in a secured way. Image steganography becomes important in this manner. Least Significant Bit hiding is the one of the modern techniques for image steganography. In this method the least significant bit of the image pixel is used to hide the secret information. This is the easiest technique available today. But the quality of the image gets distorted when the number of bits used for embedding in a pixel goes beyond three. Another method used for image steganography is blocking. This method makes use of DCT (Discrete Cosine Transforms). Initially the image is to be broken down into blocks and DCT is applied. So for each of the block there are 64 DCT coefficients and these helps in adjusting the colour and brightness of the image .By doing so the data can be hidden securely.

Rubata Riasat and Imran Sarwar Bajwa [3] proposed a scheme for color image steganography which is a hash based technique. A perfect hash function is used in this algorithm. This method can be used for any type of image formats. This method does not corrupt the image quality.
Po-Yueh Chen and Hung-Ju Lin [6] proposed a DWT (Discrete Wavelet Transform) based approach for image steganography. The embedding procedure takes place in the frequency domain. Based on the application provided, there are two basic modes as well as five different cases given for selection. After applying a 2-dimensional Haar-DWT high frequency coefficients and low frequency coefficients are generated. Embedding of secret data takes place in these high frequency coefficients while keeping low frequency coefficients as such. Before embedding some transformations takes place in the data to make it more secure. This method provides better PSNR value.

Many cryptographic algorithms are available these days. Some of the traditional cryptographic algorithms include MD5 (Message Digest 5)[7], SHA(Secure Hash Algorithm) [2][8], DES (Data Encryption Standard) [1], AES (Advanced Encryption Standard) [5], IDEA (International Data Encryption Algorithm)[1], Bit Stream Cipher[9] etc.

Abbas Cheddad [2] proposed a hash based image encryption algorithm. The digital images are encrypted in a novel way with password protection. The password is provided by the user. This new method makes use of 1D SHA-2 algorithm along with a compound forward transform. This scheme provides security as well as better performance. The drawback is that this scheme is not suitable for color images.

Koredianto Usman [1] proposed a method for image encryption for medical images based on random permutation and pixel arrangement. This scheme provides high transmission security as well as high speed processing. Initial step is the key generation. After this, rearrangement of pixels takes place. This is according to some predefined rules. For the decryption to takes place effectively there should be a bijective mapping for pixel arrangement. Column permutation as well as row permutation is done subsequently to ensure more security. The process of pixel arrangement as well as permutations is repeated several times. This algorithm works well for big

medical images too. The main disadvantage is that this method does not go with compressed data e.g. JPEG or JIF format.

Der-Chyun Lou and Chia–Hung Sung [4] proposed a steganographic scheme based on dynamic chaotic system and Euler theorem for secure communication. This is as asymmetric scheme. For the embedding process as well as for the extraction process the secret used is different hence the term asymmetric is used. The chaotic asymmetric steganography scheme (CAS) mainly has got three main steps namely, stego-matrix generation, embedding process and finally extraction process. A chaotic mapping for the stego matrix is generated .The embedding scheme make use of the local characteristics of the image. The main advantage of using this method is that in order to get back the message embedded from the stego image, the cover image is not a necessary thing. This method is effective against inverse attacks. When the image size increases the computations for chaotic mapping increases and the hence the cost increases .Moreover this method can be used only if the image is a square.

The proposed work uses a hash function to find out the locations to store the secret message. The secret message is encrypted using AES encryption. This makes it even more secure. The proposed scheme works for colour images.

2. PROBLEM STATEMENT

In the present scenario where the use of internet has grown significantly the importance of safety of data transferred is of serious concern. There are so many methods to ensure security of data transferred. Major techniques include cryptography and steganography. There are many cryptographic as well as steganographic algorithms available today. But each method has got its own drawback. The proposed algorithm makes the data more secure against attacks by the intruders. The proposed method combines steganography and cryptography in a way such that the data safety is ensured. This method is effective and secure by using a hash function for steganography and AES algorithm for encryption. In most of the image steganographic schemes the use of gray-scale images is mandatory but this method is suitable for colour images so that hidden data is not at all visible to the viewers.

