IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.7, Special Issue.3, Feb. 2019 E-ISSN: 2347-2693

Design and Development of a technique for Hidden data in Watermark Image using Steganography: An Exploration

Upendra Verma[1*], R.K. Rambola[2], Pratiksha Meshram[3]

Computer Engineering department, MPSTME Shirpur Campus, NMIMS University, India

Available online at: www.ijcseonline.org

Abstract— The improvement of sight and sound and web takes into consideration wide conveyance of computerized media information. It turns out to be significantly less demanding to alter, adjust and copy advanced data. In extra, advanced report is likewise simple to duplicate and appropriate, along these lines it might confront numerous dangers. It ended up plainly important to locate a suitable security because of the centrality, exactness and affectability of the data. Besides, there is no formal technique to be taken after to find shrouded information.

In this paper, we proposed an approach amongst Steganography and Watermarking. In this paper, another data concealing framework is introduced. The point of the proposed framework is to shroud data (information document) inside watermark picture. This paper covers three fundamental standards of security: Confidentiality, Integrity and Authentication (CIA).

Keywords— *Steganography, Watermarking, Hidden data, CIA.*

I. INTRODUCTION

These days, security of data can be arranged into more particular as concealing data (Steganography) or encryption data (Cryptography) or a blend between them. Cryptography is the act of "scrambling" messages so that regardless of the possibility that recognized, they are exceptionally hard to disentangle. Steganography and Cryptography are in actuality reciprocal procedures. Steganography is the craft of stowing away and transmitting information through obviously harmless bearers with an end goal to hide the presence of the information, the word Steganography truly implies secured or concealing composition as got from Greek. Steganography has its place in security. It is not planned to supplant cryptography but rather supplement it. Concealing a message with Steganography strategies decreases the shot of a message being recognized. Watermarking is likewise a system to guarantee the uprightness of messages. The proposed work utilized Watermarking Technique and Steganography system, which gave two layer of security to the encryption of message. Here We utilized watermarking methodology of adding unaware information to picture content keeping in mind the end goal to secure proprietors right. For the most part watermarking system can be grouped in light of the inserting area to spatial techniques and unearthly spaces.

Here, the stowing away of the data in the picture page of watermark document, through the execution of four process (determine the cover record, indicate the data document, encryption of the data and concealing the data) and the second capacity is the extraction of the concealing data through four process (indicate the stego record, remove the data document and unscrambling of the data).
As an extra work, we will utilize a watermark procedure which gives respectability to data.

II. LITERATURE SURVEY

The background study is provided so as to get familiar with the basic concepts which are the basic building blocks of the project. In this project the background consist of the basics of cryptography and Steganography.

Issues in Security of Information:
There are many issues and challenges that need to be considered when proposed system is to be designed. The major issues that affect the design, deployment and performance of this system are watermarking, cryptography and steganography.

Related Study:-

1) New Technique of Hidden Data in PE-File with in Unused Area One:-

In this approach, another arrangement of data stowing away is introduced [2]. The proposed framework plan to shroud data (information document) in unexploited zone 1 of any carrying out record (exe.file), to ensure changes made to the exe.file won't be distinguished by hostile to infection and the usefulness of the exe.file is as yet working. The framework incorporates two fundamental capacities; first is the stowing away of the data in the unexploited region 1 of PE-record (exe.file), through the execution of four process (indicate the cover document, determine the data document, encryption of the data, and concealing the data) and the second capacity is the taking out of the concealing data through three process (indicate the steno document, separate the data, and unscrambling of the data). The testing result appears; the outcome document does not make any contention with against infection programming and the exe.file still capacity as common after the concealing procedure.

