A NOVEL APPROACH FOR RECOVERY OF LOSSLESS IMAGE

NALLA NAVYA DEEPTHI,
Associate Professor,
Department of Computer Science and Engineering,

SHIRISHA MUNASA D,
Associate Professor,
Department of Electronics and Communication Engineering,

Siddhartha Institute of Technology and Sciences,
Narapally, Hyderabad, Telangana – 500 088.

ABSTRACT

A novel algorithm for generic visible watermarking with a capability of lossless image recovery has been presented. The technique depends on overlaying a range of visible watermarks of various sizes over cover images using deterministic one-to-one compound mappings of image pixel values. The reversibility of compound mappings has been demonstrated, allowing for lossless recovery of original images from watermarked pictures. The mappings can be altered to produce pixel values that are close to those of visible watermarks. As applications of the suggested general methodology, various types of visible watermarks, notably opaque monochrome and translucent full colour ones, are inserted. In the watermarked image, a two-fold monotonically growing compound mapping is generated and shown to produce more distinct visible watermarks.

I. INTRODUCTION

The advancement of computer technology, as well as the widespread use of the Internet, has made digital information reproduction and distribution easier than ever before. As a result, copyright protection for intellectual property has become a hot concern. Digital watermarking, that entails embedding specific information regarding the copyright holder (business logos, ownership details, and so on) into the medium to be secured, is one method of copyright protection. The two forms of digital watermarking methods for images are commonly classified as invisible and visible.

The first type tries to invisibly embed copyright information into host media so that, in the event of a copyright infringement, the concealed information may be extracted to determine who owns the protected host. Watermarks, whether visible or invisible, diminish the overall quality of the host media. Reversible watermarking refers to a set of approaches that allow lawful users to remove the embedded watermark and restore the original content as needed. Lossless recovery is critical in many situations wherein image quality is a major consideration. Forensics, medical image analysis, historical art imaging, and military applications are only a few instances.

II. LITERATURE SURVEY

To generate full-color images, single-chip digital cameras use a colour filter array and an interpolation approach. Although classic sampling theory can be used to create the interpolation technique, the idea that the sampled data is dispersed across three separate colour planes offers an extra layer of complexity. Current interpolation methods are frequently derived from general numerical approaches which make few assumptions on the data's nature. Considerable computational savings can be gained without sacrificing image quality if the data is recognised as image data and an appropriate image model is adopted (Adamsand Hamilton, 1997).

Bayram *et al.* (2006) examined three types of forensic features and compare and contrast the construction of classifiers for doctored and original photos. The performance of classifiers is evaluated in terms of selected controlled manipulations and also uncontrolled manipulations. The techniques for detecting image manipulation are placed through their paces in feature fusion and decision fusion situations.

By expanding our findings in the direction of M. Kharrazi et al., authors focussed our attention on the problem of blind source camera detection (2004). The paper's foundation is the interpolation of an image's colour surface due to the employment of a colour filter array (CFA). They proposed tracing the proprietary interpolation technique used by a digital camera to identify the originating camera of an image. To detect the originating digital camera, a set of visual criteria is established and then used in conjunction with a support vector machine based multi-class classifier. They also present preliminary results for determining the source of two and three digital cameras Bayram *et al.* (2005).

Buccigrossi et al. (1999) postulated a Markov model that accounts for the statistics of a wide range of images, such as photo and video, graphical, as well as medical images, utilising a linear predictor for magnitude combined with both multiplicative and additive unknowables, and demonstrate that it accounts for the statistics of a wide range of images, which include photographic, graphical, and medical images. They build an image coder called EPWIC (embedded predictive wavelet image coder) to clearly illustrate the model's power, wherein subband coefficients were encoded one bitplane at a time using this nonadaptive arithmetic encoder that uses conditional probabilities generated from the model.

III. METHODOLOGY

The proposed methodology comprises the following:

- Digital Invisible Ink (DII) Embedding
- Algorithms Developed.

The following algorithms are used in the suggested methodology:

- Battle Steganography
- Blind Hide

Module 1: Encode

The embedding of the cover picture with the image containing the data, as well as the chosen algorithm, is performed. The user chooses the algorithm that will be used to process the data and sets the password. The user also chooses the cover image, and all of this is then integrated.

