IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

IMAGE STEGANOGRAPHY

Sritama Banerjee
Assistant Professor,Computer Science and Engineering
RV University, Bangalore, India

Abstract : Steganography is the art of hiding image, text, video etc., on another image, text or video. The content owner encrypts the original image using a stream cipher algorithm and uploads cipher text to the server. The data-hider on the server divides the encrypted image into three channels and embeds different amount of additional bits or messages into each one to generate a marked encrypted image. On the recipient side, additional message can be extracted from the marked encrypted image, and the original image can be recovered without any errors. This paper proposes a method of reversible data hiding in encrypted images (RDH-EI) based on progressive recovery. Three parties are involved in the framework, including the content owner, the data-hider, and the recipient. While most of the traditional methods use one criterion to recover the whole image, we propose to do the recovery by a progressive mechanism i.e. Stream Cipher algorithm. Each symbol is encrypted without regard for any other plaintext symbol, each symbol can be encrypted as soon as it is read. Each symbol is separately encoded, an error in the encryption process affects only the character. Rate-distortion of the proposed method outperforms state-of- the-art RDH-EI methods. It is feasible in applications like cloud storage and medical systems. In cloud storage, a content owner can encrypt an image to preserve his/her privacy, and upload the encrypted data onto cloud. On the cloud side, when managing huge amount of encrypted images, an administrator can embed additional messages (e.g., labels, time stamps, category information, etc.) into the cipher text. This embedding not only saves the storage overhead, but also provides a convenient way of searching encrypted images.

IndexTerms **-** Image Steganography, Reversible Data Hiding In Encrypted (RDH-EI), Encryption, Decryption

INTRODUCTION

Idea of reversible data hiding in encrypted images (RDH-EI) originates from reversible data hiding (RDH) in plaintext images. It is suitable for applications like cloud storage and medical systems. In cloud storage, a content owner can encrypt an image to preserve his/her privacy, and upload the encrypted data onto cloud. When managing huge amount of encrypted images, an administrator can embed additional messages (e.g., labels, time stamps, category information, etc.) into the cipher text. This embedding not only saves the storage overhead, but also provides a convenient way of searching encrypted images.

On the recipient side, when a user downloads the encrypted data containing additional messages from the server, he/she can losslessly recover the original images after decryption. Some attempts on RDH-EI have been made. A content owner encrypts the original image using stream ciphering, and a data-hider embedded additional bits into cipher text blocks by flipping three least significant bits (LSB) of half the pixels in each block. On the recipient side, the cipher text image is decrypted and two candidates for each block are generated by flipping again. As the original block is smoother than the interfered embedded bits can be extracted and original image can be losslessly recovered. This method was improved in by exploiting spatial correlation between neighboring blocks to achieve a better embedding rate, which was further improved in using a full embedding strategy to achieve larger embedding rate. Secure RDH-EI can be ensured by public key modulation. RDH-EI can also be realized in encrypted JPEG bit streams by slightly modifying the encrypted data and the data extraction can only be done after image decryption. Separable RDH-EI was proposed to resolve this problem, allowing one to extract hidden data directly from the encrypted image.

NEED OF THE STUDY.

The establishment of large hospitals where hundreds to thousands of patients are treated , it has created a serious problems of biomedical waste management. The seriousness of improper biomedical waste management was brought to the light during summer 1998. In India studies have been carried out at local / regional levels in various hospitals, indicate that roughly about 1-5 kg/bed/day to waste is generated. Among all health care personnel ,ward boys , sweepers, operation theatre & laboratory attendants have come into contact with biomedical waste during the process of segregation , collection, transport, storage & final disposal . The knowledge of medical , paramedical staff & ward boys , sweepers about the biomedical waste management is important to improve the biomedical waste management practices. The biomedical waste requiring special attention includes those that are potentially infectious , sharps ,example needle , scalpels , objects capable of puncturing the skin , also plastic ,pharmaceutical & chemically hazardous substances used in laboratories etc.

