IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197 Volume 1, Issue 6 (Mar. – Apr. 2013), PP 49-53
www.iosrjournals.org

Image Steganography using Polynomial key and Covert Communications in Open Systems Environment

Babbala Sundeep[1], Bhusam Gnanaprakash[1,] Alapati Harivanditha[2], Bobbu Yaswanth[1], Dr.A. Sivasankar[3]

[1](Department of ECE ,Priyadarshini College of Engineering , India)
[2](Department of ECE ,Priyadarshini College of Engineering , India)
[3](Head of the Department, Department of ECE ,Priyadarshini College of Engineering , India)

Abstract : *Steganography, the art of hiding secrete messages inside other messages, innocuous wrapper, as until recently had been the poor cousin of cryptography, to communicate privately in an open channel. This area of study got widespread popularity after its alleged use by many extremist groups while hatching and executing their plans remotely. Because of this, in the recent past, many law enforcement and government agencies have also shown keen interest in it. There are many other reasons like Digital Rights Management applications (Watermarking and Finger Printing), which acted as catalyst too. This paper proposes a new steganographic encoding scheme which separates the colour channels of the windows bitmap images and then hides messages Randomly using polynomials in the LSB of one colour component of a chosen pixel where the colour components of the other two are found to be equal to the key selected.*

Keywords :*Steganography, Data Hiding, LSB, Polynomials.*

I. INTRODUCTION

Digital Rights Management is a method of controlling access to copyrighted material. Communication and the flow of free thought, is regarded by many as a unique virtue that is greatly attributed to the overall development of human being. Moreover it was instrumental in overall growth of the human fraternity. According to Oxford Advanced Dictionary [1], communication is defined as the activity or process of expressing ideas and feelings or of giving people information; also communications is defined as methods of sending information. Communication has many divisions, and two of the most predominant ones are interpersonal and intrapersonal. Interpersonal communication can further be divided into two, namely public and private. One problem with the public communication channel is that it may have many eavesdroppers; eavesdroppers of passive, or active nature. A Passive eavesdropper may be one who just listens and an active one will listen and modify the message. Hence we could conclude that at times public communication demands the need of covert communications; a mechanism to communicate privately in a public environment.

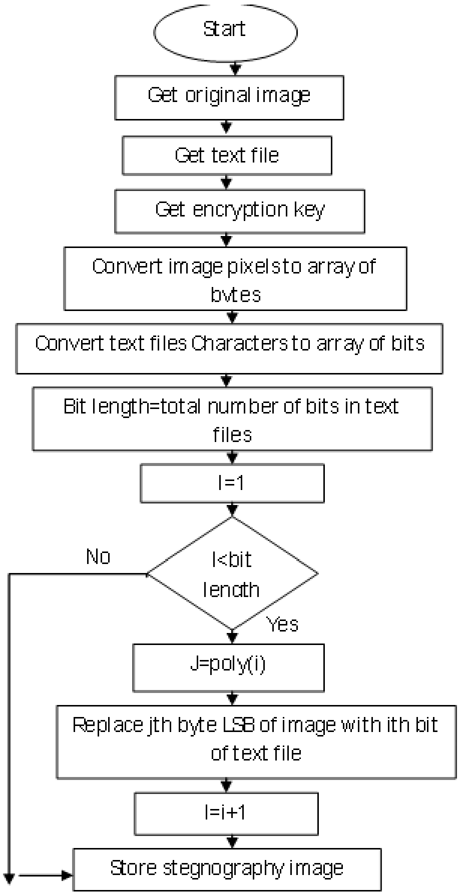
Throughout history, people have tried to find methods to hide information. History of Steganography, which is the original method of information concealment, dates back to ancient times. One of the earliest example of information hiding is the ATBASH code (2000-1500 BC) [2] used in Jewish mysticism, a cipher that substitutes the first letter of the Hebrew alphabet with the last, the second letter with the one before last, and so on. A book named Steganographia explaining many techniques for covert communication was explained by Johannes Trithemius around 500 BC and because of its very nature, the authorities never permitted him to publish the same and the book saw the light only in the mid 16th century, long after his demise [3]. The rapid growth of interest in this subject, over the last few years, is attributed to many reasons and some of the major reasons are discussed in the following paragraphs: Firstly, it got widespread popularity after the alleged use of it by many extremist groups while hatching and executing their plans, without bothering much about the geographical distance. This prompted various governments across the world to restrict the availability of covert services to the general public. This was causing inconvenience to many, which in turn has motivated open minded people to study methods by which secret messages can be embedded in seemingly innocuous cover messages through an open systems environment. The ease with which this can be done was thought by many as a potential argument against imposing restrictions. Secondly, the publishing and broadcasting industries have become interested in techniques for hiding copyright marks andserial numbers in digital images, audio and video recordings, books, multimedia products etc. The fearful fact is that it is too easy to copy a digital work, which only requires a right click. A proactive measure in this direction is the need of the hour and the industry demands one.