2) A new system for hidden data within header space for EXE-File using object oriented technique:-

In this approach, another data concealing framework is introduced [3]. The point of the planned framework is to shroud data (information document) after end of header record inside carrying out document (EXEfile) to ensure changes made to the document won't be identified by universe and the usefulness of the exe.file is as yet working subsequent to concealing procedure. In the interim, since the cover document may be utilized to distinguish concealing data, the planned framework considers beating this problem by utilizing the execution record as a cover document.

3) Novel Framework for Hidden Data in the Image Page within Executable File using Computation between Advanced Encryption Standard and Distortion Techniques:-

In this approach, another data concealing structure is displayed [4].The proposed system point is usage of structure calculation between propel encryption standard (AES) and twisting method (DT) which installs data in picture page inside executable document (EXE record) to locate a protected answer for cover record without change the measure of cover record. The structure incorporates two fundamental capacities; first is the stowing away of the data in the picture page of EXE record, through the execution of four process (indicate the cover document, determine the data document, encryption of the data, and concealing the data) and the second capacity is the extraction of the concealing data through three process (determine the stego record, extricate the data, and decoding of the data).

4) New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm:-

In this approach [5], we will recommend a team up approach amongst steganography and cryptography. This approach will design high rate and high secure information shrouded utilizing mystery key steganography and AES Rijndael technique. Too, this paper will diagram the utilization of information concealing systems and its grouping, besides we will dole out the well-worked of the AES calculation, amid this audit the creator will answer the inquiry why they utilized AES calculation. In extra to the security issues we will utilize the digital video as a cover to the information covered up. The explanation for select the video cover in this approach is the tremendous measure of single edges picture per sec which thusly overcome the issue of the information concealing amount, as the investigation result demonstrates the accomplishment of the shrouded, encryption, separate, unscrambling capacities without influencing the nature of the video.

5) On Line Secret Watermark Generation for Audio files:-

In this approach, shows an on line dynamic incredible and profitable approach [6] of sound watermarking for copyright security. In this paper I am using on line secret watermark period to create additional information (watermark) therefore in the midst of embeddings process. The Direct Sequence Spread Spectrum (DSSS) method is taken to spread the watermark bits over the entire scope of sound banners unpretentiously by making chip courses of action using the bits of watermark. The watermark is formed in sound signs without the encroachment of psycho acoustic properties of Human Auditory System (HAS) in repeat zone. The made watermark is outstanding for each stable record. The traverse of watermark depends on the size and amounts of sound record tests.

III. PROBLEM DOMAIN

In the present situation the touchy data is critical for individual. Because of different sorts of danger and assault, the security of data is a basic undertaking. Concealing data is insufficient method to give security.

In the present situation there are numerous issues with security of touchy data. The rushed advancement of sight and sound and web takes into consideration wide circulation of computerized media information. It turns out to be substantially less demanding to alter, adjust and copy advanced data. In extra, advanced report is likewise simple to duplicate and disseminate, along these lines it might confront numerous dangers. It wound up plainly important to locate a fitting assurance because of the affectability of the data.

IV. SOLUTION DOMAIN

Steganography is technique to hide information behind any object. The goal of watermarking is to ensure the integrity of information. In this paper we proposed a collaborate approach between Steganography and Watermarking.

Pseudo Code for watermarking:

```
1. Begin
2. Define Class to pad watermark tag
  2.1 Initialize X and Y Coordinate
  2.2 Define String and text for source image & offset for x and y coordinate
2.2  Define exception handling mechanism for source image
File _file = new File(srcImg);
2.3 read date file using read function
2.4 Set height and width of image
```

```
2.5 Create Buffered Image using parameter height and width
2.6 Define graphic object g
Graphics g = image.createGraphics();
2.7 Create JPEGIMage Encroder
     JPEGImageEncoder encoder =
JPEGCodec.createJPEGEncoder(out);
     encoder.encode(image);
3. Terminate Watermark Class
4. Stop
```

Model of Watermarking:

