Image Steganography using Polynomials

K. Kanthamma, K. Maheswari, G. N. Kodandaramaiah

Abstract: Steganography is the art of hiding secret messages inside other messages as until recently had been the poor cousin of cryptography, to communicate privately in open channel. The disadvantage of cryptography is that cryptanalysis's will break the secret key and secret message will be revealed .Steganography serves as a better way of securing message than cryptography. Steganography gained importance in the past few years due to the increasing need for providing secrecy in an open environment like internet. Many techniques are used to secure information such as cryptography that aims to scramble the information sent and make it unreadable while steganography is used to conceal the information so that no one can sense its existence. There have been many techniques for hiding messages in images in such a manner that the alterations made to the image are perceptually indiscernible. A new steganography encoding scheme which separates the colour channels of the windows bit map images and then hides the images randomly using polynomials in the LSB of any colour component of choose pixel. The polynomials may be of any type with constants and variables. a new steganographic encoding scheme, randomly hide messages in the LSB of any component of the chosen pixel using polynomial. If polynomial is used, hacker needs to predict more than one number. i.e. all coefficients of polynomial correctly to decode and probability of finding all right coefficients correctly is less compared to predicting single seed as in case random generator. So the strength of the stealth is increased by choosing higher dimensional polynomial.

Keywords- Steganography, messages, cryptography, polynomial, techniques.

I. INTRODUCTION

Steganography refers to the science of ***"invisible"*** communication. Unlike cryptography, where the goal is to secure communications from the steganographic techniques strive to hide the very presence of the message itself from an observer. The general idea of hiding some information in digital content has a wider class of applications that go beyond steganography. Three basic security concepts important to information on the internet are confidentiality, integrity, and availability. Concepts relating to the people who use that information are authentication, authorization, and no repudiation. When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. For some types of information, confidentiality is a very important attribute. Availability of the network itself is important to anyone whose business or education relies on a network connection.

When users cannot access the network or specific services provided on the network, they experience a denial of service. To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted the user cannot later deny that he or she performed the activity. This is known as no repudiation.

II. INFORMATION HIDING TECHNIQUES

The growth of high speed computer networks and that of Internet, in particular, has explored means of new business, scientific, entertainment, and social opportunities.

