Novel Approach to Secure Online Transaction using Stenography and AES in the Image

Ekta Chauhan[1] Prof. Unmukh Datta[2]

[1,2]Department of Computer Science and Engineering

[1,2]Maharana Pratap College of Technology Gwalior, India

Abstract— The use of electronic business (e business) over the internet is growing rapidly in the past several years. In e commerce business is done online without any face to face interaction. Several e transaction systems have been developed and their use is increasing in e commerce site. Security of the e commerce site is becoming more and more crucial. E transaction security is a challenging task because of the insecure communication channel. In our work we proposed a new algorithm to make an e commerce transaction more secure. In our algorithm we encrypt data using AES and this encrypted data are embedded to image edges to perform Stenography and to decrease the time of encryption and decryption. We are using parallel processing at different part of AES and we found or results are better than the previous work in terms of time and security aspects.

Key words: AES, Stenography, E Commerce, Parallel Processing, Etc

I. Introduction

Verification of Biometric [1] [2] is an automated technique whereby an individual’s identity is established by the investigative behavioral characteristic or single physiological trait, such as a signature, fingerprint, or retina. Physiological traits are established characteristics, such as iris patterns and palm prints. This kind of the measurement is fundamentally permanent. A behavioral characteristic — like as one's voice, signature, or keystroke dynamics — is influenced by both fewer manageable psychological factors and manageable movements. Because of behavioral characteristics can modify over time, the registered biometric reference template must be updated all time it is used. Although biometrics, which is Behavior-based can be less threatening and less exclusive to the users; physiological traits tend to suggestion superior security and accuracy. In any case, both methods offer a significantly identification of higher level than cards or passwords. Biometric traits are unique to the individual all; they can be used to protect from fraud or theft. Unlike a pin (personal identification number) or password, a biometric trait cannot be stolen, forgotten, or lost. Today there are over 10,000 computer rooms, military installations, blood banks, vaults, research labs, day care centers and ATMs to which access is organized applying strategies that scan an behavioral characteristics or individual's unique physiological. Biometric identifiers currently presented or undergrowth contains the voice pattern, iris pattern, fingerprint, face recognition, keystroke dynamics, palm print, retinal scan, and signature.

II. Basic Criteria for Biometrics Security System

There are total seven basic criteria for the security system of biometric: circumvention, uniqueness, universality, permanence, collectability, performance and acceptability [3]. As mentioned above, the priority one requirement for biometric data is considered by the uniqueness. It will specify how uniquely and differently each user, among groups of users the biometric method will be able to recognize every user. For instance, the each person DNA is unique and also replicates is impossible. Universality is the secondary criteria for the security of the biometric. Requirements for the exclusive characteristics of every person in the world are specified by this parameter, which is never be replicated. For example, iris and retinal are characteristics will achieve this requirement. Thirdly, a permanence parameter is required for all single character or trait which is documented of the system database and needs to be constant the various periods of time period. This parameter will generally be affected by age of the user.

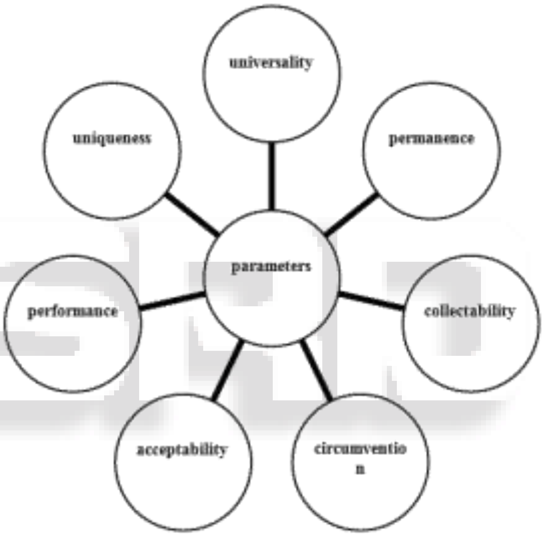


Fig. 1: Basic Criteria for Biometrics Security System

Following the parameter permanence is the collectability. The collectability parameter needs the group of every characteristic and trait of the scheme in order to authenticate their ID. Then, the presentation is the next parameter for the method which outlines how well the safety scheme works. The robustness and accuracy are the chief factors in the security system of biometric. These factors will the performance decide on the biometric safety system. The suitability parameter will select fields in which biometric skills are satisfactory. Finally, circumvention will decide how simply all characteristic and trait, providing by the user can lead to failure throughout the confirmation procedure. DNA is believed to be the most challenging characteristic leading to the failure of the confirmation procedure [4].

