www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Volume-5, Issue-3, June-2015

International Journal of Engineering and Management Research

Page Number: 256-260

A Survey paper on Latest Image Steganography Techniques

Vijilesh Krishnan V K

Department of Applied Electronics & Instrumentation, M.E.S College of Engineering, Kuttippuram, Kerala, INDIA

ABSTRACT

Steganography is a science of hiding information inside any appropriate multimedia carriers like image, audio or video. If the carrier is an image, then it is termed as image steganography. Image stegnography is mostly used because it consumes lesser bandwidth. Only the intended receiver can detect the presence of secret information inside the image. Here secret information is embedded into a cover image and generates a stego-image. In this paper concept of image steganography, is explained and review and analysis of latest image stegnography techniques is presented.

Keywords—Encryption, PVD, stego-image, LSB

I. INTRODUCTION

In Today's world, communication becomes very easy using internet technologies. So many secret messages are exchanged using internet. But these secret messages should be confidential. These messages should be hidden either by using cryptographic methods or steganography methods. In cryptography the secret message is encrypted by using key. The encrypted message is transmitted and at the receiver side it is decrypted. But the cryptographic methods always give an impression to the intruder that some secret data is exchanged. In the case of steganography methods the information is hiding in any type of multimedia carrier. So that intruder cannot detect the presence of secret information in the multimedia carrier. The word steganography is derived from the Greek words stegos means cover and grafia meaning writing. Steganography refers to covert communication for transfer of confidential information over a communication channel. Security, Capacity, imperceptibility, and robustness are the essential features of data hiding system. Steganography can be classified into three types, namely pure, symmetric & asymmetric. In pure steganography there is no need of any extra information for message extraction. Image steganography can be done in spatial domain or frequency domain. In spatial domain direct manipulation of the image pixels takes place. In frequency domain processing the image pixels need to be transformed into frequency coefficients. LSB modification techniques, Edge encryption techniques are the examples of spatial domain processing. DCT coefficient processing is an example of frequency domain processing.

Data hiding comprise of both watermarking and steganography.The algorithm to extract the hidden information is very important in data hiding system. Depending on the strategy used to embed the data in the cover medium, extraction process can be Blind or non blind. In the case of non blind water marking it uses original cover medium to find watermark. Where as in blind processing it do not have the access to original cover media. Blind detection is a difficult job.

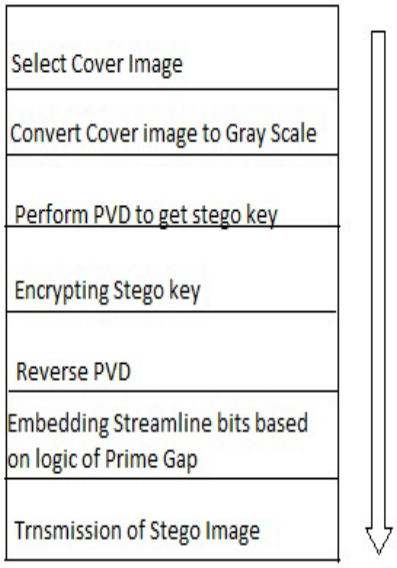
Image steganography requires Cover-Image, secret message, stego-key. The cover image is the original image of any format, which is used as a carrier for hidden secret message. Stego-key is a key used for embedding or exacting secret message. After embedding the secret message in the image, then the resulting image is termed as stego-image. The embedding can be done with or without stego-key. The stego-Image is transmitted to the receiver. The intruder or attacker may not detect the presence of secret message in the stego-image. The requirement of good steganography method is that the cover image and stego-image should not be visually separable. The various applications of steganography are copyright protection, content authentication, broadcast monitoring, Finger printing, metadata binding, covert communication etc.

ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

II. STEGANOGRAPHY METHODS

A) Snake and Ladder based algorithm

The paper titled "Snake and ladder Based algorithm for Steganographic Application of specific streamline Bits on Prime Gap Method" by Jas R Sheth is referenced here. Snake & Ladder algorithm based on game of snake and Ladder and the movement of participant based on primary & non primary value of pixel location. Prime gap function is used here. Prime gap is the difference between two consecutive prime numbers. Here the image matrix is considered as M*N board of the game. The starting address of the encrypting and decrypting streamline bits is based on the stego key. Here first convert cover image into Gray scale and perform picture value difference (PVD).Then find stego keys. Stego key=Column address of the first row and starting address= D(1, Stego key) where D is the matrix obtained after performing PVD. Encrypt stego key. For encrypting the stego key, pixel value differencing is carried out. The maximum value in the PVD matrix is computed and the stego key is stored as an offset from 255.Then do the reverse of PVD. Then embed the secret data on the image based on logic of prime gap. Then transmit stego .image. At the receiver side do the PVD to obtain stego key. Then decrypt the data by prime Gap logic. Modify the stego image to obtain secret data. This method provides safe and effective algorithm as compared to traditional Difference Steganographic methods.

