A Review on Different Data hiding Techniques

Prabal Kashyap Basumatary
Department of Computer Applications, National Institute of Technology, Kurukshetra, Haryana, India.

Prabhjot Singh
Department of Computer Applications, National Institute of Technology, Kurukshetra, Haryana, India.

Abstract – Data is considered as most indispensable Asset for an individual or an Organization and in a Present Era Information is Transferred digitally over the Internet. It is necessary to Protect information. Degree and Level of Security is Considered on Top Priority. Steganography is one of them Technique in which Presence of Message Cannot Be Found Easily. It can be used as tool for Security Purpose to Send Confidential Information using any carrier over the Internet. There are Different Approaches to Embed Secret Data into an Image Based on Size of an image, Type of an Image. The Focus of this Paper is to classify Different Decomposition Techniques. In this Paper a novel data hiding Technique is proposed which is an Improvement over Fibonacci LSB Data Hiding Technique which is Implemented on Grayscale Image and Proposed by Battisti et al[3]. The Fibonacci representation of grey level images requires Biplane of a Grayscale Image. Prime number Decomposition is based on Embedding of Secret Data on the Pixel Value. In Prime number Decomposition Outperforms the Famous LSB data hiding Technique. Best case and Worst case are Similar on a grayscale Image. Experimental Result shows that Stego-image is indistinguishable from the original image.

Index Terms – Bit-planes, Confidential Information, Cryptography, Steganography, Stego-Image.

1. INTRODUCTION

Steganography is an Art of Hiding Secret Data in a Carrier. Its Purpose is to Hide the Presence of Communication. It is Different from Cryptography. Where it Scrambles Message that cannot be Readable. Steganography Hides data it cannot be Observed Easily [2]. Embedding secret message into cover image called Stego-image. Grayscale images are the best cover images for Embedding Secret Data. Secrecy of data is important issue. Steganography offers a Reliable way to Hide Data. Embedding is parameterized by a key that makes Difficult to detect the data. It is one of the oldest problem which popular in now days .Steganography is also known as Prisoner Problem. In this Paper Decomposition and Embedding Both Have Same Meaning.

1.1 How Steganography works

Figure 1 Embedding of Data into image

Figure 2 Extraction of data from an image

2. TYPES OF STEGANOGRAPHY TECHNIQUES

Image Steganography :-

One of the most Popular Technique in which secret Message is hide in Digital image which cannot be detected By a Normal Human Eye.it provide Efficient way to hide data in Image. Different operation can be performed on image Ranging Simple to Different Transformation.

Text Steganography:-

It is one of oldest and difficult technique in which Secret message is written and Concealed in Natural Language. It is one of the challenging method in which message have lesser redundancy. There are more chance of Leaking of information because Secret message is written in natural language .

Audio Steganography:-

Audio steganography embeds the message as noise into a cover audio file at a frequency out of human hearing range. Embedding secret messages in digital sound is generally more difficult than embedding messages in other media, Sensitivity to additive random noise is also acute. Commonly used methods for audio Steganography are LSB coding, parity coding, phase coding, spread spectrum, and echo hiding [4].

Video Steganography:

It pertains to hide information in video files, which are generally collection of sound and images. Steganography methods that are applicable to sound and images are also applicable to video files. Advantage of this method is that large amount of data can be hidden inside Video with smaller amount of distortion because of continuous flow of information and that might go unobserved by observer.

3. DOMAIN BASED STEGANOGRAPHY

Spatial Domain Techniques:

It includes Bitwise Manipulation of pixel intensity and noise manipulation. There are various Approaches to embed secret

data in an image. Most common Techniques for Spatial Domain are Least Significant bit.

LSB Method:

It Replaces Least Significant bit of Cover with Secret Message. It has low Complexity with high efficiency of embedding of data in secret message. It makes small change in cover which cannot easily detected.

