International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 10 | Oct - 2021 ISSN: 2582-3930

Performance Analysis of selective image encryption algorithm Using Hybrid model

Bandaru Snehitha[1], Vasantha murali Krishna[2]

[1] Student, Department of CSE- Avanthi Institute of Engineering and Technology Visakhapatnam
[2] Assistant Professor, Department of CSE- Avanthi Institute of Engineering and Technology Visakhapatnam

---

Abstract - The use of encryption/decryption is as old as the art of communication. In war time, a cipher, often incorrectly called a code, which can be employed to keep the enemy from obtaining the contents of the transmissions. The DNA cryptography is a new technology introduced in the cryptography research. DNA can be used in cryptography for storing and transmitting the information, as well as for computation. DNA cryptography is shown to be very effective and efficient. Several DNA computing algorithms are proposed for some cryptography, cryptanalysis and steganography problems, and they are very powerful in these areas. RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. In the proposed hybrid model work, we are able to combine the DNA and RC4 techniques to carry the partial image secretly from source to destination without identifying attackers. To address the performance issues existed in previous work has been resolved in the proposed work.

Key Words: DNA encryption, RC4 stream cipher, Cryptography, Steganography.

1.INTRODUCTION

Data security means providing protection for data from unauthorized users or hackers and having high security to prevent data modification. This type of data security has gained more attention over the recent period of time due to the more increase in data transfer rate over the internet In order to improve the data security features in data transfers through internet, many techniques have been developed like: Cryptography, Steganography. Cryptography is a method to conceal information by encrypting it into cipher texts and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

2. Cryptography and Steganography

According traditional cryptography, there are many techniques to convert plain text to cipher text. The oldest schemes replace the letters in the message one by one, following a fixed recipe. The key" to such a transliteration scheme just lists all the letters in the alphabet and gives for each letter the corresponding crypto-letter. For instance,

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

G O K E A N Q U Y C P T L F H W B M V X Z R I D S J

indicates that every A will be replaced by a G, every B by an O, etc.

To decrypt schemes[1][2] of this na111ture, one just needs to reverse the transliteration; in the example above one would replace every G in the encrypted message by A, every O by B, every K by C, etc. The decoding is thus again a transliteration. For the example above, the decoding transliteration is

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

E Q J X D N A O W Z C M R F B K G V Y L H S P T I U

One of the very oldest documented transliteration schemes was used by the Roman general Julius Caesar (1st century BC). His transliterations were particularly simple because they involved only a shift of the alphabet, such as in the following example:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

U V W X Y Z A B C D E F G H I J K L M N O P Q R S T

This example was obtained by writing a second copy of the ordered alphabet for the transliteration, starting 6 steps to the right, with A underneath the letter G in the first line, and going on until T is written underneath Z; at that point, the writing gets wrapped around" and the alphabet is completed, from U to Z, by writing underneath the letters A through F from the first line. Codes of this simple shift type are called Caesar codes.

Note that the corresponding decoding transliteration

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

G H I J K L M N O P Q R S T U V W X Y Z A B C D E F

The above note which consists of moving 6 steps to the left (or equivalently, 20 steps to the right: after all, moving 26 steps is the same as not moving at all, or +26 ' 0, so that -6 ' -6 + 26 ' 20). This is again a Caesar code.

A variant on Caesar codes is obtained by not only shifting the starting point of the alphabet, but writing the alphabet in the opposite order, as in the following example

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

F E D C B A Z Y X W V U T S R Q P O N M L K J I H G

In this case the decoding scheme is the same as the encoding scheme: the transliteration replaces M by T and T by M; the same symmetry holds for all other letters.

Steganography refers to the science of invisible communication. Unlike cryptography, where the goal is to

secure communications from an un-authorized user, steganographic techniques used to hide the presence of the message itself from an observer. The idea of hiding some information in digital content has a wider class of applications that go beyond steganography. These techniques involved in such applications are collectively referred to as information hiding. For example, an image printed on a document could be annotated by metadata that could make a user to its high resolution version. In general, metadata provides additional information about an image.

