Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.710 – 715

SMART ENCRYPTION USING STEGANOGRAPHY AND PIXEL PATTERN

Mrs. Priya Karemore, Amrit Anand, Pranshu Tiwari, Utam K.Singh, Nitish Kumar, Rahul Kumar

Department of Computer Technology, Priyadarshini College of Engineering, Nagpur
Email: amritanand57@gmail.com
Contact no-+91-8087665794

ABSTRACT-Dynamic Information security has turned into a noteworthy reason for concern since gatecrashers are worried with perusing the data. It is a direct result of electronic dropping security is under danger. This paper manages the relative examination of steganography and utilizing RGB estimation of pixel. "Steganography" is a greek word which signifies "concealed composition". It is the craft of stowing away the mystery message inside of a picture. The objective of steganography is to abstain from attracting suspicious to transmission of covered up message. It serves a superior method for securing message than cryptography which give security to substance of message and not the presence. Unique message is being covered up inside of a bearer such that the progressions happened in transporter are not watched. The shrouded message in bearer is hard to identify without recovery. Distinctive strategies are depicted in this paper for steganography and utilizing RGB estimation of the pixel .In this paper we are attempting to make steganography all the more hard with the goal that it can't be wrenched effortlessly we have alter the procedure of steganography.

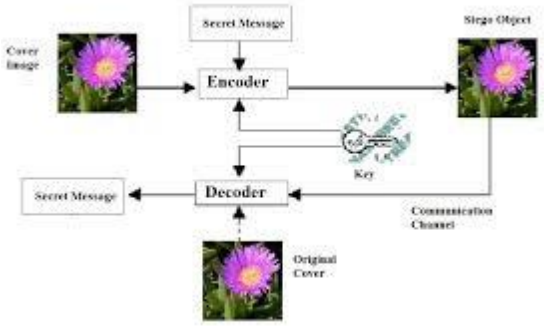
Catchphrases: Steganography, Cryptography, Secret Information

1. INTRODUCTION

In the field of Data Communication, security-issues have got the top need. Web clients oftentimes need to store, send, or get private data. The most well-known approach to do this is to change the information into an alternate structure. The subsequent information can be seen just by the individuals who know how to return it to its unique structure. A noteworthy downside to encryption is that the presence of information is definitely not covered up. Information that has been scrambled, in spite of the fact that is unintelligible, still exists as information. In the event that sufficiently given time, somebody could in the end decode the information. It is simple for the interloper to get data about the key which is utilized to scramble the mystery data. Prior to the development of advanced means, conventional strategies were being utilized for sending or accepting messages. Conventional strategies were used to scramble the message to give security from the Cryptography is an

approach to secure the plain instant messages. Cryptography was made as strategy for securing the mystery of correspondence. A wide range of strategies have been created to scramble and unscramble mystery data in request to keep the it mystery. Shockingly it is some of the time not enough to keep the substance of a message mystery, it is too important to keep the presence of the message secret. Cryptography is utilized to keep the message mystery yet it does not give mystery of the message. An answer for this issue is steganography. Steganography by word is grouped into two sections : steganos which implies "mystery or secured" and representation which signifies "composing".

The motivation behind steganography is secret correspondence to conceal a message from an outsider. A steganographic framework accordingly inserts concealed substance in spread media so as not to stimulate a spy's suspicion. Steganography is the procedure of concealing a mystery message inside of a bearer in such a way that somebody can't know the vicinity of the covered up message. The essential structure of Steganography is made up of three parts: the "bearer", the message, and the key the bearer can be a work of art, a computerized picture, an mp3, even a TCP/IP bundle in addition to other things. The article will "convey" the shrouded message. A key is utilized to translate/unravel/find the shrouded message.



2. RELATED WORK

In this we have customize the basic process of steganography .We have encrypted the plaintext into cipher text using the AES algorithm then this cipher text is converted into image using stereography. The image then converted into textual format by taking the RGB value and x,y co-ordinate of each pixel and adding some numerical value to it.

