Cardinal Digital Image Data Fortification Expending Steganography

B.praveen, Umarani Nagavelli, Anand Thota, Debabrata Samanta

***Abstract*: *In the present advanced world applications from a PC or a cell phone reliably used to complete each sort of work for expert and also amusement reason. In any case, one of the significant issues that a product distributer will confront is the issue of theft. All through the most recent few decades, all-major or minor programming has been pilfered and unreservedly flowed over the web. The effect of the uncontrolled programming theft has been gigantic and keeps running into billions of dollars consistently. For an autonomous designer or a software engineer, the effect of robbery will be colossal. Enormous organizations that make specific programming regularly utilize complex equipment strategies, for example, utilization of dongles to stay away from programming robbery. Be that as it may, this is absurd to expect to improve the situation a typical autonomous software engineer of a little organization. As a feature of the exploration, another technique for programming security that does not require restrictive equipment and other complex strategies are proposed in this paper. This technique utilizes a blend of inbuilt equipment includes and in addition steganography and encryption to secure the product against theft. The properties or strategies utilized incorporate uniqueness of equipment, steganography, solid encryption like AES and geographic area. To abstain from hacking the proposed system additionally makes utilization of self-checks in an irregular way. The procedure is very easy to actualize for any designer and is usable on both customary PCs and also versatile conditions. - Steganography is the science that includes conveying mystery information in a suitable interactive media transporter, e.g., picture, sound, and video documents. It is dependably non obvious. In this message more critical than unique flag. Steganography has different helpful applications. The fundamental targets of steganography are un perceptibility, strength (protection from different picture preparing techniques and pressure) and limit of the concealed information. These are the primary variables which make it not quite the same as different strategies watermarking and cryptography. This paper incorporates the essential steganography techniques and the primary spotlight is on the survey of steganography in computerized pictures.*

Index Terms:* *Data protection, Steganography, Stego Image, Cover Image, Software Protection, Encipher, AES, Stegano DB, LSB. Steganography, Histogram, Adjacent Pixel Difference (APD), PSNR, Capacity.

I. INTRODUCTION

Information that is exchanged via computer networks is generally specified in the form of data. Data can be stored in various formats. It can be text, image, sound, video, graphics etc. These data are stored in different devices like computers, mobiles, movie players etc.

For example, digital camera stores the picture information as image bits.For storing and retrieving information, there is a need for software and devices. Digital data or software which a computer uses can be quite easily copied which is one of its main strength as well as its weakness. Most of the data transmitted are meant for mere communication purpose but some of these might be meant for confidential purpose like say banking data or ecommerce purpose. Hence, for protecting data methods like encryption are normally used. Steganography is the science or method of hiding information within an image. The protection offered by steganography can be further enhanced and more robust by using encryption techniques before hiding the text inside an image. According to BSA (Business Software Alliance) study every year the software piracy rate is increasing which has been resulting in huge revenue loss to every software companies. To overcome this, different methods are used like Licensing Acts, Patents, cryptographic methods, dongles etc. However, these methods have not been 100% effective and using special hardware is expensive and is not a good solution for small developers or companies. This cannot be used in mobiles as well. Hence, there is a need for an alternate software protection framework that is cost effective and at the same time provides excellent protection against hackers. This paper proposes a new software protection framework, which uses cryptography, steganography as well as a new process to protect both traditional desktop applications as well as the newer mobile apps as well.

II. REVIEW OF LITERATURE

With the progressions in the field of advanced picture handling amid the most recent decade, computerized picture information concealing procedures, for example, watermarking, Steganography have increased wide notoriety. Advanced picture watermarking methods shroud a little measure of information into a computerized picture which, later can be recovered utilizing some explicit recovery calculations to demonstrate the copyright of a bit of advanced data while, Steganography procedures are utilized to conceal a lot of information covertly into some harmless looking advanced medium. In this paper we are giving a forward survey of these information concealing procedures. Rejani R et al. [12] presents another/other secure Database framework dependent on steganography for information covering up. The framework gives uprightness greater classification and

Revised Manuscript Received on January 25 , 2019.
B.praveen, Research Scholar, university Of Mysore.
Umarani Nagavelli, Research Scholar, university Of Mysore.
Anand Thota, Potti griramulu College Of university and Technology.
Debabrata Samanta, Dayanad Sagar College Of Arts, Science and Commerce, Karnatka.