Information hiding allows the metadata to travel along with the image regardless of the file format and image state (digital or analog). A special type of information hiding is **digital watermarking**. Digital watermarking is the process of embedding information into digital multimedia content so that the information (the watermark) can later be extracted or detected for a variety of uses including copy prevention and control. Digital watermarking has become an important and active area of research, and development of watermarking techniques is being used essential to address some of the challenges faced by the rapid proliferation of digital content. The only difference between information hiding and watermarking is the absence of an active adversary. In watermarking applications like copyright protection and authentication, there is an active adversary that would attempt to remove, invalidate or forge watermarks.

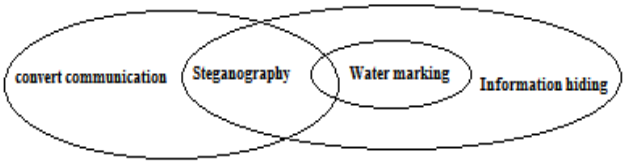


Fig 1. Relationship of steganography vs Cryptography

The dissertation consists five chapters with outlines provided below Chapter one provides an introduction. It also provides an overview of the thesis.

Chapter two provides the related work performed in the area of Encryption technique over. The chapter begins by explaining the studies performed by various researchers in the area. All the studies summarized in this section conclude by partial encryption and decryption using RC4 technique and gives the original data.

Section three explains problem study in which we explain existing system, proposed system and also architecture for the proposed system. Chapter four explains the methodology that is built using the algorithm and description of the thesis, system architecture. Chapter five explains results and discussion. It generally explains the every input,

output, sample code, and the output screens.

Chapter six gives the conclusion of the project.

3. RELATED WORK

The DNA cryptography is a new technology introduced in the cryptography research. DNA can be used in cryptography for storing and transmitting the information, as well as for computation. DNA cryptography is shown to be very effective and efficient. Several DNA computing algorithms are proposed for some cryptography, cryptanalysis and steganography problems, and they are very powerful in these areas. This method is found to be efficient in computation, storage and transmission and it is very powerful against certain attacks. Thus, this method can be of many uses in cryptography, such as an enhancement insecurity and speed to the other cryptography methods. There are also extensions and variations to this method, which have enhanced security, effectiveness and applicability.

DNA encoding and decoding for image: A DNA sequence contains four nucleic acid bases A(adenine), C(cytosine),G(guanine), T(thymine), where A and T is complement, G and C is complement. In the binary, 0 and 1 is complement, so 00 and 11 is complement, 01 and 10 is also complement. In this I use 00, 01, 10, 11 to denote C, A, T, G, respectively. For 8 bit grey images, each pixel can be expressed a DNA sequence whose length is 4. For example: If the first pixel value of the original image is 1 convert it into a binary steam is [10101101] , by using about DNA encoding rule to encode the steam, we can get a n sequence [TTGA]. Whereas use the values C, A, T, G to denote 00, 10, 11, respectively, and to decode above DNA sequence, can get a binary sequence [10101101].

4. EXISTING WORK

In this chapter a brief literature review is presented on Encryption techniques and DNA coding and RC4 encryption algorithm.

In this partial image encryption the previous paper analysis.

4.1 The Partial image encryption

4.2 Convertion into DNA coding

4.3 Encryption using RC4 encryption

4.1 Partial image encryption

According to Prasanna et al. [3] have presented an image encryption method with magnitude and phase manipulation using carrier images. Here they used the concept of carrier images and one dimensional Discrete Fourier Transform for encryption purpose and it deals with private key cryptosystem, works in the frequency domain.

Selective bit plane encryption using AES

Podesser, Schmidt and Uhl, 2002 [6], selective bit plane encryption using AES is proposed. Several experiments were

conducted on 8 bit grayscale images, and the main results retained are following: (i) encrypting only the MSB is not secure; a replacement attack is possible (ii). Encrypting the first two MSBs[2-10] gives hard visual degradation, and (iii) Encrypting three bit planes gives very hard visual degradation.

