IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

High Secure Digital Image Steganography for the Secrete Communication

K. Suganya[1], P. Sunilkumar[2]

M.Tech, Department of CSE, Periyar Maniammai University, Thanjavur, India[1]

Assistant Professor, Department of CSE, Periyar Maniammai University, Thanjavur, India[2]

Abstract: Highest state-of-the-art image steganographic approach focuses on concealing multiple secret images in a single 24-bit cover image using LSB substitution based image steganography. Steganography, the secret image is embedded in the cover image and transmitted in such a way that the existence of information is undetectable. Proposed paper a message in a cover without leaving a remarkable track on the original message. The digital images, sound files and other computer files can be used as carrier to embed the information using BSC (byte shifting calculation). In this paper, a modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. Combining both domains gives a higher level of security in which even if the use of covert channel is revealed, the true information will not be Minimized distortion using R_{LBC} (rotated Local Balance changes) algorithm. Each secret image is encrypted before hiding in the cover image. Results reveal that the proposed method successfully secures the high capacity data keeping the visual quality of transmitted image satisfactory.

Keywords: steganographic, BSC (byte shifting calculation), R_{LBC}(rotated Local Balance changes), encrypted.

1. INTRODUCTION

Steganography refers to the art and science of hiding secret information in some other media [1]. The information to be hided is called the secret message and the medium in which the information is hided is called the cover document. The cover document containing hidden message is called stego-document [4].BSC algorithms employed for hiding the message in the cover medium at the sender end and extracting the hidden message from the stego document at the receiver end is called stego system. Minimizing distortion using R_{LBC} (rotated Local Balance changes) algorithm [5]**.** In R_{LBC} algorithm Matrix hiding such as those suggested in, can be employed to reduce the hiding impact on the created misinterpretation appraisal when the payload is given. In, a workable optimum code, namely syndrome-trellis code (syndrome-trellis code), is advanced to embed near the payload-misinterpretation bound. The syndrome-trellis code uses the convolution code with an algorithm-based encoder to reduce the additive misinterpretation function [7].The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties. Figure 1 shows a block diagram of the steganography process.

In the context of steganography the cover is the object that will hide the secret data, which may also be encrypted using a stego key. The resultant file is the stego object (which will, of course be the same type of file as the cover object). The cover objects (and, thus, the stego objects) are typically images or audio files [2]. Like many security tools, steganography can be used for a variety of reasons, some are useful and some are harmful. Steganography can be used to tag notes to online images (like post-it notes attached to paper files).[1] Finally, steganography can be used to maintain the confidentiality of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing.

Generally, there are five types of Cover objects. They are Network protocols such as TCP, IP and UDP, audio that is using digital audio formats such as wav, midi, avi, mpeg, mpi etc, video, and text from any language and images files such as bmp, gif and jpg, jpeg where they can be both color and gray-scale[6]. One of the of issues that were discussed in literature Steganography research is the coefficient selection criteria in which the transformed coefficients of the cover object will be chosen by using certain threshold for effective coefficients. Mean Squared Error (MSE) order of magnitude better than what is achieved by more traditional methods.

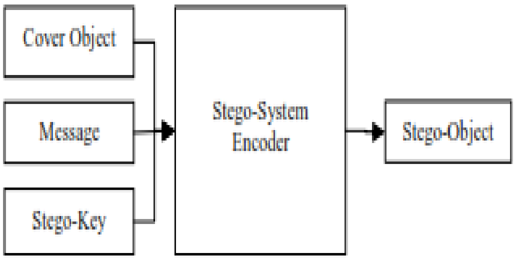

Diagram of a typical Steganography System.

2. LITERATURE REVIEW

2.1 Data hiding in binary text documents

In the past decade, a number of data-hiding schemes have been proposed in literature, however, the majority of them deals only with digital image, audio or video documents. With the proliferation of digital media such as digital

DOI 10.17148/IJARCCE.2016.53209

images, digital audio and digital video, robust digital watermarking and data hiding techniques are needed for copyright protection, copy control, annotation, and authentication. While many techniques have been exiting for digital color and grayscale images, not all of them can be directly applied to binary text images. The difficulty lies in the fact that changing pixel values in a binary document could introduce irregularities that are very visually noticeable.

