REVIEW ON DATA HIDING USING STEGANOGRAPHIC TECHNIQUES

[1]Ghule Isha Chetan, [2]Sonawane Dhanashri Hiraman, [3]Sakhala Siddhi Shashikiran, [4]KhadeTejashree Tukaram, [5]Dr. Dahake Ranjana

MET Bhujbal Knowledge City, Adgaon, Nashik

Abstract - **Nowadays, computer-basedcommunications are at the threshold of making life easier for everyone in the world; from sharing information, to communicating with each other, to exchanging electronic documents, and to checking bank balances and paying bills. Nonetheless, information security is an essential factor, which must be taken into consideration to ensure secure communications. There are significant interests in security approaches that aim to protect information and digital data, since the growing increase in uses of the internet and multimedia, have raised the interests in image steganography in order to secure and protect them. In our proposed system we are creating a feature where user will asked to select theimage & add secret message, user will also select thereceiver for decryption & enter the key for captcha,Then receiver will enter the key and decrypt the secret msg.**

Keywords: **image, audio, steganography, captcha,system.**

INTRODUCTION

The first recorded use of the term was in 1499 by Johannes Tritheism in his Steganographic, a treatiseon cryptography and steganography, disguised as a book on magic. Generally, the hidden messagesappear to be (or to be part of) something else: im- ages, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography thatlack a shared secret are forms of security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoffs's principle.[2] The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.

Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.[3] Whereas cryptography is thepractice of protecting the contents of a messagealone, steganography is concerned with concealing the fact that a secret message is being sent and its contents. Steganography includes the concealment of information within computer files. In dig- ital steganography, electronic communications mayinclude steganographic coding inside of a transport layer, such as a document file, image file, program, or protocol. Media files are ideal for steganographictransmission because of their large size. Forexample, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change

Our system consists of objective like a scalable approach system which will allow system to extends better features in future. System is built with great user interface so that user can able to usethe system easily.

In our proposed system we are creating a feature where user will ask to select the image & addsecret message, user will also select the receiver fordecryption & enter the key for captcha, Then receiver will enter the key and decrypt the secret msg.

The internet plays a key role in transferring information or data from one organization to anotherorganization. But anyone can modify and misuse thevaluable information through hacking at the time. Steganography plays a very important role in hiding the secret data or information inside the digitallycovered information

Functional requirements: may involve calculations, technical details, data manipulation and processing and other specific functionality that define what a system is

supposed to accomplish. Behavioral requirements describe all the cases where the system uses the functional requirements; these are captured in use cases.

Nonfunctional Requirements: (NFRs) define system attributes such as security, reliability, performance, maintainability, scalability, and usability. They serve as constraints or restrictions on the design of the system across the different backlogs.

The area differs in what feature of steganography isutilized in each system.

1. Confidential communication and secret datastoring

The "secrecy" of the embedded data is essential inthis area.
Historically, steganography have been addressed inthis area. Steganography provides us with:
(A) Potential capability to hide the existence ofconfidential data
(B) Hardness of detecting the hidden (i.e.,embedded) data
(C) Enhancing the secrecy of the encrypted data In practice, when you use some steganography, youmust first select a vessel data according to the size of the embedding data. The vessel should be innocuous. Then, you embed the confidential data by using an embedding program (which is one component of the steganography software) together with some key. When extracting, you (or your party)use an extracting program (another component) to restore the embedded data by the same key ("common key" in terms of cryptography). In this case you need a "key negotiation" with your party before you start confidential communication. One simplest application is to your private journal writing. Attaching a stego file to an e-mail message is another example in this application area. But you and your party must do a "sending-and-receiving" action that could be noticed by a third party. So, e- mailing is not a completely secret communication method. There is an easy method that has no key- negotiation. We have a model of "Anonymous Covert Mailing System. “There is some other communication method that uses the Internet Webpages. In this method you don't need to send anything to your party, and no one can detect your communication.
One method is shown here. Some other methods aremuch more confidential.
Each secrecy-based application needs an embeddingprocess which leaves the smallest embedding evidence. You may follow the following.
(A) Choose a large vessel, larger the better,compared with the embedding data.
(B) Discard the original vessel after embedding. Forexample, in the case of Qtech Hide & View, it leaves some latent embedding evidence even if the vessel has a very large embedding capacity. You arerecommended to embed only 25% or less for PNG / BMP output of the maximum capacity, or only 3% of the vessel size for JPEG output.