In 2005, Roman Pfarrhofer and Andreas Uhl [8], proposed selective encryption of JBIG encoded visual data exploiting the interdependencies among resolution layers in the JBIG hierarchical progressive coding mode. Engel and Uhl, 2006. In [9], a JPEG2000 lightweight encryption scheme is proposed. Only lower resolutions are compressed with classical dyadic wavelet transform. For higher resolutions, the algorithm relies on a secret transform domain constructed with anisotropic wavelet packets (AWPs)[11-12]. The aim of this proposal is to allow transparent encryption for applications requiring low-resolution preview.

Hammed A younis,Turki Y Abdalla and Abdulkareem Y Abdalla,2009 [11], proposed only 6.25%-25% of the original data is encrypted for four different images, resulting in a significant reduction in encryption and decryption time.

According to this paper International Journal of Computer Applications (0975 – 8887) Volume 63– No.16, February 2013.

5. PROPOSED WORK

In proposed system we discuss the partial encryption of an image using DNA coding. So in this an image is selected and for encryption that a part of image which we think it is important will be selected for encryption[24] and that is transformed to DNA format. That is the image pixels are converted to DNA sequence A, C, G, T and these sequences are encrypted using RC4 Encryption.

They propose a novel concept of combined partial image encryption using phase manipulation and sign encryption. Entire encryption process involves two stages where image to be encrypted are applied to phase manipulation block. In first stage Fourier Transform (FT)[23][25] is applied to get phase and magnitude of the input image. Phase of the image are scrambled to get modified image after applying Inverse Fourier Transform. In second stage the modified image is partially encrypted by using sign encryption.

According to ali.a yassin,Iraq basrah, the algorithm rely on two images , the first is representing the image that we want encryption it and the second key image is deriving from it. The high performing is very active of algorithm when we deal with pixels parts of both images , these parts are calling edge pixels that calculate in canny method. At last we are performed encryption operation by using "XOR" for each layers in input and key images for producing encrypted image.

According to Priyanka Agrawal and Manisha Rajpoot[13-18] explained a concept where important part of the image that can efficiently achieve by conceptually selecting the part of the image which is further used in its normal mode of operation for encryption. Once encryption is done, the encrypted data is sent along with remaining original part of the message, ensuring its secured transmission and distribution over public networks.

According to V.V.Divya, S.K.Sudha and V.R.Resmy[19-21]. The image to be encrypted is decomposed into 8X8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT ,Then, only selected DCT coefficients i.e the DCT coefficients correlated to the higher frequencies of the image block are encrypted. For encryption the DCT coefficients are xored with pseudorandom bit, Pseudorandom bit is generated by Non-Linear Shift back Register. The bits generated by Non-Linear Shift back Register cannot be predicted so cryptanalysis becomes difficult. To enhance the security further the unencrypted DCT coefficients are shuffled.