4. LSB DECOMPOSITION

One of the Simplest System for Embedding Data into Digital Cover By Least Significant Method. Let us Assume that there Are N×N image in which each pixel value represent by a Decimal Number in the range.In a Gray-Scale Image, with 8 bit Precision per Pixel, Each Pixel value Lies between[0,255] .

2^8 =256.

The Embedding Strategy is based on Sequential insertion or Selection Embedding of the message in the Noisy area of an Image.LSB Decomposition offers low Computational Complexity with high Embedding Capacity [3].Image File larger size than size of message Works Better with LSB.Changes or Modification of LSB Bit should be made. Gradual change in shade occur when we Embedding secret message on Gray scale Image[3][4]. Minimal Change in bit value cannot alter the quality of image. Quality of Image remain same as Original and cannot be detected Easily by Human Eye.

Figure 3. Original Image Figure 4 Stego-Image

In the Above two Images Both are Seems same but there is a difference that one image is an original image while other image contain Secret data which cannot be Easily Distinguishable by a Human Eye.

5. FIBONACCI DECOMPOSITION

It was introduced in 13th Century. In Fibonacci LSB data hiding technique, it consists a sequence which is generated using Fibonacci. Fibonacci series is generated to check the decomposition in different bit plane.

To embedded secret message bit into pixel first it has to qualify zeckendorf condition. If zeckendorf condition failed then extraction of data is not possible. Fibbonacci LSB data hiding technique as an improvement a novel data hiding is proposed by Battisti et al.[2]. The Fibonacci sequence is redundant.natural number which may represent as sum of Fibonacci number.In Zeckendorf Conditon, it states that each positive integer can be represented as a Sum of Distinct number in Sequence of Fibonacci number using no two consecutive number.

In the Embedding Process Pixels are Selected and further decomposed. Plane is also selected in which data is to be embedded. Same Embedding Scheme is to Applied to Different Bit Planes resulting in more robust data hiding. It does not allow a fixed size embedding due those unsuitable pixels which are not eligible to hide data. To deal with Redundancy zeckendorf condition should be qualified. If a Pixel unsuitable or not good Candidate then next candidate pixel is selected and side information in a Table is updated.

The Sequence of Fibonacci number is Defined as

$$\begin{cases} 0 & n < 0 \\ 1 & n = 0 \\ F(n\text{-}1) + F(n\text{-}2) & n > 0 \end{cases}$$

The Fibonacci Number Generation Formula are

$F(n) = F(n-1) + F(n-2)$ For every $n \geq 2$

6. PRIME NUMBER DECOMPOSITION

In Prime Number Decomposition Embedding is done by replacing secret data bit by (virtual) Bit-plane After embedding if representation is not valid then it is skipped. This Technique also guarantees the existence of inverse function but also correctness for Extraction of secret embedded Message Bit. There are no such conditions which are needed to qualify. Prime Decomposition gives Less Distortion in high bit planes.

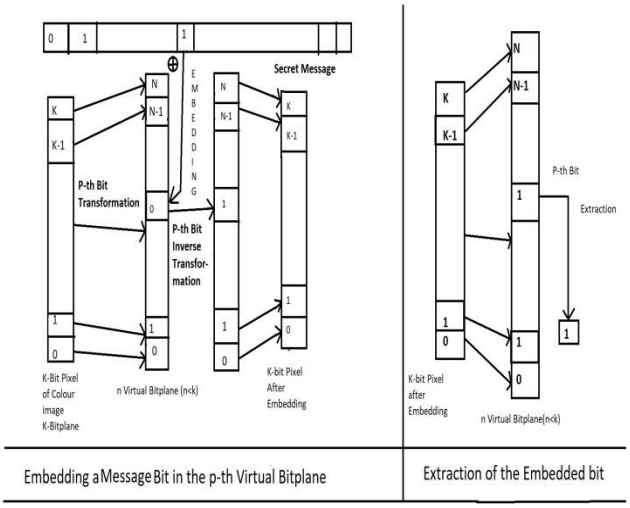

Figure 5 Generalized data-Hiding technique

If we have k-bit cover image only k bit planes are available to embed data. Increasing bit plane cause increase in distortion. Prime number Decomposition focuses on increase the total number of available and embeddable bit plane with minimum Distortion [1].