They propose a new method for data hiding in binary text documents by embedding data in the 8-connected boundary of a character. They have identified a fixed set of pairs of five-pixel long boundary patterns for embedding data. One of the patterns in a pair requires deletion of the center foreground pixel, whereas the other requires the addition of a foreground pixel. A unique property of the exiting method is that the two patterns in each pair are dual of each other changing the pixel value of one pattern at the center position would result in the other. These techniques cannot be directly applied to binary images where the pixels have either 0 or 1 value. Arbitrarily changing pixels on a binary image causes very noticeable artifacts. A different class of embedding techniques must therefore be developed for binary images. This has important applications in a wide variety of document images that are represented as binary foreground and background .e.g. text documents.

2.2 Textural features for steganalysis

Digital media are getting more and more popular. Not only multi-level images, video and audio are in digital form, but binary document images are also digitized in many applications including legal documents, digital books, maps, and architectural and electronic drawings. On the other hand, the data hidden in the image texture area has been known difficult to detect for years, and the modern steganographic schemes tend to embed data into complicated texture area where the statistical modeling becomes difficult. Based on these observations, they propose to learn and utilize the textural features from the rich literature in the field of texture classification for further development of the modern steganalysis. As a demonstration, a group of textural features, including the local binary patterns, Markov neighborhoods and cliques, and Laws' masks, have been selected to form a new set of 22,153 features, which are used with the FLD-based ensemble classifier to steg analyze the BOSS base. An average detection accuracy of 83.92% has been achieved. It is expected that this new approach can enhance our capability in steganalysis.

Steganography and steganalysis is a pair of modern technologies that have been moving ahead swiftly in the last decade. The conflicting between these two sides is a driving force for the rapid development. That is, each side learns from its counterpart. From the modern steganalysis point of view, the machine learning framework, consisting of statistical features and classifier, has been first utilized. In the first four statistical moments of wavelet coefficients and their prediction errors of nine high frequency sub bands from three-level decomposition are used to form a 72dimensional(72-D) feature vector with the modern classifier SVM for steganalysis. F5 and model-based steganographic schemes, a group of 23 features, including both the first and second order statistics, have been used together with a calibrate technique.

2.3 secure data hiding in binary document images for authentication

Steganography is the art of hiding the data into some media like text, audio, video or some another media secretly. In this paper, they present a data hiding algorithm for binary document images. This algorithm is based on the Distance- Reciprocal Distortion Measure [1] that is used to evaluate the amount of distortion caused by flipping a particular pixel in binary document images. The pixels that will cause less distortion after flipping are preferred candidates for flipping. They do the embedding by enforcing the odd-even features of non-uniform blocks and employ a 2-D shifting to provide security for tamper proofing and authentication. Experiments show that the watermark-embedded document image has good quality and tampering of content can be detected successfully.

A secure data hiding algorithm for binary document images is exiting in this paper. This algorithm is based on the Distance-Reciprocal Distorting Measure that provides an efficient way to select the pixels to flip in embedding. The distortion due to flipping is calculated online and able to take the effect of a large area of neighbor pixels into accounts. Data is embedded by enforcing the odd-even features of non-uniform blocks and the 2-D shifting is employed to provide security against tampering. Experiments show that the marked image has good quality and tampering can be detected in the extraction.

3. PROPOSED SYSTEM DESIGN FOR ENCRYPTING AND DECRYPTING IMAGE VISUALIZATION

3.1 Colour image using LSB substitution based BSC (byte shifting calculation) algorithm

Proposed paper, a modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. The image truthfulness and the authentication is the main aim of this paper. Each secret image is encrypted before hiding in the cover image.

