International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Secure Image Steganography Using Bit Shift Encryption & MLSB Approach

Raminder Jit Singh Kahlon[1], Vinay Bhardwaj[2]

[1]Research Scholar, SGGSWU

[2]Assistant Professor, SGGSWU

Abstract: ***Steganography is a technique for the secure transmission of data over the network. In this process, the secret information is transmitted by hiding this behind a signal or image or video. Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us. In this process, the secret information is transmitted by hiding this behind a signal or image or video. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format. There is a limit to the size of a file which you can embed information into. There is no provision for encryption in Least Significant Bit (LSB). The main motivation behind the work is that to make LSB more detectable and more secure and also the data that is sent behind the image is in more quantity.***

Keywords: Stegnography, Image Stegnography, LSB, MLSB, Security, Data Hiding

1. Introduction

1.1 Steganography

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing defining it as "covered writing". In image steganography the information is hidden exclusively in images. The idea and practice of hiding information has a long history. In History the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels [7].

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret.

Figure 1.1: Stenography

Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

1.2 Different Kinds of Steganography

1.2.1 Text stenography: Hiding information in text is the most important method of steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance.

1.2.2 Image stenography: Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key.

1.2.3 Audio stenography: Audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.

1.2.4 Video Steganography: Video Steganography is a method to conceal any sort of records into a convey. Video document. The utilization of the feature based Steganography can be more qualified than other interactive media documents, on account of its size and memory prerequisites. Video Steganography is a system to hide any sort of records in any extension into a carrying Video file.

1.3 Steganographic Techniques

1.3.1 Substitution Technique: In the substitution technique; the redundant parts are covered with a secret message. This technique includes the Least Significant Bit Substitution method, where we choose a subset of cover elements and substitute the least significant bits of each element by the message bits .Message may be encrypted or compressed before hiding.

1.3.2 Transform Domain Technique: In the transfer domain technique; the secret message is embedded in the transform space (e.g. frequency domain) of the cover. An example of this method includes the Discrete Cosine Transform (DCT) domain. The cover image is split into 8*8 blocks and each block is used to encode one message bit.

1.3.3 Spread Spectrum Technique: This technique uses the concept of spread spectrum. The message is spread over a wide frequency bandwidth. The signal to noise ratio in every frequency band is so small that it is difficult to detect. Even if parts of message are removed from several bands, enough information is present in other bands to recover the information.

1.3.4 Statistical Techniques: In the statistical techniques, the information is encoded by changing several properties of the cover. The cover is split into blocks and each block is used to hide one message bit .If the message bit is one, then the cover block is modified otherwise the cover block is not modified. This technique is difficult to apply because a good test must be found that allows for proper distinction between modified and unmodified cover blocks.

1.3.5 Distortion Techniques: The information is stored by distorting the signal. The encoder applies a sequence of modifications to the cover. This sequence corresponds to the secret message. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message. This method is not used in many applications because the decoder must have access to the original cover.

1.3.6 Protection of Data Alteration: We take advantage of the fragility of the embedded data in this application area. If it is implemented, people can send their "digital certificate data" to any place in the world through Internet. No one can forge, alter, nor tamper such certificate data. If forged, altered, or tampered, it is easily detected by the extraction program.

1.4 Applications of Steganography

- Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.
- It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside [5].
- Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, Steganographic methods can be used to hide this.
- E-commerce allows for an interesting use of steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open ecommerce transaction verification.
- Paired with existing communication methods, steganography can be used to carry out hidden exchanges. Governments are interested in two types of hidden communications: those that support national security and those that do not. Digital steganography provides vast potential for both types. Businesses may have similar concerns Regarding trade secrets or new product information.
- The transportation of sensitive data is another key use of steganography. A potential problem with cryptography is that eaves droppers know they have an encrypted message when they see one. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites [13].

