ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

A Proposed Method in Image Steganography using Prime Sequence

Renu[1], Dr. Priti Sharma[2]

M.Tech Student, Department of Computer Science and Application, M.D University Rohtak, Haryana[1]

Assistant Professor, Department of Computer Science and Application, M.D University Rohtak, Haryana[2]

Abstract: Steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Itincludes the concealment of information within computer files. This paper considers an information theoretic model for steganography with a passive adversary being proposed. This paper considers an information theoretic model for steganography with a prime number insertion with being proposed. The adversary's task of distinguishing between an innocent cover message C and modified message S containing hidden information is interpreted as a testing problem. Depending on this evenness, the character is encrypted differently. This paper describes how image degradation improve with this technique as well enhance security with proposed prime technique**.**

Keywords: Cryptography, Least Significant Bit (LSB), Prime Sequence Generator , Steganography.

I. INTRODUCTION

Today networks are seriously threatened by network attacks. Cryptography may be used at different levels of a security model. This paper presents an approach of ASCII based cryptography with LSB based image stenography for security purpose of data transaction in the network and the internet. Here, encryption is applied to the even or odd ASCII value of the character which represents the data. A character in the plain text is always changed to the ASCII value and adding a key value with it gets back the cipher text. This value is then converted to the equivalent binary number. Substitute these bits in the LSB position in each pixel which describes the image. The receiver collects these bits from the image and converting them in equivalent decimal number which is the cipher text and subtracting the key value from it, we get the ASCII value of the plain text.

Converting this ASCII value to the equivalent character representation, we get the original text. A cryptanalyst can normally find the key but in this approach a combination of two prime numbers is used for encryption.

Basic Block Diagram

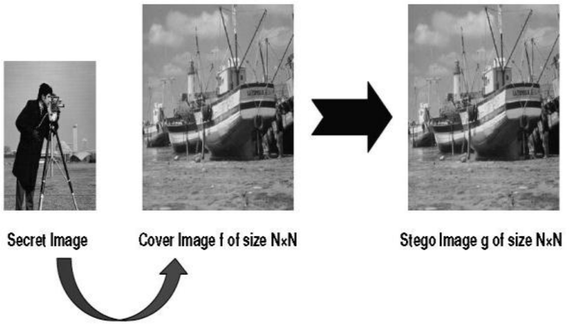


Figure 1. Image Steganography

A. Steganography

Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography means "covered writing" in Greek. As the goal of steganography is to hide the presence of a message and to create a covert channel, it can be seen as the complement of cryptography, whose goal is to hide the content of a message. The object may be an image, audio, video or text only.

1) Image Steganography

Image steganography technique can be divided into two groups: those in the Image domain and those in the Transform Domain . Image domain technique embed message in the intensity of the pixels directly, while for transform domain, images are first transformed and then the message is embedded in the image .

Steganography is a two-step process:

Step 1) Creating a stego image which is a combination of message and carrier

Step 2) Extracting the message image from the stego image.

Variations are in the techniques that are used to generate the stego image using the carrier and the message image. [21] On the sender side, a Cover image is selected and then message is hidden using a secret key and message embedding algorithm. Secret key is basically used to find out the pseudorandom pixel locations where the data will be hidden. Secret key is to be shared between sender and receiver. Thus, it works as password such that even if someone breaks the algorithm then also the message can't be extracted until he/she knows the secret key. Stego image is obtained as output (as shown in Figure).

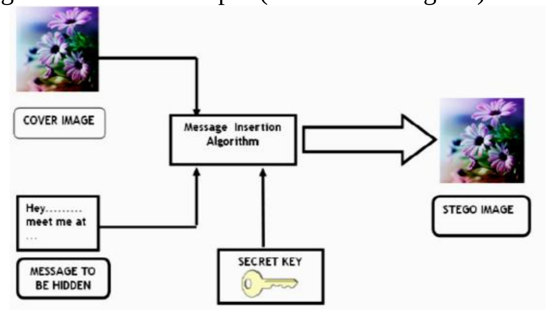


Figure 2: Image Steganography : Message Extract

DOI 10.17148/IJARCCE.2015.4619

On the receiver side, Stego image is taken as input and by using the same secret key and message retrieval algorithm, message is extracted (as shown in Figure 3).

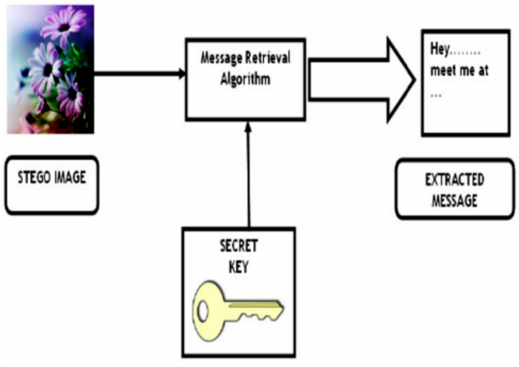


Figure 3: Image Steganography : Message Retrieval

II. EXISTING TECHNIQUES & MODEL

B. LSB (Least Significant Bit) method

It is one of the most common and easiest methods for message hiding. In this method, message is hidden in the least significant bits of image pixels .Changing the LSB of the pixels does not introduce much difference in the image and thus the stego image looks similar to the original image. In case of 24-bit images three bits of pixel can used for LSB substitution as each pixel has separate components for red, green and blue.

Advantages:
1.) Simplest and easiest to implement.
2.) Chances of message insertion are 100%.