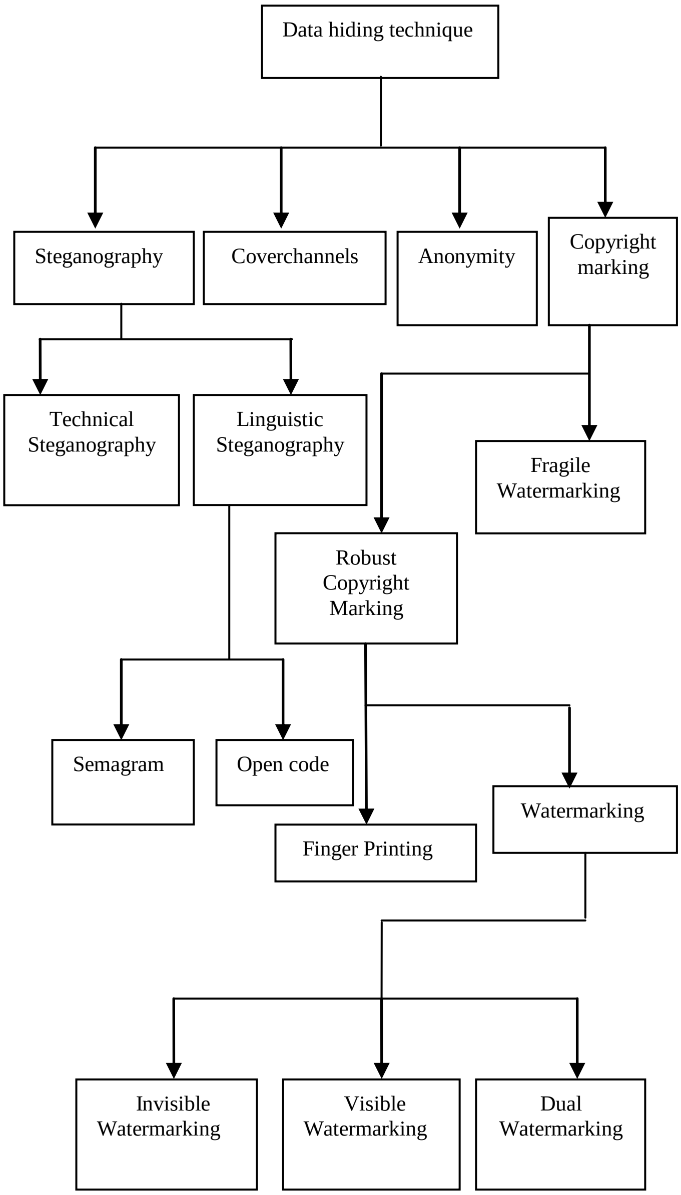


Figure 1: data hiding technique

Manuscript Received on December 2014.

Dr. K. Kanthamma, Associate Professor in Gates Institute of Technology, Gooty (A.P) India.

K. Maheswari, Associate Processor in Gates Institute of Technology, Gooty (A.P), India.

Dr. G.N. Kodandaramaiah, Professor in Kuppam Engineering College, KUPPAM, India.

Ironically, the cause for the growth is also of the apprehension- use of digital formatted data. Digital media offer several distinct advantages over analog media, such as high quality, easy editing, high fidelity copying. The ease by which digital information can be duplicated and distributed has led to the need for effective copyright protection tools.

Various software products have been recently introduced in attempt to address these growing concerns. It is done by hiding data (information) within digital audio, images and video files. One way such data hiding is digital signature, copyright label or digital watermark that completely characterizes the person who applies it and, therefore, marks it being his intellectual property. In the present era of computers and fast communication, one needs to protect communicated information (message or plain text) from unauthorized user , while sending it through any electronic media. Information requires the protection protocol. Digital supports like CDROM can contain the huge amount of the information. But they are volatile and it can be easily processed. Data content can easily copy, modified or converted in other formats by any intruders. There are various techniques have been developed to protect the data. The various information hiding techniques can be classified as shown in below figure.

Current day Steganography scenarios are driven by the copyright and usage concerns of creators of digital media. A steganographic procedure known as watermarking is the insertion of hidden text, hereafter referred to as a watermark, containing an identity into a media stream by its owner so that suspicious streams in the future may be tested for the presence or absence of the mark.

III. STEGANOGRAPHY

The word Steganography comes from the Greek name “stenos” (hidden or secret) and “graphy” (writing or drawing) and literally means hidden writing. Steganography uses techniques to communicate information in a way that is hidden. The most common use of Steganography is hiding information image or sound within the information of another file by using a **stego key** such as password is additional information to further conceal a message. Like many security tools, Steganography can be used for variety of reasons, some good, some not so good. Steganography can also be used as a way to make a substitute for a one-way hash value. Further, Steganography can be used to tag notes to online images. This procedure is divided into several operations. a) Encryption b) Data chunking c) Applying steganography d) Sending this chunked files e) File recombination f) Decryption.

Encryption:

The algorithm would require secret message (M), a wrapper (W) and a pseudorandom seed Generated by polynomial (S) as input. In Windows bit map format, every image will have three separate colour channels; a channel dedicated for the red component (R Com), another one for the green component (G Com), and a third one for the blue component (B Com). After separating the colour channels, the program would go through each pixel to find all those pixels where the watermark bits embedded. Spatial details of every such pixel will be stored in an array named Candidate Pixel (CP) and the total numbers of such potential candidate pixels are calculated. If the length of the message (in bits) is more than the length of CP then a message will be displayed prompting the unsuitability of the wrapper under consideration. If the wrapper is found to be suitable then a pseudorandom number will be generated from a pre-decided polynomial, by making use of the seed, which was agreed beforehand by both the parties. The pseudorandom number will be mapped to the Target Pixel index (TP) of CP by using the polynomial, with the length of the CP.

