International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017),e-ISSN:2455-2585
International Conference on
Recent Explorations in Science, Engineering And Technology (ICRESET'19)
Volume-5, Special Issue-March, 2019.

EFFICIENT STEGANOGRAPHIC TECHNIQUE USING SECURED DATA HIDING WITH BIT STREAM DATA TRANSFER

S. DEVIPRIYA M .Tech(Assistant professor), SUJITHA.S, NANDHINI.V, KALPANA.P

Department of Information Technology,
KGiSL Institute of Technology

Abstract: A JPEG Steganographic scheme, which accounts the effects of embedding in the spatial domain tend to exhibit higher security and introduce less artifacts that can be captured by the prevalent steganalyzers. Proposal of dual image JPEG steganography image one is cover image and another spatial embedding image by incorporating statistics of both the spatial and DCT domains. The spatial statistics of the decompressed JPEG images are firstly with data and hide in embed space with the distortion measures of some efficient steganographic schemes in the spatial domain and the result which can be embedding entropies of spatial blocks in alignment with DCT blocks are then transformed in to the DCT domain to obtain the distortion measures for JPEG steganography. Experimental results show method outcome of image steganographic state-of-the-art JPEG steganographic schemes, i.e., J-UNIWARD and UERD, for the most effective feature set GFR at present and rivals them for other feature sets. Most effective one in the method is more security means of transfer of data.

I. INTRODUCTION

JPEG steganography expects to insert mystery messages into DCT coefficients so that the stego pictures are factually imperceptible from spread pictures. The previous two decades have seen the fast development of picture stenographic correspondence .These days, the most predominant methodology for picture steganography is to treat the message inserting as source coding with fidelity requirements, where the sender conceals her messages while limiting an installing twisting. This structure for the most part comprises of an appropriately planned bending capacity and a technique for encoding the messages to limit the twisting, where H is the equality check grid of code C, and C(m) is the coset relating to disorder m. For JPEG steganography, a portion of the bending capacities are gotten straightforwardly from the DCT area, e.g., UED and UERD with the targets of keeping up the factual undetectibility subsequent to installing in the DCT space and keeping the low computational unpredictability. The UED and UERD exploit the general changes of the factual model for JPEG pictures by enabling the installing modifications to be corresponding to the CVs (coefficient of variety) of DCT coefficients. Along these lines, we can take the full preferred standpoint of the insights of both the spatial and DCT spaces in the plan of the mutilation measure for JPEG steganography. Exploratory outcomes demonstrate that the proposed plan outflanks both JUNIWARD and UERD by an unmistakable edge when assessed with GFR, and can match them in opposing against DCTR [19] and CC-JRM [20] with a much diminished computational expense.

II. LITERATURE REVIEW

A. Reversible data hiding

A novel reversible data hiding algorithm is proposed in which recovering the original image without any distortion from the marked image after the hidden data have been extracted. Using this algorithm utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image. It can embed more data than many of the existing reversible data hiding algorithms. It is proved analytically and shown experimentally that the peak signal-to-noise ratio (PSNR) of the marked image generated by this method versus the original image is guaranteed to be above 48 dB.

This lower bound of PSNR is much higher than that of all reversible data hiding techniques reported in the literature. The computational complexity of our proposed technique is low and the execution time is short. The algorithm has been successfully applied to a wide range of images, including commonly used images, medical images, texture images, aerial images and all of the 1096 images in CorelDraw database. Experimental results and performance comparison with other reversible data hiding schemes are presented to demonstrate the validity of the proposed algorithm.

B. Expansion Embedding Techniques For Reversible Watermarking

Reversible watermarking enables the embedding of useful information in a host signal without any loss of host information. Tian's difference-expansion technique is a high-capacity, reversible method for data embedding. However, the method suffers from undesirable distortion at low embedding capacities and lack of capacity control due to the need for embedding a location map. We propose a histogram shifting technique as an alternative to embedding the location map. The proposed technique improves the distortion performance at low embedding capacities and mitigates the capacity control problem. Using this new technique better exploits the correlation inherent in the neighborhood of a pixel than the difference-expansion scheme. Prediction-error expansion and histogram shifting combine to form an effective method for data embedding. The experimental results for many standard test images show that prediction-error expansion doubles the maximum embedding capacity when compared to difference expansion. There is also a significant improvement in the quality of the watermarked image, especially at moderate embedding capacities