2. Literature Review

G.R.Manjula et al (2015) This paper presents a novel 2-3-3 LSB insertion method. The image steganography takes the advantage of human eye limitation. It uses color image as cover media for embedding secret message. The important quality of a steganographic system is to be less distortive while increasing the size of the secret message. In this paper a method is proposed to embed a color secret image into a color cover image. A 2-3-3 LSB insertion method has been used for image steganography. Experimental results show an improvement in the Mean squared error (MSE) and Peak Signal to Noise Ratio (PSNR) values of the proposed technique over the base technique of hash based 3-3-2 LSB insertion [2].

Bailey and Curran (2006) Author described an image based multi-bit steganography technique to increase capacity hiding secrets in number of bits, i.e. Stego-1bit, Stego-2bits, Stego-3bits and Stego-4bits. Stego-1bit is the simplest of this, where it inserts the secret message data into one MLSB (lower order bit) of the image pixels, which is undetectable. It is known that insertion of hidden bits into lowest order MLSB in all color RGB channels of the image pixels is unnoticeable. In the Stego-2bits method two bits of lower order MLSB in RGB image steganography is used; Stego-2bits doubled the capacity of message hiding with negligible security reduction [3].

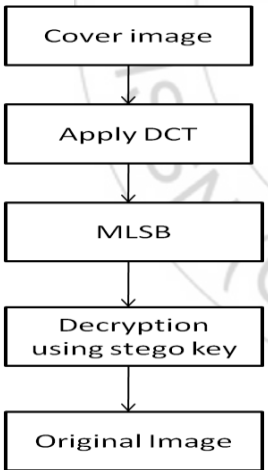
Chapman, M. Davida G, and Rennhard M. et al (2011) Author want to propose that most of the data hiding methods in image steganography used a technique utilizing the Least Significant Bits (LSB) of the pixels, i.e. the LSB of each

pixel is replaced to hide bits of the secret message. This, normally, produce changes in the cover media but with no significant effect. All the LSBs of pixels of cover image can be used for hiding the secret bits [4].

Gutub et al. (2010) Author described if the first indicator selection is the Red channels in the pixel, the Green is channel 1 and the Blue is the channel 2 i.e. the sequence is RGB. In the second pixel if we select, Green as the indicator, then Red is channel 1 and Blue is channel 2 i.e. the sequence is GRB. If in third pixel Blue is the indicator, then Red is channel 1 and Green is channel 2. The sequence of the algorithm is given below. The first 8 bytes at the beginning of the image are used to store the size of the hidden message, which is also used to define the beginning of the indicator channel sequence [6].

Debiprasad Bandyopadhyay et al (2014) This paper presents a novel approach of building a secure data hiding technique in digital images. The image steganography technique takes the advantage of limited power of human visual system (HVS). It uses image as cover media for embedding secret message. The most important requirement for a steganographic algorithm is to be imperceptible while maximizing the size of the payload. In this paper a method is proposed to encrypt the secret bits of the message based on chaos theory before embedding into the cover image. A 3-3-2 LSB insertion method has been used for image steganography [7]

3. Methodology



Steganography is done for secure transmission of data on network. Various phases for data steganography are described below:

Phase 1: Select on cover image for data embedding cover image should be a color image containing red, green and blue pixels.

Phase 2: In the second phase apply modified least significant bits

- Decompose the cover image into different bands i.e. LL,LH,HH,HL
- Convert into integer value using threshold
- Embed the secret message in the middle using modified MLSB
- Obtain stego-image.

Phase 3: In this phase extract secret data using the stego-key and convert the duplicate message into original message. This recovery of the duplicate audio/video/image can be done using encoding key. In the last we get the original message.

4. Results and Discussions

Table 4.1: Parameters Comparison on the basis of PSNR

Image	(MLSB)	(4LSB)
Image 1	41.68	26.69
Image 2	45.69	35.40
Image 3	49.98	39.56
Image 4	53.78	48.45
Image 5	43.48	28.56

Table 4.1 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. The parameter PSNR has been evaluated for different images and values has been represented in tabular form for proposed and existing technique .