Confirmation amid access or altering of private information. The proposed DB framework utilizes steganography procedure to store a database of records. The framework enables a client to make fundamental tables and records, which are avoided others inside a picture. In this paper, we propose a design, which can be utilized by application engineers to recover information from the made database in a simple way. The proposed technique is exceedingly helpful for use as an inserted DB additionally in portable processing as it can store little measure of information effectively.

Bertrand Anckaert et al. [6] distinguishes the basic shortcomings of existing methodologies, coming about because of the static idea of protection and the inconceivability to keep the duplication of advanced information. Another plan is exhibited that empowers a progressively powerful nature of guard and makes it harder to make an extra, similarly helpful duplicate. Besides, it empowers a fine-grained authority over the appropriated programming. Its quality depends on decent variety: each introduced duplicate is extraordinary and refreshes are custom fitted to work for one introduced duplicate as it were.

In [6] information is concealed utilizing Three layers in Audio. Objective of this work is to expand dimension of security with the goal that information can be monitored. Vipul madrakar et al. [7] proposes an insurance plot utilizing cryptography and PVD and LSB blend of steganography. Shamim Ahmed Laskar and Kattamanchi Hemachandra proposed [9] a superior JPEG steganography alongside a substitution encryption strategy. The methodology utilizes the discrete cosine change (DCT) strategy utilized in the recurrence space for stowing away scrambled information inside picture. Minati Mishra et al. [8] talks about some unique kinds of information concealing systems.

III. PROPOSED METHOD

STEGNOS which means “secret” and “graphic” which means “writing”. However, in concealing content, the essence of Steganography is concealing script or private information into other folder e.g. image, text, sound video. Text steganography-A steganography method which employs content as the shield media is named a text steganography. It is one of the most challenging forms of steganography method. Audio steganography-A steganography method which employs audio as shield media is called as audio steganography. It is the utmost stimulating chore in steganography. It is the utmost challenging job in steganography. This is because the human auditory system (HAS) has a huge vibrant variety that it can listen over. Hence, even a miniature conversion in acoustic eminence also can be identified by the human ears. Video steganography-A steganography method which employs video as the bind media is called video steganography. Image steganography-A steganography method which employs visual impressions as the cover media is called an image steganography. Concealing private texts in exponent visual impressions is most extensively employed technique as it can receive benefits of the inadequate supremacy of the human visual system (HVS) and also because visual impressions have great volume of excessive data that can be used to conceal a private text. Numerous steganography methods are recognized to conceal the information efficiently. Some renowned steganography algorithms are LSB, RGB, PVD, etc.

IV. PROPOSED WORK

Considering hindrances and focal points of the current procedures another insurance structure proposed. It joins the benefits of cryptography, steganography and equipment highlights. The new technique is formulated in such a way, to the point that the usage is simple and less lumbering and hard to hack or break by others. This assurance plan can be material to both work area applications and additionally versatile applications and any sort of uses. The calculation has two sections one is the Authentication calculation and second is the insurance calculation. Enrollment process utilizing confirmation calculation is the initial step. Following stage is the stego token creation and afterward append this with the product to ensure. The last advance is the product execution stage where the approval calculations to check the validness.

V. SUBSTANTIATION ALGORITHM

Any product when it is at first introduced should be enrolled. From this progression will begin the procedure for ensuring application. To accomplish this, there is a need to distinguish some one of a kind property of the PC, which can be utilized for enlistment reason. The best choice here is to make utilization of the unique hard circle id, macintosh address, and motherboard sequential and so on to confirm the PC on which the product is introduced. The motivation behind why these are picked is on the grounds that these are remarkable to a PC and can't be changed effectively. Truth be told, to build the insurance levels a mix of these can likewise be utilized.

Step 1: Fetch the HDD serial number or MAC address and user information.

Step 2: Encrypt it using AES encryption standard and write it in afile.

Step 3: Send the file to the License Server

Step 4: Fetch the user mail id along with the information collected by step 3.

Step 5: Locate the user using GPS (Optional step).

Step 6: User authentication information is saved in License server.

VI. FORTIFICATION ALGORITHM

Step 1: Creation of user authentication information.

Step 2: Fetch the Identity information from the stored file (HDDSerial number, MAC Address) place, name, email id etc.

Step 3: Apply the steganoDB package.