2. Protection of data alteration

We take advantage of the fragility of the embeddeddata in this application area. We asserted in
the Home Page that "the embedded data can rather be fragile than be very robust." Actually, embeddeddata are fragile in most steganography programs.
Especially, Qtech Hide & View program embeds data in an extremely fragile manner. We demonstrate this in the other page. However, this fragility opens a new direction toward an information-alteration protective system such as a "Digital Certificate Document System." The most novel point among others is that "no authenticationbureau is needed." If it is implemented, people cansend their "digital certificate data" to any place in the world through Internet. No one can forge, alter,nor tamper such certificate data. If forged, altered, or tampered, it is easily detected by the extraction program.

3. Access control system for digital contentsdistribution

In this area embedded data is "hidden", but is"explained" to publicize the content.

Today, digital contents are getting more and more commonly distributed over Internet than before. Forexample, music companies release new albums on their Webpage in a free or charged manner.
However, in this case, all the contents are equally distributed to the people who can make access to thepage. So, an ordinary Web distribution scheme is not suited for a "case-by-case" and "selective" distribution. Of course it is always possible to attach digital contents to e-mail messages and send them tothe customers. But it will takes a lot of cost in time and labor.

If you have some valuable content, which you think it is distributable if someone really needs it, and if it is possible to upload that content on Internet in somecovert manner. And if you can issue a special "access key" to extract the content selectively, you will be very happy about it. A steganographic scheme can help realize this type of system.

We have developed a prototype of an "Access Control System" for digital content distribution through Internet. The following steps explain thescheme.

(1) A content owner classify his/her digital contentsin a folder-by-folder manner, and embed the whole folders in some large vessel according to a steganographic method using folder access keys, and upload the embedded vessel (stego data) on his/her own Webpage.

(2) On that Webpage the owner explains the contents in depth and publicize worldwide. The contact information to the owner (post mail address,e-mail address, phone number, etc.) will be posted there.

(3) The owner may receive an access-request from acustomer who watched that Webpage. In that case, the owner may (or may not) creates an access key and provide it to the customer (free or charged)..

In this mechanism the most important point is, a"**selective extraction**" is possible or not.

4. Media Database systems

In this application area of steganography secrecy isnot important, but **unifying two types of data intoone** is the most important.

Media data (photo picture, movie, music, etc.) havesome association with other information. A photo picture, for instance, may have the following.
(1) The title of the picture and some physicalobject information
(2) The date and the time when the picture wastaken
(3) The camera and the photographer's information
Formerly, these are annotated beside each picture in the album.

LITERATURE SURVEY

1. Data Encryption & Decryption UsingSteganography, N. Manohar etal**.,[1]** This paper studied that Video steganography is a method that processes secure communication. When we see the history of steganography, it was hidden in many ways such as tablets covered with wax, & written onthe stomachs of rabbits. Here in this paper, considering the video steganography methods toperform secure steganography communication. Many methods have been proposed for video steganography but they're no more different types offormats, secured, quality, of the results. So herepropose secure steganography methods i.e. Secure base LSB method, Neural Networks & Fuzzy logic,and check their using PSNR and MSE data of the methods. That data-set has collected is from video streams. And the result was seen with the moreformats, more security, quality of outputs, & accuracy values of PSNR & MSE which is better than other proposed methods.

2. Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography, Mehdi Sharifzadeh etal.,[2] This paper shows that, In digital image steganography, thestatistical model of an image is essential for hiding data in less detectable regions and achieving better security. This has been addressed in the literature where different cost-based and statistical model- based approaches were proposed. However, due to the usage of heuristically defined distortions and non-constrained message models, resulting in numericallysolvable equations, there is no closed-form expression for security as a function of payload. Theclosed-form expression is crucial for a better insight into image steganography problem and also improving performance of batch steganographyalgorithms. Here, we develop a statistical frameworkfor image steganography in which the cover and the stego messages are modeled as multivariate Gaussianrandom variables. We propose a novel Gaussian embedding model by maximizing the detection errorof the most common optimal detectors within the adopted statistical model. Furthermore, we extend theformulation to cost-based steganography, resulting ina universal embedding scheme that improves empirical results of current cost-based and statisticalmodel-based approaches. This methodology and its presented solution, by reason of assuming a continuous hidden message, remains the same for anyembedding scenario. Afterward, the closed-form detection error is derived within the adopted model for image steganography and it is extended to batch steganography. Thus, we introduce Adaptive Batch size Image Merging steganographer, AdaBIM, and mathematically prove it outperforms the state-of-the-art batch steganography method and further verify itssuperiority by experiments.