This will enable us to insert the secret data bit randomly across the wrapper thereby increasing the stealth of the system. Once embedded, all the colour channels will be concatenated to form the innocuous Stego Image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret messages. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they each represented by a byte. In other words, one can store 3 bits in each pixel. In this process the previously recombined file is to be decrypted so that the Receiver can get the original file which is sent from the sender. And now by entering the secret information the receiver is supposed to get the original file which is sent by the receiver.

Data Decryption:

In this procedure the file which is in the binary form and it is now embedded in some form and now this file is in the hidden format and any secret information is added by the sender and if the receiver wants to get the original image then he needs to extract the embedded image with the help of the secret information provided by the sender. When the receiver will receive the file will be in the embedded form and by extracting it he can use or read the original object file which is sent by the sender.

File Recombination:

In this process the chunked files are supposed to be recombined to get the whole File and this procedure are done on the receiver end, so the receiver must have the stego-key or any secret information from the sender so that the receiver can get the original file.

Image Steganography:

Image steganography has gotten more popular press in recent years than other kinds of steganography, possibly because of the flood of electronic image information available with the advent of digital cameras and high-speed internet distribution. Image steganography often involves hiding information in the naturally occurring “noise” within the image, and provides a good illustration for such techniques.

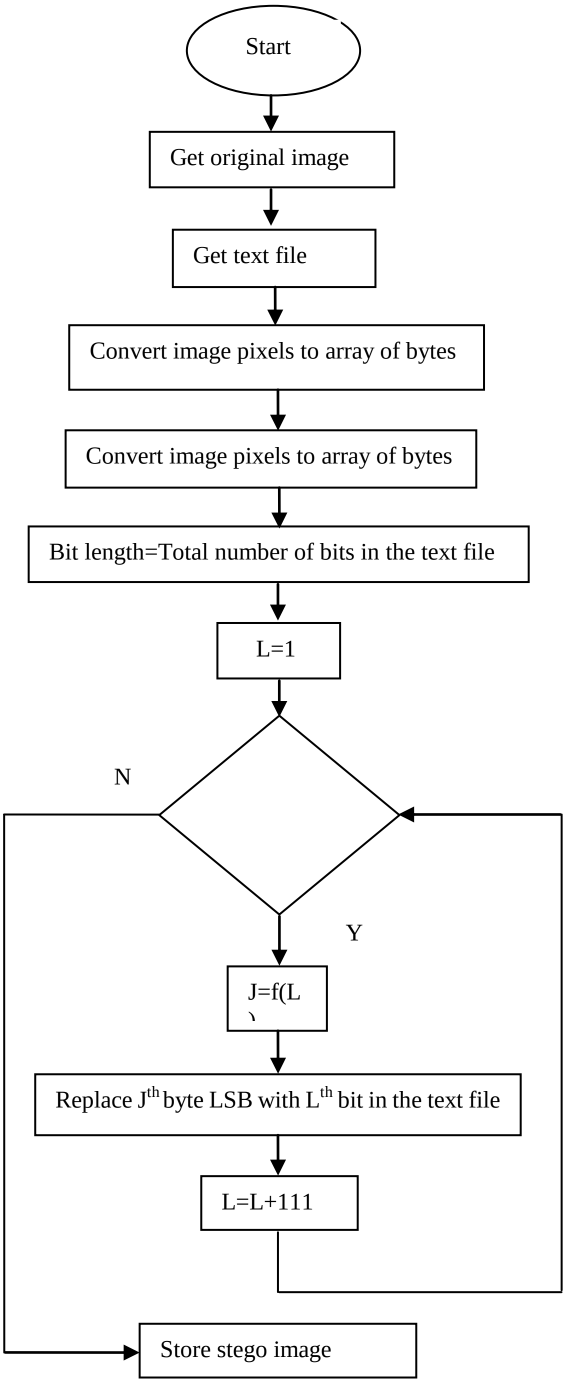

Start
Get original image
Get text file
Convert image pixels to array of bytes
Convert image pixels to array of bytes
Bit length=Total number of bits in the text file
L=1
N
Y
J=f(L
)
Replace Jth byte LSB with Lth bit in the text file
L=L+111
Store stego image

Figure 2: LSB Encoding Flow chart

Most of information contain some kind of noise. Noise cab new described as unwanted distortion of information within the signal. Within an audio signal, the concept of noise is obvious. For images, however, noise generally refers to the imperfections inherent in the process of rendering an analog picture as a digital image. For example, the values of colors in the palette for a digital image will not only not be the exact colors in the real image, and the distribution of these colors will be also be imperfect. The instantaneous measurement of photons made by a digital camera also captures the randomness inherent in their behavior, leading to a set of "imperfect" measurements which balance out to become a digital image.