Step 4: Embed the encrypted data inside the given image using Pixel Pattern based Steganography algorithm.

Step 5: Save the encoded image file at the receiver's end.

Step 6: For each execution of the protected software checks for this encoded key.

Step 7: Extract the key from the stego image.

Step 8: Decrypting the encrypted text using AES.

Step 9: If the key does not match/What happens when a person tries to pirate the software?

VII. RESEARCH METHODLOGY

Create steganoDB structure,

"First Name":"UTK", "Last Name":"SHARMA", "Email":"utksharma@gmail.com", "Address Line1":"124#Lane 15", "Address Line2":"S-Nagar", "Address Line3":"Bhopal -90", "Phone":"9998793453"

I."Key":"U2FsuopdGVkX19L7/IiYCBYbur74oNTBL/nB a MPfgg+s=".

Significant File Conception:

This algorithm is performed from the server side on acceptance the process key from the operator. The data received from the operator via content file is entrenched in the cover visual impression employing SteganoDB algorithm and Pixel Pattern grounded Steganography algorithm employed in this segment will then conceal the key into a visual and this subsequent visual file is sent to the operator.

{ "First Name":"UTK", "Last Name":"Sharma", "Email":"utksharmar@gmail.com", "Address Line1":"124#Lane 15", "Address Line2":"S-Nagar", "Address Line3":"Bhopal-90", "Phone":"9998793453".

"Key":"U2FsuopdGVkX19L7/IiYCBYbur74I5oNTBL/n BaMPfgg+s

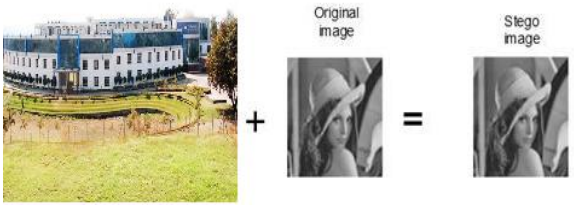

Figure 1: STEGO IMAGE

The enrollment programme will receive the HDD successive digit, encode the HDD successive digit and direct it by email to the confirmation server on the internet. Along with the key programme there will be a segment existing which will analyse the existence of the main file, and then it will interpret the main file and will analyse if the interpreted assessment is alike with the real HDD key. If both of them are alike, then only the programme will perform. There will an update segment which will recurrently analyse the authorized internet server for any programme updates by moving along the enrollment data as well. If the enrollment data is not authentic, it will depart and will make the programme inoperative. At the server side there will be a distinct programme segment which will get the enrollment invitation along with the encoded HDD successive digit. It will conceal the HDD successive digit within the visual and will direct the visual back to the operator to finish the enrollment . The safety segment will employ very little system assets and thus, the operator will not practice any deterioration in presentation. The AES algorithm for interpreting script from main visual will be at the operator side however to the operator its functioning will be obvious. At the server side there will be encrypting of the content into the main visual.

VIII. CATEGORIZER/FILE FORTIFICATION

If there is a need to get data from text within a word document, then the api's provided by Microsoft can be used. Once the input file is provided to the API, it will read the document and will extract the text from the document. The Authentication information becomes one of the input of file protection. It is the key to deciphering the message. The contents of the word file get using API functions and embed it inside the cover image using Pixel Pattern based Steganography algorithm. In addition, the authentication information also is embed using the Steganodb structure kept inside the cover image. Moreover, gives the output as picture.

While extracting the contents of the file at the receiver side the software will check the authentication information, if the authentication is right the contents of the file is extracted and gives the output as text format.

IX. ENACTMENT ANALYSIS

The registration information stored is as below which will be encrypted value of HDD serial number or MAC address. For the test purpose 4 test cases with test data was used. Two for HDD and two for MAC address taken. Normally for protection purpose, methods include cryptography, steganography, dongles, serial numbers and other protection techniques. Its usability, convenience, implementation easiness, maintenance of algorithm, extensibility, cost and its security capability is considered

X. STEPS TO IMPLEMENT DATA HIDING IN IMAGE

- Take an input image.
- Find out the pixel values.

Select the pixel on which we want to insert data. This process of selection of pixel is done as user's choice he may choose pixel continuous or alternate or at a fixed distance.

- Insert the data values in pixels.

XI. CONCLUSION

Another product insurance system has been proposed, which utilizes another pixel design based steganography calculation, consolidating it with encryption and also remarkable equipment properties. This proposed system can be utilized to ensure ordinary PC applications and versatile applications against theft.