III. Advanced encryption standard (AES)

In the late 1990s, the NIST (U.S. National Institute of Standards and Technology) shown a competition to the develop a replacement the DES. The winner, announced in the 2001, is the Rijndal algorithm, destined to become the novel AES. Rijndael mixes up the SPN model by containing

Galios field operations in the all round. Somewhat alike to RSA modulo mathematics operations, the Galios field operations create apparent gibberish, but can be mathematically inverted. AES has Safety is not an absolute; it's a relative between cost and time. Any question about the safety of the encryption should be posed in positions on how great cost, and how long time will it take an attacker to discover a key? Presently, there are theories that military intelligence facilities possibly have the economic and technical means to attack keys equivalent to about the 90 bits, although no civilian scholar has really reported or seen of such an ability. Demonstrated and Actual systems today, within the bounds of the commercial budget of about 1 million dollars can be a holder key lengths is about 70 bits. An aggressive estimate of the rate of scientific development is to assume that skills will dual the speed of computing devices each year at an unaffected cost. If exact, 128-bit keys would be in concept be in the range of the military budget within the 30-40 years. An illustration of the present status of AES is given by following example, where we take up an attacker with the ability to construct or obtaining a method that attempts keys at the rate of the one billion keys per second. This is at least 1000 times quicker than the fastest personal computer in 2004. Under this statement, the attacker will need about the 1000000000000000000000 years to try each probable key for the weakest type, AES-128.The key length should thus be selected after determining for how extended security is obligatory, and what the cost should be to brute force a secure key. In various military circumstances a few hours or days safety is sufficient – after that the war or the task is complete and the document uninteresting and value without. In different cases a all time may not be extensive sufficient. There is currently no evidence that the AES has any weaknesses, creation any attack other than thorough search, i.e. brute force, likely. It is necessary to confirm all and each implementations safety, but hard since it needs careful analysis by experts. A most important aspect of an evaluation of some particular implementation is to define that such an analysis has been made, or can be conducted [5], [6].

IV. STEGANOGRAPHY

Steganography is the art of hiding a message, image, or file within another message, image, or file. The word Steganography comes from Greek word Steganos (covered) and Graphy (writing).Therefore steganography means covered writing. The objective of steganography is to hide a secret message within a cover-media in such a way that in such a way that others cannot detect the presence of the hidden message.

Different types of steganography are:

- Text Steganography: The method of hiding secret information in a text is known as text steganography.
- Image steganography: The image steganography is the process in which we hide the data within an image.
- Audio steganography: The method of hiding secret information in an audio is known as audio steganography.
- Video steganography: The method of hiding secret steganography [7]

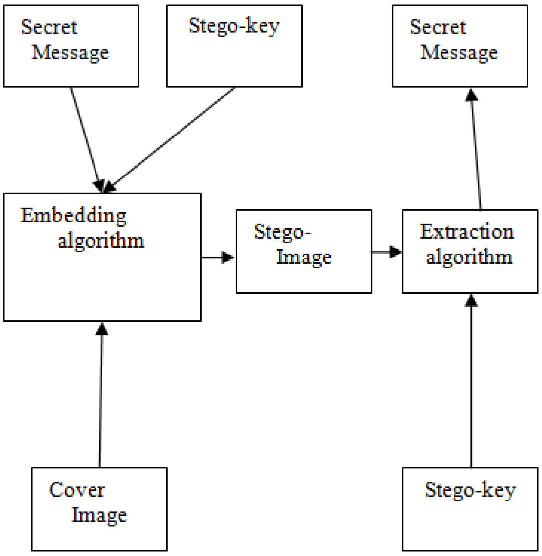


Fig. 3: Basic model of steganography

Some terms which are used in the context of cryptography and steganography.

- Plain text: original message.
- Cipher text: scrambled message.
- Key: It is used for encryption and decryption.
- Encryption: It is the process of transforming plain text into cipher text.
- Decryption: It is the process of transforming cipher text into plain text.
- Cover-Image: Original image which is used as a carrier for secret knowledge.
- Stego-Image: After embedding a message in to cover image is known as stego-image.
- Stego-Key: A key is used for Embedding and extraction.
- Cryptanalysis: It is the study of examining data methods in order to reading the hidden aspects of the structures.
- Steganalysis: It is the study of detecting messages hidden using steganography.

