European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 07, 2020

Detecting Bio-Metric Finger Patterns Using Lsb Substitution Machine Learning Method

M P Rajakumar[1], Dr. V. Lokeswara Reddy[2], Dr.G. Nalinipriya[3], Dr.S. Thanigaivel[4], M R Arun[5]

[1]Associate Professor, Computer Science and Engineering, St.Joseph's College of Engineering, OMR, Chennai, Tamilnadu, India - 600119.
[2]Professor, Department of Computer Science & Engineering, K.S.R.M College of Engineering, Tadigotla (Village), Krishnapuramu,Kadapa,Y.S.R (Dt), Andhra Pradesh, India--516004.
[3]Professor, Department of Information Technology, Saveetha Engineering College, Saveetha Nagar, Chennai, Tamilnadu, India- 602105.
[4]Assistant Professor, Department of Biotechnology,Saveetha school of Engineering,Saveetha Institute of Medical and Technical sciences, Chennai, India -602105.
[5]Professor, 262-1A,Anna Street, Vivekananda Nager, Avadi, Chennai, Tamilnadu, India-600054.

Abstract - This paper introduces a new way to hide a message in a digital image on a spatial domain. In this way two bit messages are embedded in one pixel, which can not only change the most important bit pixel, but also the second bit level and the fourth bit level, but the embedding process at each stage only allows a bit of alternation to occur. This fast and versatile solution achieves cutting-edge results in steganographic applications with linear time and space complexity with respect to Number of cover elements. We report extensive test results for a large number of relative payloads and various distorted profiles, including the wet paper channel. Compared to the LSB-matching method, the results show that they have an acceptable ability to embed this data and that the steganalysis algorithm cannot detect it. Most newer coding schemes used in steganography (matrix embedding, wet paper codes, etc.) can be implemented using this framework.

KeyTerms: Biometric Inputs, Steganology, LSB-Compatibility, Bit Plane, Spatial Domain

1. INTRODUCTION

There are two mainstream approaches to steganography experience covers such as digital media objects: steganography designed to protect the selected cover model and steganography that reduces embedding distortion defined as heuristic. Steganography is the art of secret communication. Its purpose is to hide the existence of communication as opposed to cryptography and to make it impossible for those without proper keys to understand communication. Digital images, videos, audio files and other computer files can be used as "covers" or carriers to hide confidential messages that contain irrelevant or unnecessary information. After embedding the secret message in the cover message, it is called a stego image [1].

It is important that the stego-image does not have trace elements that can be identified due to message embedding. A third party may use such handicrafts to indicate that there is a secret message. In this paper, an image is used as a carrier to hide image data. This is called

image steganography. The simplest form of steganography is the low-key bit (LSB). LSB relies on embedding data in the smallest bit pixels, which can lead to small changes in the human careless cover image [2].

Since this method can be easily disassembled, there is a greater chance of attack. To increase the security and size of stored data, new custom LSB technology is used. Instead of storing data in all important pixels, the host tries to use more than one in the pixel without affecting the visual appearance of the image. It uses side information of neighboring pixels to calculate the number of bits that can be carried in pixels of the host-image to hide confidential data [3].

Steganography is the art and science of writing hidden messages, protected by ambiguity so that no one other than the sender and the intended recipient can doubt the existence of the message. The word steganography is of Greek origin, meaning "hidden writing" which means "hidden or preserved" from the Greek word. In 1499, JoharnesTritemius wrote a book on cryptography and steganography in his steganography, which became a book about magic. Usually, the messages look different: pictures, articles, shopping lists or any other cover text, scientifically, the hidden message may be in an invisible ink between the visible lines of the private character [4].

The only advantage of steganography over cryptography is that messages do not attract their attention. Clearly encrypted messages - no matter how fragile - are suspicious and are criminalized in countries where encryption is illegal. Therefore, while cryptography protects the content of the message, steganography is used to protect the messages and the parties communicating. Hiding information in computer files involves steganography. In digital steganography, electronic communication involves steganographic coding in a transport layer, such as a document file, image file, program, or protocol [5].