3.1Population and Sample

This paper presents the method of recursive information hiding of secret images by random grids, which hides the additional secret information in the shares of the larger secret in a recursive manner. The proposed method increases the information conveyed per bit of shares to nearly 100%, and has the size of each share same as that of the original secret image without any expansion. The smaller size of the shares makes their further processing such as storage and distribution more efficient. In this paper, we have presented a method of recursive information hiding of secret images by random grids. The proposed method generates the shares of size same as the origin a secret image size without any expansion, which is the advantage as compared to the scheme of recursive information hiding by visual cryptography. It also increases the information conveyed to per bit of shares to nearly 100% same efficiency obtained. The proposed method has the application in secure distributed information storage and serves as a stenographic channel to embed hidden information, which may be used for authentication .

3.2 Data and Sources of Data

[2] The images are very largely used in our daily life; the security of their transfer became necessary. In this work a novel image encryption scheme using stream cipher algorithm based on nonlinear combination generator is developed. The main contribution of this work is to enhance the security of encrypted image. The proposed scheme is based on the use the several linear feedback shifts registers whose feedback polynomials are primitive and of degrees are all pairwise coprimes combined by resilient function whose resiliency order, algebraic degree and nonlinearity attain Siegenthaler's and Sarkar, al.'s bounds. This proposed scheme is simple and highly efficient. In order to evaluate performance, the proposed algorithm was measured through a series of tests. These tests included visual test and histogram analysis, key space analysis, correlation coefficient analysis, image entropy, key sensitivity analysis, noise analysis, Berlekamp-Massey attack, correlation attack and algebraic attack. Experimental results demonstrate the proposed system is highly key sensitive, highly resistance to the noises and shows a good resistance against bruteforce, statistical attacks, Berlekamp-Massey attack, correlation attack, algebraic attack and a robust system which makes it a potential candidate for encryption of image. The numerical networks knew a strong growth in the last few years. The circulation of the images on these networks is very largely used in our daily life, and more their use is increasing, more their safety is vital. For example, the images to be transmitted can be collected and copied during their course without losses of quality. The intercepted images can be thereafter the subject of an exchange of information and illegal numerical storage. It is thus necessary to make incomprehensible of the transferred files and to protect them from any undesirable interception. The modern cipher of the data is very often the only effective means to answer these requirements. [3] This paper analyzed the different techniques for embedding and security.Feature selection strategy implemented here gives relevant features to be used for training and thus reduces the training complexity. Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. The output image by hidden data is not visually recognizable.It does not directly obtain the feature importance .[4] Although cryptography and steganography could be used to provide data security, each of them has a problem. Firstly, the Advanced Encryption Standard (AES) algorithm has been modified and used to encrypt the secret message. Secondly, the encrypted message has been hidden using method . Therefore, two levels of security have been provided using the proposed hybrid technique.

3.3 Theoretical framework

Proposed technique provides high embedding capacity and high quality stego images. Encryption using Block cipher algorithm. Nevertheless, nothing can be revealed when camouflage images printed on paper are stacked together, and nor can they be stacked together to reveal the secret image on the screen of a cell phone. Another drawback is that the camouflage transparencies must be stacked and aligned with extreme precision. When the camouflage transparencies are not put together exactly in position, the secret image cannot be revealed. Finally, when the scheme is applied on the computer, the stacking action is simulated by using the OR operator. That is, if there exists any pixel whose color is black, the final color of the stacked pixel will also be black. In this paper, instead of the OR operator, we decide to use the MODULE operator. Moreover, the camouflage images are stored in a low computation device (such as cell phone or PDA). When a certain number of persons want to work together and recover the secret image, they just show their cell phones and transmit the camouflage images to each other by using infrared rays. By using the MODULE operator, our method can give better image quality than Yang's method, which our experimental results will demonstrate later.

RESEARCH METHODOLOGY

There are many methods have been used to provide data security whether by using encryption, Steganography or combination between them. We are making use of RDH-EI techniques and Stream Cipher algorithm.

3.1 Data Embedding System with Content Owner

KSE-100 index is an index of 100 companies STEGANOGRAPHY aims to hide secret messages into innocuous digital media without drawing suspicion. It faces challenges posed by modern steganalysis. This intends to detect the traces of data hiding. We select steganography image and Then Read hidden Data from the Source. The Embedding System has activated after Start the Image and data read from source. In this module we have Embed the data's inside of image pixel. The data will be hidden, then the embedded image has stored in server.

3.2 Image Degrade by data hider

While complete the embedding process, next start the image Degrade Process. Here, we retrieve the embedded image from server then apply decomposing function to the selective image.