Thirdly the volume of communication lines are increasing exponentially and in fast developing countries like India, there is a high chance of covert communication going unnoticed in this bedlam. According to the Telecom Regulatory Authority of India (TRAI), Indians owned 429.72 million phones, 391.76 mobiles and 37.96 million landlines, at the end of March 2009. Total Broadband subscribers' base has reached 6.22 million by the end of March 2009 growing at a staggering 59.48 % during March 2008 to March 2009 and both the mobile and the broadband subscribers' are ever growing [4]. It is an enormous task for the law enforcement and intelligence agencies to monitor this entire 435.94million plus phones and broadband connections - deciding which communication to intercept and which one to leave, because of the huge volume of traffic.

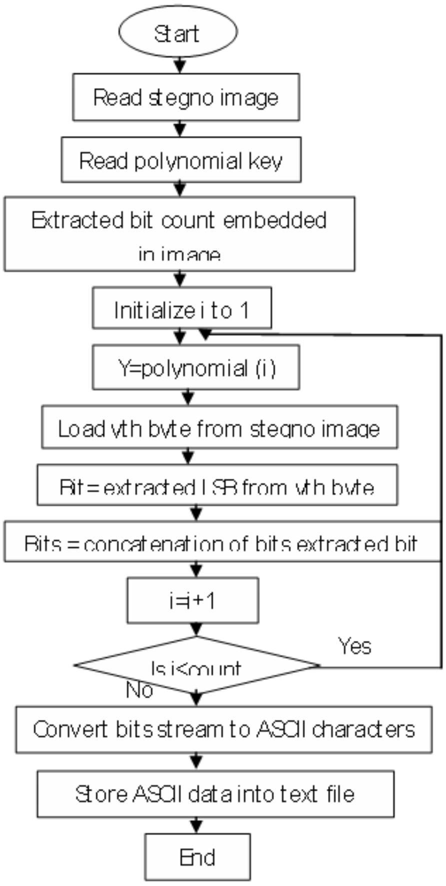
II. Information Hiding In Bitmap Images Using Lsb Based Chromatic Steganography Using Polynomial

Redundancy is one of the major aspects of creation. A close inspection reveals that redundancy does exist, and exists in abundance. Computer files are not an exception to this fact. For e.g. an image on a computer is represented by tons and tons of pixels, which in turn have many redundant information's. The simplest technique here is to fabricate the redundant bits so as to do the covert communication. For e.g. each pixel of an image consists of a variation of all three primary colors, red, green and blue, in a standard 24-bit bitmap, requiring 8 bits each for these three colors. i.e.there are 256 different variations, ranging from 00000000 to 11111111, for each colour in a pixel. So, to represent the colour white, the code would look like 11111111 11111111 11111111. Keeping in mind that, the human eye cannot distinguish the difference between too many colours, the colour 11111110 11111110 11111110 would look exactly the same as white, which means that the last digit in every bit in every pixel could be changed without much visual degradation of quality. This is the basis of the Least Significant Bit Insertion technique. We require 8 bits to represent an ASCII text and there are three potential slots extra in every pixel of a picture. Therefore, in a conducive environment, with every three pixels, one ASCII text could be concealed. In order to make this practical to the user, a computer program would be needed. After typing in the secret message and determining a suitable cover message, the program would go through every pixel to find the potential candidate pixels and will change the least significant bit to represent each bit of the message. The image could then be sent to the recipient who in turn runs his program to take off the least significant bits to form the secret message.