Problem Statement

Suitable for steganographic transmission as media files are large in size. As a simple example, the sender can start with a harmless image file and adjust the color of every hundredth pixel to match the letter of the alphabet, which is unlikely to be noticed by anyone who has not specifically looked for a very subtle change [6].Although steganography is an ancient subject, its modern formulation is based on the prisoner problem suggested by Simmons, where two prisoners want to communicate in secret. All of their communication goes through a warden, who, if they suspect any exchange, puts them in solitary confinement.

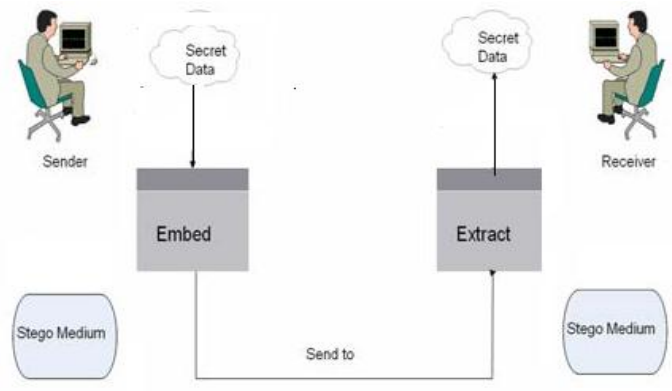

Figure 1.Steganographic LSB Pattern Matching

Sutiayal et al, The free warden may be passive or active to examine all information exchanged between inmates. The passive warden examines the communication and determines whether it contains confidential information. If she suspects communication that contains hidden information, she listens to the exchange communication discovered by the passive warden and reports to some outside party, allowing the message to be blocked. The active warden, on the other hand, tries to change the communication with deliberately hidden information in order to remove the information [7].

Wong et al, when converting domain methods to specific domains, a hidden process, such as low-key bit (LSB) reset, takes place within a specific domain; Hide data in another domain, such as the Violet domain. The simplest form of steganography is the low-key bit (LSB). LSB relies on embedding data in the smallest bit pixels, which can lead to small changes in the human careless cover image. Since this method can be easily disassembled, there is a greater chance of attack. The LSB method severely affects image statistics, such as histograms. By checking the image's histogram the attacker can learn about hidden communication. A good solution to eliminate this error is LSB adjustment. LSB-matching is a major breakthrough in steganography techniques, and many have derived ideas from it [8].

Cho and Chai et al, the simplest form of steganography is the low-key bit (LSB). LSB relies on embedding data in the smallest bit pixels, which can lead to small changes in the human careless cover image. Since this method can be easily broken, there is a high chance of attack. This requirement includes all the features of a steganographic algorithm, which can lead to generally unused and suspicious images. For example, abnormal file size is a property of the image, which may cause the warden to inquire further about the image..

Machine Learning – LSB Substitution

A. Adaptive LSB Substitution

The LSB method above can be easily broken; This can cause further damage to the attack. To increase the security and size of stored data, new custom LSB technology is used. Instead of storing data in all important pixels, the host tries to use more than one in the pixel without affecting the visual appearance of the image. It uses side information of neighboring pixels to calculate the number of bits that can be carried per pixel of the host-image to hide confidential data. In our method, two neighboring pixels of the input pixel are used to determine the number of bits to be included in the pixel. Confidential information is embedded in the host-image through a simple LSB reinstallation with a pixel configuration process.

The pixel value difference between the upper pixel and the left pixel of the input pixel is used to determine the embedding of the data in the pixel. If the pixel is in the edge area, more bits can be placed in the pixel than in the soft space. If we know how many bits a pixel can carry, we can embed the hidden bits in the pixel with a simple LSB re-installation. The pixel adjustment process is applied to increase the image quality of the stego-image and to reduce embedding error .