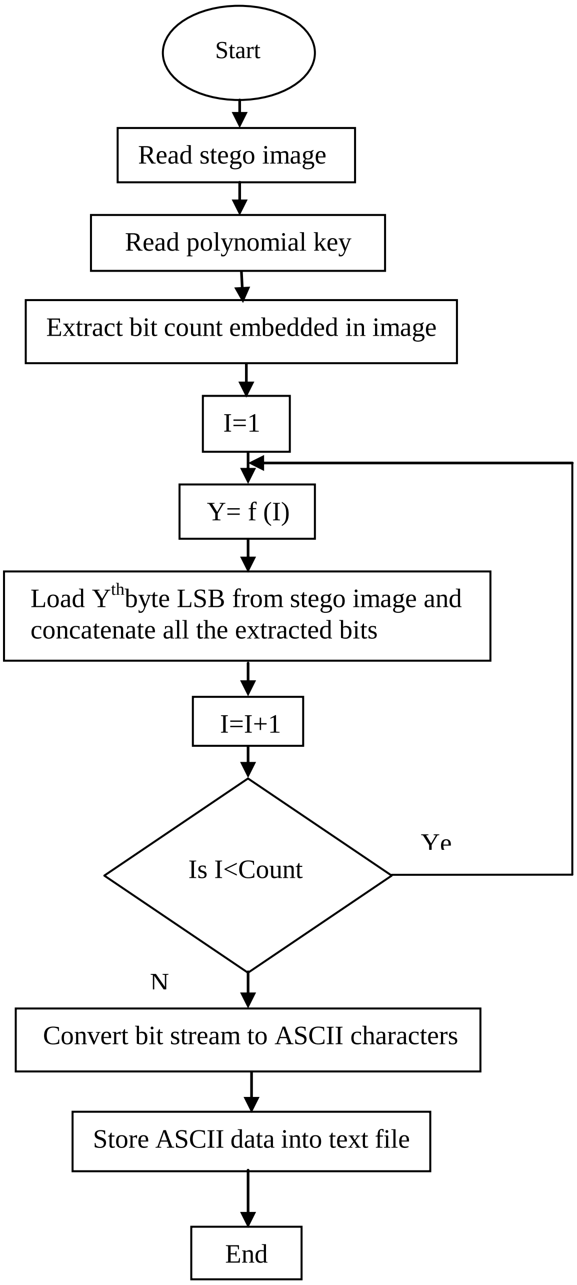

Start
Read stego image
Read polynomial key
Extract bit count embedded in image
I=1
Y= f (I)
Load Ythbyte LSB from stego image and concatenate all the extracted bits
I=I+1
Is I<Count
Ye
N
Convert bit stream to ASCII characters
Store ASCII data into text file
End

Figure 3: LSB decoding flow chart

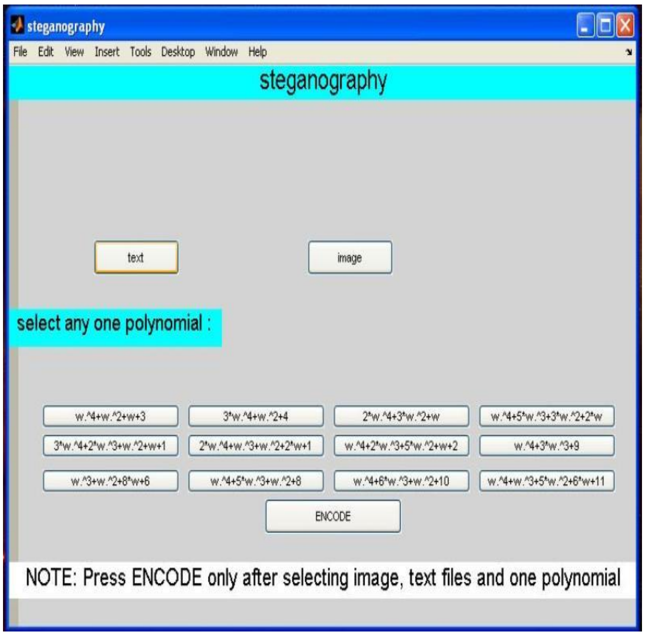
By changing the least significant bit (LSB) in the color representation for selected pixels, information can be hidden while often not significantly changing the visual appearance of the image; this is known as "image downloading". The greater the number of bits used to represent colors, the less obvious the changes in palette values are in the visual representation of the final image. While changing the LSB in order to hide information is a widely used steganographic method.