C. ***Reversible watermarking using interpolation techniques***

Watermarking embeds information into a digital signal like audio, image, or video. Reversible image watermarking can restore the original image without any distortion after the hidden data is extracted. In our previous paper , we present a novel reversible watermarking scheme using an interpolation technique, which can embed a large amount of covert data into images with imperceptible modification. Different from previous watermarking schemes, we utilize the interpolation-error, the difference between interpolation value and corresponding pixel value, to embed bit or by expanding it additively or leaving it unchanged. Due to the slight modification of pixels, high image quality is preserved. Experimental results also demonstrate that the proposed scheme can provide greater payload capacity and higher image fidelity compared with other state-of-the-art schemes.

d. Improving various reversible data hiding schemes via optional codes for binary covers

In reversible data hiding (RDH), the original cover can be losslessly restored after the embedded information is extracted. Kalker and Willems established a rate-distortion model for RDH, in which they proved out the rate-distortion bound and proposed a recursive code construction. In our previous paper, we improved the recursive construction to approach the rate-distortion bound. In this paper, we generalize the method in our previous paper using a decompression algorithm as the coding scheme for embedding data and prove that the generalized codes can reach the rate-distortion bound as long as the compression algorithm reaches entropy. By the proposed binary codes, we improve three RDH schemes that use binary feature sequence as covers. The experimental results show that the novel codes can significantly reduce the embedding distortion. Furthermore, by modifying the histogram shift (HS) manner, we also apply this coding method to one scheme that uses HS, showing that the proposed codes can be also exploited to improve integer-operation-based schemes.

e. Commutative encryption and watermarking in video compression

A scheme is proposed to implement commutative video encryption and watermarking during advanced video coding process. In H.264/AVC compression, the intra-prediction mode, motion vector difference and discrete cosine transform (DCT) coefficients' signs are encrypted, while DCT coefficients' amplitudes are watermarked adaptively. To avoid that the watermarking operation affects the decryption operation, a traditional watermarking algorithm is modified. The encryption and watermarking operations are commutative. Thus, the watermark can be extracted from the encrypted videos, and the encrypted videos can be re-watermarked. This scheme embeds the watermark without exposing video content's confidentiality, and provides a solution for signal processing in encrypted domain. Additionally, it increases the operation efficiency, since the encrypted video can be watermarked without decryption. These properties make the scheme a good choice for secure media transmission or distribution.

III EXISTING SYSTEM

While there may seem to be no point to a file system which is guaranteed to either be grossly inefficient storage space-wise or to cause data loss and corruption either from data collisions or loss of the key (in addition to being a complex system, and for having poor read/write performance), performance was not the goal of StegFS. However, since in a steganographic file system, the number of files are unknown and every byte looks like an encrypted byte, the authorities cannot know how many files (and hence, keys) are stored. The user has plausible deniability--he can say there are only a few innocuous files or none at all, and anybody without the keys cannot gainsay the user.Other methods exist; the method laid out before is the one implemented by stegnoFS, but it is possible to steganographically hide data within audio files Scram Disk or the Linux loopback device can do this.

a) Disadvantages of existing system

The algorithm used in Existing system is Error Expansion Algorithm and Error Correcting Code Algorithm. Error Expansion Algorithm is used to generate RDH codes. Error Correcting Code Algorithm is used to encode plain data bits for data extraction and image restoration can be achieved. The disadvantage of the algorithm are does not provide satisfactory security**.**

IV PROPOSED SYSTEM

Generally, a steganographic file system is implemented over a steganographic layer, which supplies just the storage mechanism. For example, the steganographic file system layer can be some existing files, each file contains a chunk of data (or a part of the file system).The final product is a file system that is hardly detected (depending on the steganographic layer) that can store any kind of file in a regular file system hierarchy through audio. Among different information hiding techniques proposed to embed secret information within audio file, Least Significant Bit (LSB) coding method is the simplest way to embed secret information in a digital audio file by replacing the least significant bit of audio file with a binary message. Hence LSB method allows large amount of secret information to be encoded in an audio file.BET (block entropy transformation) is applied with the proposed system to enhance the security in the system level security. To improve the security performance of JPEG steganography in the spatial domain, the statistics of JPEG decompressed images should be taken into consideration in the design of the distortion function. For the image covert communication, the steganography in the spatial domain is much more thoroughly investigated than the one in the JPEG domain. In line with the aforementioned design the proposed new JPEG steganographic scheme by transforming the distortion function for spatial images into the one for JPEG images.