Cover-Object - Refers to the object used as a carrier to embed messages. Many different materials are used to embed messages in images, audio, video, text structures and HTML pages.

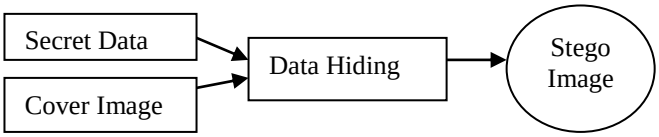

Figure 2.Stego Image Bio-Metric Finger Pattern Formation from Cover Image

Stego-object - refers to an object that contains a hidden message. So the goal of the steganographer is to create a stego object that carries the messages given by the cover object.

In the pure steganography framework, Silver does not know the technique of embedding the message, and she secretly shares it between Alice and Bob. However, it is generally accepted that the algorithm in use is not secret, but only the key used by the algorithm is kept secret between the two parties and this umption is also known as the Kercho principle in the field of cryptography.

Secret message, for example, is the password (encrypted) used to provide seeds for a pseudo-random number generator to select pixel locations in the image cover-object to embed the secret message. Silver does not know the secret key that Alice and Bob share, but they do know the algorithm they use to embed messages. Warden Silver Alice and Bob are inactive or active, with the freedom to check all messages being transmitted. The inactive warden checks a message and tries to find out if it contains a hidden message. If this seems to be happening, she will suppress the message and / or take appropriate action, otherwise she will allow the message without any action.

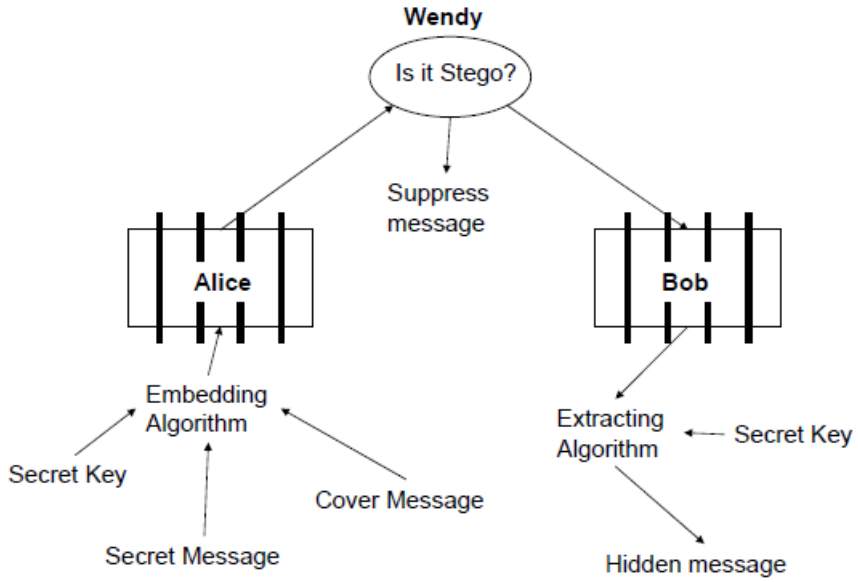

Figure 3. LSB Substitution machine learning - Stego Image process

B. Text LSB Substitution – Algorithm

As a simple example of LSB substitution, imagine “hiding” the character ‘G’ across the following eight bytes of a carrier file (the LSB s are underlined):

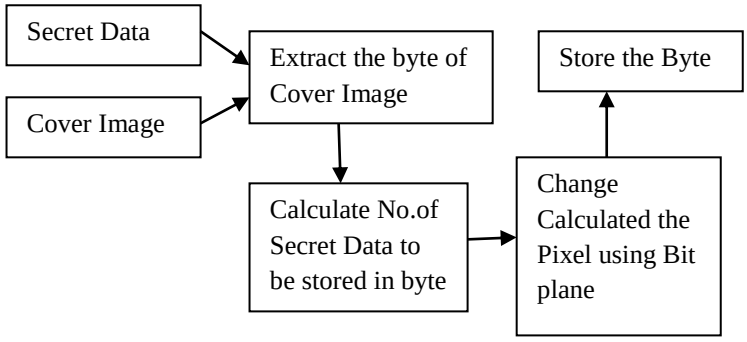

Fig 4. LSB Matching Process

10010101 00001101 11001001 10010110
00001111 11001011 10011111 00010000

A 'G' is represented in the American Standard Code for Information Interchange (ASCII) as the binary string 01000111.