There are many methods for image steganography, however. an algorithm was used that attempts to avoid statistical distortion by taking advantage of the discrete cosine transforms that are used to compress and approximate a digital image. The image is a bitmap image which is compressed to a jpeg image by the tool as the secret message is embedded.

IV. RESULTS

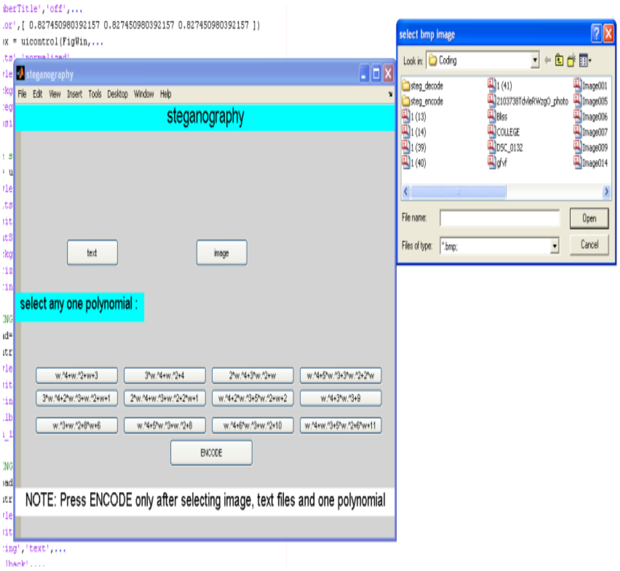
In testing we used 4288x2848 resolution image with 24-bits depth of colour

Encoding :



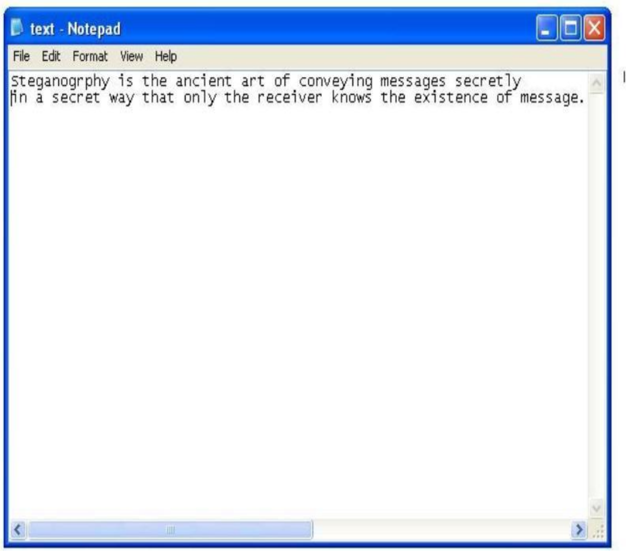
NOTE: Press ENCODE only after selecting image, text files and one polynomial