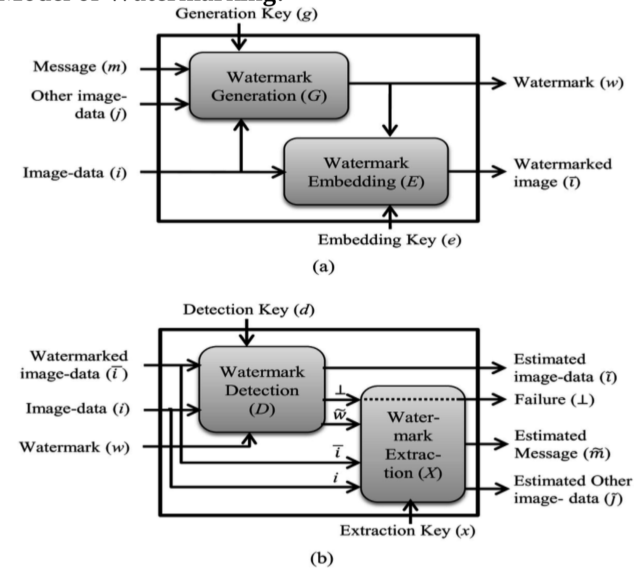


Fig. 1

The watermark era work creates an appropriate watermark (w). In any of the information concealing process, a watermark generation (g) capacity can be the installing information (e.g., picture data (j) and message (m)) alongside implanting key and watermarked picture (w) has been gained from it. In an impelled function, a watermark may require to have properties like , in a copyright security function, a watermark may ought to be "intense" against certain getting ready techniques and also ambushes. . Dissatisfaction to consider those things may realize specific flaws and security inadequacies. In spite of the way that watermark period is predominantly obliged by the necessary properties, it starts with critical information sources and their properties.

Watermark installing, E() As the information concealing part, watermark inserting capacity considers where and how to implant the watermark fulfilling different prerequisites of the cover objects (here, computerized pictures). For instance, 'perceptual closeness' prerequisites (that control which pixels can be adjusted to what degree) of restorative pictures may restrain the inserting area [17]. (We will talk about the 'perceptual likeness' property in detail in area 4.1.) There are diverse areas (e.g., spatial, change) for inserting, which are figured straightforwardly from an info picture. Implanting sorts may likewise be unique (e.g., imperceptible, invertible or reversible, dazzle, and so forth - will be examined in area 4). Independent of the inserting area, space and sort, nonetheless, an implanting capacity E(•) can take a watermark, w and the first picture information, I as contribution to yield the watermarked picture information, ī.

Watermark identification D() :
This capacity helps settle on a goal choice (e.g., to announce whether the substance is credible) and additionally start additionally activities (e.g., to remove the inserted information, to connect with and hold clients of the watermarked objects). In various application situations, the extra errands may shift and rely upon the parallel choice (i.e, pass or fall flat). The essential thought is that D(•) separates the implanted watermark and recovers another adaptation of the watermark, from the data sources. On the off chance that the recovered adaptation coordinates the extricated rendition, a pass flag is returned. (The pass flag is considered to pass the parameters, for example, the substantial watermark, the evaluated picture information, and so forth to its reliant module that plays out the extra errands, which will be indicated later in Figure 2.) Otherwise, a disappointment is yield. The primary limitations for this capacity consequently can be the base mistake probabilities (e.g., false negative/positive rates) and calculation time. Like the capacities, G(•) and E(•), the interior plan of D(•) can likewise differ, however it by and large takes watermarked picture information, ī, unique picture information, I and a watermark, w to yield either an expected picture information, ĩ, message m ˜ m~ and other picture information, j ˜ j~ , or a disappointment, ⊥. negative/positive rates) and computation time. Like the functions, *G*(·) and *E*(·), the internal design of *D*(·) can also vary, but it generally takes watermarked image data, *ī*, original image data, *i* and a watermark, *w* to yield either an estimated image data, *ĩ*, message *m* ˜ m~ and other image data, *j* ˜ j~ , or a failure, ⊥.

