ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 5, July 2012

A New Fragile Approach for Optimization in Invisible Image Watermarking by Using Symmetric Key Algorithms

Vandana Tehlani

***Abstract*- In the information technology and communication, the most important factor has been the security of information and one of the methods is watermarking. The Watermarking aims to validate the host and the undeniable identity of the legal owner. In this paper, we will concentrate on hidden watermarks. At one time, it deals with two different images in BMP to hide information. The message will be dividing evenly in both images to maximize the security of image watermarking. It utilizes the LSB manipulation method and the images addresses used as key are also encrypted for performance improvement with existing Symmetric key algorithms. There are two options to choose either DES or AES algorithm to get optimized output. We are using spatial domain for hiding actual information inside images.**

This paper gives a brief idea about the new image watermarking approach that make use of LSB algorithm for embedding the data into the bit map images (.bmp) which is implemented through the Microsoft .NET framework.

Keyword: DES, AES, LBS method, Invisible Image Watermarking.

I. INTRODUCTION

The information can be encrypted in several forms. There are many different methods have been developed to encrypt and decrypt data in order to keep the message secret. For securing the secrecy one of the advanced method is Watermarking.

Watermarking is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of data. In this method the data which is to be sent is concealed in any multimedia file like image, video or an audio file.

We are going to deal with Image Watermarking and hence hereafter if we refer Watermarking it actually keeps points to image Watermarking.

This approach consists of following terminologies:

1. *Plaintext:* The original data that has to be communicated to the recipient.
2. *Cover Image:* An Image which is acts as a cover in which the secret message is to be concealed.
3. *Embedding Process:* The process of embedding or inserting the secret text into the cover image with the help of any suitable algorithm.
4. *Watermark Image:* The image resulted after the completion of embedding process which looks as exactly as the cover image without any suspicion of the presence of secret text inside it.
5. *Extraction Process:* The process of extracting or revealing the original message from a received watermark image by using the same algorithm that the sender has chosen.
6. *Optimization:* It is a collection of methods and techniques to design and make use of engineering systems as perfectly as possible with respect to specific parameters. [1]

II. TYPES OF WATERMARKING

Digital watermarking is the process of Embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners. There are two types of digital watermarking as follows-

1) Visible Watermarking
2) Invisible Watermarking

In *visible* digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark.

In *invisible* digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of watermarking, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals.

Watermarking techniques are used to decide the domain, there are two types of techniques for images, and they are-

1) Frequency Domain Watermarking
2) Spatial Domain Watermarking

- *Frequency Domain Watermarking*: First convert the image to the frequency domain and then apply the watermark in the low frequency regions.

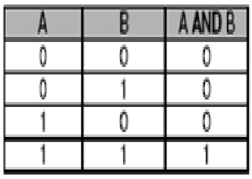
- *Spatial Domain Watermarking*: Just change some of the values of the pixels in the lower bit plane; e.g., Change some of the bits from 1 to 0 or 0 to 1. [13] The Spatial Domain Watermarking is classified in different classes.

In this paper, we are using Spatial Domain Watermarking with the invisible watermarking Images with the best known watermarking method that works in the spatial domain is the LSB (Least Significant Bit), which replaces the least significant bits of pixels selected to hide the information. The "LSB watermark" options save the final images in BMP format as it is a format with no compression.

III. LSB MANIPULATION IN IMAGES

In the digital representation, images are the most popular cover objects for watermarking. Applied in the spatial domain, this method of watermarking is very effective method for hiding actual information inside images. In this manipulation, the information to be watermarked (simple text in this case) is converted to 'bits' [0-1]. Then "random" chosen pixels are ANDed with the number 254 ["00000001"] so the LSB is turned to 0. Finally, the information is inserted by adding the watermark info bits to the luminance value of the chosen pixels.