3. PROPOSED WORK

Most of the steganographic algorithms available today is suitable for a specific image format and these algorithms suffers from poor quality of the embedded image. The proposed work does not corrupt the images quality in any form. The striking feature is that this algorithm is suitable for almost all image formats e.g. jpeg/jpg, Bitmap, TIFF and GIFF. The entire process consists of mainly two steps:

1. Embedding
2. Extracting

A.Embedding

The simple block diagram for embedding is shown in the figure 1.

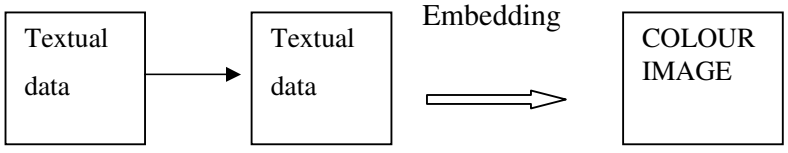

Figure 1.Block diagram showing the embedding procedure

The textual data entered by the user is encrypted using AES algorithm. After encryption, the encrypted data is stored in the colour image by using a hash function.

- Textual Data

The user has to enter the textual data i.e. the secret information that is to be hidden in the image. User can select the image in which the information is to be embedded. Medium sized images always give the best results. Let us take an example for the textual data "tomorrow is a holiday'.

- Encryption

AES encryption of the textual input data takes place.Advanced Encryption Standard (AES) algorithm is symmetric cipher algorithm used in applications that require fast processing. AES algorithm supports data and key combinations of size 128, 192 and 256 bits. AES allow data of length 128 bits. 128 bits data is divided into four blocks, in which each block perform different operations. The blocks are organised in 4x4 matrixes which is called states. The blocks operate on array of bytes. Encryption of data include four transformation steps and encryption is completed when it completes Nr rounds where Nr= 10, 12, 14. The four transformation steps are Bytesub, Shiftrows, Mixcolumns, and Addroundkey transformations as shown in figure [2].

Bytesub transformation is a non linear byte Substitution method. This transformation is done using an s-box or substation block. S-box is constructed by multiplicative inverse and affine transformation. The Figure of s-box for Bytesub transformation is shown below. Second transformation is Shiftrows transformation. This is a simple byte transposition. The last three rows of state are taken and the bytes in the last three rows are shifted cyclically. Then offset of the left shift varies from one to three bytes. Mixcolumns transformation is method in which columns of states are taken and matrix multiplication of columns is done. Here bytes are taken as polynomials, numbers are not taken. A fixed matrix is multiplied with each column vector. Addroundkey transformation is the final transformation step. It is a simple XOR operation between the roundkey and the working state. This transformation is an inverse of its own.

The total number of steps of an encryption procedure is as shown by Figure of AES algorithm. The initial step is an Addroundkey. Next step consists of a data block consisting of four transformations like Bytesub, Shiftrows, Mixcolumns and Addroundkey. To this data block a round function is applied. This step is performed iteratively up to Nr times. The number of iterations will depend on the key length. The decryption structure is similar to the encryption transformations. In decryption the transformations are Inverse-Bytesub, the Inverse-Shiftrows, the Inverse-Mixcolumns, and the Addroundkey. Key schedules are identical for encryption and decryption.

After applying AES encryption the embedding of the data takes place with the help of hash based algorithm. The result of the above textual data after AES encryption is "U2FsdGVkX189yEbyefY0Vh289mcNKBanCKM8exZvkzi4U1qI9sXRBCmOx9zP3YkZ".
After this divide the encrypted text into groups of three, e.g. [U2F] [sdG] [VkX] [189] [yEb] [yef].