Model for Stegnography:

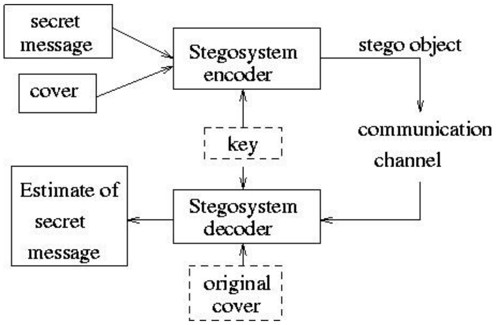
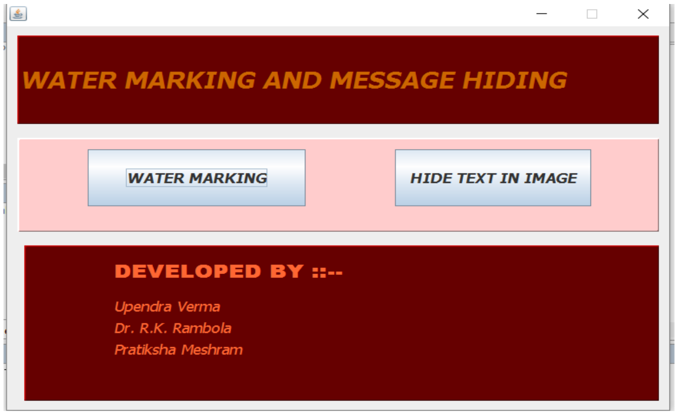


Fig. 2

After Observing the above models of water marking & stegnography theses method is applied & implemented in renowned industry, the implementation of the results have been shown below.

V. RESULT ANALYSIS

1. Front Interface:


WATER MARKING AND MESSAGE HIDING

DEVELOPED BY ::--

Upendra Verma
Dr. R.K. Rambola
Pratiksha Meshram

Fig. 3

2. Interface for Digital Water Marking:

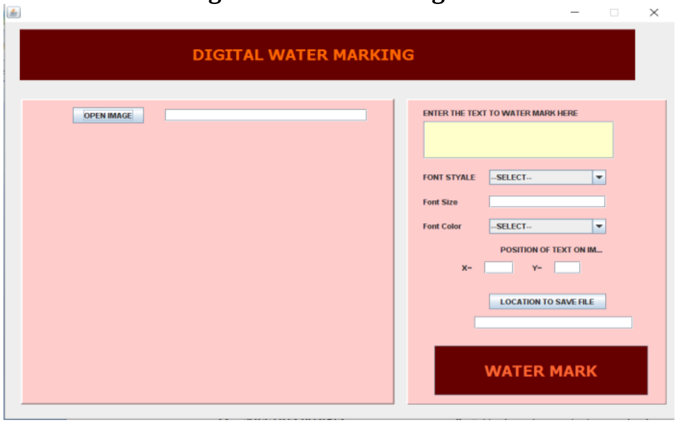
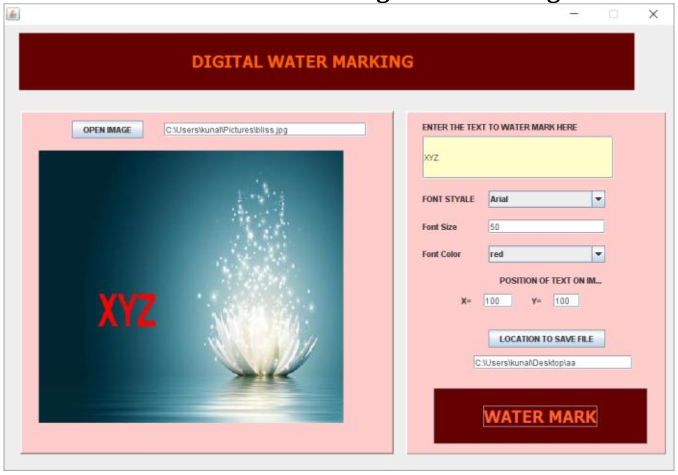