a) Advantages of proposed system

The proposed method carries out the transformation in an indirect way. Specifically, the block embedding entropy is employed as the proxy between the distortion measures of spatial and JPEG images. In proposed algorithm use the audio to hide the text. Among different information hiding techniques proposed to embed secret information within audio file, Least Significant Bit coding method is the simplest way to embed secret information in a digital audio file by replacing the least significant bit of audio file with a binary message. Hence the method allows large amount of secret information to be encoded in an audio file. Steps to hide secret information are:

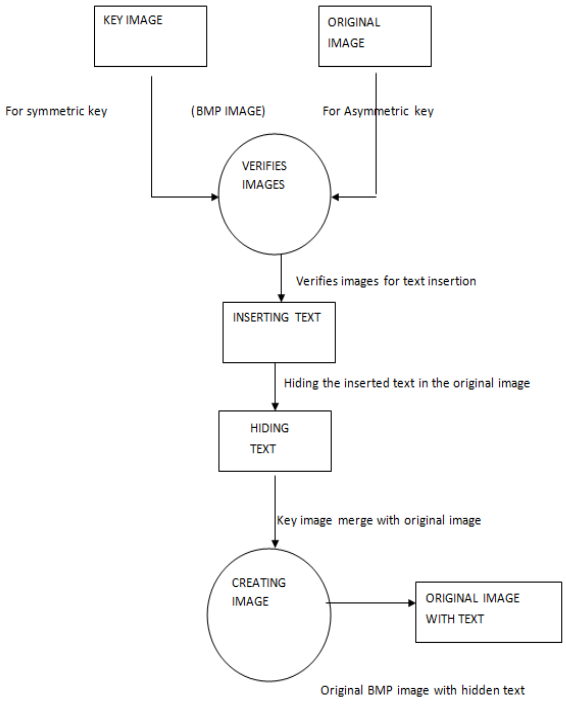
a. Covert the audio file into bit stream.

b. Convert each character in the secret information into bit stream.

c. Replace the LSB bit of audio file with the LSB bit of character in the secret information.

This proposed method provides greater security and it is an efficient method for hiding the secret information from hackers and sent to the destination in a safe and undetectable manner. This proposed system also ensures that the size of the file is not changed even after encoding and it is also suitable for any type of audio file format.

V IMAGE COMPRESSION WITH TEXT – FLOW DIAGRAM



VI RELATED WORK

The below work has been divided into main five section of modules. The modules are:

1. Image verification.
2. Text hiding.
3. Image & text processing.
4. Decryption.
5. Text and image extraction

1. Image verification

The intro module that contains the input methodology, which gets the image as input and text for hiding. The image should be in bitmap format, this is because bitmap naturally have the capacity of handling the pixel flexibility. So we are using bitmap format here. Here we want to initialize the original file to the embedded and the key file which use to embed the original file with the secret document. The original file is no more needed after the process; this is because a new file will be generated after the process.

2. Text hiding

A key image will be given as input, this key image act as a symmetric key. With the help of the symmetric key the document will be hided inside the image and the key will be converted into frames. With the converted frames a new image will be generated, the generated new image will can be stored in the user defiled area. With the new generated image the doc will be scarce into pixels, so the other people can't able to see the document embedded in to the image. We can use the same key file to the extraction process also.

3. Image & text processing

While hiding the text, the text will be converted into pixels and scarce inside the image. This process will be done according to pixels and the color of the pixels mentioned in the images. Usually high resolution images will take longer time to do this process. This is because pixel ratio will be differing from high resolution image to low resolution image. After that the key file will be taken from the image (i.e.) pixels from the image . And the next process will be triggered

4. Decryption

In the module the scarce pixels will be retrieved with the help of the key image and again roll back as the image format. Here user wants to specify the correct location where the stegano image wants to be stored.

5. Text and image extraction

This Module will finalize the process. Here the text and the image will be extracted separately. This process will also do according to the key image. So user can finally view the hidden.

6. Text and audio extraction

This Module will finalize the process. Here the audio and the image will be extracted separately. This process will also do according to the key image. So user can finally view the hidden.