The current study took windows bit map image file format with loss less compression in to consideration. The proposed 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 (rCom), another one for the green component (gCom), and a third one for the blue component (bCom). After separating the colour channels, the program would go through each pixel to find all those pixels where the value of the rCom and gCom is equal to that of the supplied R and G values. 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-decidedpolynomial, 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. Here in the algorithm, we have embedded data in bCom where the colour coefficients of the rCom and gCom were found to be equal to that of the chosen key; but the combinations may be changed so as to increase the stealth of the system. The algorithm performing the above said concept is shown below:


Start
Get original image
Get text file
Get encryption key
Convert image pixels to array of bytes
Convert text files Characters to array of bits
Bit length=total number of bits in text files
I=1
I<bit length
No
Yes
J=poly(i)
Replace jth byte LSB of image with ith bit of text file
I=i+1
Store stegnography image

LSB Encoding Method


Start
Read stegno image
Read polynomial key
Extracted bit count embedded in image
Initialize i to 1
Y=polynomial (i)
Load yth byte from stegno image
Bit = extracted LSB from yth byte
Bits = concatenation of bits extracted bit
i=i+1
Is i<count
Yes
No
Convert bits stream to ASCII characters
Store ASCII data into text file
End

LSB Decoding Method

The Stego Image could then be send to the recipient through open systems environment, who in turn runs his program to extract those randomly stored least significant bits of bCom component where the colour coefficients of the rCom and gCom are found to be equal to that of selected keys i.e. R and G. Thus the secret message could be communicated covertly[10]. The algorithm implementing the decoding procedure is shown above:

If we compress the secret message before embedding, using any available text compression algorithm, like Run length encoding scheme, we may further reduce the message length, thus reducing the entropy and in turn enhancing the robustness of the system. Also the great thing about this insertion technique is that because the secret message is encoded into the color channels, the message is not lost even if the file is compressed.

III. RESULTS

Figure 1 and 2 are images with a resolution of 2272 × 1704 with 24-bit color depth. The sizes of the two windows bitmap images shown are 11.0 MB (11,614,464 bytes). Fig. 1 is unmodified where as Fig. 2 the modified one and an encrypted secrete message is also shown. It is impossible for the human eye to find a visual difference between two of the above shown images. Since the visual difference test was unable to find any positive results, some statistical tests were exercised with the intention to prove that the image was tampered. If the image happen to be modified then at least some of image's statistical properties may deviate from a norm. Here also no significant difference in the quality of the cover and stego image were found. We therefore conclude from the basic statistical test that there is no evidence from the current experiment to suggest that the proposed system deteriorate the quality of the image. The different tests conducted and there results are tabulated in table 1

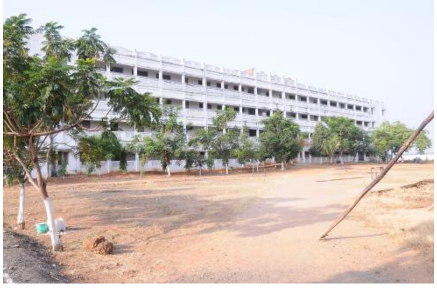


Figure1: Original Image

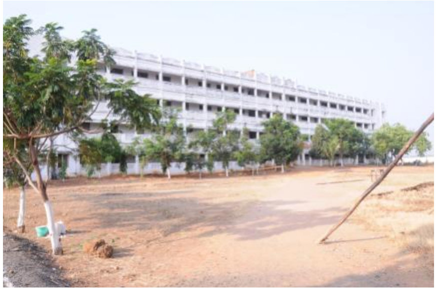
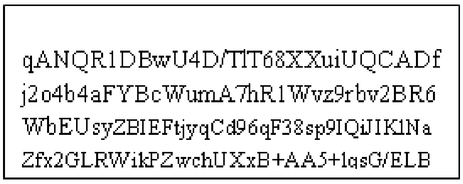


Figure2: Stego Image



```
qANQR1DBwU4D/TlT68XXuiUQCADf
j2o4b4aFYBcWumA7hR1Wvz9rbv2BR6
WbEUsyZBIEFtjyqCd96qF38sp9IQiJIK1Na
Zfx2GLRWikPZwchUXxB+AA5+1qsG/ELB
```