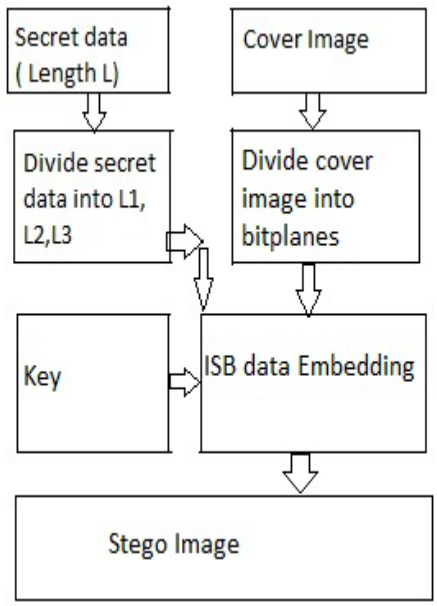


The proposed method has an efficient outcome as compared to other PVD methods.

The future works on this algorithm is on RGB scale using multiple switching across three planes thus enabling to triple the amount of data to be encrypted also encrypting the stego keys in the frequency domain.

B) A High Capacity Blind Steganographic technique

The paper titled "Data Hiding in intermediate Significant Bit planes, A High Capacity Blind Steganographic Technique" by Shabir A parah, Javaid A Sheikh, G.M Bhat is referenced here. In this method secret data to be transmitted is hidden in the intermediate significant bit planes of a cover image. First divide the secret data into Blocks. The data to be embedded in the bit planes divided into three variable length data vectors of continuously decreasing lengths. The data vector with total length L is divided into three variable length data vectors, L1, L2 & L3. Also divide the cover image into constituent bit planes. Then embed the divided data vectors in the intermediate significant Bit planes of cover image. The embedding process is carried out in data embedder. Also used a private key for the control of embedding process. Based on the pseudo random number generation method, the private key is obtained. This key ensures highly randomized data embedding. The security of data embedding is a function of key length. The used PRNG (Psuedo Random number generation) is capable of addressing all the locations in the first three intermediate significant Bit planes where data is to be embedded. The PRNG uses 18 bit seed word to generate the key. The philosophy behind data embedding in the proposed system is that more significant the bit planes, lesser the amount of data embedded in it. At the receivers side extraction algorithm uses stego image along with the same key used for data embedding. The extraction is blind detection since it does not needs the original cover image. Tool used for the simulation is MATLAB 7.



Embedding more and more data in cover image results in deterioration of the image quality. So the attacker can easily understand that there are some secret data

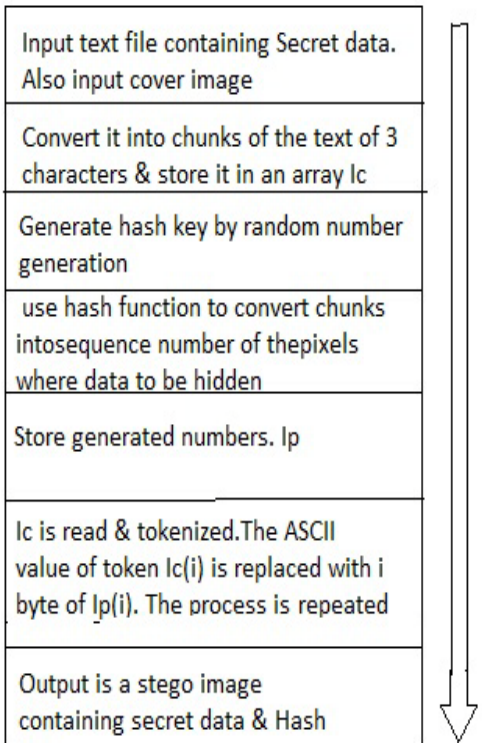
embedded in the cover image. So reasonable amount of data selected here to embed d in the cover image. Here embedding capacity is fixed as 25%.
Hiding capacity is defined as the amount of data that can be hidden in the cover image without disturbing the quality of the cover image. It is calculated mathematically as HC=n/N*100. Where n=total message bits & N=total image bits. PSNR (peak Signal to Noise Ratio) gives the quality of the image when secret data is embedded.
PSNR=10 $\log_{10}$ 255^2/mse db, where

$$mse = \left[\frac{1}{N*M}\right]^2 \sum_{i=1}^{N} \sum_{j=1}^{M} (X_{ij} - \bar{X}_{ij})$$

Where N, M are the image dimensions.
The proposed method on n average provides 8 db improvements in PSNR comparing with other spatial domain watermarking method.