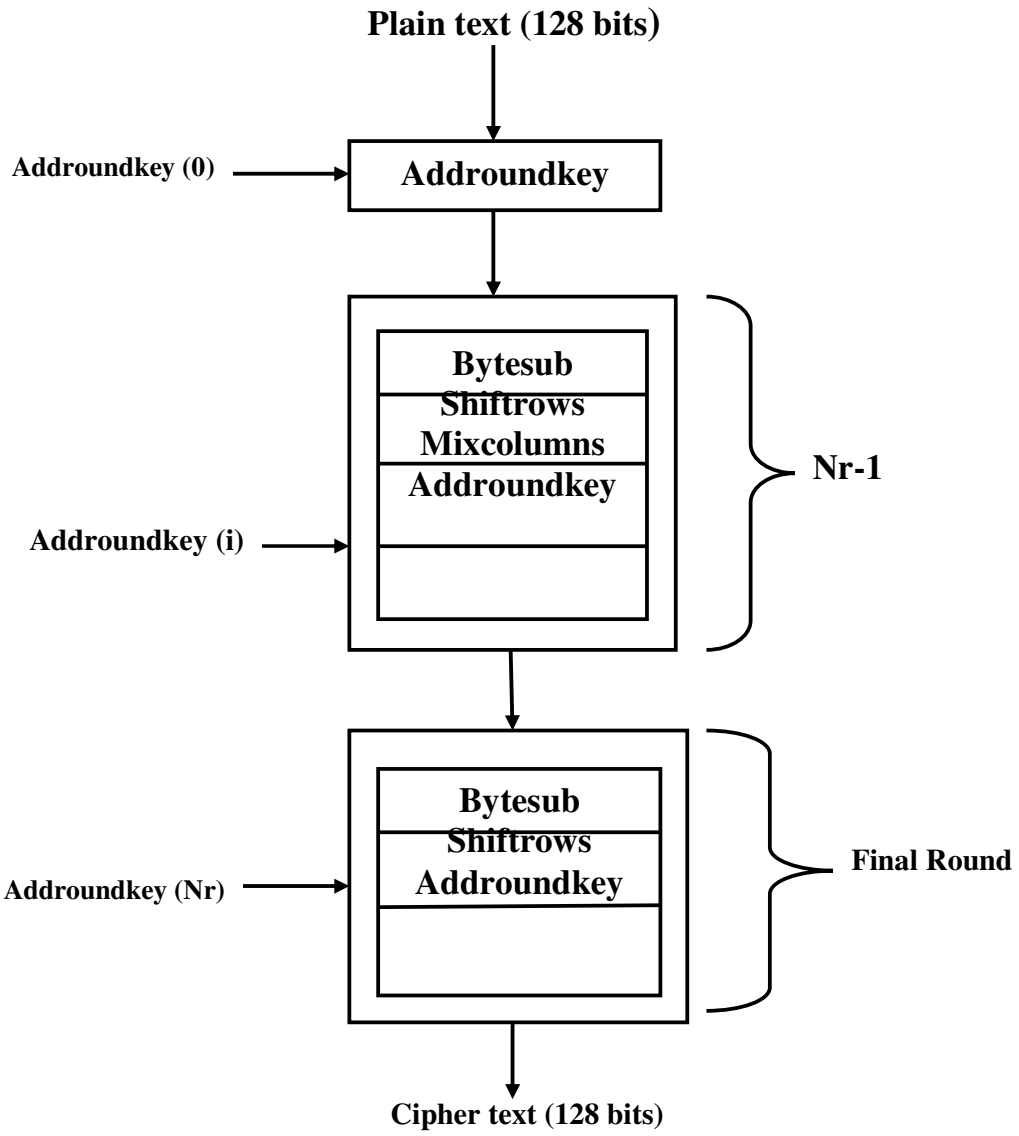

Figure 2. AES encryption Algorithm

- Embedding procedure

For embedding of the data in the color image, hash based algorithm is used for better efficiency [3]. The whole algorithm is shown in the figure 3.