V. LITERATURE REVIEW

Hemang A. Prajapati, Dr. Nehal G. Chitaliya et al present that In the last few years communication technology has been improved, which increase the need of secure data communication. For this, many scholars have utilized much of the their time and efforts in an effort to discover appropriate ways for hiding documents. There is a method used for hiding the important information imperceptibly, which is Steganography. Steganography is the art of hiding information in such a way that prevents the detection of hidden messages. The process of using steganography in conjunction with cryptography, called as Dual Steganography. This paper tries to elucidate the basic concepts of steganography, its various types and techniques, and dual steganography. There is also some of research works done in the steganography field in the past few years [8].

Rekha D.Kalambe, Rakesh Pandit, Sachin Patel et al present that Steganography is the hiding ability the existence of the document in another medium transmission to achieve the communication which is secret. It does not cryptography restore, but quite boost the safety applying its features which is abstruse. In this paper, we have measured on a cryptography and Steganography methods which offer extremely protected skin tone information hiding. Biometric characteristic used to apply the steganography is a skin tone region of images. Here useful document is entrenched within the skin region of the image which will give an outstanding protected place for information hiding. For this finding skin tone is needed to be achieved. Different stages of the applied the hiding information by cropping an image interactively.. Algorithm of Cryptography is used to change the secret information into an unreadable form before embedding; which offers a strong backbone for information safety. This study paper attentions on the illuminating the method to protect message or document with non-repudiation and authenticity. So with this object oriented steganogaphy we can track skin tone objects in the an image with the satisfactory and higher security PSNR .Modern steganography's aim is to keep its mere presence undetectable [9].

Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn et al presents that method of the hiding knowledge have lately become significant in a no. of the application areas. Digital video, audio, and pictures are progressively furnished with individual, but imperceptible marks, which may hold a secreted serial number or copyright notice or even help to stop the illegal copying directly [10].

Md. Khalid Imam Rahmani, Kamiya Arora, Naina Pal et al present that The two important security features that deal with transmitting document or knowledge over several mediums like the Internet are cryptography and steganography. Steganography deals with the presence of the knowledge is hiding and cryptography deals with the hiding contents of an information. Both of them are used to ensure safety. But none of them can simply satisfy the basic safety requirements, i.e. the features such as capacity, robustness and undetectability etc. So a novel technique based on the grouping of both steganography and cryptography well-known as Crypto-Steganography, which overcome each other's weaknesses and make challenging for the intruders to steal sensitive or attack knowledge is being proposed. This paper also defines the basic concepts of cryptography and steganography on the basis of earlier literatures presented on the topic [11].

Mehdi Hussain, et al present that The security of digital data's significance has been improved due to the boost of internet communication. Providing safety for client server communication over the internet is a serious topic due to open world digital eavesdroppers. Commonly, authentication of PIN is required for the forming a connection between the environment of the client and server. The password on the client is confirmed by the server ends of the establish a connection which is valid. Verification of the password is Successful initiates the server and the client to achieve further safe response and request mechanisms. The difficulty of the authentication password over insecure network presents in many application areas, such as remote logins of computer networks, web login. Hence the significance of the confidential transmission of the password over the insecure internet becomes the necessity of safe authentication. In this paper, we suggested a protected password transmission over the internet for verification of the environment of the client/ server applying the image steganography and encryption. Client password is the first encoded and then embedded in an image applying a steganographic algorithm at the client side and the transmitted over a dangerous network to the web server. On the other side of the server, remove the safely password from an image steganography decoding algorithm, decrypt and confirmed it's with SQL database server. In the case if the intruder steals the image over the network she/he will be unable to decrypt the password from the image. The prototype of the suggested method is implemented using the ASP.net, JavaScript, and Html for confirmation purpose [12].

VI. PROPOSED METHODOLOGY

In e commerce money transaction must be sure to secure our payment information like our password which may be biometric identified like fingerprint, iris, voice, etc. in this paper, we focus on AES encryption algorithm and Stenography with applying pixel swapping to encrypt the input image for the secure transaction purpose. This paper has a target on compress the time of encryption and decryption adopting multithreading. Consider following conspiracy to explain the proposed work.