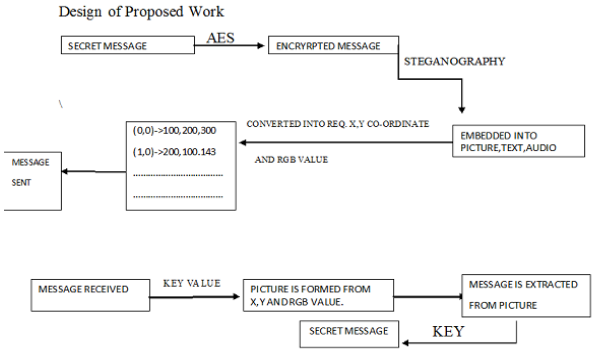
Then plain text is encrypted using AES algorithm providing second layer of protection that is hard to crack. In this paper we have used the 256 bit AES algorithm which is not only the highest level of AES algorithm and is impossible to crack. In RGB Picture Steganography portrays new calculation for RGB picture based steganography. This calculation presents the idea of putting away variable number of bits in every channel (R, G or B) of pixel in light of the genuine shading estimations of that pixel.

3. EXISTING TECHNOLOGIES

Hiding of data inside an image is simply called steganography. A lot of steganography techniques are used frequently to cover an information, [7] is an image steganography technique and [8] is an JPEG based steganography technique. In this we have redo the fundamental procedure of steganography .We have encoded the plaintext into figure content utilizing the AES calculation then this figure content is changed over into picture utilizing stegenography. The picture then changed over into literary configuration by taking the RGB estimation and x,y co-ordinate of every pixel and some numerical value to it.

At that point plain content is scrambled utilizing AES calculation giving second layer of assurance that is difficult to break. In this paper we have utilized the 256 piece AES calculation which is not just the most abnormal amount of AES calculation and is difficult to break.

4. PROPOSED TECHNIQUE



The above picture shows the proposed work of how we are going to perform the discussed approach.

In this we have re-try the key strategy of steganography .We have encoded the plaintext into figure content using the AES computation then this figure substance is changed over into picture using steganography. The photo then changed over into abstract setup by taking the RGB estimation of each pixel.

By then plain substance is mixed using AES figuring giving second layer of confirmation that is hard to break. In this paper we have used the 256 bit AES estimation which is not only the most anomalous measure of AES computation and is hard to break.

In this we have re-try the crucial system of steganography .We have encoded the plaintext into figure content using the AES count then this figure substance is changed over into picture using steganography. The photo then changed over into artistic setup by taking the RGB estimation of each pixel.

5. ENCRYPTION PROCESS

STEP 1:

In first step we have to encrypt the plain text into cipher text using AES Encryption process.

STEP 2:

In this step the cipher text or encrypted text is converted into image form by the process of steganography.

STEP 3 :

Then this image is converted into textual format using the respective value of each pixel RGB value and alpha value which shows the brightness value of each pixel, we have inserted the x,y co-ordinate of each pixel.

The textual format is sent to respective receiver. Before sending we add some value to is so that if hacked it become complex to recreate the original picture.

6. DECRYPTION PROCESS

STEP 1:
The textual format is received by the receiver.

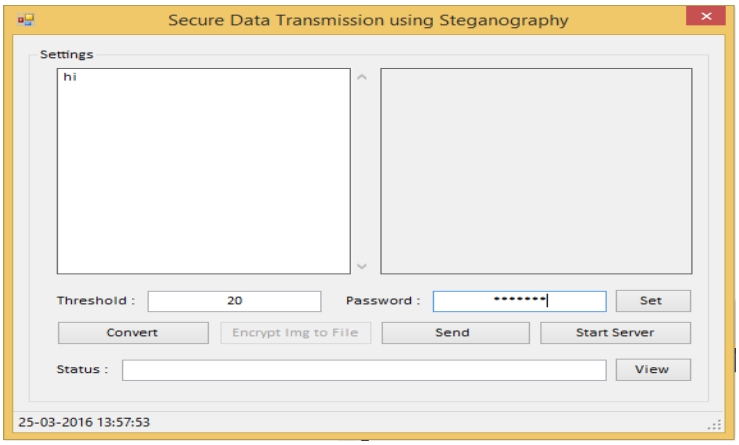
STEP 2:
This textual format which contain the RGB value and x,y co-ordinate of pixel is converted into the required picture.

STEP 3:
After forming the picture the cipher text is retrieved and then decrypted using the required key.