Fig. 4

3. Interface for Watermarked Tag added to Image File:


OPEN IMAGE: C:\Users\kunal\Pictures\bliss.jpg

ENTER THE TEXT TO WATER MARK HERE: XYZ

FONT STYALE: Arial

Font Size: 50

Font Color: red

POSITION OF TEXT ON IM... X= 100 Y= 100

LOCATION TO SAVE FILE: C:\Users\kunal\Desktop\aa

Fig. 5

4. Interface for Steganography:

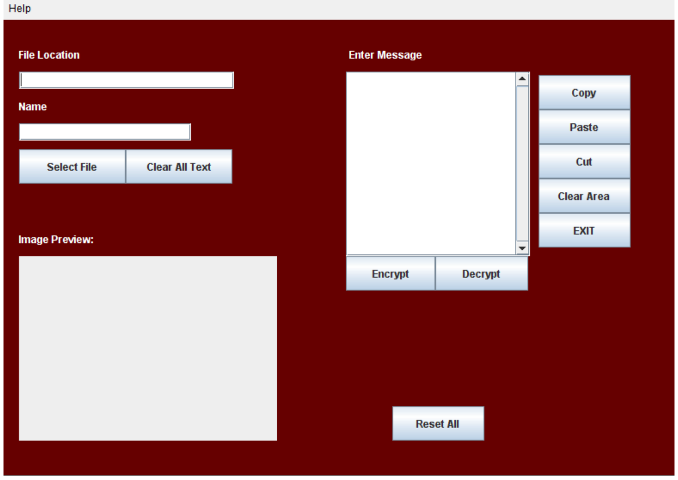
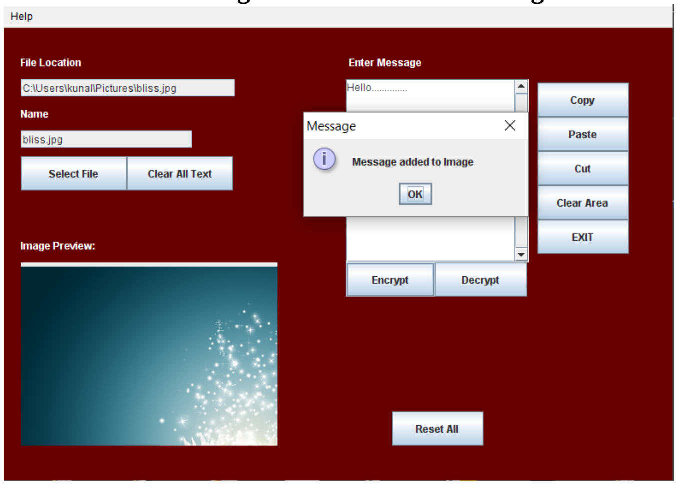


Fig. 6

5. Interface for hiding information behind Image:


File Location: C:\Users\kunal\Pictures\bliss.jpg

Name: bliss.jpg

Enter Message: Hello..............

