International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 03 | Mar -2020 ISSN: 2582-3930

RRW - A ROBUST AND REVERSIBLE WATERMARKING TECHNIQUE FOR RELATIONAL DATA

[1]M.Keerthika ,[2]M.Sabari Ramachandran, [3]N.Balasubramanian
[1]Student of Computer Application
[1]Master of Computer Application
[1]Mohamed Sathak Engineering College, Ramanathapuram, Tamil Nadu , India

Abstract: The image processing techniques have share relational data and providing a key value means for secret data. Image process rights are imposed using steganography.The certain modification as a result viewed by the secret image. The main future is database and also smallest image in the watermatked Content. In this paper image processing approach to numerical data based on the Steganogeaphy technique has been proposed. Consequently image process to ensure encoding decoding for the original data recovery. Steganography and watermarking techniques are two methods used to hides information within the cover file. Several different file formats are used in both techniques, such as text, image, audio and video. This paper concluded the latest issues and challenges faced in two methods which that using to hide information. As well as to find a possibility other ways to hide information that is mentioned earlier with the increase in research on information hiding .

Key words: Water marking, Steganography, Secret image, Key values.

1. Introduction

Now a day's digital world can be accessed and exchanging through the internet. The recipient awaited him and saved he message was revealed it was history his head again. It was history and exchanging to the computer through the first use of steganography. The digital data is publically available watermarking mainly used techniques. It can't be easily changed by unauthenticated user for,

(1) Data preprocessing
(2) Encoding
(3) Decoding
(4) Images.

So securing data is difficult task and provide Variety of solutions and protection of different Steganography is used main method.Watermarking data is stored different digital in reversible water marking and its formats. Which image, audio, video, texts a processing for encoding. Insert to the relational data. Data mining is a huge and large valid key and viewing buy a secret amount of data's stored in the database. The invalid key proceed do not watermarking is used to the steganography open the secret image. Steganography is an advanced technique in watermarking.

2. Related work

Steganography simply takes one piece of the earliest reference to reversible data information and hides it within another. Embedding we could fine. Computer files (images, sounds recording even disks) mainly phases for watermarking contain unused for insignificant areas of data. Such as original image embedding steganography takes advantage of these are as procedure watermarked Replacing them with information. technique. Be exchanged without anyone knowing what really for image format. Reversible water lies inside of them. An image o the space shuttle marking has found transmit in sender to receiver in secret message. A huge of the private letter. The friend experimentation watermark rumor has it that terrorist's used steganography application such as military message one to another. Messenger phase watermarked in the secret image of the information.

3. System analysis

The Information detail blue prints of Steganography can be used for watermarking installments. This is the nature of by including hide information about the steganography. Since of hiding license of data authentication (hidden information from plain sight is proves the authenticity of data), tracking (hidden very important). Because important information identifies the true owner / author of message and if you do not want other and enhancement of data (including new message. Hide your information third party information). The first one is that the files person. Containing digitized images or sound can be altered to a certain extend without losing. Internet nowadays is the most popular, effective and faster media for data transmission. Thus, the data senders and data receivers via the internet

need a highly secure method of data protection in order to avoid a variety of problems such as hacking and leave dropping. Cryptography and steganography are two fields for data security and protection. Cryptography converts the secret message into some other forms, such that it is not understandable to anyone; however, this technique has a limitation that the encrypted message is visible to everyone. In this way over the internet, intruders may try to apply head and tail method to get the secret message. Steganography differs from cryptography the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret Steganography is the process of hiding a secret message within a large medium such as, text, audio, video and image. This is implemented in such a way that information is concealed to everyone except for the intended sender and receiver. Hiding information inside image with a secret message is popular technique nowadays and can easily be spread over the World Wide Web Practically, 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 redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image is the most common cover media in steganography in which it is used to hide information. One type of images is the digital color image that is defined as a collection of pixels which usually stored in 24-bit files and uses RGB color model with each primary color represented as 8-bit each. There are some proposed methods in literature that used RGB color channel for steganography such as hide a large amount of data (image, audio, text) file into color image which is proposed in. The authors used adaptive image filtering and adaptive image segmentation with bits replacement on the appropriate pixels. These pixels were selected randomly rather than Sequentially by using new concept defined by main cases with their sub cases for each byte in one pixel. Their results show that the algorithm can embed efficiently a large amount of data that has been reached to 75% of the image size with high quality of the output. Another proposed method in used to perform variable length bits embedding in RGB colored channel of color image. Two types of channels were used. One is called indicator channel which indicates how many data bits are hidden in the data channel, the other is data channel which is used for embedding data bits. The secret message is converted using two kinds of plain text RSA plaintext and IDEA plain text. The authors in proposed a technique which is a combination of both steganography and cryptography for better security of secret of information. In RGB image each pixel (24-bits) has R channels 8-bits; G channel 8-bits and B channel 8-bits. One of the channel is used as indicator channel and remaining two channel are used for hiding secret message. The indicator channel is chosen based on the sum of color values and embedding is, as 4 bit in each selected channel satisfying some conditions. Another stego method in is proposed to hide secret data in different position of RGB image, which require element like cover image, secret message, two secret keys (key1 is a circular ID array with only 0 or 1 value is allowed and key2 is a ID array with 8-digits). LSB of red value of pixel is XOR with key1 bits then result is used for taking decision that secret information bit will be placed in blue or green color. Key2 is used to describe the position where secret information placed. This process is carried out repeatedly until all secret information bits are placed. It is concluded that this approach was very beneficial and secure against attacks and very effective way of hiding information without any visible distortion in the carrier image. In a genetic algorithm (GA) based steganography technique in frequency domain using discrete cosine transform has been proposed. A 2×2 sub mask of the source image was taken in row major order and Discrete Cosine Transformation was applied on it to generate four frequency components. Two bits of the authenticating image were embedded into each transformed co-efficient except the first one. In each co-efficient second and third positions from LSB were chosen for embedding in the transform domain. Stego sub intermediate image was generated through reverse transform. Sub mask from this intermediate image was taken as initial population. New generation followed by crossover was applied on initial population to enhance a layer of security. Rightmost three bits of each byte were taken; a consecutive bitwise XOR was applied on it in three steps which generated a triangular form. The first bit of each intermediate step was taken as the -output and crossover was performed on two consecutive pixels where two LSB bits of two consecutive bytes were swapped. The dimension of the hidden image is embedded followed by the content. Reverse process was followed during decoding. Finally, in a new technique was proposed based on optimization in steganography. The technique proposed was a combination of GA implemented on image steganography. This may however increase the time complexity of the algorithm but it will result in increasing robustness.