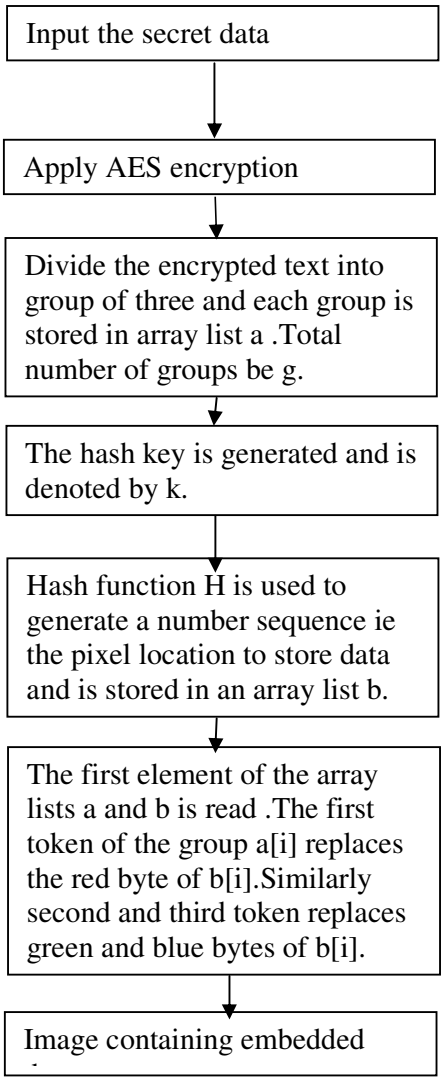

Figure 3. Block diagram of the proposed method for embedding

Algorithm for embedding

1. Input the text which is the secret data used for embedding.
2. Apply AES encryption to the input text.
3. After encryption, the encrypted data is divided into groups of three each .The number of groups is denoted by g. The groups are stored in an array list named a.
4. A random number is generated for the use for hash key and is denoted as k.
5. The number of group g and the hash key k is inputted to the hash function H [10]. This hash function generates a number sequence which shows the locations in which secret data is to be stored. The number sequence is stored in another array list named b.
6. The first elements of the array lists a and b are read. The first token from the array list a[i] replaces the red byte of the array list b[i].The second token from the array list a[i] replaces the green byte of the array list b[i] .The third token from the array list a[i] replaces the blue byte of the array lists b[i] .

7. Finally the output is the image containing the embedded data and the hash key k and the AES encryption key.

B.Extraction

The extraction procedure is just the reverse of embedding. The simple block diagram for extraction is shown in figure 4.

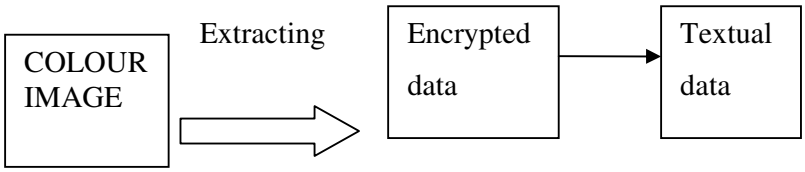

Figure 4. Block diagram showing the extraction procedure

Initially the colour image is to be loaded which contains the embedded data. From that colour image the encrypted data is to be extracted. Then the decryption procedure is applied to get back the original text message.

The algorithm for extraction is explained in the block diagram shown in the figure 5

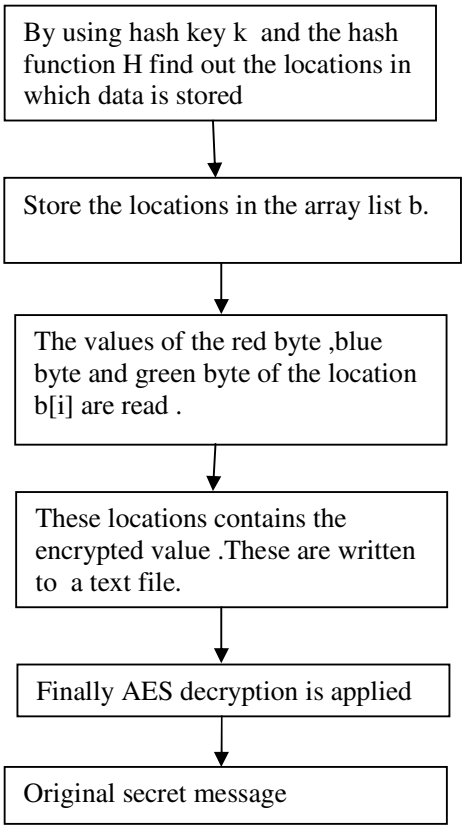

Figure 5. Block diagram containing the extraction procedure

Algorithm for extracting

1. Input the image containing the embedded data. The image can be of any format e.g. .jpeg/.jpg, .bmp, .gif etc
2. With the help of hash key k and hash function H find out the number sequence. These are the locations in which secret data is stored.
3. Store the data locations in an array list b. Read the data from these locations. The red byte, green byte and blue byte contains encrypted data. These are written into a text file
4. Decrypt the data written in the text file using the AES decryption and by using the same key as used for encryption.
5. The final output is the secret data.