Results reveal that the proposed method successfully secures the high capacity data keeping the visual quality of transmitted image satisfactory. We aim to resolve the tradeoff between high quality and low cost

Step 1: image statistics-aware test.

Input: Cover image
Output: Cover image
Action: number of byte calculation

Calculate number of bytes in data file that is supposed holding a text of the serial key of any software that is sending. Store the result in an Integer variable size of data.

Step 2: Hiding Procedure

Input: Pre-processed cover image

DOI 10.17148/IJARCCE.2016.53209

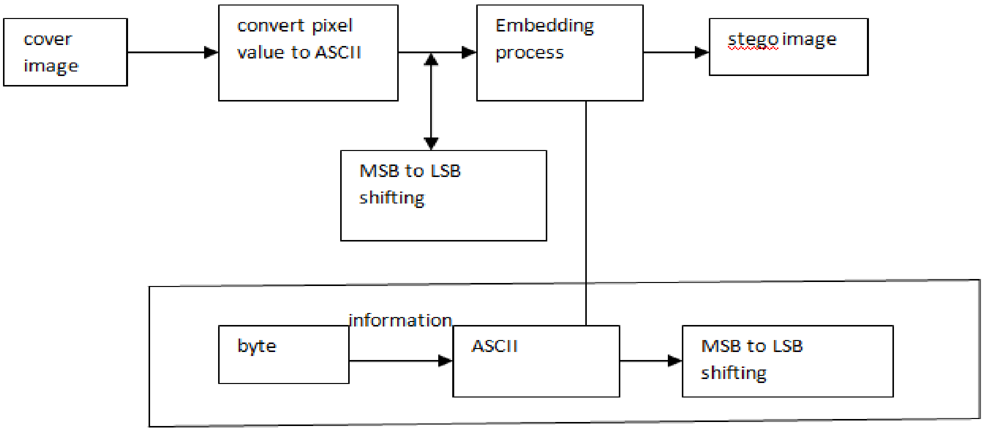

Figure2. Data Embedding Process

Read character from data file and convert the ASCII value of the character into equivalent binary value into a 8 bit integer array

Step 4: Repeat Step 1 to Step 4 until a terminating character is found

Step 5: From the Cover Image file Read the RGB color of each pixel. Read the character 1 by 1 from data file and convert the ASCII value of the character into equivalent binary value into a 8 bit array suppose A in such a way so that MSB to LSB it will be stored like A[7] to A[0].

Step 6: Read the last bit of each pixel i.e. from RGB (8+8+8) bits, read the blue color's 8 bits (i.e. the last 8 bits of the pixel's colour).

Step 7: Repeat this Step 5 to Step 8 for 8 x size of data times. This number of pixels actually needs to Read to hide all bits of data file. If (c0 > c1) and (i0 > i1) or (c1 > c0) and (i1 > i0) the set integer variable flag to 0 Otherwise set flag to 1. Now write the value of flag i.e. either 0 or 1 just at the left position of the last bit of the first pixel's information of the Stego Image file that is started to use to store the data.

Step 8: open a Cover Image file in read mode. Open a new Stego Image file in write mode. Read the header information from Cover Image File. Write this header information to Stego Image File.

Step 9: From the Cover Image file Read the RGB colour of each pixel. Read the bit stream of data file one by one.

Step 11: repeat the Step from 13 to 16

Step 12: extraction Procedure

Input: Pre-processed cover image

Open the Stego image File in read mode Read the bit just before the last bit of first pixel in Stego Image File. Based on its Value set integer variable check flag 0 or 1. Read each pixel of the Stego Image file. If check flag is 0 then read the last bit of each pixel that is the LSB of color blue and put it directly in an Array otherwise take the invert value of the last bit & Put it on Array Read the each of 8 Pixel in this way & then content of the array converts into decimal Value that is actually ASCII value of hidden character.