4. Steganography Technique

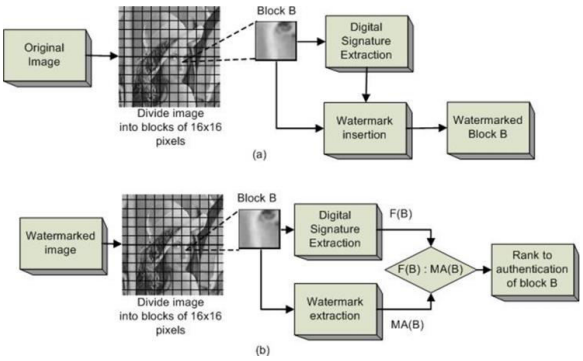

Figure 1: Steganography technique

In their functionality the other principle deals steganography hides the traces of with the human inability to distinguish image communication while cryptography color or sound quality Color won't result in uses encryption to make the process of data to be concealed to this secret information message this is the nature of including hide information about the steganography. Since of hiding (license of data) authentication (hidden information information from plain sight is proves the authenticity of data), Tracking (hidden) very important because important information identifies the true owner / author of message and if you do not other (data) and enhancement of data including new message. Steganography system involves inserting an identifier be it a message, the secret message or a marker into a medium that will not be affected. The most important object inserted into a cover medium is the secret message or serial numbers or secret code. When this information is embedded, the steganography technique ensures that it will not be detected and assess by any unauthorized person. The cover message that hosts the embedded is called a stego object . The cover message is required to be disposed of after the receivers got it in order to prevent an accidental reuse. Capacity or (Data rate) refers to the amount of ratio of the data able to be embedded into a cover file and the amount of the cover file that will host the embedded file without degrading the cover file condition to the message .The ratio between the quantity of the host file and the embedded file has to be made as a steganography rule of used. Steganography techniques are simple to work under large embedded data rate or a huge resistance to any alteration same not under all conditions. The relation is made in such a way the higher the increase in one the lower the other one becomes. Bit plane tool methods that apply LSB insertion and noise handling. LSB steganography technique achieves a huge success as the basis steganography technique used for both audio and image. It allows huge amount of information to be hidden in the cover message with little compression through the use of LSB technique. These requirements were explained before being mutually competitive and cannot be clearly optimized at the same time. This observation is schematically depicted. Absolute improductivity and high robustness cannot be used simultaneously. On the other hand, if robustness is an issue the message that can be reliably hidden cannot be too long.

Algorithm 1: Steganography procedure based GA at the sender stage

Input: Load the cover image of size ; Load the secret message/image ( ) of size . Output: The of the secret message or image hidden in with the best blocks permutation. Begin ,

Step 1: Calculate [N1,M1]=Size(I) and [N1,M2]=Size(S).

Step 2: Convert secret massage / image into vector of length(S) .

Step 3: Determine the number of cover blocks that are needed to hide as,

No_blk_sec=L/blk

Step 4: Determine the new size of the cover image which is n x M_1 as,

n = floor(N^1/n^0-b/k-sec)

Step 5: Initialize the population of size by rearranging the order of the blocks of the secret message using uniform random number generator. Each gene in a chromosome contains index of image pixel. Step 6: Use genetic algorithm to find the optimal distribution of secret message blocks in cover as $f_{i,j}$=seg_i-txt_j described in For each chromosome , the best position of each block (gene) is determined by converting each block of cover image to vector then compare all pixels of this vector with one pixel of blocks of secret message then choose minimum different of Eq.

Step 7: Hide the secret message/image within cover to create .