3. A mobile forensic investigation intosteganography, Catrin Burrows etal.,[3] Thispaper studied that, Mobile devices are becoming a more popular tool to use in day-to-day life; thismeans that they can accumulate a sizeable amount ofinformation, which can be used as evidence if the device is involved in a crime. Steganography is one way to conceal data, as it obscures the data as well asconcealing that there is hidden content. This paper will investigate different steganography techniques, steganography artefacts created and the forensic investigation tools used in detecting and extracting steganography in mobile devices. A number of steganography techniques will be used to generate different artefacts on two main mobile device platforms, Android and Apple. Furthermore, Forensic investigation tools will be

employed to detect and possibly reveal the hidden data. Finally, aset of mobile forensic investigation policy and guidelines will be developed.

4. Directional Pixogram: A New Approach forVideo Steganography, Mohammed Baziyad etal.,[4] This paper explain that, A video signal can be expressed as a 3D signal where the rows and columns of pixels represent the first and the second dimension, while the third dimension is the time. The3D nature of video signals has produced an additionalsource of data redundancy; that is, the temporal redundancy. Utilizing signal redundancy is the fundamental driving force for steganographytechniques. In this paper, the Directional Pixogram isproposed to optimally exploit the redundancy in a video segment. The Directional Pixogram is a 1D vector that starts from a certain initial position and then grows in the direction of the motion vectorassociated with that initial position. It is expected thatthis temporal vector will contain highly correlated pixels. Therefore, the Discrete Cosine Transform (DCT) can express this vector within few significantDCT coefficients leaving a large amount of insignificant DCT coefficients. Thus, experimental results have shown that the proposed DirectionalPixogram is able to obtain outstanding stego quality while hiding with very high hiding capacities.

5. A novel approach to Steganography using pixel-based algorithm in image hiding, Jawwad A R. Kazi etal[5] This paper studied the Steganography isthe technique of hiding data under image to prevent itfrom being unintentionally accessed by anyone else. This process involves a plain text and an image file. By looking at the need of steganography we have proposed a new algorithm which will satisfy the aimof steganography. In our algorithm, we will have a cover image file and the message. Then the cover image's pixel will be taken into consideration. In thatwe will embed each bit of secret text. This process will be continued until the last bit of secret text. Afterthis step, the data is hidden under the image. Then wewill send this image file to our client and client will have reverse process to retrieve original text from theimage. We will then compare our algorithm with BLIND HIDE steganography algorithm on the basis of accuracy, precision, recall and f1-score. We will also check for the output image quality generated byboth algorithms on structural similarity measure to reach proper consensus