In this technique it does not allow to embed secret message in higher bit plane. In decomposition of a prime number, the value which has more than one represent in the number system highest lexicographically is chosen. Pixel value bit is replaced by secret message bit. It gives more efficient way to hide data in an image. Change LSB will not Affect in Change in Quality of Image.

7. COMPARATIVE STUDY ALL LSB DECOMPOSITION TECHNIQUES

Table 1. Technique used in LSB Data Hiding

Classical LSB	Classical LSB data hiding uses the simplest approach. In classical LSB data hiding, the least significant bit of a pixel is manipulated in order to embed the desired image.
Fibonacci Technique	In Fibonacci LSB Decomposition, the bit planes are decomposed so as to generate more bit planes and then the secret message is embedded on following the Zeckendorf theorem.
LSB data hiding by prime numbers	In LSB data hiding using prime numbers, the bit planes are decomposed by using sum of prime numbers. After that the secret message is Embedded Lexicographically.

Table 2. Embedding Techniques used in LSB data hiding

Classical LSB	Data of least significant bit of the cover image is Replaced by Secret message Bits
Fibonacci Technique	Technique uses Fibonacci sequence for generation of bit planes and data is inserted if it passes the Zeckendorf condition.
LSB data hiding by prime numbers	A k-Bit to n-Bit Map is Created where the Value of n is $\sum_{0}^{n-1} P_i \geq 2^k - 1$ Data is inserted bit by bit matching the k-bit to n-bit mapping sequence

Table 3. Weight Functions

Classical LSB	The least significant bit of the image pixel is manipulated. In case of 8 bit image it is the 8^{th} bit of each byte. For 24 bit image the RGB color code are changed [12].
Fibonacci Technique	$F_p(0)= F_p(1)=1$ $F_p(n)= F_p(n-1) + F_p(n-p-1)$ $\forall\ n \geq p+1\ ,\ n \in N$
LSB data hiding by prime numbers	$P(0)=1, P(i)=P_i\ \forall\ I \in z^+$ $P_i=i^{th}$,Prime $P_0=1, P_1=2, P_2=3, P_3=5, \ldots$

Table 4. Numbers of bit planes generated

Classical LSB	8 bit planes using gray scale 8bit Lena image.
Fibonacci Technique	12 bit planes using gray scale 8bit Lena image.
LSB data hiding by prime numbers	15 bit planes using gray scale 8bit Lena image.

8. CONCLUSION

Data will remain cornerstone for all organization. Steganography is a way to hide the data in combination with cryptography it become more secure and robust. Privacy is also a main aspect so steganography could be used like terror group already using this type of Technique. Images can be hide Large amount of Malicious content i.e. Like Trojan horse, type of virus. Stegography is a vast domain with a Different Embedding Scheme each Scheme has its own nature. Different Decomposition Techniques give different Result on Different Types of Images. In some Cases Decomposition Technique over qualifies Traditional Embedding Scheme sometime best case and worst case are same. In Some Technique during Embedding phase some condition needs to be qualified so that it Provide validation and Robustness. Many stego-experts suggest grayscale images suitable for hiding of Secret data.but colour image Provide more capacity of data hiding.it depend on end user which type of data is to be Embedded.

REFERENCES

[1] D. Sandipan, A. Ajith, S. Sugata, An LSB Data Hiding Technique Using Prime Numbers, The Third International Symposium on Information Assurance and Security, Manchester, UK, IEEE CS press, 2007.