5.1 SYTEM ARCHITECTURE

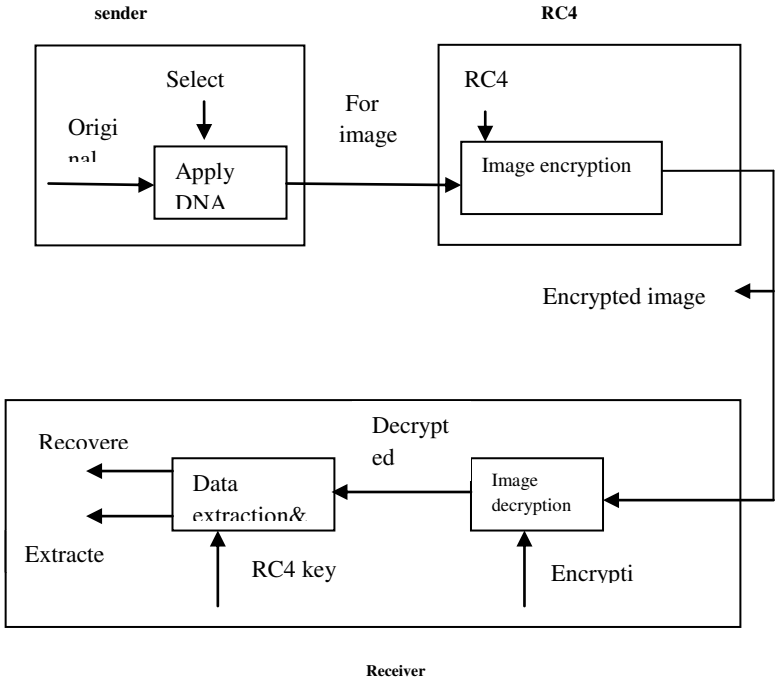


FIG 2: System Architecture

5.2 METHODOLOGY

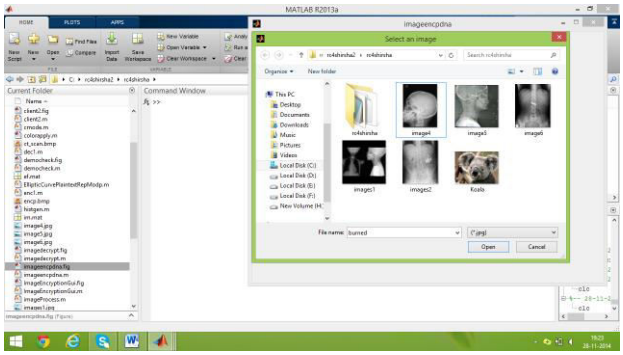
Here in this System Architecture we can clearly find how does the process goes on, so here we have 2 steps at the sender side and 2 steps at the receiver side
At the sender side

1. First the sender has to select the image.
2. And in that select the particular area of interest.

3. For that selected area of interest DNA transformation to be applied.
4. And to these DNA sequences the RC4 encryption to be applied.
5. So that we get the encrypted image, which to be send to the receiver.
6. At the receiver side
7. We receive the encrypted image.
8. This image to be decrypted, that is the RC4 decryption to be applied.
9. And then again the reverse DNA transformation to be applied.
10. So we get the encrypted image.

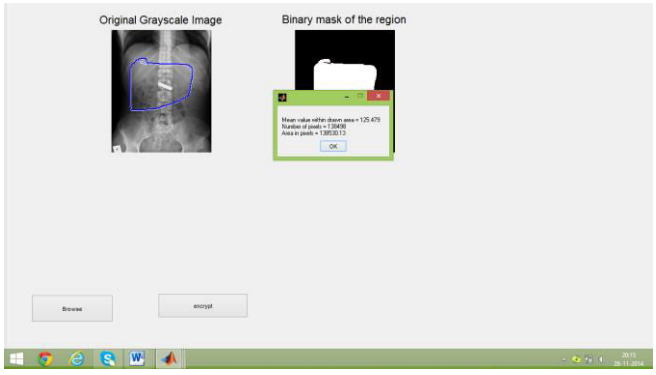
5.3 Implementation:

5.3.1 Selecting image from folder



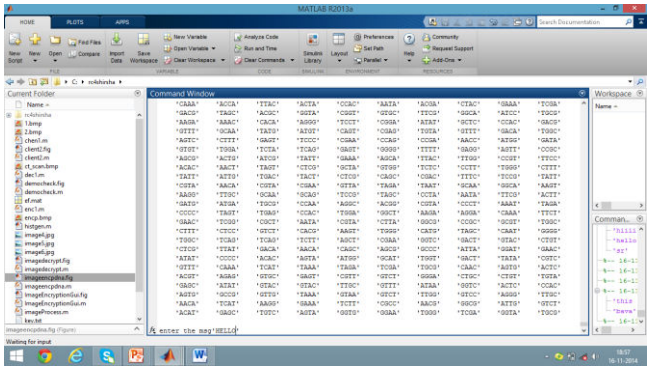
In the above figure we can see a screen where folder is opened. So here we have to choose any image which can later be used for encryption. For this we have to first choose an image by clicking on it. And then click on open button to select it or encryption.