Perfect hash function is used in this algorithm and hence no chance for hash collisions. This makes the algorithm more effective. The use of AES for encryption makes the data more secure and safe.

4. TOOL SUPPORT

The proposed algorithm was implemented in MATLAB. The GUI is shown in the figure 6 and 7.

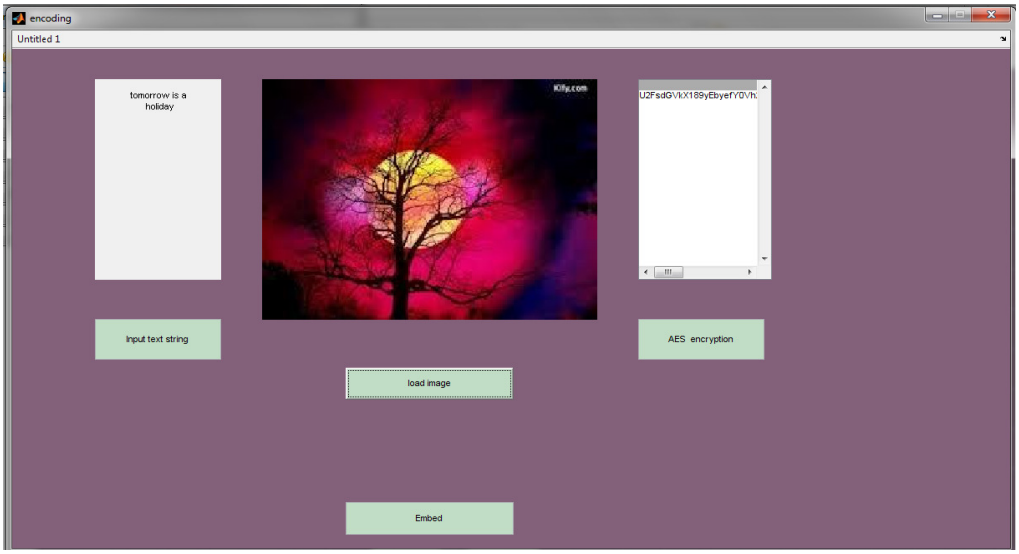

Figure 6. GUI for embedding secret information

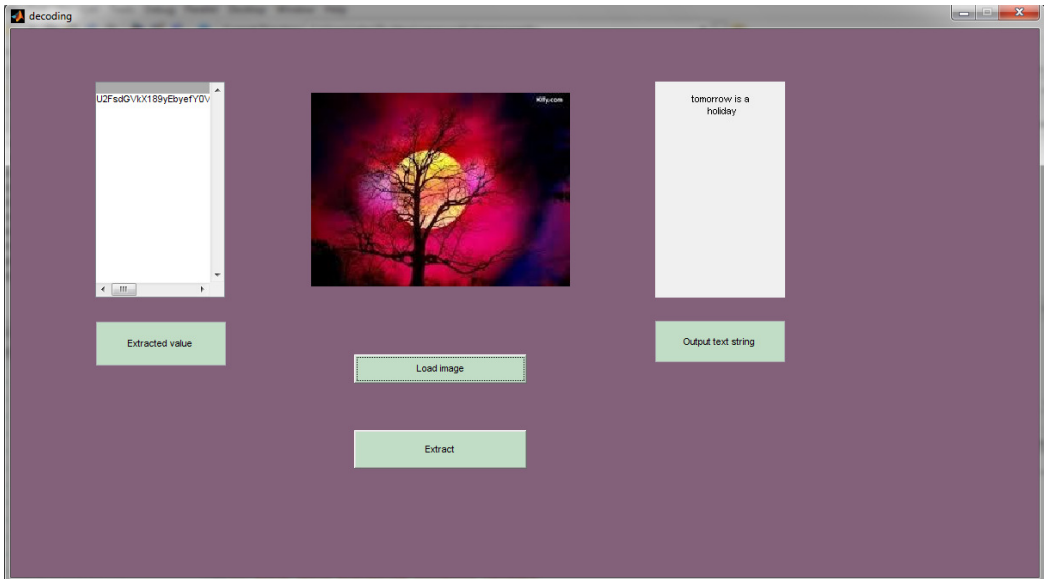

Figure 7. GUI for extracting secret information

5. EVALUATION

We have tried with texts with different word lengths. The proposed system goes well for small data size as well as with large data size. A comparison study was done with different existing methods in terms of security. Our method is found to be very effective