Step 13: If terminating character's ASCII found print nothing otherwise print the corresponding character of the calculated ASCII value. Repeat Step 3 to Step 6 until

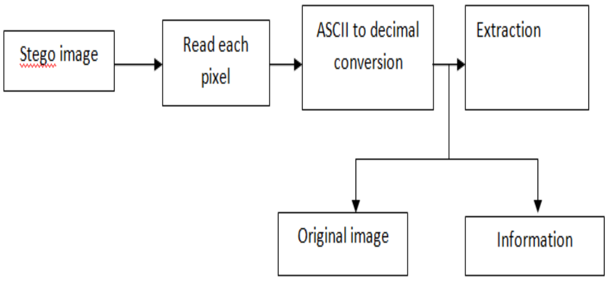

Figure3. Data Extraction Process

decimal value of terminating character's ASCII is found. This is the Pixel Information after Encoding. Here data is being inverted and embedded at the last bit of the blue color of each pixel of Cover Image so that the minimum modification is needed on required pixel information. As flag is set to 1, this flag value would be stored in 1st pixel's bit which is just before the last bit of color blue of Cover Image. Extraction would be done based this value.

3.2 Spinning Misinterpretation calculation

Let the pattern Ti, j denote a local neighbourhood of a monochrome balance which is cantered at the location (i, j) and covered by a 3 × 3 size grid.

Ti, j = {Ic, I0, I1, • • • , I7}

Herein, the white and black pixels are assined with "0" and "1", respectively.

$$LTP^{c}_{i,j} = \min_{b=0,1,2,3} \sum_{k=0}^{7} (I_c \oplus I\,(k+2b) \bmod 8) \text{ x } 2^{k}$$

The final value corresponding to Ti, j is assigned with

$LTP^{crmi}_{i,j} = \min \{LTP^{c}_{i,j}, LTP^{cc}_{i,j}\}$

A hiding operation that can better preserve an image model is usually more secure [8], Further, message hidden in the image balance area has been known difficult to be determining [7], Inspired by these, the advanced spinning misinterpretation function is formed as the detectable hiding changes in the complement, turn, and following-invariant local balance distribution

$$\Delta_{i,j} = \sum_{t=0}^{255} \quad H_t^{x} - H_t\Big|^{Yi,j} \qquad \Big|$$

where HX and H Yi, j t are the histogram coefficients

DOI 10.17148/IJARCCE.2016.53209

$$Ht = \sum_{i=1}^{l_w-2l_h-2} \sum_{j=1} \delta(LTP^{crmi}_{i,j} = t)$$

Finally, the spinning misinterpretation associated with pixel ii, j is assigned with the weighted sum of complement, turn, and following-invariant local balance changes, formed as

$$Di,j = \sum_{t=0}^{255} w_t \; H_t^x - H_t \Big|^{\gamma i,j} \quad + \beta \quad \Big|$$

Where the α and β can be tuned to control the sensitivity of the misinterpretation score to the borderline structure. They are experimentally set as α = 1/2 and β = 1/2, which can reach the best image aspect. Further, we define the misinterpretation score map **D** as the matrix that consists of Di, j as its (i, j)-th element. A steganographic scheme should only change the pixels with the lowest misinterpretation scores.

3.4 Minimized distortion using R_{LBC} (rotated Local Balance changes) algorithm

Matrix hiding such as those suggested in [6]. can be employed to reduce the hiding impact on the created misinterpretation appraisal when the payload is given. In [8], a workable optimum code, namely syndrome-trellis code (syndrome-trellis code), is advanced to embed near the payload-misinterpretation bound. The syndrome-trellis code uses the convolution code with an algorithm-based encoder to reduce the additive misinterpretation function. Examples of such approaches as [8]–[1] have also been reported to obtain good performances. Motivated by this, we employ the syndrome-trellis code to implement our steganographic scheme.

Step 1: image statistics-aware test.
Input: Cover image
Output: Cover image
Action: Overcoming the Spinning Constraint

Given the misinterpretation scores of all the Pixels in an image, syndrome-trellis code is then employed to find the stego vector with the minimum total misinterpretation to finish the hiding. However, the probability of pixels being "wet" (that is, pixels not suitable for spinning) is high in binary images. As a reaction, highest finding of stego vectors in syndrome-trellis code will fail. To find with this problem, the cover image is divided into non-overhang blocks first.