5.4 Selecting area of interest



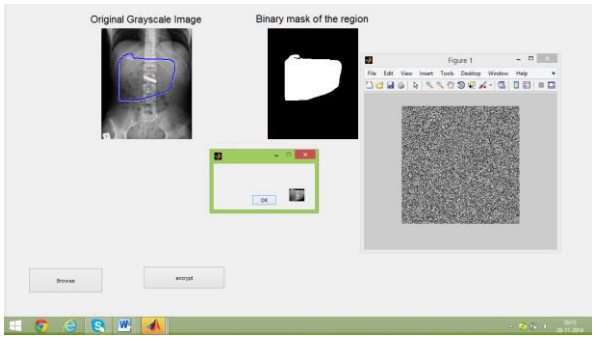
The above figure describes how to select an area of interest in an image. So here an image will be displayed after selecting an image for encryption. In this image we have to select an area of interest by left clicking the mouse button and draw an area of interest on that image after that the masked region of the image will be shown as in the above figure. And a prompt button will be displayed showing the area of pixels.

5.5 Generating the values



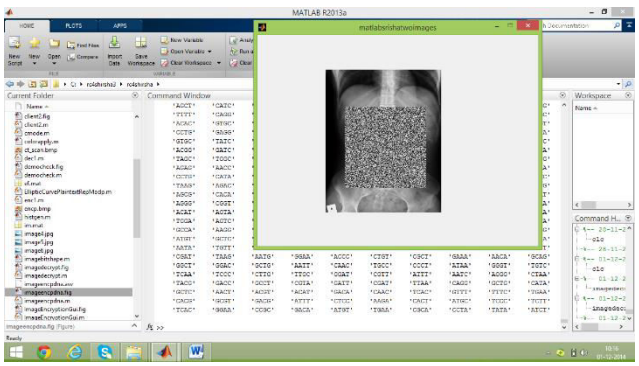
The above figure describes how the values are generated in the command window of Mat lab. So here we see the values AGCT, TAGT, GTTA… so on hence these are the values which are generated after the RC4 encryption is applied on the DNA values.

5.6 Encrypted part of image



The above figure describes how the selection of area of interest will be done. So here we select the area of interest and after that the binary masked region will be displayed. And a prompt of selected area will be appeared, after clicking on the ok button the encrypted image data will be displayed in a window as shown above.

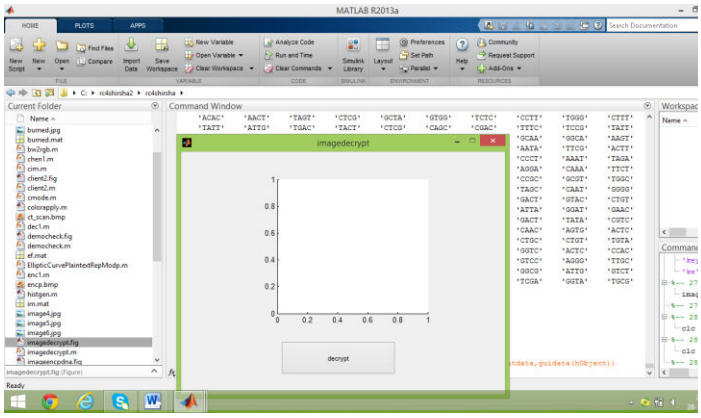
5.7 Encrypted part along with total image



The above figure describes how the image looks after the encryption process applied on the image data. So here we can see the window displaying the command prompt in mat lab where the values are generated and after this the image will be displayed on the screen as shown above. As it is partial

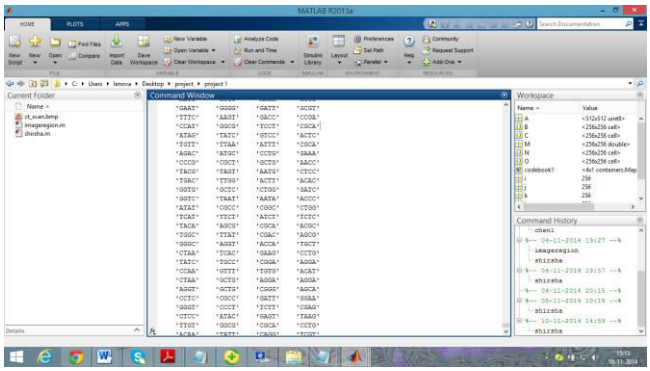
image encryption we see both the encrypted part i.e the area of interest along with the total image which is not encrypted.