VII CONCLUSION

Using steganographic technique , JPEG steganographic utilizing area change of square implanting entropy is displayed. It changes the spatial mutilation measures into the DCT space by joining the square implanting entropy of various spaces, and exploits the insights of both the spatial and the DCT area in the structure of the contortion work for JPEG steganography. The future work may include, the application creates a stego audio in which the personal data is embedded is protected with a password which is highly secured. The main intention of the proposal system is to develop a steganographic application that provides good security.

REFERENCES:

[1] Xianglei Hu, Yun-Qing Shi. "*Efficient JPEG Steganography Using Domain Transformation of Embedding Entropy*" DOI 10.1109/LSP.2018.2818674, IEEE Signal Processing Letters.

[2] M.S.Vijaykumar, *"Data Hiding with Adaptive Bit stream Steganography Cryptosystem,"*

International Journal of Engineering Science and Computing" , ISSN 2321 3361 ,IJESC vol. 8, Issue no. 3, pp. 16141 -2, Mar - 2018.

[3] W. Luo, F. Huang, and J. Huang, "*A more secure steganography based on adaptive pixel-value differencing scheme*," Multimedia Tools and Applications, vol. 52, pp. 407–430, 2011.

[4] T. Filler and J. Fridrich, *"Design of adaptive steganographic schemes for digital images,"* in Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XIII, vol. 7880, 2011, pp. OF 1–14.

[5] V. Sedighi, R. Cogranne, and J. Fridrich, "*Content-adaptive steganography by minimizing statistical detectability,*" IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 221–234, 2016.

[6] B. Li, S. Tan, M. Wang, and J. Huang, "*Investigation on cost assignment in spatial image steganography,"* IEEE Transactions on Information Forensics and Security, vol. 9, no. 8, pp. 1264–1277, 2014.

[7] T. Filler, J. Judas, and J. Fridrich, "*Minimizing additive distortion in steganography using syndrome-trellis codes,"* IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 920–935, 2011.

[8] J. Kodovsk´y, J. Fridrich, and V. Holub, "*Ensemble classifiers for steganalysis of digital media*," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 432–444, 2012.

[9] L. Guo, J. Ni, and Y. Q. Shi, *"Uniform embedding for efficient JPEG steganography*," IEEE Transactions on Information Forensics and Security, vol. 9, no. 5, pp. 814–825, 2014.

[10] M. Carter and R. Bruce, Op Amps for Everyone. Texas Instruments, 2009.

[11] X. Zhang, "*Efficient data hiding with plus-minus one or two*," IEEE Signal Processing Letters, vol. 17, no. 7, pp. 635–638, 2010.

[12] F. Huang, J. Huang, and Y. Shi, "*New channel selection rule for JPEG steganography*," IEEE Transactions on Information Forensics and Security, vol. 7, no. 4, pp. 1181–1191, 2012.

[13] W. Tang, B. Li, W. Luo, and J. Huang, "*Clustering steganographic modification directions for color components,*" IEEE Signal Processing Letters, vol. 23, no. 2, pp. 197–201, 2016.

[14] T. Denemark, M. Boroumand, and J. Fridrich, *"Steganalysis features for content-adaptive JPEG steganography*," IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1736–1746, 2016.

[15] P. Bas, T. Filler, and T. Pevn´y, *"Break our steganographic system: the ins and outs of organizing BOSS*," in Proc. 13th International Workshop on Information Hiding, 2011, pp. 59–70.

[16] V. Holub and J. Fridrich, "*Low-complexity features for JPEG steganalysis using undecimated DCT*," IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 219–228, 2015.

[17] X. Song, F. Liu, C. Yang, X. Luo, and Y. Zhang, *"Steganalysis of adaptive JPEG steganography using 2D Gabor filters*," in Proc. 3rd ACM Workshop on Information Hiding and Multimedia Security, 2015, pp. 15–23.

[18] "*Gibbs construction in steganography*," IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 705–720, 2010.

[19] R.Cogranne,V.Sedighi,andJ.Fridrich,"*Practicalstrategiesforcontentadaptive batch steganography and pooled steganalysis*," in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, 2017, pp. 2122–2126.

[20] L. Guo, J. Ni, W. Su, C. Tang, and Y. Q. Shi, "*Using statistical image model for JPEG steganography: Uniform embedding revisited,"* IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2669–2680, 2015.