ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

Statistically Undetectable JPEG 2000 Steganography

R.Priya[1] , R.Kavitha[2], D.Sudha[3] , S.Amsaveni[4]
Associate Professor[2], Assistant Professor[134]
Department of Electronics and Communication Engineering[1234]
Bharathiyar Institute of Engineering for Women
Tamil Nadu, India
mailmepriya47@gmail.com[1] , kavitharbe@gmail.com[2], dsudha.ayyanar@gmail.com[3], amsaece.veni@gmail.com[4]

Abstract- Steganography is the process of hiding data and an effort to conceal the existence of the embedded information. Steganography, the secret message is hidden in any of the secret medium and then transmitted to the receiver with more security. Steganography is a powerful tool which increases security of communication. In this paper, we proposed a class of new distortion functions known as uniform embedding distortion function is presented to increase the efficiency. By using discrete cosine transform, the best code word with undetectable data. Steganography hides the secret message so that intruders can't detect the communication. When hiding data into the intersected area, thus provides a higher level of security with more efficient data mean square error is reduced and embedding capacity is increased.

Index Terms- JPEG steganography, minimal-distortionembedding, Uniform embedding distortion.

I. INTRODUCTION

Network security is becoming more and moreimportant as people spend more and more time connected. Compromising network security is often much easier than compromising physical or local security, and is much more security with statistically undetectable data.Security in computer networks is an extremely active and broad area of research, as networks of all sizes are targeted daily by attackers seeking to disrupt or disable network traffic.Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Generally, messages will appear to be something like images, articles, shopping lists, or some other cover text and, classically, themessage may be in invisible ink between the visible lines of a private letter. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganography coding inside of a transport layer, such as a document file, image file, program of covert communication where the sender embeds secret message into an original image (cover) with a shared key to generate a stego image. The ability to display a single file with different resolutions also promises to be helpful in many

industry applications where a certain image may be display with only a low resolution at times, while in other processes a clearer picture may be needed.

A. OBJECTIVE

The main objective is to make the transmittedinformation invisible by embedding the information in the cover medium. It is used to enhance the security and robustness of the information against attacks.

II. DATA HIDING SCHEME

1. A modification to the JPEG algorithm thatinserts LSB's in some of the lossless stages or pilots the rounding of the coefficients of the DCT.
2. Steganography can be said to protect bothmessages and communicating parties.
3. An attacker cannot usually even know if themessage was embedded, and it will be very hard to extract it without knowing the right keys.
4. Two consecutive blocks can be overlapped to form a combined block. Hiding more amounts of data into the intersected area. Get a joint solution for intersected coefficients.

III. SYSTEM ARCHITECTURE

1. Carrier File - A file which has hidden information inside of it.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

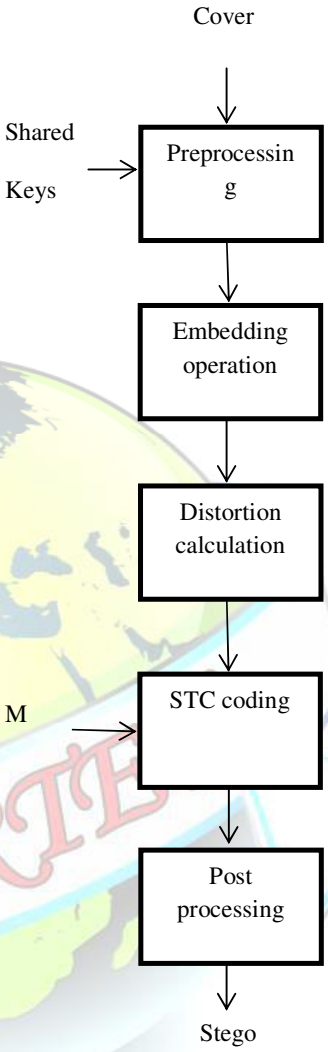
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

2. Steganalysis - The process of detecting hidden information inside of a file.
3. Stego-Medium - The medium in which theinformation is hidden.
4. Redundant Bits - Pieces of information inside a file which can be overwritten or altered without damaging the file.
5. Payload - The information which is to be concealed.

Thesteganalyst is usually something of a forensic statistician, and must start by reducing this set of data files which is often quite large; in many cases, it may be the entire set offiles on a computer to the subset most likely to have beenaltered. The problem is generally handled with statistical analysis. A set of unmodified files of the same type, and ideally from the same as the set being inspected, are analyzed for various statistics.