A. *At Sender Side-*

1) To convert the first picture into binary code.
2) Divide binary code into obstructs, all pieces contains 16 characters (128bits).
3) Apply AES encryption procedure to change over plain text hinders into cipher text block.
4) AES Algorithm has the accompanying steps.

The main step is taking info plain content, then apply Key Expansion-Round keys are derivational from the figure key applying Rijndael's key calendar. Starting Round (Add Round Key- singular byte of the state is joined with the round key utilizing bitwise XOR) Rounds (Sub Byte singular byte is supplanted with another from lookup table. Movement Rows individual line of the state is cycle moving. Blending Columns- a blending procedure which works on the segments of the state, consolidate the 4 bytes. Include Round Key) Final Round (Sub Bytes, Shift Rows, then Add Round Key)

5) Transfer these cipher text into binary code.
6) Encrypt picture is inserted into the cover picture by utilizing an LSB method by applying stego key and discovering a picture is called stego picture and apply the Algorithm of Pixel Swap utilizing a pseudo–random succession than send to the recipient.

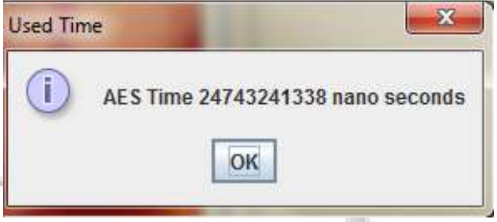
B. *At Receiver Side-*

1) Change the got picture into binary code.
2) Embedded stego binary picture into figure content bit and translating, select the pixels utilizing the same Pseudo-irregular arrangement.
3) Convert the content and isolated into pieces, every one of the 16 characters.
4) Application unscrambling procedure to a cipher code piece of discovering a secret picture purpose

C. Base paper screenshot

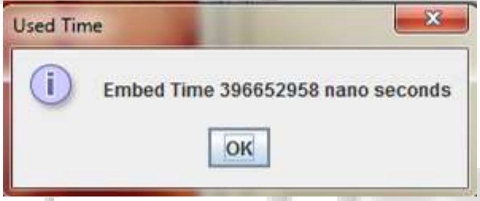
First open the main menu which contains encoding, decoding and exit the function. Encoding is used for the converted input image into encrypt image, decoding is used for converting decrypt image into input image and last function is the exited is use for come out from working area It contains some steps:-

1) First open the main menu and select the encoding function now open another screen which is divided into two parts, first is the original image and second is steganographed image.
2) Now select the fingerprint image, then select the embedded image before embedded giving a file name for saving file's purpose then embed it.
3) It represents the three timing which is represented below Fig.1 present the base paper AES time, which is show encrypting them, Fig.2 present the base paper embedded time, which is embedding a fingerprint image with another image and Fig.3 present the base paper total (AES and embed time) time.



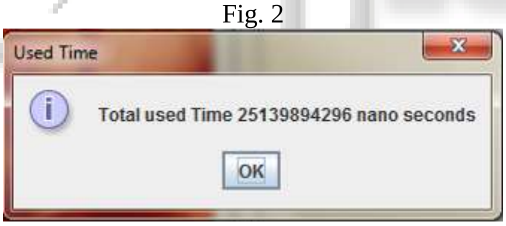
AES Time 24743241338 nano seconds

Fig. 1



Embed Time 396652958 nano seconds

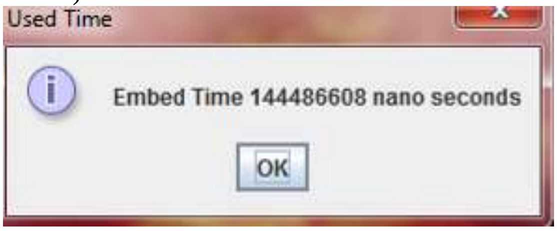
Fig. 2



Total used Time 25139894296 nano seconds

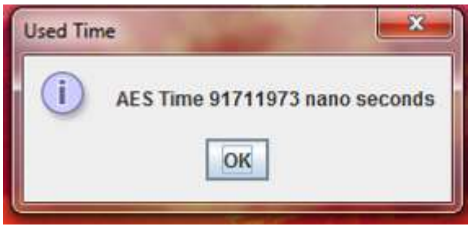
Fig. 3

4) After encoding performs the decoding. Select the decoding from the main menu and then open decoding screen and present three buttons open, decode and reset.
5) First open the image which is already encoded and decode the selected image. After deciding we find again three times Fig.4 present the base paper decade, embedded, Fig.5 present the base paper AES time time which is show decrypting time and Fig.6 present the base paper total used (AES and embed time) time.