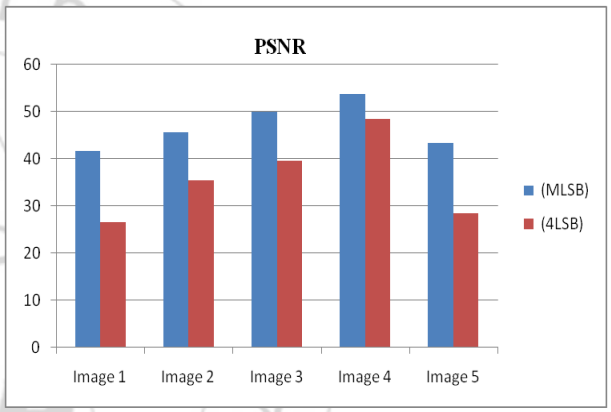


Figure 4.1: Comparison graph of proposed work with exiting using PSNR

Fig.4.1 represents graphical representation of performance evaluation parameter correlation with existing approach. As graph represents proposed wok provide better PSNR than existing approach.

Table 4.2: Parameters Comparison on the basis of MSE

Image	(MLSB)	(4LSB)
Image 1	6.58	10.69
Image 2	2.36	9.24
Image 3	5.69	15.36
Image 4	3.59	8.69
Image 5	4.36	9.38

Table 4.2 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. The parameter MSE has been evaluated for different images and values has been represented in tabular form for proposed and existing technique .

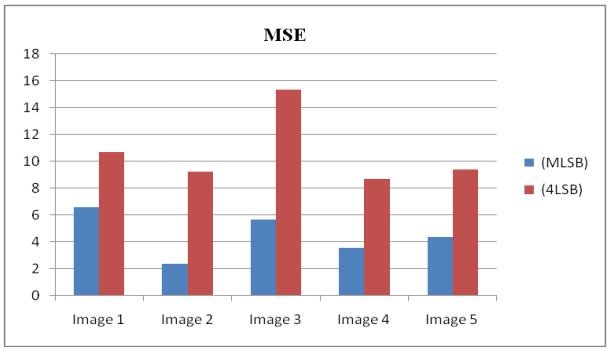


Figure 4.2: Comparison graph of proposed work with exiting using MSE

Fig.4.2 represents graphical representation of performance evaluation parameter MSE with existing approach. As graph represents proposed work provide less mean square error than existing approach.

Table 4.3: Parameters Comparison on the basis of SSIM

Image	(MLSB)	(4LSB)
Image 1	0.92	0.87
Image 2	0.95	0.89
Image 3	0.98	0.93
Image 4	0.91	0.81
Image 5	0.96	0.90

Table 4.3 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. The parameter SSIM has been evaluated for different images and values has been represented in tabular form for proposed and existing technique

Figure 4.3: Comparison graph of proposed work with exiting using SSIM

Fig.4.3 represents graphical representation of performance evaluation parameter SSIM with existing approach. As graph represents proposed wok provide better SSIM than existing approach.

Table 4.4: Parameters Comparison on the basis of Correlation

Image	(MLSB)	(4LSB)
Image 1	0.99	0.91
Image 2	0.98	0.93
Image 3	0.99	0.92
Image 4	0.99	0.92
Image 5	0.97	0.90

Table 4.4 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. The parameter Co-relation has been evaluated for different images and values has been represented in tabular form for proposed and existing technique.

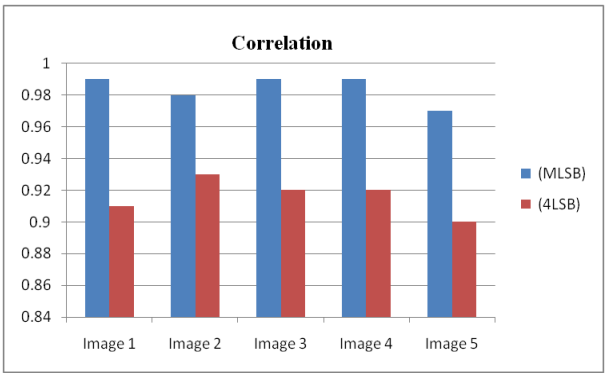


Figure 4.4: Comparison graph of proposed work with exiting using Correlation

Fig.4.4 represents graphical representation of performance evaluation parameter correlation with existing approach. As graph represents proposed wok provide better correlation than existing approach.