[2] C. Shao-Hui, Y. Tian-Hang, G. Hong-Xun, Wen, A variable depth LSB data hiding technique in images, International Conference on Machine Learning and Cybernetics, 2004, Vol. 7, 26-29 pp. 3990 – 3994, 2004.
[3] F. Battisti, M. Carli, A. Neri, K. Egiaziarian, A Generalized Fibonacci LSB Data Hiding Technique, 3rd International Conference on Computers and Devices for Communication (CODEC-06), Institute of Radio Physics and Electronics, University of Calcutta, December 18-20, 2006.
[4] Sumeet Kaur; Savina Bansal; R. K. Bansal "Steganography and classification of image steganography techniques"2014 International Conference on Computing for Sustainable Global Development (INDIACom) Year: 2014,Pages: 870 – 875
[5] W. Bender, D. Gruhl, N. Morimoto, and A.Lu(2000), "Techniques for data hiding", IBM Systems Journal, Vol 35, No. 3-4, pp 313-316.Lee, Y.K. and Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:
[6] J. Fridrich, M. Goljan, and R. Du, "Distortion-Free Data Embedding," to be published in Lecture Notes in Computer Science, vol. 2137, Springer-Verlag, Berlin,2001
[7] N.F. Johnson and S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software," Lecture Notes in Computer Science , vol. 1525, Springer-Verlag, Berlin, 1998, pp. 273-289.
[8] L.M. Marvel, G. W. Hartwig, and C. Boncelet, Jr., "Compression-Compatible Fragile and Semi-Fragile Tamper Detection", Proc. SPIE. Security and Watermarking of Multimedia Contents, San Jose, California, January 2000, pp. 140-151.
[9] A. K. Jain, Advances in mathematical models forimage processing, Proceedings of the IEEE,69(5):502–528, May 1981.
[10] R. Chandramouli, M. Kharrazi, and N. Memon, "Image Steganography and Steganalysis: Concepts and Practice", T. Kalker et al. (Eds.) IWDW 2003, LNCS 2939, Springer-Verlag Berlin Heidelberg, 2004, pp. 35–49
[11] Z. Zhao, N. Yu, and X. Li, "A novel video watermarking scheme in compression domain based on fast motion estimation", In: Proceedings of IEEE International Conference on Communication Technology, 2003, pp. 1878-1882.
[12] P. Salee, "Model–based Steganography", In: Proceeding of the 2nd International workshop on digital water marking, Seoul, Korea, October 20-22 2003 , LNCS , vol.2939, pp. 254-260.
[13] N. Provos and P. Honeyman, "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003, pp 32-44.
[14] Fabien A.P.Petitcolas, Ross J. Anderson and Markus G. Kuhn, " Information hiding - a survey", Proceedings of the IEEE Special issue on protection of multimedia content, Vol.87, No. 7, pp. 1062-1078, July 1999.
[15] G.J. Simmons, "The Prisoner's Problem and the Subliminal Channe". In: Proceedings of CRYPTO '83. Plenum Press, 1984, pp 51-67.
[16] A Piva, M. Barni, F. Bartolini, V. Cappellini, "DCT-Based Watermark Recovering Without Resorting to the Uncorrupted Orignal Image", in [10], 1997 pp. 520-523.
[17] T.G. Handel, M.T. Stanford, III. "Hiding Data in the OSI Network Model", In: [1] pp.23-38 ,1996.
[18] L. M. Marvel, C. G. Boncelet, C. T. Retter, "Reliable Blind Information Hiding for Images", *Proc. Information Hiding Workshop*, 1998-April.
[19] M. D. Swanson, B. Zhu, A. H. Tewfik, "Transparent robust image watermarking", *Proc. IEEE International Conference on Image Processing (ICIP96)*, vol. III, pp. 211-214, 1996.
[20] T. Handel, M. Sandford, "Hiding data in the OSI network model", In Anderson, Red: Information Hiding: Proceedings of the 1st International Workshop on Information Hiding, Cambridge, U.K., Springer June 1996, pp 23-38.