The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as *true colour*. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.[4] [12]



A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

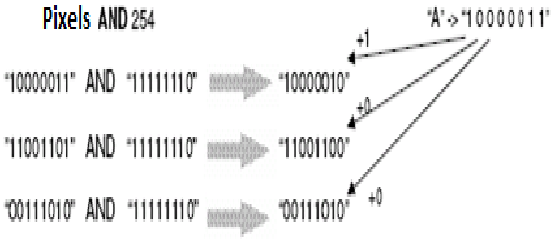

Pixels AND 254
'A'->'10000011'
+1
"10000011" AND "11111110"
"10000010"
+0
"11001101" AND "11111110"
"11001100"
"00111010" AND "11111110"
"00111010"
+0

Fig- Least Significant Bit manipulation

It's best that we work with a true color image. This way, we can manipulate the LSB of a pixel-color without the human eye understanding the difference. Specifically, the blue color of pixels is chosen because it's the most unnoticed for the human eye. This method is very fragile. It will fail holding the watermark even with the slightest manipulation of the image. This is why this method can be used for image authenticity and maximizes the robustness of the hidden data.

This paper will focus on hiding information in images by LSB manipulation. At the time of encryption, the message will be hiding in two different images evenly. Inverse of same process follows at decryption, LSB manipulated first image gives half message and another half message will be given by second image. We can use more than two images to hide information further. These images information will be optimally secured by using symmetric key algorithm such as DES and AES.

IV. WORKING ALGORITHM

A. Data Encryption Standard

DES is an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is never quoted as such. Every 8th bit of the selected key is discarded, that is, positions 8, 16, 24, 32, 40, 48, 56, 64 are removed from the 64 bit key leaving behind only the 56 bit key.

The algorithm's overall structure is shown in Figure: there are 16 identical stages of processing, termed rounds. There is also an initial and final permutation, termed IP and FP, which are inverses. Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the Feistel scheme.

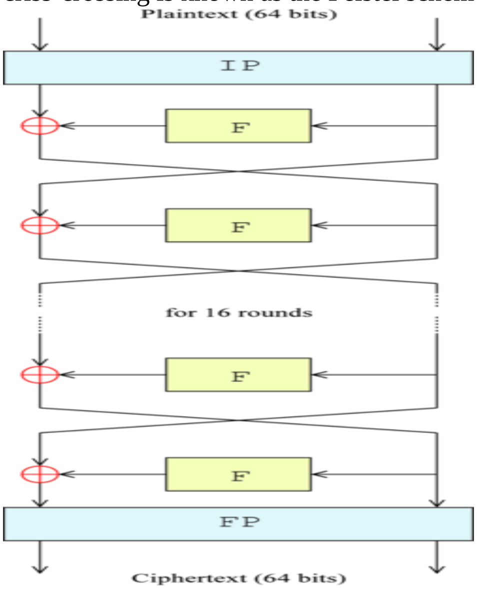


Figure: The process of DES algorithm

B. Advanced Encryption Standard

AES Originally called Rijndael.It is based on a design principle known as a substitution-permutation network. It is fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistel network.

AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael is specified with block and key sizes in any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field.

The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. The numbers of cycles of repetition are as follows:

10 cycles of repetition for 128 bit keys.
12 cycles of repetition for 192 bit keys.
14 cycles of repetition for 256 bit keys.

Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

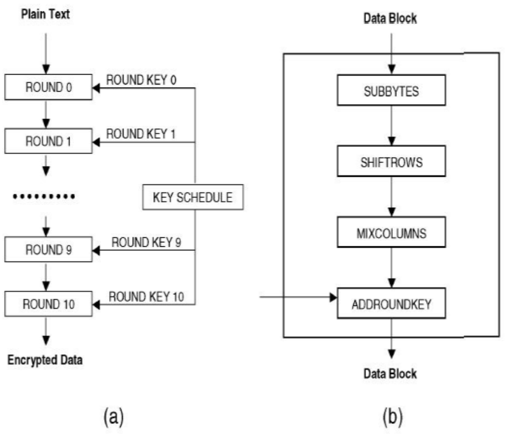


Fig. 1. (a) The data-path for data block and key size of 128 bits, (b) generic structure of one internal round.

V. PROPOSED WORK & METHODOLGY

We effectively using LSB method and DES and AES algorithm and derived a watermarked model. There are only two functions, one for embedding and one for detecting the watermark. This approach will surely enhance the performance and security and the steps are to be taken place in the following order,

1. Getting the images are loaded from the user.

2. Now filling the information for encrypting message accompanied that will be encrypted in two images which are divided evenly.