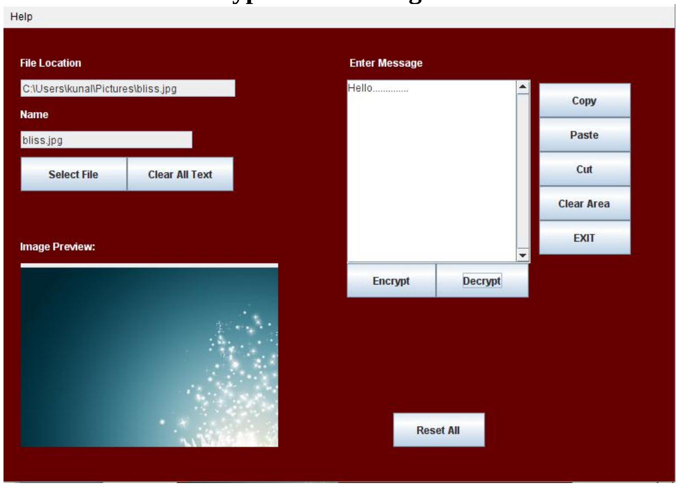
Message

Message added to Image

OK

Fig. 7

6. Interface for Decryption of message:


File Location: C:\Users\kunal\Pictures\bliss.jpg

Name: bliss.jpg

Enter Message: Hello..............

Fig. 8

VI. CONCLUSION

Giving security is basic to the foreseen far reaching sending of administrations. Computerized Watermarking, the craft of powerful data, inserting in mixed media information, has pulled in much enthusiasm by specialists everywhere throughout the world. The principle objective of this composition is to research the Watermarking strategy with Steganography. The application gives the suitable arrangement and arrangement speaks to the base security necessities.

REFERENCES

[1] A.A.Zaidan, B.B.Zaidan, Fazidah Othman, "*New Technique of Hidden Data in PE-File with in Unused Area One*", International Journal of Computer and Electrical Engineering (IJCEE), Vol.1, No.5, ISSN: 1793-8198, pp 669-678.

[2] Al-Nabhani, Y.; Zaidan, A.A.; Zaidan, B.B.; Jalab, H.A.; Alanazi, H.O.; "*A new system for hidden data within header space for EXE-File using object oriented technique"* 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT),Volume:7, Pages:9-13, Digital Object Identifier: 10.1109/ICCSIT.2010.5564461.

[3] 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 in the Image Page within Executable File Using Computation between Advanced Encryption Standard and Distortion Techniques ",* International Journal of Computer science and information security, IJCSIS Vol.3, No. 1, July 2009, ISSN:1947-5500.

[4] Alaa Taqa, A.A Zaidan, B.B Zaidan.*"New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm ",* International Journal of Computer and Electrical Engineering, Vol. 1, No. 5 December, 2009,ISSN:1793-8163.

[5] Vimal Bibhu, "*On Line Secret Watermark Generation for Audio files* ", International Journal of Computer and Electrical Engineering, Vol. 1, No. 5 December, 2009 ISSN:1793-8163.

[6] Jafari, R.; Ziou, D.; Mammeri, A.*;" Increasing compression of JPEG images using steganography* " , 2011 IEEE International Symposium on Robotic and Sensors Environments (ROSE), Page(s): 226 - 230 , Digital Object Identifier: 10.1109/ROSE.2011.6058519.

[7] M. Young, *The Technical Writer's Handbook.* Mill Valley, CA: University Science, 1989.

[8] M. Reid, R. J. Millar, and N. D. Black, *"Second-generation image coding: an overview,"* ACM Computing Surveys (CSUR), vol. 29, pp. 3-29, 1997.

[9] Chopra D.; Gupta P.; Gaur S. B.C.; Gupta A.; *"Lsb Based Digital Image Watermarking For Gray Scale Image,"* IOSR Journal of Computer Engineering, 2012. IOSRJCE 2012, vol.6, pp. 36, 41, Sep. -Oct. 2012.

[10] Mohammad Shirali-Shahreza and Sajad Shirali-Shahreza, *"Steganography in Silence Intervals of Speech*", Institute of Electrical and Electronics Engineers (IEEE), International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008.

[11] J. Bajpai and A. Kaur, *"A literature survey - various audio water-marking techniques and their challenges*," International Conference -Cloud System and Big Data Engineering (Confluence), pp. 451–457,Jan. 2016.

[12] M. Kutter. *"Digital Watermarking: Hiding Information in Images"* Ph.D. thesis 2045, Swiss Federal Institute of Technology, Lausanne, Switzerland, 1999.