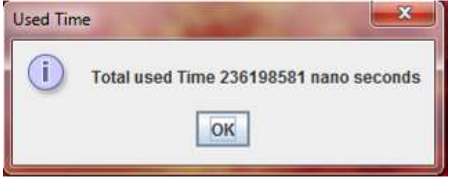
Embed Time 144486608 nano seconds

Fig. 4



AES Time 91711973 nano seconds

Fig. 5

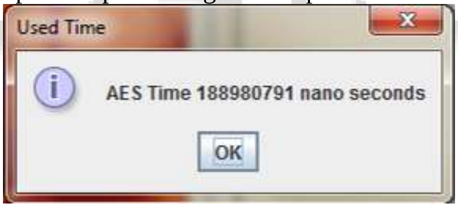


Total used Time 236198581 nano seconds

Fig. 6

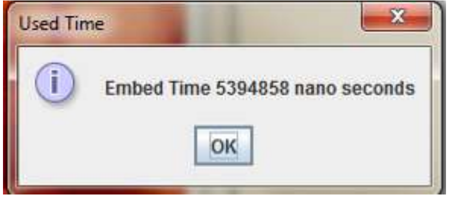
D. Final paper screenshot

6) First open the main menu and select the encoding function now open another screen which is divided into two parts, first is the original image and the second is two part image. Because applying the parallel processing.
7) Now select the fingerprint image, then select the embedded image before embedded giving a file name for saving file's purpose then embed it just like base paper.
8) It represents the three timing which is represented below Fig.7 present the base paper AES time, which is show encrypting them, Fig.8 present the base paper embedded time, which is embedding a fingerprint image with another image and Fig.9 present the base paper total (AES and embed time) time. These all time less than base paper time because here applying the parallel processing for compress the time purpose.



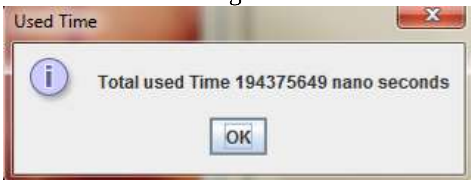
AES Time 188980791 nano seconds

Fig. 7



Embed Time 5394858 nano seconds

Fig. 8

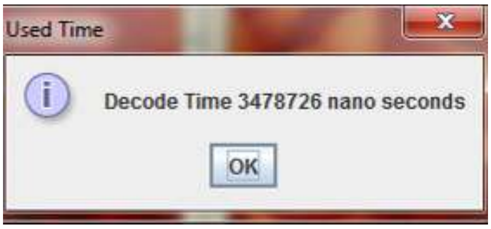


Total used Time 194375649 nano seconds

Fig. 9

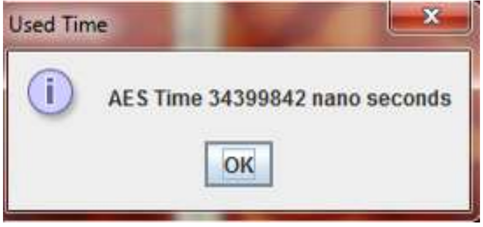
9) After encoding performs the decoding. Select the decoding from the main menu and then open decoding screen and present three buttons open, decode and reset just like base paper, but it contains two similar size part area for deciding because decoding is also performed parallel.

10) First open the image which is already encoded and decode the selected image. After deciding we find again three times Fig.10 present the base paper decade, embedded, Fig.11 present the base paper AES time time which is show decrypting time and Fig.12 present the base paper total used (AES and embed time) time. It is less than base paper decoding time.



