ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 10, Issue, 06(I), pp. 33294-33297, June, 2019

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

NETWORK DATA SECURITY USING LSB STEGANOGRAPHY

***RusiaRituraj, [1]Mishra Bharat and [2]Tiwari, RK**

*Ph.D. (CS) Research Scholar, MGCGVV, Chitrakoot (MP) India
[1]Department of Physical Science, MGCGVV, Chitrakoot (MP) India
[2]Department of Physics, Govt. M. S. Golvalkar College, Rewa (MP) India

DOI: http://dx.doi.org/10.24327/ijrsr.2019.1006.3645

ARTICLE INFO

Article History:
Received 10th March, 2019
Received in revised form 2nd April, 2019
Accepted 26th April, 2019
Published online 28th June, 2019

Key Words:

Cryptography, Steganography, Stego-image, Data Hiding, Encryption, Decryption, Multimedia Information, Embedding, etc.

ABSTRACT

In the past few years, number of applications are developed to access multimedia systems and content over web. The security and integrity of information, has become one of the most needful problem for sharing secure information over web. Steganography is a means to achieve this task.
In this paper, the hash function has been implemented and integrated into a secure package to protect multimedia information through the network. The hash function uses the LSB (Least Significant Bit) method. The algorithm has been tested with own made steganography application in the windows environment. It has been proved that extracting any information from embedded image is hard for any eavesdropper with computational resources.

INTRODUCTION

A picture is an image, that has been completed or copied and set away in electronic structure. A picture can be delineated to the extent that vector structures or raster outlines. A photograph is a social event of numbers that involve unmistakable light powers in different domains of the image. This numeric depiction shapes a system and the individual point of convergence is suggested as pixels (picture part). Grayscale pictures utilize 8 bits for every pixel and can demonstrate 256 intriguing colors or colors of dull. Digital color photographs are regularly verified in 24-bit records and utilize the RGB color model. All color groupings for the pixels of a 24-bit picture are taken from three crucial tints: RGB and every fundamental shading are tended to by 8 bits. As necessities are in one given pixel, there can be 256 x 256 x 256 uncommon proportions of RGB [1][2][3].

Steganography, is an art of concealing secure information in the image pixels. In this technique we can embed the text information bits into the image pixel bits and protect over secreate information from the eavesdropper at the time of communicating information through network. The fundamental point in stego is to hide the very presence of the message in the spread medium. To implement the steganography, we can use LSB techniques to hide information bits into the image pixel bits [4]. Steganography is the art of communicating messages by embedding them into multimedia data or digital images. It is desired to maximize the amount of hidden information while preserving security against detection by unauthorized persons. Steganography system Like the Least Significant Bit "LSB" should fulfil the same requirements posed by the "Kerckhoff principle" in cryptography [5].

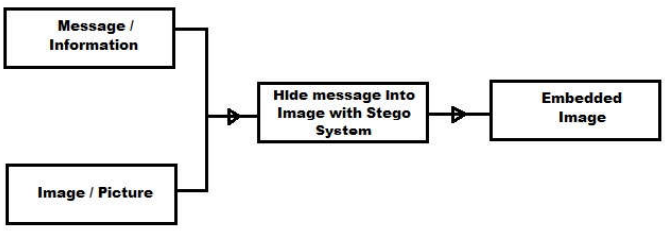

Figure 1 Process of Embedding message into image

Corresponding author:* **Rusia Rituraj,
Ph.D. (CS) Research Scholar, MGCGVV, Chitrakoot (MP) India

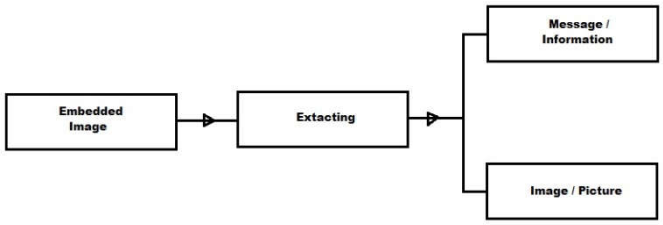

Figure 2 Process of Extracting

Related Work

Patil S. S., *et. al*. (2016), the study shows that the authors provided a new method known as multi-stage mystery statistics hiding which integrates two exceptional techniques of encryption, particularly: able to be seen cryptography and steganography. The initial step of this methodology is to apply a strategy alluded to as half conditioning, which is utilized to diminish the pixels and improve the preparing. There after obvious cryptography is performed. It delivers the offers which structure the essential dimension of security, and afterward steganography is connected utilizing the LSB plan to conceal the offers in various media like picture, sound, and video [6].