5.8 Decryption button



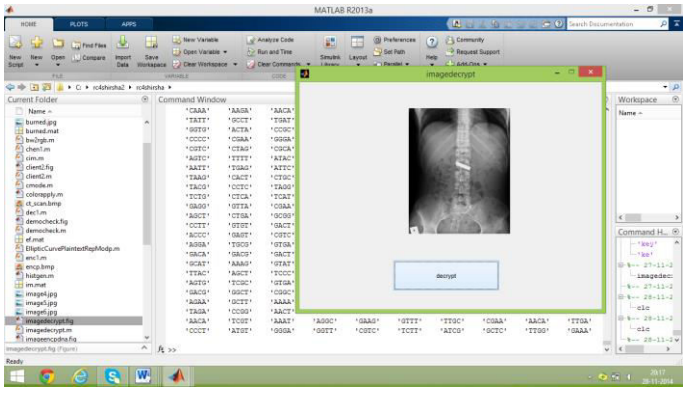
The figure describes the starting of decryption process, here we see the window displaying a decryption button. So by clicking on the decryption button the decryption of the image takes place and the image will be displayed later.

5.9 Generating decryption values



The above figure describes how the values will be displayed in the command window of Mat lab. These values are decrypted values of the image. So that from these values the original image can be generated back.

5.10 Image after decryption



The above figure describes how the decrypted image displayed after the decryption process. So here we see the image is displayed in a window. This is displayed only after the decryption button is clicked.

6. CONCLUSION

In this paper we have presented an analysis and implementation of selective image encryption algorithm using mat lab. The technique proposed in this paper is easy to understand and can easily be implemented through mat lab. This technique can be very useful in various fields of life where partial encryption is required. Partial encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile network. So we have presented methods to encrypt images for a secure transfer purpose. We have shown that the quality of the encryption depends on the chosen crypto-system. Encryption increases the entropy of the image and thus the number of bits necessary by pixel. From the viewpoint of security, the experimental results reveal that the proposed partial encryption technique achieves better security than the individual encryption approaches. The encrypted images are low and are resistant to statistical attacks including the cipher text-only attack and the known/chosen plaintext attack. The proposed algorithm has the best performance, the lowest correlation and the highest entropy than the existing partial encryption methods. Hence better security has been provided.

ACKNOWLEDGEMENT

The heading should be treated as a 3rd level heading and should not be assigned a number.

REFERENCES

[1]. Nidhi S Kulkarni, Balasubramanian Raman, and Indra Gupta, “Selective encryption of multimedia images”, NSC 2008, December 17-19, 2008.

[2]. Gaurav Bhatnagar , Q.M. Jonathan Wu, Selective image encryption based on pixels of interest and singular value decomposition, Digital Signal Processing 22 (2012) 648–663.

[3]. Priyanka Agrawal and Manisha Rajpoot A Fast and Secure Selective Encryption Scheme using Grid Division Method, IJCA vol.51 no.4,pp 29-33, Aug -2012.

[4]. Panduranga H T et al. / International Journal of Engineering and Technology (IJET) “Selective Image encryption for medical and satellite images”.

[5]. Marc Van Droogenbroeck and Raphaël Benedett “Techniques for a selective encryption of uncompressed and compressed images”.

[6]. Rafael_C._Gonzalez,_Richard_E._Woods,_Steven_L._E “Digital image processing”.

[7] R.Norcen, M.Podesser, A.Pommer, H.P.Schmidt,A.Uhl,Confidential storage and ransmission of medical image data,Computers in Biology and Medicine 33(2003) pages 277-292.