These eight bits can be "written" to the LSB of each of the eight carrier bytes as follows:

1001010***0*** 00001101 1100100***0*** 10010110
0000111***0*** 11001011 10011111 0001000***1***

In the sample above note that only half of the LSBs are actually changed.

Image LSB Substitution

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24 bit image, a bit of each of the red, green, blue color 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 x 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example a grid for pixel of 24 bit image can be as

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours.

These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference.To increase the security

and the size of stored data, a new adaptive lsb technique is used. Instead of storing the data in every least significant bit of the pixels, this technique tries to use more than one bit in a pixel in such a way that this change will not affect the visual appearance of the host image. It uses the side information of neighboring pixels to estimate the number of bit which can be carried in the pixels of the host-image to hide the secret data.

A. LSB Module – Set 1

Description: This Module consists of developing Two sub modules. The one is encryption module and the decryption module. These two sub modules are the main core for the application.

Encryption Module - In Encryption module, its consists of Key file part, where key file can be specified with the password as a special security in it. Then the user can type the data or else can upload the data also though the browse button, when it is clicked the open file dialog box is opened and where the user can select the secret message. Then the user can select the image file through another open file dialog box which is opened when the image button is clicked. Where the user can select the bmp file and then the Hide button is clicked so that the secret data or message is hidden in Picture through LSB matching revisited technique.

Decryption Module - This module is the opposite as such as Encryption module where the Key file should be also specified same as that of encryption part. Then the user should select the encrypted image and then should select the extract button so that the hidden message is displayed in the text area specified in the application or else it is extracted to the place where the user specifies it.

In that case by changingone bit plane in a pixel, two bits of message should betransmitted. In our method there are only three ways that apixel is allowed to be changed:

- Its least significant Bit would alter (So the gray level of the pixel would increased or decreased by one level)
- The second less significant bit plane would alter (So the gray level of the pixel would increase or decrease by two levels)
- The fourth less significant bit plane would alter (So the gray level of the pixel would increase or decrease by eight levels)

So

Correct Detection rate = (nss + ncc) / ntot
ntot= nss + ncc + nsc + ncs
nss = number of stego image which detected as stego
ncc = number of cover image which detected as cover.
nsc = number of stego image which detected as cover.
ncs = number of cover image which detected as stego.

Although this number is included in the first 8 bytes of the grid, only 3 underline bits need to be changed according to the embedded message. Since each primary color has 256 intensities, only half the bits of the image need to be modified to hide the secret message with the maximum cover size, changing the LSB of the pixel causes small changes in color intensity.These changes are incomprehensible to the human eye - so the message is successfully hidden. With a well-chosen image, the message can be hidden even from the second most important bit, but still no difference is visible. To increase security and the size of stored data, new custom LSB technology is used. Instead of storing data in all important pixels, the host tries to use more than one in the pixel without affecting the visual appearance

of the image. It uses side information of neighboring pixels to calculate the number of bits that can be carried in pixels of the host-image to hide confidential data.

B. LSB module- Set 2

Description: Two sub-modules are developed in this module. One of them is the encryption module and the decryption module. These two sub-modules are the main focus of the application.

Encryption Module - An encryption module that contains a key file section where the key file can be specified as a password with special security. The user can then type in the data or even upload the data with the browse button, clicking on it will open the Open File dialog box and allow the user to select the secret message. The user can select the image file through another open file dialog box that opens when the image button is clicked. Users can select the BMP file and click the Hide button to hide the confidential data or message in the image via the LSB Matching Revised Technique.