Figure 4: Encoding main window



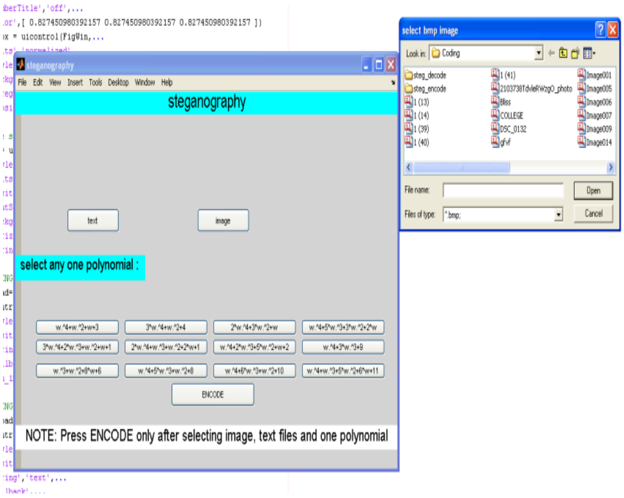
NOTE: Press ENCODE only after selecting image, text files and one polynomial

Figure 5: selecting text file



Steganogrphy is the ancient art of conveying messages secretly
in a secret way that only the receiver knows the existence of message.

Figure 6: text file



NOTE: Press ENCODE only after selecting image, text files and one polynomial

Figure 7: image selection window

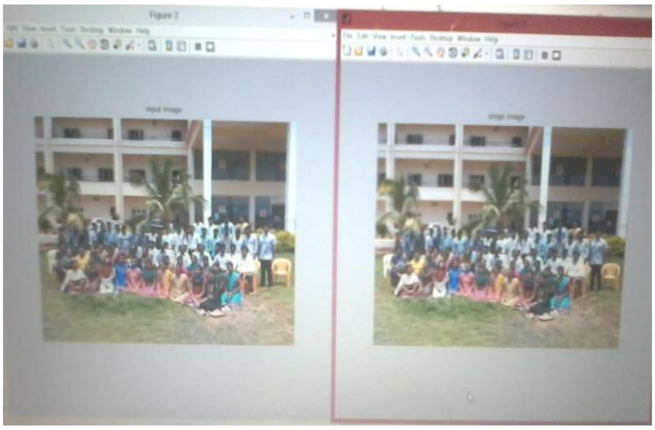


Figure8: stego image

Decoding:

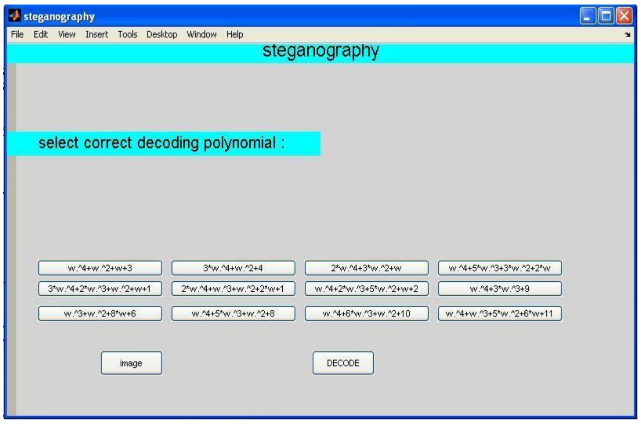


Figure 9: decoding window

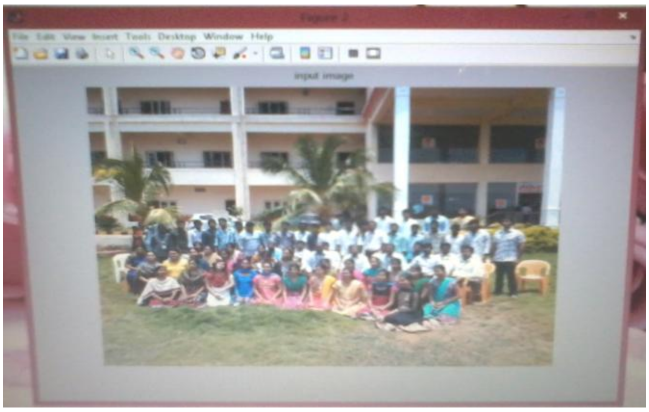
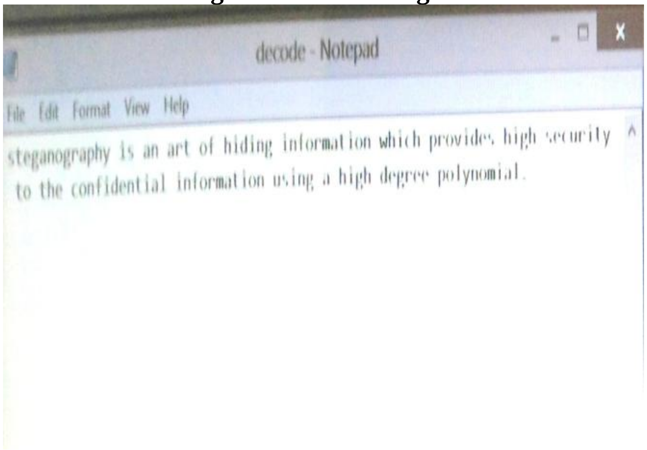