3. These will be manipulating the LSB of a

pixel-colour without the human eye understanding the difference by using true colours.

4. The encrypted images data location is treated as key that will be again encrypted by either DES or AES algorithm.

5. After insertion process complete, the new images are saved as a bitmap format (.bmp).

6. Now the images are ready to be watermarked.

7. The detection process is exactly opposite to get the output.

Now, User needs to run the application. The user has two tab options in dot net framework. If user selects *Encoding*, application gives the screen to select image files, information for adoption to save in the image file and one symmetric key algorithm to choose. If user selects *Decoding*, application gives the screen to select only image file and ask same chosen symmetric key algorithm to display the secrete information.

This project has two methods – Encrypt and Decrypt. The model for encryption and decryption of images are designed with the objectives to file. In encryption the secrete information is hiding in BMP images only to save without any compression in image files. Decryption is getting the secret information have confidentiality and security in transmission of the image based data as well as storage, with the help of suitable symmetric key algorithms.

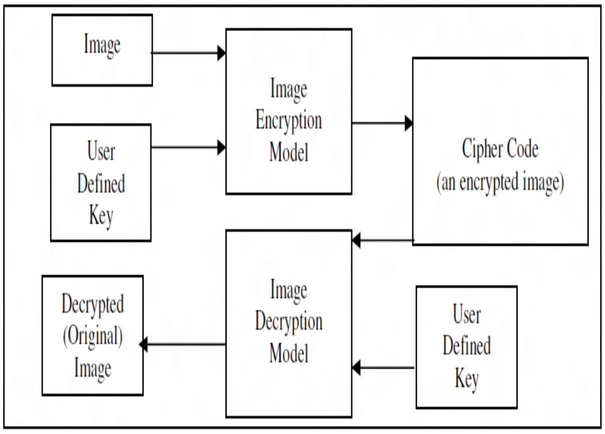


Figure4: Block Diagram of Image Watermarking

I primarily concentrated on the data security issues when sending the data over the network using watermarking techniques. The main objectives of the project are

- Using of different symmetric key algorithms and more than one image for hiding them in means of security and quality of hiding.
- Increasing the efficiency and accuracy of hiding the data through algorithms using Microsoft .NET framework.

The proposed method will help to secure the content with in the images and encryption of image files address with help of symmetric key algorithm to make the document much securer because even though if the unauthorized person succeeds in being able to hack the image, the person will not able to read the message as well as acquire the whole information which is hidden in two images. Hence, unauthorized will not make any type of changes.

VI. APPLICATIONS

There are various watermarking applications for images, as follows-

1. *Copyright protection* is probably the most common use of watermarks today. Copyright owner information is embedded in the image in order to prevent others from alleging ownership of the image.
2. *The fingerprint* embeds information about the legal receiver in the image. This involves embedding a different watermark into each distributed image and allows the owner to locate and monitor pirated images that are illegally obtained.
3. *Prevention of unauthorized copying* is accomplished by embedding information about how often an image can be legally copied.
4. *In an image authentication* application the intent is to detect modifications to the data.
5. *Medical applications* Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible/invisible Watermarking.[5]

VII. EXPERIMENTAL RESULT

This paper has an aim to prevent the information by hiding in images from intruders and people who don't have the permission. We apply the LSB insertion by encrypting into two images for hiding one secret message whose half data encrypt in one image and next half data encrypt in second image. Symmetric key (DES or AES) algorithm as choice for image address encryption to get optimization. The experiment will show, encrypted images can not show real view until these images are decrypted by user key. Finally, these decrypted images can be identified by secret message on the images.

To be able to compare the performance of this improvement on the LSB method, the images on Figures will be used as cover with BMP (Bit Mapped Picture) format and watermarked images named as stego-image. These are so similar that no one would ever think to examine the contents of the file.