Decryption module - This module is the opposite of the encryption module, where the key file must be specified in the same way as the encryption part. The user can then select the encrypted image and select the Extract button to display the hidden message in the text area specified in the application or capture it to the location specified by the user.

LSB reinforcement is a known steganographic method. In this embedding scheme, only the LSB level of the cover image is replaced with a secret bit stream according to the pseudorandom number generator (PRNG). As a result, some structural inequality (always reducing pixels when data is hidden, increasing strange pixels) has been introduced, so it is very easy to detect the presence of a hidden message even at low embedding rates with some reported stagnation algorithm.

LSB Matching (LSBM) uses minor modification to replace LSB. If the secret bit does not match the cover image's LSB, + 1 or - 1 will be randomly added to the corresponding pixel value. Statistically, each modified pixel has the same ability to increase or decrease the value, so the obvious asymmetric hand-held objects introduced by the LSB re-establishment can be easily avoided. The purpose of this paper is only going to change a little bit.

2. CONCLUSION

With the advent of digital cameras and the advent of high speed internet distribution of electronic image information, image steganography has become more popular than any other type of steganography in recent years. It uses a compatible LSB recovery method to effectively hide data. Safe in the picture. In this paper, a variety of images are used as cover images and all types of data such as video and audio are stored and retrieved with good accuracy. Adaptive LSB technology works more efficiently with security and accuracy than traditional LSB technology. Analyzing the sound of images is another method we cannot explore. Adding hidden data adds random sound, so a properly tuned voice detection algorithm can detect whether an image has steganographic data. This paper maintains the spatial data of the cover image. By utilizing the features of DCT, frequency envies virtues can be effectively used to hide confidential data that is more resistant to noise.

3. REFERENCES

[1] WeiqiLuo,FangjunHuang,Jiwu Huang, “Edge Adaptive Image Steganography Based on LSB Matching Revisited”, IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, June 2019.

[2] S. Manikandan, K. ManikandaKumaran, ''Performance Analysis of Mobile Ad-Hoc Network Routing Protocols using Network Simulator – 2", COMPUSOFT, An International Journal of Advanced Computer Technology, ISSN:2320-0790, Vol.03, Issue: 06, pp-957-960, June-2014.

[3] Chan,C.K.,Cheng,L.M.,"Hiding data in images by simple LSB Substitution", Patteren Recognition 37,469-474,2014.

[4] Chang, C.C.,Lin.,M.H.,Hu, ?Y.-C., "A fast and secure image hiding scheme based on LSB substitution", Int.Journal of Pattern Recognit. AndArtif.Intell.16(4),399-416,2018.

[5] S.Manikandan and Mr. S. Pasupathy, "An Efficient Streaming-Application on Distributed Hybrid Cloud Platforms", International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682,Vol.3, No.2, February'2019.

[6] Suk-Ling Li, Kai-Chi Leug, L.M. Cheng, Chi-kwong Chan, performance Evalution of a Steganographic Method for Digital images Using Side Match, icicic 2006, IS16-004,Aug 2016.

[7] J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2016.

[8] Westfeld and A. Pfitzmann, "Attacks on steganographicsystems,"in*Proc. 3rd Int. Workshop on Information Hiding*, 2017, vol. 1768, pp.61–76.

[9] S. Manikandan, K. Raju, R. Lavanya, R. G. Gokila, "Bluetooth based Face-to-Face Proximity Estimation on Smart Mobile", Journal of Android and IOS Applications and Testing, Vol.2, Issue-1, pp-1-4,2017

[10] 10. S. Manikandan, P.Suganya, K. Raju, P.Ponnaruvi, "Object Removal and Error Concealment Using Mean Shift Algorithm in Free Moving Camera Videos", EIJO Journal of Engineering, Technology And Innovative Research (EIJO–JETIR), ISSN: 2455 - 9172, Volume – 1, Issue – 2, May - June 2016, Page No. : 05 - 08.