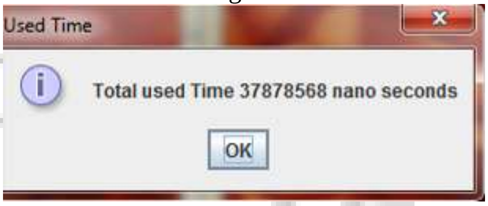
Decode Time 3478726 nano seconds

Fig. 10



AES Time 34399842 nano seconds

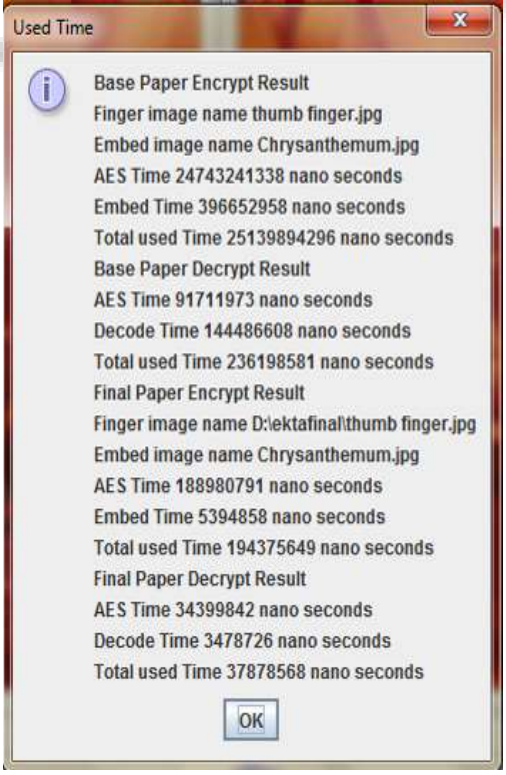
Fig. 11



Total used Time 37878568 nano seconds

Fig. 12

11) And in last show all time base paper (AES, embedded and total time) and final paper (AES, embedded and total time).



Base Paper Encrypt Result
Finger image name thumb finger.jpg
Embed image name Chrysanthemum.jpg
AES Time 24743241338 nano seconds
Embed Time 396652958 nano seconds
Total used Time 25139894296 nano seconds
Base Paper Decrypt Result
AES Time 91711973 nano seconds
Decode Time 144486608 nano seconds
Total used Time 236198581 nano seconds
Final Paper Encrypt Result
Finger image name D:\ektafinal\thumb finger.jpg
Embed image name Chrysanthemum.jpg
AES Time 188980791 nano seconds
Embed Time 5394858 nano seconds
Total used Time 194375649 nano seconds
Final Paper Decrypt Result
AES Time 34399842 nano seconds
Decode Time 3478726 nano seconds
Total used Time 37878568 nano seconds

Fig. 13

VII. CONCLUSION

With the help of this paper, we are presenting a novel technique to make more secure big e commerce transaction and with the help of parallel processing which is applied an AES. We are able to reduce the encryption time and we are clearly seen with the help of results for the security purpose use of AES and Stenography is quite impressive. In future work we can apply AES and Stenography with parallel processing to enhance the security of e commerce transaction.

REFERENCES

[1] www.biometrics.org
[2] www.cse.msu.edu/biometrics
[3] Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001
[4] Sandra Maestre, Sean Nichols "DNA Biometrics", 2009
[5] A.W. Naji, Shihab A. Hameed, B.B.Zaidan, Wajdi F. Al-Khateeb, Othman O. Khalifa, A.A.Zaidan and Teddy S. Gunawan, ― Novel Framework for Hidden Data‖, International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No 1 ISSN: 1947-5500, P.P 73-78,3 Aug 2009, USA.
[6] Hamdan. Alanazi, Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan, ―New Frame Work of Hidden Data with in Non Multimedia File‖, International Journal of Computer and Network Security, 2010, Vol.2, No.1, ISSN: 1985-1553, P.P 46-54,30 January, Vienna, Austria
[7] Shristi Mishra And Ms.Prateeksha pandey,” A Survey on Crypto-Steganography” International Journal on Recent and Innovation Trends in Computing and Communication Volume: 3 Issue: 2,pp: 81-84.
[8] Hemang A. Prajapati, Dr. Nehal G. Chitaliya,” Secured and Robust Dual Image Steganography: A Survey”, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, January 2015,pp:30-37.
[9] Rekha D.Kalambe, Rakesh Pandit,Sachin Patel,” Survey Paper of Encrypted Data Hiding using Skin Tone Detection”, International Journal of Computer Applications (0975 – 8887) Volume 79 – No5, October 2013,pp:6-10.
[10] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn,” Information Hiding|A Survey”, Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.pp:1062-1078.
[11] Md. Khalid Imam Rahmani, Kamiya Arora, Naina Pal,” A Crypto-Steganography: A Survey”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014,pp:149-155.
[12] Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Ishrat Batool and Muhammad Arif,” Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography”, International Journal of Security and Its Applications Vol.9, No.2 (2015), pp.179-188
http://dx.doi.org/10.14257/ijsia.2015.9.2.17