3.3 Image segmentation

An image is decomposed into several sub-lattices, where pixels within the same sub-lattice are separated by a distance larger than the support width of the potential function and apply the CMD function Cost assignment and data embedding are performed in each sub-lattice sequentially.

3.4. Additive Distortion Function

The distortion function quantifies the effect of modifying an input cover object to the corresponding output stegno object. A distortion function is considered *additive* when it is expressed as a sum of embedding costs for individual pixels which element-wisely evaluate the effect of respective embedding modification.

3.5. Decode and Process Cost analysis by recipient

An end of the steganography Process, we decode the message using steganography image. After embedding for a sub-lattice, the costs of pixels in the remaining sub-lattices are updated. And find the performance analysis in cost and secure level.

.

Step: 1 Divide I and J into N non-overlapping blocks respectively.

Step: 2 Pair the blocks of I and J, such that $(B_1,T_1),(B_2,T_2),,,,,,,,$
(B_n,T_n), where B_i is an original block of I,T_j is the corresponding target block of J.

Step 3: Transform B_i toward T_i and generate a T_i' similar to T_i.

Step 4: Replace each T_i with T_i' in the target image J to get the transformed image J'.

Step 5: Embed accessorial information into J' with an RDH method to generate the encrypted image E(I).

3.4Statistical tools and econometric models

This section elaborates the proper statistical/econometric/financial models which are being used to forward the study from data towards inferences.

3.4.1 Descriptive Statistics

In general, HS-based RDH is implemented by modifying host image's histogram of a certain dimension. It has two major advantages. On the other hand, the location map used to record underflow/overflow locations is usually small in size especially for low ER case. Reversible Data Hiding methods are increasing in number as per the requirements to attain an Optimal state, In this survey it is found that according to some predefined rules the data is embedded in the Original Image or host image by choosing an optimal value. This method is an iterative method based on the size of Host image and data the optimal value is calculated using value modification under a payload distortion criterion method and moreover practical Reversible Data Hiding is obtained. In this procedure host image is divided into subset of small size images and the differences between the sub images are calculated wherever the value of difference is less the data is embedded and recovery is done in the reverse process. Histogram Shifting is recommended as one of the most important technique in the area of Reversible Data Hiding where the best results can be obtained. In this survey the author describes the overview of recent techniques involving Data Hiding using Histogram Shifting where the concentration is done on the improvement of image quality and also to increase the payload capacity in the host image. Moreover the PSNR is also has been considered to improve over the existing techniques.

3.4.2 Clustering

The system includes three parties: the content owner, the data-hider, and the recipient. The content owner encrypts the original image and uploads the encrypted image onto a remote server. The data-hider divides the encrypted image into three sets and embeds message into each set to generate a marked encrypted image. The recipient extracts message using an extraction key. Approximate image with good quality can be obtained by decryption if the receiver has decryption key. When both keys are available, the original image can be losslessly recovered by progressive recovery. It is not necessary to assign costs simultaneously. Increasing a pixel value and decreasing a pixel value do not necessarily have the same cost. It will also be helpful in the non-additive case. Clustering embedding modifications in the neighborhood of unpredictable pixels should be beneficial to enhance the security of non-additive steganography as well. It achieves better statistical undetectability against the state-of-the-art steganalyzers.

3.4.3 Comparison of the Models

The existing system present an improved histogram-based reversible data hiding scheme based on prediction and sorting. A rhombus prediction is employed to explore the prediction for histogram-based embedding. Sorting the prediction has a good influence on increasing the embedding capacity. Characteristics of the pixel difference are used to achieve large hiding capacity while keeping low distortion. In addition, we exploit a two-stage embedding strategy to solve the problem about communicating peak points. We also present a histogram shifting technique to prevent overflow and underflow. The system we present an efficient extension of the histogram modification technique by considering the difference between adjacent pixels instead of simple pixel value. The distribution of pixel difference has a prominent maximum since image neighbor pixels are strongly correlated. Hence, there are a lot of candidates for embedding data. This observation leads us toward designs in which

the embedding is done in pixel differences. Meantime, we find that sorting the prediction has much shaper histogram which would lead to significant performance improvement for histogram-based embedding. As a result, a rhombus prediction is employed in our scheme for increasing the embedding capacity. We also use a histogram shifting technique to prevent overflow and underflow.