[8] J.C.Borie, W.Puech, M.Dumas, Encrypted Medical Images for Secure Tranfer, International Conference on Diagnostic Imaging and Analysis ICDIA 2002,Shanghai, P.R China August 18-20 pages 250-255.
[9] Nidhi S Kulkarni, Balasuramanian and Indra Gupta. 2008, "Selective encryption of multimedia images", XXXII National Systems Conference, NSC 2008, December 17-19.
[10] Parameshachari B D and Dr. K M Soyjaudah, 2012, "A Study of Binary Image encryption using Partial Image Encryption Technique" International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.3, pp-955-959.
[11] Parameshachari B D and Dr. K M S Soyjaudah, 2013, "A New Approach to Partial Image Encryption" Proceedings of ICAdC, AISC 174, pp. 1005–1010, © Springer India 2013.
[12] Parameshachari B D, Panduranga H T and Dr. K M S Soyjaudah, 2012, "A Overview on Partial Image Encryption Approaches", International Journal of Engineering Research and Development (IJERD), Volume 1, Issue 2, pp. 49-54.
[13] Lala Krikor, Sami Baba, Thawar Arif, Zyad Shaaban Faculty of Information and technology, Applied Science University "Image Encryption Using DCT and Stream Cipher."
[14] H. Cheng and X. Li. Partial Encryption of Compressed Images and Videos. IEEE Trans. On Signal Processing, 48(8):2439–2445, Aug. 2000.
[15] W. Puech and J. Rodrigues, "Crypto-compression of medical images by selective encryption of DCT", 13th European Signal Processing Conference, Turkey, September 2005.
[16] Rodrigues, J.M. Puech, W. Bors, A.G. "Selective Encryption of Human Skin in JPEG Images", IEEE International Conference on Image Processing, 2006.
[17] Han Shuihua, Yang Shuangyuan, "An Asymmetric Image Encryption Based on Matrix Transformation" Department of Information System, School of Managemnet, Xiamen University.
[18] Xiliang Liu, "Selective encryption of multimedia content in distribution networks: challenges and new directions", Proceedings of Communications, Internet, and Information Technology (CIIT 2003), Scottsdale, AZ, USA, Nov. 2003.
[19] Prasanna SRM et al, 2006, "An image encryption method with magnitude and phase manipulation using carrier images", IJCS 1(2):132–137
[20] H. Cheng and X. Li. 2000, "Partial Encryption of Compressed Images and Video", IEEE Transactions on Signal Processing, 48(8), pp. 2439-2451.
[21] M. Podesser, H. P. Schmidt and A. Uhl. 2002, "Selective Bitplane Encryption for Secure Transmission of Image Data in MobileEnvironments", 5th Nordic Signal Processing Symposium, on board Hurtigruten, Norway, October 4-7.
[22] Pfarrhofer, R., Uhl, A.2005, "Selective Image Encryption Using JBIG" In: Dittmann, J., Katzenbeisser, S., Uhl, A. (eds.) CMS 2005. LNCS, vol. 3677, pp. 98–107. Springer, Heidelberg.
[23] Ju-Young Oh, Dong-Il Yang, Ki-Hwan Chon, 2010, "A Selective Encryption Algorithm Based on AES for Medical Information", the Korean Society of Medical Informatics.
[24] Parameshachari B D ,K M Sunjiv Soyjaudah, PhD. Sumitrha Devi K A, PhD. " Secure Transmission of an Image using Partial Encryption based Algorithm".
[25] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), 83-91.
[26] Cherian, A., Raj, S.R. and Abraham, A. (2013), 'A Survey on different DNA cryptographic methods', International Journal of Science and Research, Vol. 2, No. 4., pp. 167-169.

BIOGRAPHIES

I am V.Murali completed B.Tech in ANITS College in 2006. I completed M.Tech - Computer science in Andhra university in 2009. I am Current working as a Assistant professor –CSE in Avanthi Engineering College, Visakhapatnam. He published many research papers in top journals like UGC,SCOPUS.

This is bandaru snehitha, completed B.Tech in computer science and engineering. Current pursuing M.Tech – CSE in Avanthi Engineering College, Visakhapatnam. She published some research papers in top journal.