C) Perfect hashing based approach for Secure Steganography

The paper titled "A new perfect hashing based approach for secure steganography" By Imran Sarwar Bajwa, Rubata Riasat is referenced here. They presented a perfect hashing based approach for information hiding in the gray scale images. There are some algorithms those uses hash functions to hide data in images. The examples of such algorithms are MD5, SHA but these algorithms provide susceptible security. Perfect hashing function is fast, avoids any hash collision, and supports very large key sets. The tool used for the experiment is VB.NET. Here first read the text file containing secret message. Then make chunks of the text of three characters and store. To generate a hash key use random number generation technique. Then select a cover image. Apply perfect hashing algorithm on cover image and stored characters to obtain stego image. For retrieving the textual data from stego image, the same hash key is required. For data transmission on the internet, the file format such as jpeg is used.



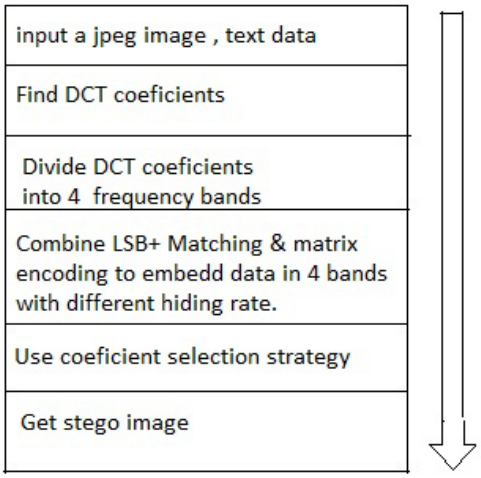
The results of the experiments were compared to the other available approaches for grey-scale image stegnography. Result shows that this approach not only provides good security but also provides fast speed for coding/decoding and at the same time able to handle large data-sets.

They present a prototype tool in this paper that is implementation of the presented approach and also proof of concept. The designed system has ability to hide text in an image without losing the quality of the image up to an extent. This system specifically works for efficient and secure data hiding in images to make possible large-sized data image stenography and transmission over internet. The proposed approach is fully automated.

D) Secure Jpeg Steganography by LSB+ matching and multi-band embedding

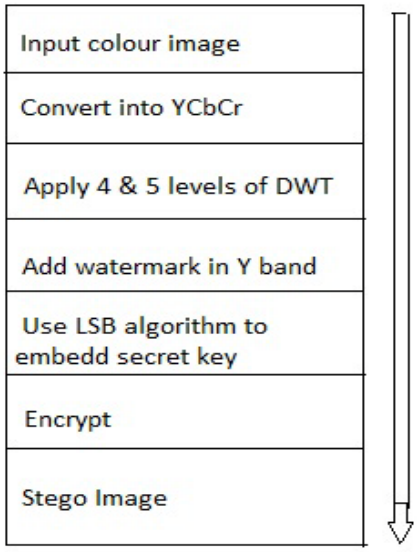
The paper titled "Secure JPEG Steganography by LSB+ Matching and Multi-Band Embedding" by Hao-Tian Wu, Jiwu Huang is referenced here. This method mainly focused on the JPEG images. An embedding algorithm called LSB+ matching is used here. These algorithms preserve the marginal distribution of DCT coefficients. The data embedding is not done in the Block Wise manner but in the frequency order. First Divide DCT coefficients into four bands, namely, the direct current (DC), low frequency Middle- frequency and high-frequency. Via matrix encoding, low data hiding rate and high embedding efficiency are achieved in high-frequency band, while the hiding rate is increased in the middle-frequency and DC bands, and highest in the low-frequency band. In addition, a coefficient selection strategy is employed to make the hidden

message less detectable. The proposed algorithm is implemented on a set of 10000 images and tested with four steganalytic algorithms. The experimental results show that it outperforms the F5, nsF5 and LSB+ algorithms in terms of detection accuracy for the JPEG images at various levels of q.