Furthermore, we use a two-stage embedding strategy to solve the problem about communicating peak points. In the following, we now outline the principle of the proposed reversible data hiding algorithm. The distribution of pixel difference has a prominent maximum since neighbor pixels are strongly correlated. Further, we use prediction and sorting to enhance the correlation of neighbor pixels in order to improve the embedding capacity. In addition, one common problem of virtually histogram-based techniques is that they have to transmit pairs of peak and minimum points to recipients. To solve this problem, we introduce the two-state strategy to embed the overhead information. We also use a histogram shifting technique to prevent overflow and underflow. As a result, the evaluation results show that the proposed scheme have significantly improved our previous work and derived better performance. The proposed scheme provides high capacities at small and invertible distortion. On one hand, the maximum modification to pixel values can be controlled and thus the embedding distortion can be well limited. This method can provide an embedding rate (ER) up to 0.5 bits per pixel (BPP) and it significantly out performs previous compression-based works. In particular, Tian employed a location map to record all expandable locations, and afterwards, the technique of location map is widely adopted by most RDH algorithms. Later on, work has been improved in many aspects. In, proposed a method by constructing a payload dependent location map. Another improvement of method is the work introducing a new capacity parameters determination strategy. Besides aforementioned works many HS-based RDH algorithms have also been proposed so far.

RESULTS AND DISCUSSION

4.1 Results of the proposed system

A new RDH-EI protocol for three parties is proposed. Main improvement is extending the traditional recovery to the progressive based recovery. The progressive recovery based RDH-EI provides a better prediction way for estimating the LSB-layers of the original image using three rounds, which outperforms state-of-the-art RDH-EI methods. Since RDH-EI is equivalent to a rate-distortion problem, capability of the method should be evaluated by both the distortion and the embedding rate.

4.2 Future Scope

In this work it explores only a small part of the science of steganography. As a new displine, the reisagreat deal more research and development to do, the following section describe areas for research which were offshoots of, or tangential to, our main objectives. 1. Detecting Steganography in Image Files Can steganography be detected in images files? This is difficult question. It may be possible to detect a simple steganographic technique by simple analyzing the low order bits of the image bytes. If the Steganographic algorithm is more complex, however, and spreads the embedded data over the image is random way or encrypts the data before embedding, it may be nearly impossible to detect. 2. How wide spread is the Use of Steganography? If a technique or set of techniques could be devised to detect steganography, it would be interesting to conduct a survey of images available on the internet to determine if steganography is used, by whom and for what purposes. Steganographic applications are available on the Internet, but it is not known if they are being used.

3. Steganography on the World Wide Web The world wide web(www) makes extensive use of inline images. There are literally millions of images on various web pages worldwide. It may be possible to develop an application to serveasa web browser to retrieve data embedded in web page images. This “stego-web” could operate on top of the existing WWW and be a means of covertly disseminating information.

4. Steganography in printed media. If the data is embedded in an image, the image printed, then scanned and stored in a file can the embedded data be recovered? This would require a special form of a steganography to which could allow for in accuracies in the printing and scanning equipment.

5. Anti-steganography measures As was seen in this thesis, JPEG garbles any unencoded steganographically embedded data. Also, palettization (mapping a large number of colors in an image to a smaller subset of colors) of an image will it unsuitable for steganography. It is likely, as with JPEG, that some means may be employed to prevent loss of steganographically embedded data when its wrapper file is processed. The question remains open as to what is the most effective anti Steganographic tool so rest of tools.

REFERENCES

[1] Chin-Chen Chang ,Pei-Yu Lin, Zhi-Hui Wang, Ming-Chu Li ,”A Sudoku-based Secret Image Sharing Scheme with Reversibility” in journal of communication, vol. 5, No. 3, 1, January 2010.

[2] Belmeguenai Aissa, Derouiche Nadib, Redjimi Mohamedc, “Im-age Encyption Using Stream Cipher Based on Nonlinear Combination Generator with Enchanced Security”, vol. 1, No. 1, 2013.

[3] “Secure Data Hiding Technique Using Video Steganograpy and Watermaking “, 2014.

[4] Marwa E.Saleh, Abdelmgeid A.Aly, Fatma A. Omara,”Data Security Using Cryptography and Steganography Techniques”, International Journal of Advanced Computer Science and Applications, in vol. 6, No. 6, 2016.