Figure10: cover image



steganography is an art of hiding information which provides high security to the confidential information using a high degree polynomial.

Figure11: decoded message

V. CONCLUSION

Explored several steganography techniques and the various detection algorithms associated with them. Zeros hiding proved to be easier to analyze than bit-o-steg and can hide significantly more data. Bit-o-steg can only hide data in coefficients that were not dropped, thus limiting the amount of data we can hide. However, it greatly enhances the effectiveness of the steganography since it uses a key, making it much more challenging to detect. In the end we found both effective, but the complexity of bit-o-steg makes it more promising. By investigating the power in various components of our images we discovered how to detect data hidden via the zero hiding method. Detecting bit-o-steg required us to draw on past steganography research and statistically analyze the effects of this type of data hiding. The methods and accompanying detection schemes we developed broadened our understanding of steganography, which, unlike encryption, allows secret data to be traded hands without raising an eyebrow.

REFERENCES

1. Image Steganography using Polynomials and Covert Communications in Open Systems EnvironmentA. Siva Sankar, T. Jayachandra Prasad and M.N. Giriprasad published in International Journal of Software Engineering. Volume 1, Number 1 (2010), pp. 87—94 © International Research Publication House http://www.irphouse.com
2. An Overview Of Image SteganographyT. Morkel , J.H.P. Eloff , M.S. Olivier published byInformation and Computer Security Architecture (ICSA) Research GroupDepartment of Computer Science
3. Lsb Based Image Steganography Using Polynomials And Covert Communications In Open Systems Environment For DrmbyA Siva Sankar T Jayachandra Prasad M N Giriprasad published in International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET, Mumbai, India.
4. Cryptography (Security By Des) By M.RAJ KUMAR and M.SYEDALI
5. Murray, A.H., and R.W Burchfiled (eds.), The Oxford English Dictionary, Oxford, England: Clarendon Press, 1933.
6. J. Bright, Jeremiah (AB; New York 1965) 209; R.K. Harrison, Jeremiah and Lamentations (Winona Lake 1973)
7. D. Kahn, 'The History of Steganography' in Anderson, pp. 1-5. http://www.trai.gov.in/WriteReadData/trai/upload/PressReleases/671/pr21apr09no38.pdf
8. Oosterwijk, Herman and Paul T. Gihring; DICOM Basics, 3rd ed.; OTech, Inc., Aubrey, TX;2002
9. D. Kahn, 'The Codebreakers - The Story of Secret Writing', Scribner, New York, New York, U.S.A., 1996. ISBN 0-684-83130-9.
10. G.J. Simmons , "The prisoners' problem and the subliminal channel" , Advances in Cryptology : Proceedings of CRYPTO 83, (ed. D. Chaum), Plenum , New York , 1984,pp.51-67.
11. NF Maxemchuk, Electronic Document Distribution", AT & T Technical Journal v 73 no 5 (Sep/Oct 94) pp 73 - 80
12. A. Westfeld and A. Pfitzmann, "Attacks on Steganographic System", Proc. Information Hiding-3 Int'l Workshop in Information Hiding, Springer- Verlag, 1999, pp. 61-76.
13. JijjuA.Mathew& Prof. Gurmit Singh, "Stegnography and Covert Communications in open systemsenvironment", 2009 IEEE, pp.847-849.
14. K.Sukumar, et.al., " Multi-Image –Watermarking Scheme based on Framelet and SVD", 2009 IEEE, pp. 379-388 .