Battle Steganography

"Battleship Steganography" is performed by this algorithm. The image is first filtered, and then the highest filter values are used as "ships." The algorithm then "shoots" at the image at random until it discovers a "ship," at which point it clusters its shots in the hopes of "sinking" the "ship." It drifts away once in a while to look for additional ships. As a result, the message is concealed at random, but it is frequently hidden in the "ideal" sections to hide in, thanks to the ships. It goes aside to look for other ships so that we don't lose too much detail in one part of the image. It's safe since retrieving the message requires a password. It's reasonably effective since it hides the majority of the information in the best regions (assuming the values are set correctly).

Blind Hide

This is the most basic method of concealing information in an image. It hides invisibly as it starts pixel by pixel at the top left corner of the image and works its way across (then down - in scan lines) the image. As it progresses, the least significant bits of the pixel colours are changed to fit the message. The least significant bits, starting at the top left, are read off to decrypt the process. It's quite easy to read out the least significant bits, therefore this isn't really secure. It's also not very clever: if the message doesn't completely occupy the available area, only the top portion of the image is deteriorated, while the bottom remains untouched, making it simple to see what's changed.

ADVANTAGES IN PROPOSED SYSTEM

- No explicit security modules, such as password input prompts or decryption programmes, are required aside from the message extractor.
- Ensures robustness
- Ensures security
- Ensures dependability

IV. RESULTS

Java is a computer language as well as a platform. The Java programming language is a high-level language that has all of the buzzwords listed below:

- Simple
- Architectural form neutral
- Object-oriented design
- Portable

- Distributed

Input output design:

ENCODING FORM

Input :

To get two cover images and one message image, the Encode tab was established.

The message has been decoded using the Decode tab.

The Simulate tab is used to test the watermarking process.

The Analysis tab is used to investigate the watermarking process.

Output :

With encoding utilised to encode the material, the two cover images were evaluated for disguising the text message.

To decode the original, decode it.

ALGORITHM SELECTION

Input:

Selection of encoding algorithm will be made

Message image will be selected here.

Cover image will be selected here.

Output:

Algorithm will be selected to encrypt the images.

The cover images and the message content will be encrypted according to the algorithm selected

Algorithm will be selected for decoding operation

SECRET MESSAGE HIDING

Input:

The password will be given when the algorithm has been chosen in order to perform secure communication.

As input, two cover images and one message image will be provided.

As an input, battle stenography will be chosen.

Output:

The message's security has been ensured by the use of a password.

The location of the output image will be specified.

The output image will be saved in the path you specify.

DECODING

Input:

To save the content, the cover image has been chosen.

With the stated algorithm, decrypt the image.

It will be provided the inverse of the encoding module.

Output: The original message will be separated from the two cover graphics in the output.

To differentiate the cover image from the message image, the DCT method will be utilised.

Input: Following the decoding operation, the decoding algorithm will be utilised to obtain the supplied document.

For retrieval, a password will be required.

The message will be retrieved using the decoding algorithm that was chosen.**MESSAGE**

EXTRACTION

Output: The original image will be discovered after the two cover images have been trimmed.

If the correct password is entered, the image will open.

The recipient will retrieve the message image after all of the details have been provided.

MESSAGE RETRIEVAL

Input: The decoding procedure is carried out.

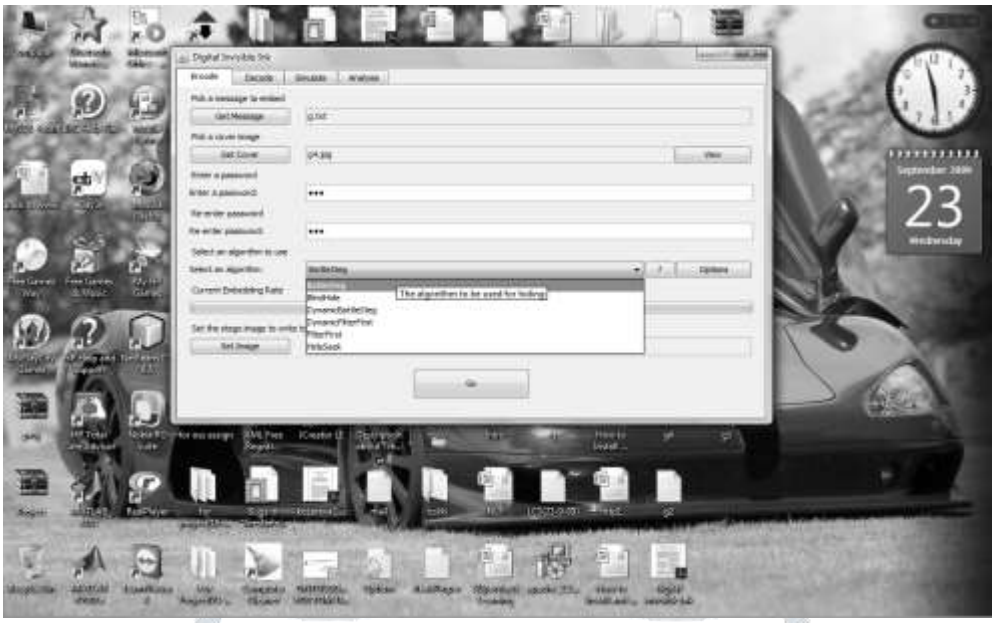
The recipient will be shown the message.