Step 2: Hiding Procedure
Based on the advanced misinterpretation appraisal and syndrome-trellis code, the steganographic scheme is composed in this sub region. It consists of the hiding and excerption procedures, whose block diagrams

Step 3: Calculate the misinterpretation score map of X. Divide the binary message **m** into non-overhang message segments of lengths elect all the no uniform blocks in **X** and the corresponded misinterpretation score blocks in **D**

Step 4: Consider all the selected blocks in **X** as an ensemble **X** and all the selected blocks in **D** as an ensemble **D**. Scramble **X** and **D** with the same scrambling seed so that each scrambled pixel still corresponds to the correct misinterpretation score at the same location

Step 5: further divide it into great pixels of size lI×lI, whose values and misinterpretation scores are calculated for each great pixel, whose value needs to be changed, flip the pixel with the lowest misinterpretation score in it

Step 6: Repeat Steps 5 and 6 until all the message segments have been embedded

Step 7: descramble the embedded image blocks successively replace each no uniform block in the cover image with the corresponded stego block to obtain the stego image **Y**syndrome-trellis code.

4. CONCLUSION

We can conclude that the suitability of steganography as a tool to conceal highly sensitive information has been discussed by using a new methodology This suggests that an image containing encrypted data can be transmitted to anybody any where across the world in a complete secured form. Downloading such image and using it for many a times will not permit any unauthorized person to share the hidden information. Thus, a new technique has been proposed to hide data in a binary image. The used algorithm is secure and the hidden information is quite invisible. A modification to this algorithm can increase further security to hide data. Statistical analysis of 0s and 1s can be applied block by block on data bit stream to make the algorithm more complex & achieve a new methodology to hide data in a more secured way In this paper, we exploit the balance property of binary images and propose a secure binary image steganographic scheme by minimizing the misinterpretation on the balance. The advanced complement, turn, and following-invariant local balance pattern is tolerant of binary image processing and thus can stably describe the local structure of binary image balance.

REFERENCES

[1] Q. G. Mei, E. K. Wong, and N. D. Memon, "Data hiding in binary text documents," Proc. SPIE, vol. 4314, pp. 369–375, Aug. 2001.
[2] Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," IEEE Trans. Commun., vol. 50, no. 8, pp. 1227–1231, Aug. 2002.
[3] M. Wu and B. Liu, "Data hiding in binary image for authentication and annotation," IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528–538, Aug. 2004.
[4] H. Yang and A. C. Kot, "Pattern-based data hiding for binary image authentication by connectivity-preserving," IEEE Trans. Multimedia, vol. 9, no. 3, pp. 475–486, Apr. 2007.
[5] H. Yang, A. C. Kot, and S. Rahardja, "Orthogonal data embedding for binary images in morphological transform domain—A high-capacity approach," IEEE Trans. Multimedia, vol. 10, no. 3, pp. 339–351, Apr. 2008.
[6] M. Guo and H. Zhang, "High capacity data hiding for binary image authentication," in Proc. Int. Conf. Pattern Recognit., Aug. 2010, pp. 1441–1444.
[7] H. Cao and A. C. Kot, "On establishing edge adaptive grid for bilevel image data hiding," IEEE Trans. Inf. Forensics Security, vol. 8, no. 9, pp. 1508–1518, Sep. 2013.
[8]. N.F. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen", Computer, Vol. 31, Isuue 2, February 1998, pp. 26-34.
[9]. W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding", IBM Systems Journal, Vol. 35, Issue 3-4, 1996, pp. 313-336
[10]. R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", 2001 International Conference on Image Processing, October 7-10, 2001, Thessaloniki, Greece, Vol. 3, pp. 10191022.

DOI 10.17148/IJARCCE.2016.53209