Karthikeyan B., *et. al*. (2016), This study shows that the paintings present a way based totally on combining both sturdy encryption set of rules furthermore, steganographic procedure to create the correspondence of elite records protected, loose and phenomenally difficult to disentangle. An encryption set of principles is employed first to scramble the SM sooner than encoding it into a QR code. The encoded picture is mixed to accomplish a new safety plane. The mixed QR code is at some point or another installed in an appropriate cowl photograph, which is then exchanged safely to supply the name of the amusement measurements. They connected an LSB strategy to play out the DI steganography. At the collector's viewpoint, the mystery measurements is recovered through the unraveling procedure. Along these lines, a four-degree security has been rendered for a SM to be exchanged [7].

Padmavathi, *et. al*. In this study, she directed an exhibition investigation study on different calculations like DES and AES, RSA consolidating with LSB swap procedure which serves well to reach determinations on the 3 encryption methods dependent on their exhibitions in any application. It has been concluded from their work that AES encryption is superior to anything different strategies as it represents less encryption, unscrambling times and furthermore utilizes fewer cradle gaps [8].

Kaustubhchoudhary *et. al*. displayed a definite write about picture properties in LSB plane. His work delineates the bit plane cutting framework in detail, which shortens the significances of MSB and LSB planes of a picture [9].

Proposed Methodology

Stego-keys are used to generate the stego-tables and table indices. In 24-bit images, to hide an image in the LSBs of each byte of a 24-bit image, can store 3 bits in each pixel (RGB). For example, the letter C can be hidden in three pixels. The original raster data for 3 pixels (9 bytes) may be (the highlighted bits are the least significant bit in each byte):

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for letter C is 01000011. Inserting the binary value for C in the three pixels would result as

(00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001001 00100111 11101001)

The underlined bits are the only four actually changed in the eight bytes used. In average, for LSB technique requires that only half the bits in an image be changed. We can hide data in the least and second least significant bits and still the human eye would not be able to discern it. Here is an example in a large scale of 1024 x 768.

Figure 3 Cover Image in PNG format.

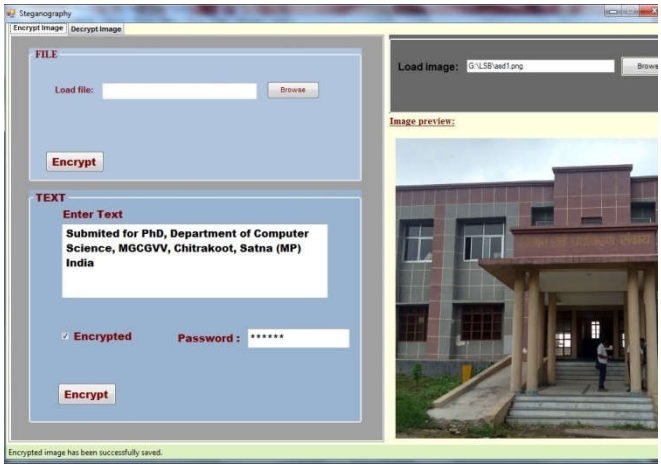

Figure 4 Encryption process

Package shows at the time of encryption. In this process hide or embed the text into the cover image with an encrypt password.

Figure 5 Embedded image in PNG format

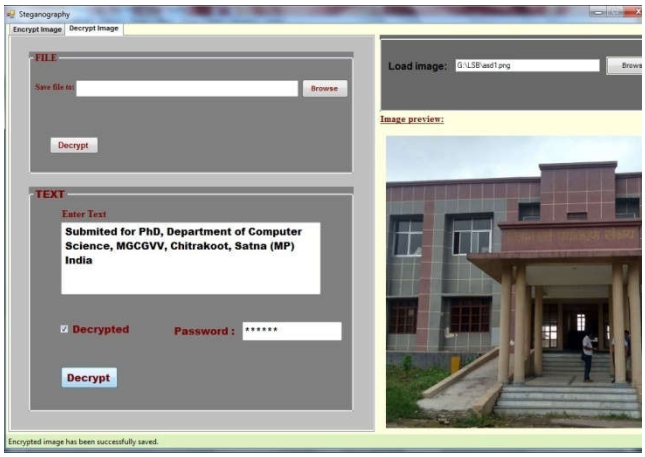

Figure 6 Decryption process

Package shows at the time of decryption. In this process extract text information from the embedded image with a decrypt password. If password is wrong, then decrypt text as garbage text.