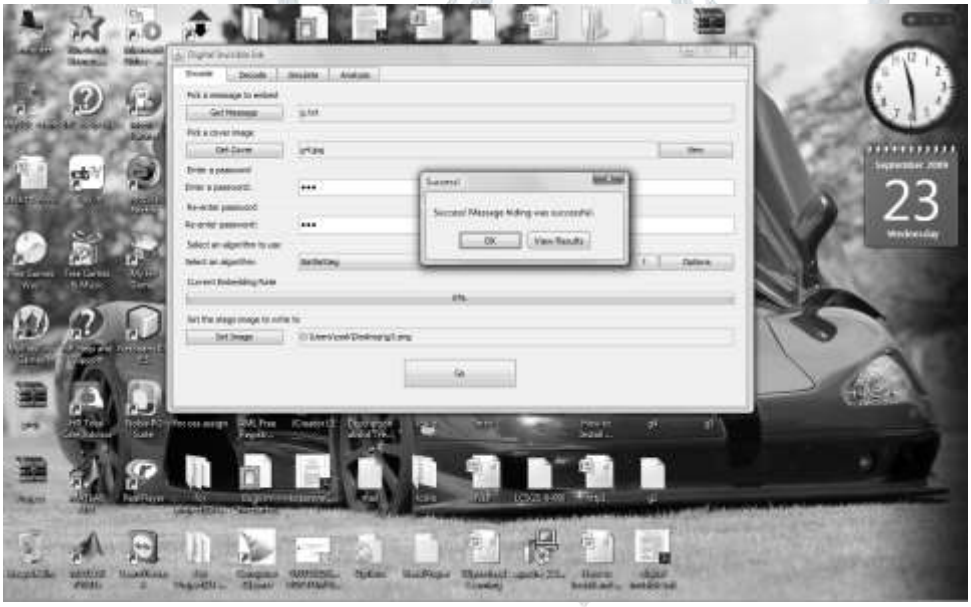
When encoding, the message may be in the same format as when it was sent.

Output: The original text file has been retrieved as an output.

The message will be saved in the reciever's specified path.

SAMPLE SCREENS





V. CONCLUSION

Choosing the right methods is the key to steganographic secrecy success. But, a stego medium that appears to be harmless may, upon closer inspection, actually broadcast the existence of embedded data. The field of clandestine communications and steganography will continue to evolve. The effort to develop more robust technologies that can withstand picture alteration and attacks is continuing. The more information is made available to the public via the Internet, the more owners of that information must guard against theft and misrepresentation.

REFERENCES

[1] http://www.java2s.com/

[2] http://www.javaworld.com/javaworld/jw-01-1998/jw-01-bookreview.html

[3] Database Programming with JDBC and Java by O'Reilly

[4] Head First Java 2nd Edition

[5] http://java.sun.com/javase/technologies/desktop/

[6] Adams, J., and Hamilton, J. (1997) 'Design of practical filter array interpolation algorithms for digital cameras'. Proc. SPIE.

[7] Bayram, S., Avcibas, I., Sankur, B. and Memon, N. (2006) 'Image manipulation detection," Journal of ElectronicImaging, Volume 15, Issue4, 041102 (17 pages), vol. 15(4).

[8] Bayram, S., Sencar, H. T. and Memon, N. (2005) 'Source Camera Identification Based on CFA Interpolation', Proc. of IEEE ICIP.

[9] Buccigrossi, R.W. and Simoncelli, E.P. (1999) 'Image compression via joint statistical characterization in the wavelet domain', IEEE Transactions on Image Processing, 8(12):1688.1701.

[10] [5] Chang, Y.C. and Reid, J.F. (1996) 'RGB calibration for analysis in machine vision'. IEEE Transactions on Pattern Analysis and Machine Intelligence, 5(10):1414–1422.