Table1.Comparison with other methods

Method Used	Security
IDEA	Good
MD5	Good
Proposed Method	Excellent

6. CONCLUSION AND FUTURE WORK

The proposed method combines both steganography and cryptography thereby boosting the security of the data. Hiding of large textual data is possible. While doing so quality of the image does not get disturbed. Main striking feature is that images of almost all formats can be used for hiding data. In future the algorithm can be improved so that more security is guaranteed. In future embedding capacity can be greatly enhanced and can be able to withstand against all types of attacks. This method can be extended to embed in audio as well as video for secure multimedia transmission.

ACKNOWLEDGEMENTS

We would like to thank our project guide Mrs. Sobha T, Associate Professor,Computer Science and Engineering,Adi Shankara Institute of Engineering and Technology, Kalady, for her utmost guidance in our project work.

REFERENCES

[1] K. Usman, H. Juzoji, I. NakajiIm, S. Soegidjoko, M. Ramdhani, T. Hori, and S. Igi, "Medical image encryption based on pixel arrangement and random permutation for transmission security," in Proceedings of IEEE 9th International Conference on e-Health Networking, Application and Services, Taipei, Taiwan, 2007, 19-22 June.pp.244-247.

[2] Cheddad, Abbas; Condell, Joan; Curran, Kevin; McKevitt, Paul, "A Hash-based Image Encryption Algorithm" , Optics Communications, Volume 283, Issue 6, p. 879-893. March, 2010

[3] Rubata Riasat, Imran Sarwar Bajwa, M. Zaman Ale "A Hash-Based Approach for Colour Image Steganography" 978-1-61284-941-6/11/$26.00 ©2011 IEEE

[4] D.C. Lou and C.R Stmg, "A steganographic scheme for secure communications based on the chaos and Euler theorem," IEEE Transactions on Multimedia, 6(3X2004)501-509.

[5] M. Zeghid, M Machhout, L Khriji, A Baganne, and R Tourki, "A modified AES based algorithm for image encryption," International Journal of Computer Science and Engineering, 1(IX2006) 70-75.

[6] Po-Yueh Chen and Hung-Ju Lin "A DWT Based Approach for Image Steganography", in International Journal of Applied Science and Engineering 2006. 4, 3: 275-290.

[7] Y. Wang, X Liao, D. Xiao, and K.W. Wong, "One-way hash function construction based on 2D coupled map lattices," Information Sciences, 178(5X2008)1391-1406.

[8] I. Ahmad and AS. Das, "Hardware implementation analysis of SHA -256 and SHA -512 algorithms on FPGAs," Computers & Electrical Engineering, 31(6X2005)345-360

[9] Wen, M. Severa, and W. Zeng, "A format-compliant configurable encryption framework for access control of video," IEEE Trans. Circuits Syst. Video Technol, 12(6X2002)545-557.

[10] Thomas R Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein Introduction to Algorithms, Second Edition MIT Press and McGraw-Hill, 2001. Section 11.5:Perfect hashing, pp. 245-249.

Authors

Rinu Tresa M J

The author did B.Tech in Computer Science and Engineering from M.G Unive rsity, Kerala, India. Now pursuing M.Tech in Computer science and Engineering from M. G university.

Athira M Babu

The author did B.Tech in Computer Science and Engineering from M.G University, Kerala, India. Now pursuing M.Tech in Computer science and Engineering from M. G university.

Sobha T

The author is an Assistant professor, Computer Science and Engineering,Adi Shankara Institute of Engineering and Technology, Kalady,Kerala,India.The author did B.Tech from Univeristy Colleg e Of Engg, Thodupuzha, Kerala, India and M.Tech from University of Kerala, Kariavattom. Now registeredfor Ph.D at Cochin University of Science And Technology, Cochin.