5. Conclusion

5.1 Conclusion

Steaganography is the process for hiding secret information behind any cover object for secure transmission of data. In proposed work cover object has been selected for embedding of secret information behind pixels of the object. Cover object has been divided into different color regions from a particular true color image. To develop more secure steagnography user authentication has been validated by the proposed work that embedded a onetime password during embedding process in the cover objects bits. Password has been transmit to only authenticated user via message or mail. User authentication has been checked as the user provide the password for extraction of data. If a valid user provide correct password then he/she is able to extract data from cover object. The proposed work has been compared with various previous approaches on the basis of performance evaluation parameters. As illustrated from results proposed work provides much secure steganography than previous LSB, 2LSB data embedding approaches. So by analyzing parameters one can conclude that proposed work provides much better results than previous approaches utilized for image steganography.

5.2 Future Scope

In the future reference the proposed approach can be used in real world application for secure transmission of secret information. In future, approaches can be developed so that it can be utilized for various color intensity levels for embedding of secret information. Artificial intelligence can be used for extraction of best region for embedding of secret information so that image data will not distort.

References

[1] S. K. Moon "Application of data hiding in audio-video using anti forensics technique for authentication and data security" Advance Computing Conference (IACC), 2014, pp 1110 – 1115.
[2] G.R.Manjula "A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography in Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM), 2015, pp 11-15.
[3] Bailey, K, Chen, L. H.(2006) "An evaluation of image based steganography methods", Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88,IEEE.
[4] Chapman, M. Davida G, and Rennhard M. (2011) "A Practical and Effective Approach to Large Scale Automated Linguistic Steganography" IEEE, VOL. 30, No.2, pp. 67-75
[5] Gutub, A., Kurinji, R.(2008) "Pixel Indicator High Capaciy Technique for RGB Image Based Steganography", WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, U.A.E., pp. 154-159,IEEE.
[6] Gutub, A., Verma, K. ; Sahoo, A.(2010) "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, Vol. 2, No.1, pp. 193-198,IEEE.
[7] Debiprasad Bandyopadhyay Kousik Dasgupta (2014)"A Novel Secure Image Steganography Method Based On Chaos Theory In Spatial Domain" conf. on International Journal of Security, Privacy and Trust Management (IJSPTM),pp-11-22.
[8] Marwaha, P., Marwaha, P.(2010) "Visual cryptographic steganography in images", Second International conference on Computing, Communication and Networking Technologies, pp. 34-39, IEEE.
[9] Mahata, S.K., Gunsch, G.H. ; Claypoole, R.L., Jr. ; Lamont, G.B.(2012) "A Novel Approach of Steganography using Hill Cipher", International Conference on Computing, Communication and Sensor Network (CCSN), pp. 0975-888, IEEE.
[10] Mazen Abu Zaher, Mohammadi, M.(2011) "Modified Least Significant Bit (MLSB)" IEEE Conf. on MLSB, pp. 60-67.
[11] Singh, Gupta, S. ; Saini, S.(2015) "A methodological survey of image segmentation using soft computing techniques", IEEE Conf. on Computer Engineering and Applications (ICACEA), pp. 419 – 422.
[12] Suhad A.H.Al-An, Dubey, R.(2007) "Steganography Image in Image using Modified method in Least Significant Bit (LSB) substitution", IEEE conf. on MLSB, 2007, pp. 65-70.
[13] Androutsos, Plataniotis, K.N. ; Venetsanopoulos,(1997) A.N."Efficient image database filtering using colour vector techniques", IEEE Conf. on Electrical and Computer Engineering, pp.827–830, vol. 2
[14] Mehboob, B.(2009) "A stegnography implementation", IEEE Conf. on Biometrics and Security Technologies, pp. 1-5.