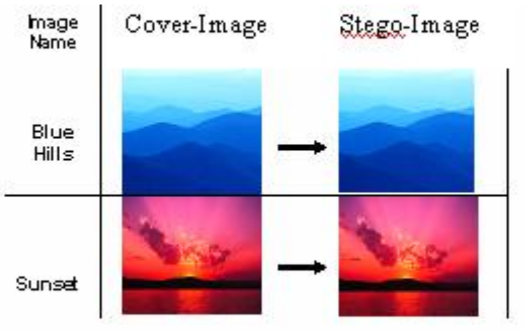


Fig: Blue hills and sunset bitmap images before and after data hiding.

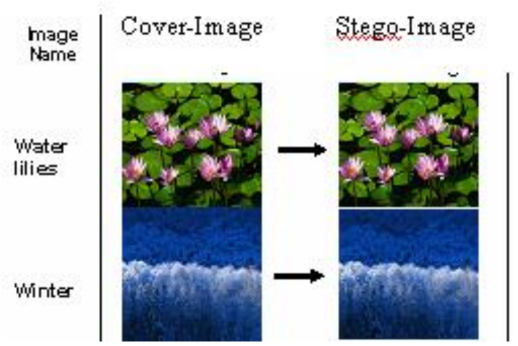


Fig: Water lilies and winter bitmap images before and after data hiding.

VIII. CONCLUSION

In this work, we have taken a rigorous approach that arriving at the watermarking is an effective way to obscure data and hide sensitive information. We have explored the limits of watermarking theory and practices with less security. We printed out the enhancement of the image watermarking system using LSB approach to provide a means of secure communication. Applied in the spatial domain, this method of watermarking based on Microsoft .Net framework is the optimized method for hiding actual information inside two images with two algorithms i.e., DES and AES for increasing security. This method is very fragile. It will fail holding the watermark even with the slightest manipulation of the images. This is why this optimized method can be used for image authenticity.

Watermarking, like cryptography, will play an increasing role in the future of secure communication in the "digital world". This approach of secure communication will be enhancing by using both types, visible and invisible watermarking which is known as dual watermarking.

IX. REFERENCES

[1] G. Manikandan, M. Kamarasan, P. Rajendiran, R. ManikandanA Hybrid Approach for Security Enhancement by Modified Crypto-Stegno Scheme,EuroJournals Publishing, Inc. 2011

[2] Digital watermarking of images, SGN-1650/1656 Signal ProcessingLaboratory,http://www.cs.tut.fi/~selinumm/watermarking/watermarking.pdf

[3] [4] Russell K. Meyers and Ahmed H. Desoky, An Implementation of the Cryptosystem Signal Processing and Information Technology, IEEE International Symposium, Dec. 2008

[4] T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier 3 An Overview of Image Stenography,(ICSA) Research Group Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa July 2005

[5] Keshav S Rawat, Dheerendra S *Members, IEEE,* Digital Watermarking Schemes for Authorization Against Copying or Privacy of Color Images, Indian Journal of Computer Science and Engineering.

[6] Diaa Salama Abdul. Elminaam, H M Abdul Kader and M M Hadhoud3, Performance Evaluation of Symmetric Encryption Algorithms, in IJCSNS I, vol.8, Dec 2008.

[7] Nadeem, A. and Javed, M.Y., A Permance Comparison of Data Encryption Alhorithms, IEEE Information and Communication Technologies,05,First International Conference, February,2006, pp.84-89

[8] Tingyuan Nie Chuanwang Song and Xulong Zhi Performance Evaluation of DES,(ICBECS), 2010 International Conference, IEEE, Apr. 2010

[9] "*Digital watermarking*" definition from http://en.wikipedia.org/wiki/ Digital_ watermarking

[10] R.Chandramouli and Nasir Memon,Analysis of LSB Based Image Stegnography Techniques, IEEE 2001

[11] Yamuna Govindarajan, Yamuna Govindarajan. Quality - Security uncompromised and Plausible Watermarking for Patent Infringement. International Journal of Image Processing

[12] Ms.Soniya Vijayakumar, Image Stegnography Based On Polynomial Function JGRCS, march 2011

[13] Ravi Sharma, Digital Watermarking Article, paper presentation, http://www.slideshare.net/ravi33s/watermark-12641562 april 2012.

Author:

Vandana Tehlani,
Engineer, M.Tech Student (CSE) from TIT, RGPV University, Bhopal.