The current techniques frequently give a solitary layer of security and henceforth are very simple to hack/split by and large. Nonetheless, the proposed strategy utilizes distinctive layers of insurance. The new steganography calculation isn't anything but difficult to

distinguish as it doesn't change the pixels of a picture. Furthermore, on top it utilizes solid encryption calculation like AES to gives outrageous security.

It additionally can utilize Reallocation based checks and CRC based self-checks to ensure that the product is totally secured against any hacking technique. The main goal of this paper is to review different data hiding techniques which includes cryptography and steganography The prime emphasis is on content steganography which is one of the most challenging forms of steganography methods. Text steganography comprises how concealed visual can be fixed and how it can be directed through the internet by fooling grabbers. Several complications are faced when transporting significant information over the network.

REFERENCES

1. Zhang and Wang, “Binary power data hiding scheme”1434-8411/@2015 Elsevier.
2. R.Rathna Krupa, “An overview of image hiding techniques in image processing”ISSN:2321-2381@2014 Published by the standard international journals .
3. Vipul Sharma and Sunny Kumar, “A new approach to hide text in images using steganography”ISSN: 2277 128X@2013,IJARCSSE.
4. W-C Kuo and C-C Wang, “Data hiding based on generalized exploiting modification direction method” TheImaging Science Journal Vol 61 IMAG 324 @ RPS 2013.
5. Aarti Mehndiratta, “Data hiding systemusingcryptography and steganography:A comprehensive modern investigation.”e-ISSN:2395-0056,p-ISSN:2395-0072@2015,IRJET.NET.
6. B.Subramanan “Image encryption based on aes key expansion” in IEEE applied second international conferenceon emerging applicaton of information technology,978-0-7695-4329-1/11,2011.
7. Vipul Madhukar Wajgade,Dr. Suresh Kumar,Stegocrypto – A Review of Steganography techniques usinCryptography”,International Journal.OfComputeengineeringTechnology,ISSN:22229-3345,vol. 4,2013,pp. 423-426
8. T. Sharp, An implementation of key-based digital signal steganography, Proc. of the 4th Information Hiding Workshop, vol. 2137, pp. 13-26, Springer, 2001.
9. J. Mielikainen, LSB matching revisited, IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287,2006.
10. X. Li, B. Yang, D. Cheng, and T. Zeng, A generalization of LSB matching, IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69-72, 2009.
11. Syed K A Khadri,, Debabrata Samanta, M Paul,” Message Encryption Using Text Inversion plus N Count: In Cryptology”, International Journal of Information Science and Intelligent System (IJISIS), pp. 71-74, Volume 3, Number 2, 2014.
12. Syed K A Khadri,, Debabrata Samanta, M Paul,” Novel Approach for Message Security”, International Journal of Information Science and Intelligent System (IJISIS), pp. 47-52,Volume 3, Number 1, 2014.
13. Syed K A Khadri,, Debabrata Samanta, and M Paul, "Approach of Message Communication Using Fibonacci Series: In Cryptology", Lecture Notes on Information Theory, Vol. 2, No. 2, pp. 168-171, June 2014. doi: 10.12720/lnit.2.2.168-171.
14. Syed K A Khadri,, Debabrata Samanta, M Paul,” Message communication using Phase Shifting Method (PSM)”,International Journal of Advanced Research in Computer Science (IJARCS), Volume 4, Number 11, pp.9-11 ,November-December 2013.
15. Syed K A Khadri,, Debabrata Samanta, M Paul,” Secure Approach for Message Communication”, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), pp. 3481-3484, Vol. 2, Issue 9, September 2013.
16. Dipti Kapoor Sarmah, Neha bajpai, “ Proposed System for Data Hhiding Using Cryptography and Steganography”, International Journal of Computer Applications (0975 – 8887), Volume 8 – No. 9, October 2010.
17. R. Rejani, D. Murugan and Deepu V. Krishnan, “Novel Software Protection Framework Using Steganography, Cryptography, Uniqueness of Hardware and Self-Checks”.
18. Bertrand Anckaert, Bjorn De Sutter and Koen DeBosschere, “Software Piracy Prevention through Diversity”,Proceedings of the 4th ACM workshop on Digital rights management, pp. 63-71, 2004.