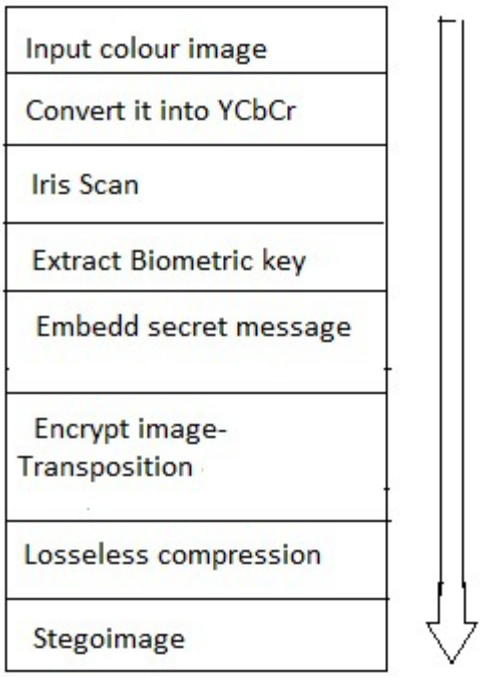
E) Combining Cryptography, Steganography and watermarking

The paper titled "New Proposed practice for secure Image combining Cryptography Steganography and watermarking based on various parameters" by Rupesh Gupta, Dr.Tanu Preet Singh is referenced here. Combining three major security techniques. First convert colour image into YCbCr. Then apply four levels and five levels DWT. Then select Y band to add watermark. Add secret message using LSB algorithm. Then encrypt. Here combined both decryption and encryption algorithm and compare it with the existing algorithm which will show better results for PSNR, MSE and Embedding Capacity after noise attacks.



III. PROPOSED METHOD

Hybrid stegno system is proposed here. It provides more security. It is a combination of image encryption, user authentication, and steganography and image compression. To protect user authenthenticity use of biometric key is one of the important methods. It uses physical characteristics of the human being. These include Fingerprints, palm prints, retina or Iris, facial structures etc. Biometric method is more secure method of authentication because it requires physical presence of human being and it is untraceable. Here unique biometric key is generated from iris scan.



IV. CONCLUSION

Security of communication using internet technology becoming a major issue. Steganography & cryptography are the two major security mechanisms used for secure data communication. Steganography is the art of hiding information. In this survey paper five latest Steganographic methods are explained along with block diagram representation. Also proposed a hybrid stegno system, which is a combination of different security mechanisms.

REFERENCES

[1] Gaurav Bhatnagar and Q. M. Jonathan Wu, "Biometric Inspired Multimedia Encryption Based on Dual Parameter Fractional Fourier Transform", IEEE Transaction on Systems, Man, and Cybernetics: Systems 2014

[2] I-Jen Lai, Wen-Hsiang Tsai, "Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding", Information Forensics and Security, IEEE Transactions on , vol.6, no.3, pp.936,945, Sept. 2011
[3] H. Narasimhan and S. Satheesh, "A randomized iterative improvement algorithm for photomosaic generation", in Proc. NaBIC, Coimbatore, India, Dec. 2009, pp. 777–781
[4] S. Battiato, G. Di Blasi, G. Gallo, G. C. Guarnera, and G. Puglisi, "Artificial mosaic by gradient vector flow," in Proc. Eurographics, Creete, Greece, Apr. 2008, pp. 53–56
[5] Hae-Yeoun Lee, "Generation of Photo-Mosaic Images through Block Matching and Colour Adjustment", International Journal of Computer, Information, Systems and Control Engineering Vol:8 No:3, 2014.
[6] Suk-Ling Li, Kai-Chi Leung, Cheng, L. M. Chi-Kwong Chan, "Data Hiding in Images by Adaptive LSB Substitution Based on the Pixel-Value Differencing", First International Conference on Innovative Computing, Information and Control, vol.3, no., pp.58,61, Aug. 30
[7] Jas R Sheth, 'Snake and ladder Based algorithm for Steganographic Application of specific streamline Bits on Prime Gap Method'
[8] Laura A Granka, Matthew Feusner, Lori Lorigo," Eye Monitoring in online Search", 2008.
[9] I.Qunis, G. Amati, V. Plachouras, B. He, C. Macdonald and C. Lioma, "A High Performance and Scalable Information Retrieval Plateform", In SIGR Workshop on Open Source Information Retrieval, 2006
[10] T. Fagni, R. Perego, F. Silvestri, and S. Orlando., "Boosting the performance of Web Searching Engines: Caching and pre-fetching Query Results by Exploring historical usage Data", ACM Trans. Inf. Syst., 24(1): 51-78, 2006
[11] Prashant Dhake, Sonali Nimbhorkar "Hybrid cryptosystem for maintaining Image security using biometric fingerprints", 2015 international Conference on pervasive computing.