Step 8: Cipher the fit chromosome obtained from GA by adapting the BITXOR function to increase security. Step 8: Calculate PSNR for that have minimum MSE Return The of the secret message or image hidden in with the best blocks permutation.

End

5. Conclusion

Hide your information the first one is that the files person containing digitized. Images or sound can be altered to a certain extend without losing their functionality. The other principle deals with the human inability to distinguish image color or sound quality. Color won't result in any perceivable change of that color. The process of data to be concealed is compressed and hidden within another file. The first step is to found a file which will be used to the hide message (also called a carrier or a container). The next step is to Embedded the message one wants to the hide within carrier using a step technique.1.Replace least bit of each byte in the [carrier] with a single bit for the hiddenMessage.2. Select certain bytes in wich to embedded message using random number Generator resampling the bytes to pixel mapping. Applications in a broadcast monitoring system. Identifying data is added to the audio/video. Two Kinds of monitoring active and passive. Passive monitoring recognize the content being broadcast. Compares received signals against database of known Steganography can be used for watermarking installments. This is the nature of (by including hide information about the steganography. Since of hiding license of data authentication hidden information from plain sight is proves the authenticity of data, tracking because important. Information identifies the true owner / author of message and if you do not want other data and enhancement of data including new message. Hide your information .The first one is that the files person containing digitized. Images or sound can be altered to a certain extend without losing their functionality. The other principle deals with the human inability to distinguish image color or sound

quality. Color won't result in any perceivable change of that color. The process of data to be concealed is compressed and hidden within another file. The first step is to found a file which will be used to the hide the message (also called a carrier or a container). The next step is to Embedded the message one wants to the hide within carrier using a step technique.Replace least bit of each byte in the [carrier] with a single bit for the hidden message. Select certain bytes in wich to embedded message using random number generator resampling the bytes to pixel mapping. Applications in a broadcast monitoring system. Identifying data is added to the audio/video. Two kinds of monitoring active and passive. Passive monitoring recognize the content being broadcast. Compares received signals against database of known Content very expensive as large frames need to be compared useful for monitoring of competition. Active monitoring related information that is broadcast along with the content. Relatively easier to implement identification information is easily to interrupter. Co-operation of broadcasting Mechanism. Stegano means covered or secret graph means writing it's called for covered secret writing. The information that is covered are secret and how we write that information that is graphy. Advanced technique for information hiding. Where different members share their data in various proportions. We also plan to extend RRW for non-numeric data stores.

References:

[1] A.Z. Al- Othman, A. A. Manaf and A. M. Zeki, "A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation", IJCSI International Journal of Computer Science Issues, Vol. 9, no. 1, 201

[2] S. B. Kumar, D. Bhattacharyya, P. Das, D. Ganguly and S. Mukherjee, "A tutorial review on Steganography", International Conference on Contemporary Computing (IC3-2008), Noida, India, 2008, pp. 105-114

[3] P. Dutta, D. Bhattacharyya, and T. Kim, "Data Hiding in Audio Signal: A Review", International Journal of Database Theory and Application, Vol. 2, No. 2, June 2009

[4] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, and S. Pogreb, "Techniques for data hiding", IBM Systems Journal, Vol. 39, No. 3-4, pp. 547 – 568, 2000.

[5] Atoum, M. S. (2015). A Comparative Study of Combination with Different LSB Techniques in MP3 Steganography. In Information Science and Applications (pp. 551-560). Springer Berlin Heidelberg.

[6] Atoum, M. S., Ibrahim, S., Sulong, G., and Zamani, M. (2013). A New Method for Audio Steganography Using Message Integrity, Journal of Convergence Information Technology, 8(September), 35–44.

[7] Atoum, M. S., Ibrahim, S., Sulong, G., and Ahmed, A. (2013).New Secure Scheme in Audio Steganography (SSAS). Australian Journal of Basic and Applied Sciences, 7(6), 250–256.

[8] Atoum, M. S., Ibrahim, S., Sulong,G. and Ahmed, A. (2012). MP3 Steganography: Review. Journal of Computer Science issues, 9(6).

[9] Atoum, M. S., Suleiman, M., Rababaa, A., Ibrahim, S., and Ahmed, A. (2011). A steganography Method Based on Hiding secretes data in MPEG / Audio Layer III. International Journal of Computer Science and Network Security, 11(5), 184-188.

[10] Atoum, M. S., Rababah, A. and Al-attili, A. Audio Files. International Journal of Computer Science and Network Security, 11Computer Science Applications and Technologies (ACSAT) ,Sarawak, Malaysia.

[11] Atoum, M. S. (2015, August). New MP3 Steganography Data Set. In IT Computer Science Application and Technologies(ACSAT), Sarawak, Malasiya I.

[12] Y.-C. Liu, Y.-T. Ma, H.-S. Zhang, D.-Y. Li, and G.-S. Chen, "A method for trust management in cloud computing: Data coloring by cloud watermarking," International Journal of Automation and Computing, vol. 8, no. 3, pp. 280–285, 2011.

[13] "Walmart to start sharing its sales data," http://www.nypost.com/p/news/business/walmart-opensup, last updated: 09:55 AM on February 4, 2012, last accessed: July, 20 2013.