By uniformly "spreading" the embedding modifications to quantized DCT coefficients of all possible magnitudes, the average changes of first- and second-order statistics are possibly minimized, especially in the small coefficient, which leads to less statistical detectability, and hence, more secure steganography.

DATA EMBEDDING



Data Embedding

DATA EMBEDDING STEPS

1) Preprocessing
2) Embedding operation
3) Distortion function
4) STC coding
5) Post processing

Preprocessing

The preprocessing is adopted to generate the cover, i.e., the quantized DCT coefficients for data embedding. When input image is original BMP image, the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

process starts from the implementation of JPEG compression. In this way, the side-information, i.e., the rounding error is available for a more secure data embedding. Then the rounding errors obtained .When the input image is in JPEG format, the entropy decoding isapplied to generate the quantized DCT coefficients c directly.

Embedding Operation

The scramble stego DCT coefficients and embedding operation are performed. For scrambled AC coefficients the distortion of a modified coefficient, the embedding operation itself should be defined. The important of reducing a chance of the information being detected during the transmission

Distortion Calculation

Compute the embedding distortion for each scrambled non-zero AC coefficient using the sided UED defined in where the additional rounding error of the embedding distortion for each scrambled non-zero AC coefficient using the JC-UED defined.

STC Coding

Since the embedding operation is deterministic as in which is guided by the rounding error we can only use the binary STC. Let the binary vector are used in corresponding embedding cost ρ as input parameters, the binary STC coding is then applied to embed secret message m. The output of coding is scrambled.

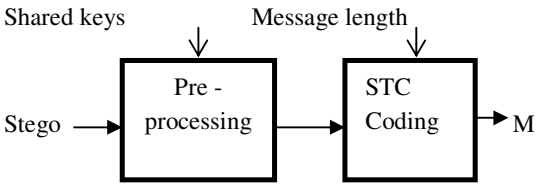
Post processing

Once the modified pattern is obtained, the cover x is modified with to obtain stego y. The k is defined as secret key function. For both cases, the entropy coding is then applied to generate stego JPEG image after y is descrambled.

Cover image

To conceal the very existence of communication, the stego image has to be statistically undetectable from its cover counterpart. Steganography hides the existence of the message so that intruders can't detect the communication and thus provides the major requirements of data hiding are that the hidden data must be imperceptible. Therefore, the two conflicting objectives, i.e., undetectability and embedding payload, should be carefully considered when devising a steganographic scheme. The embedding operation is deterministic as in which is guided by the rounding error is scrambled into stego image in the data embedding operation.

DATA EXTRACTION



Data extraction

Data Extraction steps

Data extraction is the process of extracting the original image from the stego image of the scrambled message.

Preprocessing

For a stego JPEG image, the quantized DCT coefficients are obtained by entropy decoding, which are then scrambled with the shared key K to generate the scrambled non-zero AC coefficient.

Shared keys

To conceal the very existence of communication, the stego image has to be statistically undetectable from its cover counterpart of the generating the secret messages.

STC Decoding

The STC decoding binary STC and ternary STC is then applied to extracted message. The decoding is the reverse operation of the encoding method. The syndrome trellis coding method is the used for both binary and ternary.

IV. PROBLEM DEFINITION

The main advantage of steganography overcryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages, no matter how unbreakable will arouse suspicion, and may inthemselves be incriminating. In computing, the detection of the encoded packages is called steganalysis. The simplest method to detect modified files, however, is to compare them to known originals. Easy to protect the digital data and provide privacy of information transmitted across the World Wide Web. To make the transmitted information invisible by embedding the information in a cover media and try to enhance the security and the robustness of the information against attacks and image processing techniques.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

A. ADVANTAGES

1. Hide more amounts of data than existingsystem.
2. More security.
3. Hackers cannot guess about the pixel colorvalues.

V. HIDING A MESSAGE INSIDE IMAGES

Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in news groups. The use of steganography is which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited. To hide a message inside an image without changing its visible properties, the cover source can be altered in "noisy" areas with many color variations, so less attention will be drawn to the modifications.

V1 Discrete Cosine Transform

A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations.

DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and output data are shifted by half a sample. The use of cosine rather than sine functions is critical for compression, since it turns out that fewer cosine functions are needed.

VII. REASONS FOR USING DIGITALIMAGES

1. It is the most widely used medium being used today.
2. Takes advantage of our limited visual perception of colors.
3. This field is expected to continually grow ascomputer graphics power also grows.
4. Many programs are available to apply steganography.