SYSTEM ARCHITECTURE

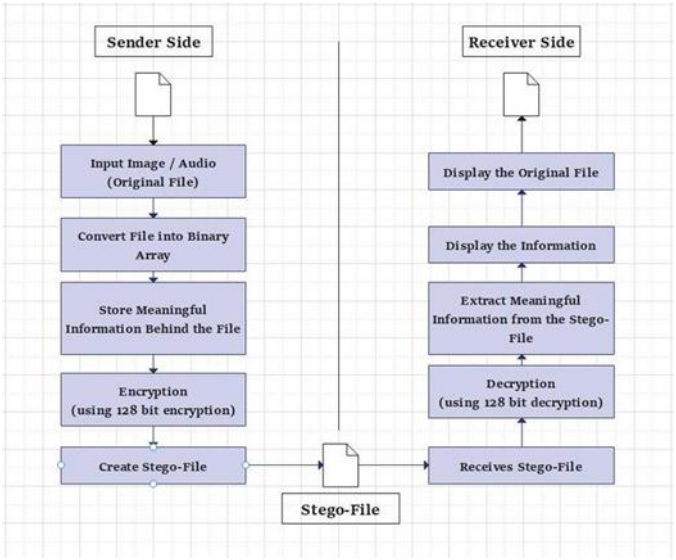


Fig -1: System Architecture Diagram

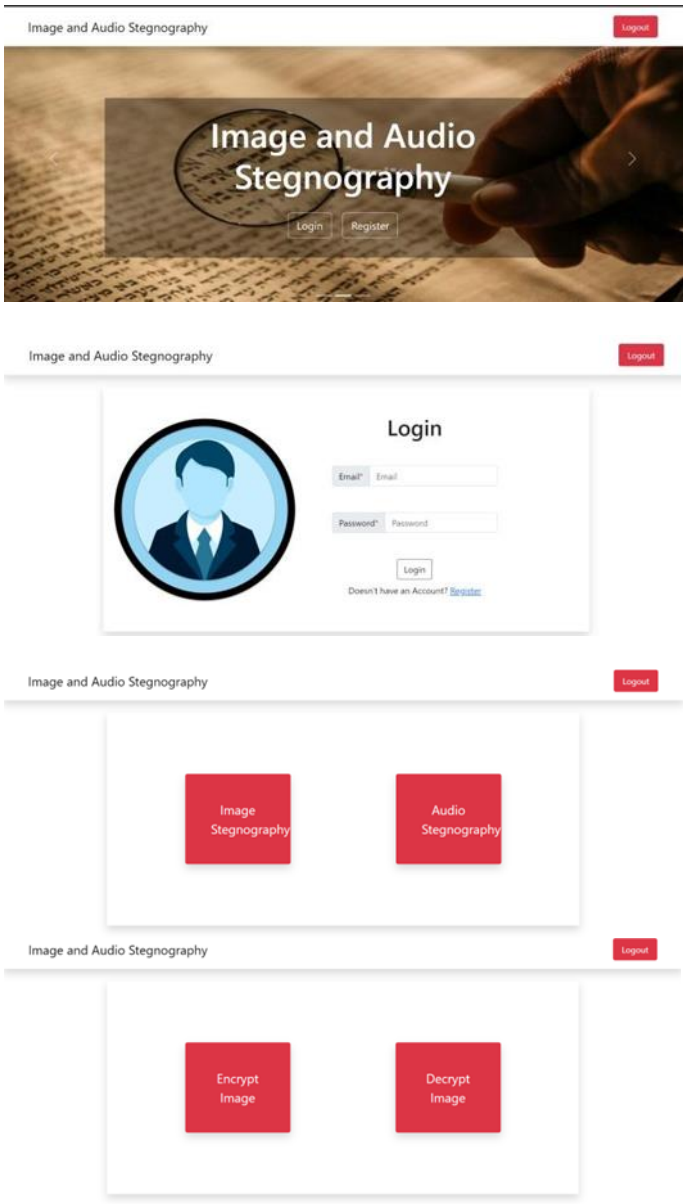
ALGORITHM

1. Start
2. Select Image or Audio
3. Enter Receiver's Email Address
4. Enter Secret Message
5. System will generate Random Key Automatically.
6. Encrypt the Secret Message and Random Generated Key using Hash Algorithm.
7. Generate the Cipher Text using Receiver's Email,Encrypted Secret Message and EncryptedRandom Generated Key.
8. Store that Cipher Text into Image / Audio using LSB Algorithm and Create Stego-File.
9. Send that Stego-File with any Communication Medium to the Receiver.

10. Receiver upload that File to the System.
11. If Receiver is Authenticated, then he have the Access of Decrypt the Message, OtherwiseSystem gives "Access Denied" message.
12. If the receiver is Authenticated then, The RandomGenerated Key get Decrypted and shown to the Receiver as a Captcha Format.
13. When Receiver inserts the Valid Captcha then hegot the access to show the Decrypted Message orActual Message send by the Sender.

IMPLEMENTATION AND ANALYSIS

INPUT:



ANALYSIS TABLE :

Sr. No.	Text File Size	Word Count	Image Size Before Encryption	Image Size After Encryption
1	12.3 kb	1	86 kb	521 kb
2	15 kb	180	115 kb	756 kb
3	22.5 kb	1472	162 kb	1.11 mb
4	30.8 kb	3093	219 kb	1.60 mb
5	40.5 kb	5225	379 kb	3.12 mb
6	49.8kb	4278	70.9kb	748kb
7	60.6kb	5570	127kb	1.3mb
8	72.2kb	6967	340kb	3.45mb
0	80.8kb	8022	917kb	9.14mb
10	90.8kb	9329	978kb	9.96mb

CONCLUSION

We are overcoming the drawback of existing system, and providing a smart system that will not only monitor and control our data with security but also supply it too whenever necessary. We are tryingachieved more than 90% detection accuracy using image processing algorithm with lowest falsepositive rate.