RESULT DISCUSSION

The proposed scheme is implemented in Visual Studio platform using standard LSB.Description/Comparison between cover image and embedded image.

Table 1 Description/Comparison between Cover Image and Embedded Image

Sr.	Particulars	Cover Image	Embedded Image
1	File format	.PNG/.JPG/other image format	.PNG
2.	File Size (in KB)	3314	15826

We are using MATLAB platform for PSNR and MSE calculation.

Table 2 Calculation parameters

Parameter	With .JPG cover image	With .PNG cover image
PSNR	84.97	114.78
MSE	0.0054	0.000176

A 1024 x 768 image has the potential to hide a total of 2,359,296 bits (294,912 bytes) of information and a 1024 x 768 image has the potential to hide a total of 1,656,792 bits (207,099 bytes) of information. The relative entropy between the cover image and the stego image is zero. The resulting stego and the cover images should be indistinguishable by the naked eye.

CONCLUSION

An advantage of the proposed scheme is that the extracting algorithm is simple and easy to implement. When receiving a stego-image, the receiver uses the same stego-keys to generate the same stego-tables and table indices as those used in the embedding process to extract the originally encrypted data. Then decryption and decompression procedures are consequently done to obtain the plaintext.

Here, we presented an implementation to a package that contains LSB technique using hash functions steganography. This package can be used to deal, secure multimedia in communication channels as in the Internet. We need to protect themselves from theft and false representation to information.In presented Secured Package Machinery achieved the two cryptographic principals' objectives: (i) Secrecy or privacy, to prevent the unauthorized disclosure of data and (ii) Authenticity or integrity, to prevent the unauthorized modification of data. If a message is encrypted and then embedded in an image, it becomes even more secure. If an encrypted message is intercepted, by the unauthorized person knows the text is an encrypted message. Nevertheless, with steganography, the unauthorized person may not know that a hidden message even exists.

Reference

1. Hunt R.W.G., "Bits, Bytes, and Square Meals in Digital Imaging", Proceedings of IS&T/SID Fifth Color Imaging Conference: Color Science, Systems, and Applications,pp. 1-5, 1997.
2. Ohno Shin, "Color in Digital Photography, Color Quality of Digital Photography Prints", Proceedings of IS&T/SID Fifth Color Imaging Conference: Color Science, Systems, and Applications, pp. 100-104, 1997.
3. Mintzer Fred, "Developing Digital Libraries of Cultural Content for Internet Access", IEEE Communications Magazine, v37, pp. 72-78, Jan 1999.
4. Mohammed A.F. Al-Husainy, "Image Steganography by Mapping Pixels to Letters", Journal of Computer Science, ISSN: 1549-3636, pp. 33-38, 5(1), 2009.
5. Anderson Ross J., Petitcolas Fabien A.P., "On the Limits of Steganography", *IEEE Journal of Selected Areas in Communications*, pp. 474-481, 16(4), May 1998.
6. Patil S. S. and Goud S., "Enhanced multi-level secret data hiding", 2016.
7. Karthikeyan B., Kosaraju A. C., Gupta S., "Enhanced security in steganography using encryption and quick response code",International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 2308-2312, IEEE 2016.

8. Padmavathi B., RanjithaKumari S., "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution", *International Journal of Science and Research* (IJSR), India Online ISSN: 2319-7064, pp. 170-174, 2(4), Apr 2013.
9. KaustubhChoudhary,"Properties of Images in LSB Plane", *IOSR Journal of Computer Engineering (IOSRJCE)*, ISSN: 2278-0661, pp. 08-16,3(5), Jul-Aug 2012.

How to cite this article:

RusiaRituraj, Mishra Bharat and Tiwari, RK., 2019, Network Data Security Using Lsb Steganography. *Int J Recent Sci Res.* 10(06), pp. 33294-33297. DOI: http://dx.doi.org/10.24327/ijrsr.2019.1006.3645

****