VIII. STEGANALYSIS

Steganalysis is the art and science of detectingmessages hidden using steganography; this is analogous tocryptanalysis applied to cryptography. The goal ofsteganalysis is to identify suspected packages, determinewhether or not they have a payload encoded into them, and, if possible, recover that payload. Unlike cryptanalysis, where it is obvious that intercepted data contains a messagethough that message is encrypted, steganalysis generallystarts with a pile of suspect data files, but little informationabout which of the files, if any, contain a payload. Some of these are as simpleas spectrum analysis, but since most image and audio filesthese days are compressed with lossy compression.Algorithms, such as JPEG and MP3, they also attempt tolook for inconsistencies in the way this data has beencompressed. This distortion is predictable. One case where detection of suspect files isstraightforward is when the original, unmodified carrier isavailable for comparison. Comparing the package againstthe original file will yield the differences caused byencoding the payload and thus the payload can beextracted.

IX. CONCLUSION

Image Steganography as a whole has existed inmany forms throughout much of history. ImageSteganography can be used as beneficial tool for privacy. The project "Steganography" after being tested and was found to be achieving what is meant for. But thissystem never provides a full proof solution for all theirproblems in the user point of view. The system has beendesigned in such a way that it can be modified with verylittle effort when such a need arises in the future. Thesystem has been found to work efficiently and effectively.Due to its higher user friendliness, others may use thesedocuments as a prototype for developing similarapplication.By using the properties of the DCT and thefrequency domain developed the zeros hiding method.It greatly enhancesthe effectiveness of the steganography since it uses a key, making it much more challenging to detect. Minimal-distortion embedding framework is a practical approach to implement JPEG steganography with high embedding efficiency. In this paper, an efficient JPEG steganography scheme which utilizes syndrome trellis coding (STC) and uniform embedding distortion (UED) strategy is presented. The uniform embedding is similar in spirit to spread spectrum communication. By uniformly “spreading” the embedding modifications to quantized DCT coefficients of all possible magnitudes, the average changes of first- and second-order statistics are possibly minimized, especially in the small coefficient, which leads to less statistical detectability, and hence, more secure steganography. A class of new distortion functions has known as uniform embedding distortion function (UED) for both non side-informed and side-informed JPEG steganography are developed to incorporate the uniform embedding.These schemes

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

developed broadened of steganography which unlike encryption allows secret data to be traded handswithout raising an eyebrow.

X. FUTURE ENHANCEMENT

Due to time and computing limitations, could notexplore all facets of steganography and detectiontechniques. The method which is unable to explore was toanalyze the noise of the pictures. Adding hidden data add random noise, so it follows that a properly tuned noisedetection algorithm could recognize whether or not apicture had steganographic data or not.To evaluate the high embedding efficiency with statistically undetectable data are remains as future work. Future enhancements and plans which areenvisioned for the system are the following:

1. The stego image which contains the
Confidential data is visible as it is the cover image.
2. Going to hide the data in an image after
Encrypt the confidential information and extract the databut which must be decrypt by the same key that was usedto encrypt the data.

REFERENCES

[1] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," IEEE Trans. Inf. ForensicsSecurity, vol. 6, no. 3, pp. 920–935, Sep. 2011.
[2] A. Westfeld, "F5—A steganographic algorithm," in Proc. 4th Inf. Hiding Conf., vol. 2137. 2001, pp. 289–302.
[3] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: Dead ends challenges, and opportunities," in Proc. 9th ACM Workshop Multimedia Security, Dallas, TX, USA, Sep. 2007, pp. 3–14.
[4] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique
for minimal distortion steganography," in Proc. 8th Inf. Hiding Conf., vol. 4437. Jul. 2006, pp. 314–327.
[5] V. Sachnev, H. J. Kim, and R. Zhang, "Less detectable JPEG steganography
Method based on heuristic optimization and BCH syndrome coding," in Proc. 11th ACM Workshop Multimedia Security, Sep. 2009, pp. 131–140.
[6] T. Filler and J. Fridrich, "Design of adaptive steganographic schemes for digital images," Proc. SPIE, vol. 7880, p. 78800F, Jan. 2011.
[7] C. Wang and J. Ni, "An efficient JPEG steganographic scheme based on the block entropy of DCT coefficients," in Proc. IEEE ICASSP, Kyoto, Japan, Mar. 2012, pp. 1785–1788.