REFERENCES

[1] N. Manohar; Peetla Vijay Kumar., Data Encryption & Decryption Using Steganography, 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS).

[2] Mehdi Sharifzadeh., Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography, IEEE Transactions on Information Forensics and Security PP(99):1-1 DOI:10.1109/TIFS.2019.2929441

[3] Catrin Burrows; Pooneh Bagheri Zadeh, A mobile forensic investigation into steganography, 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security).

[4] Mohammed Baziyad; Tamer Rabie; Ibrahim Kamel, Directional Pixogram: A New Approach for Video Steganography, 2020 Advances in Science and Engineering Technology International Conferences (ASET)

[5] Jawwad A R. Kazi, Gunjan N. Kiratka., A novel approach to Steganography using pixel-based algorithm in image hiding, 2020 International Conference on Computer Communication and Informatics (ICCCI).

[6] Jain M.P., Trivedi P.V., Effective Audio Steganography by using Coefficient Comparison in DCT Domain, International Journal of Engineering Research & Technology 2(8) (2013).

[7] Santosa R.A., Bao P., Audio-to-Image Wavelet Transform based Audio Steganography, 47th

[8] Jayeeta Majumder et al., "High Capacity Image Steganography using Pixel Value DifferencingMethod with Data

Compression using Neural Network", International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 12, October 2019, ISSN 2278 - 3075.
[9] Y. Huo, Y. Qiao and W Gao, "High Capacity Steganography on Float-Point Number with Single Precision", 2020 2nd International Conference on Video Signal and Image Processing, pp. 48-54, 2020, December, [online]
[10] Ayidh Alharbi et al., "A SteganographyTechnique for Images Based on Wavelet TransformFDSE 2017", LNCS 10646, pp. 273-281, 2017.
[11] H. A. Al-Korbi, A. Al-Ataby, M. A. Al-Taee and W. Al-Nuaimy, "High-capacity image steganography based on Haar DWT for hiding miscellaneous data", 2015 IEEE Jordan Conferenceon Applied Electrical Engineering and Computing Technologies (AEECT), pp. 1-6, 2015,
[12] S Hemalatha et al., "A SECURE AND HIGH CAPACITY IMAGE STEGANOGRAPHYTECHNIQUE", Signal & Image Processing: An International Journal (SIPIJ), vol. 4, no. 1, February2013.
[13] S.K. Muttoo et al., "A Multilayered SecureRobust and High Capacity Image Steganographic Algorithm", World of Computer Science and Information Technology Journal (WCSIT), vol. 1, no. 6, pp. 239-246, 2011, ISSN 2221-0741.
[14] S.K. Muttoo et al., "A Multilayered SecureRobust and High Capacity Image Steganographic Algorithm", World of Computer Science and Information Technology Journal (WCSIT), vol. 1, no. 6, pp. 239-246, 2011, ISSN 2221-0741.
[15] Liu and Lee, "High-capacity reversible image steganography based on pixel value ordering EURASIP", Journal on Image and Video Processing, 2019.
[16] I.J. Kadhim et al., "High capacity adaptiveimage steganography with cover region selection using dual-tree complex wavelet transform", Cognitive system research, vol. 60, pp. 20-32, May 2020.
[17] V. Verma, S.K. Muttoo and V.B Singh, "Enhanced payload and trade-off for image steganography via a novel pixel digits alteration", Multimedia Tools Appl, vol. 79, pp. 7471-7490, 2020.
[18] K.A Kingsley, "Improving data hiding capacityin code based steganography using multiple embedding", Journal of Information Hiding and Multimedia Signal Processing, vol. 11, no. 1, pp. 14-43, March 2020.
[19] . W. Selesnick, "The double-density dual-tree DWT", IEEE Transactions on Signal Processing,vol. 52, no. 5, pp. 1304-1314, May 2004.
[20] J.R. Flynn, S. Ward, J. Abich and D Poole, "Image Quality Assessment Using the SSIM and theJust Noticeable Difference Paradigm" in Engineering Psychology and Cognitive Ergonomics.Understanding Human Cognition. EPCE 2013.Lecture Notes in Computer Science, Berlin, Heidelberg:Springer, vol. 8019, 2013.