7. EXPERIMENTAL ANALYSIS

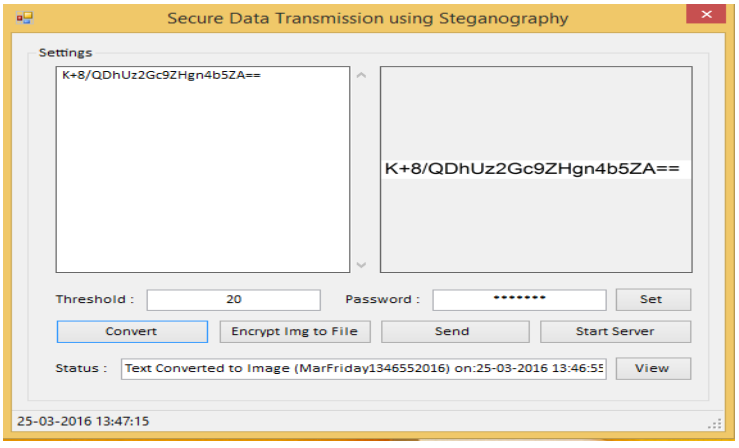
STEP 1:

We have the plain text 'hi' and threshold value which we have to add to the RGB and x, y co-ordinate, and key is 'welcome'.



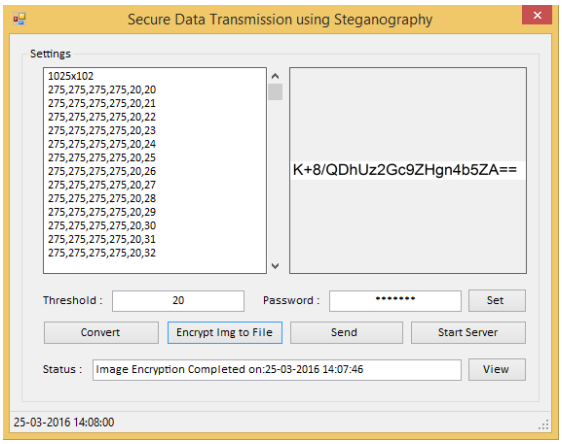
STEP 2:

This is encrypted using AES algorithm and converted into image format.



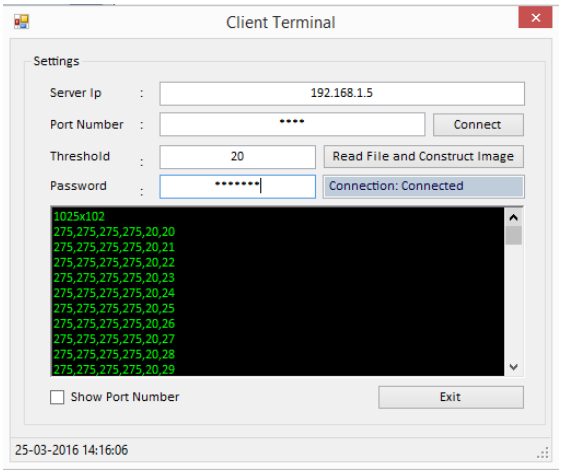
STEP 3:

Then this is converted into the RGB and x, y co-ordinate.



STEP 4:

This textual format is send to the receiver and the respective receiver receives the message.



STEP 5

After receiving the message it is converted into image and cipher text is retrieved from it and decrypted into the original plain text.

8. CONCLUSION

Thus in this paper we proposed an added level of security by customizing the basis process. This process make it difficult to retrieve the message if hacked. We have used AES algorithm of 256 bit which is the highest level of encryption standard. We have also used a threshold value which add a specific numerical value thus making it impossible to retrieve the message if hacked as the required image cannot be formed. Some of the application of it can be used in the military or some specific organization.

References

- *Wayner, Peter (2002). Disappearing cryptography: information hiding: steganography & watermarking. Amsterdam: MK/Morgan Kaufmann Publishers.*
- *Fridrich, Jessica; M. Goljan; D. Soukal (2004). "Searching for the Stego Key" (PDF). Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking*
- Akbas E. Ali (2010). "A New Text Steganography Method By Using Non-Printing Unicode Characters"
- Patrick Philippe Meier (5 June 2009). "Steganography 2.0: Digital Resistance against Repressive Regimes"
- Kundur D. and Ahsan K. (April 2003). "Practical Internet Steganography: Data Hiding"