Secret Message

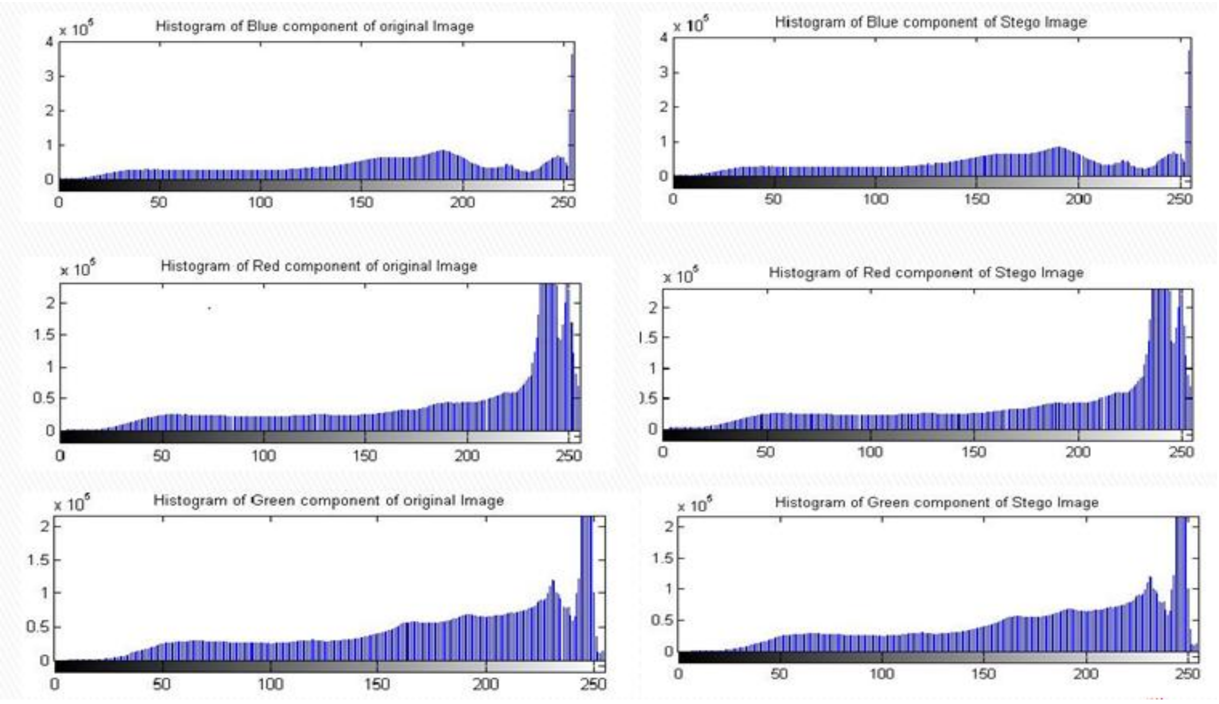


Figure 3 : Histogram results

Test name	Original image	Stego image
Mean	117.231369	117.231369
Standard deviation	93.502419	93.502411
Median	205.000000	205.000000
Size	36636672.0000000	36636672.000000

Table 1 : Statistical results

IV. Conclusion

In the paper, the authors have introduced a new steganographic encoding scheme which separates the colour channels of the windows bitmap images and then randomly hide messages in the LSB of one component of the chosen pixel using polynomial where the colour coefficients of the other two are found to be equal to the keys selected.

References

[1]. Murray, A.H., and R.W Burchfiled (eds.), The Oxford English Dictionary, Oxford, England: Clarendon Press, 1933.

[2]. J. Bright, Jeremiah (AB; New York 1965) 209; R.K. Harrison, Jeremiah and Lamentations (Winona Lake 1973)

[3]. D. Kahn, 'The History of Steganography' in Anderson, pp. 1-5.

[4]. http://www.trai.gov.in/WriteReadData/trai/upload/PressReleases/ 671/pr21apr09no38.pdf

[5]. Oosterwijk, Herman and Paul T. Gihring; DICOM Basics, 3rd ed.; OTech, Inc., Aubrey, TX;2002

[6]. D. Kahn, 'The Codebreakers - The Story of Secret Writing', Scribner, New York, New York, U.S.A., 1996. ISBN 0-684-83130-9.

[7]. 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.

[8]. NF Maxemchuk, Electronic Document Distribution", AT & T Technical Journal v 73 no 5 (Sep/Oct 94) pp 73 - 80

[9]. 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.

[10]. JijjuA.Mathew& Prof. Gurmit Singh, “Stegnography and Covert Communications in open systemsenvironment”, 2009 IEEE, pp.847-849.

[11]. K.Sukumar, et.al., “ Multi-Image –Watermarking Scheme based on Framelet and SVD”, 2009 IEEE, pp. 379-388