Drawbacks:
1.) Not vulnerable to different attacks.
2.) Intruder can easily guess and change the LSB's of the image pixels, thus original message gets destroyed.
3.) Causes some distortion in the original image
4.) Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image will destroy the message

C. Masking and Filtering

Basically, this method is used for 24-bit and grey scale images. It is similar to placing watermarks on the image. Steganography only hides the information where as watermarks becomes part or attribute of the image. This ethod is more robust than LSB in terms of some image processing like - compression, cropping which makes it suitable in lossy JPEG images. Masking images involves changing the luminance of the masked area.

Advantages:
1.) Immune to image manipulation
2.) Robust technique

Drawbacks:
This method is mostly used for only 24 bit and grey scale images.

D. Parity Checker Method

In this method, concept of even and odd parity is used. '0' is inserted at pixel value when it contains odd parity i.e. no. of 1's in the binary value of pixel must be odd similarly, '1' is inserted at pixel value if it contains even parity i.e. no. of 1's in the binary value of the pixel must be even. If the corresponding parity does not exist at pixel location for 0 or 1 then it is made by adding or subtracting 1from the pixel value. For retrieval of message, if odd parity is present, then '0' is the message bit and if even parity is present, then '1' is the message bit.

Advantages:
1.) Increases chances of message insertion.
2.) Steganalysis is difficult because whole pixel is used instead of particular bits as used by LSB method.
3.) Difference between cover image and stego image is difficult to be observed by naked eye.

Drawbacks:
1.) If intruder changes the LSB, then parity also changes and thus the method fails.
2.) In some situations when odd or even parity not present, then it can be made by both +1 or -1. So, it creates confusion, which one to choose.

E. Pixel value Differencing (PVD) technique

In this method, Wu & Tsai selected two consecutive pixels for embedding the message. By checking the difference between two consecutive pixels ,payload of Wu and Tsai method is determined and it serves as basis to find out whether the two pixels belongs to an edge area or smooth area. If the difference is large, it means pixels belong to an edge area and more secret data can be embedded at this location. On the other hand, if difference is small, it means pixels belong to smooth area and less secret data can be embedded at this place. If the original difference value is unequal to the secret message, then the two consecutive pixels are directly adjusted so that the difference value can stand for the secret data.

Advantages:
1.) Works better than LSB which directly embed secret data without considering the difference between the two pixels.
2.) Stego images produced are very much similar to the original image.

Drawbacks:
1.) Considerable stego image distortion can occur when the PVD method adjusts the two consecutive pixels in order to hide the secret data in the difference value.
2.) Falling off boundary problem may occur when the two consecutive pixels are located in extreme edge or smooth areas or when the values of two consecutive pixels contrast.

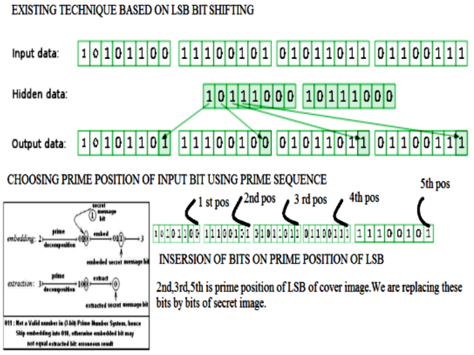

EXISTING TECHNIQUE BASED ON LSB BIT SHIFTING
Input data:
1 0 1 0 1 1 0 0 | 1 1 1 0 0 1 0 1 | 0 1 0 1 1 0 1 1 | 0 1 1 0 0 1 1 1
Hidden data:
1 0 1 1 1 0 0 0 | 1 0 1 1 1 0 0 0
Output data:
1 0 1 0 1 1 0 1 | 1 1 1 0 0 1 0 0 | 0 1 0 1 1 0 1 1 | 0 1 1 0 0 1 1 1
CHOOSING PRIME POSITION OF INPUT BIT USING PRIME SEQUENCE
1 st pos
2nd pos
3 rd pos
4th pos
5th pos
secret message bit
embedding: 2 prime decomposition 010 embed 011 3
embeded secret message bit
extraction: 3 prime decomposition 100 extract 0
extracted secret message bit
011 : Not a Valid number in (3-bit) Prime Number System, hence Skip embedding into 010, otherwise embedded bit may not equal extracted bit: erroneous result
INSERSION OF BITS ON PRIME POSITION OF LSB
2nd,3rd,5th is prime position of LSB of cover image.We are replacing these bits by bits of secret image.

Figure 4 : Existing Technique Bases On LSB Bit

DOI 10.17148/IJARCCE.2015.4619

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

III. PROPOSED MODEL

A. Prime sequence

First, we need to find a number n belongs N such that all possible pixel values in the range [0; 2k ¡1] can be represented using first n natural numbers in our n-bit prime number system, so that we get n virtual bit-planes after decomposition. To find the n is quite easy, since we see, and we shall prove shortly that, in n-bit Natural Number System, all the numbers in the range [0; n(n+1)=2] can be represented. So, our job reduces to finding an n such that n(n+1) 2 ¸ 2k ¡ 1, i.e., solving the following quadratic in-equality n2 + n ¡ 2k+1 + 2 ¸ 0.

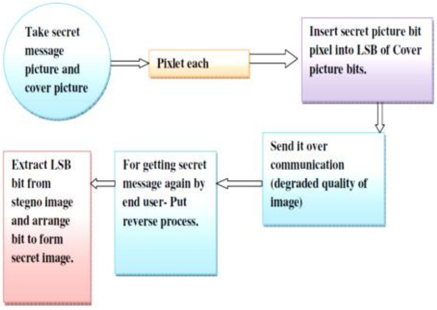
$$=> n \geq \frac{-1+\sqrt{2^{k+3}+9}}{2}, n \in Z^{+}$$

To n-bit numbers (natural number decomposition), n > k, marking all the valid representations (as discussed in previous section) in our natural number system. For an 8-bit image the set of all possible pixel-values in the range [0; 255] has the corresponding natural number decomposition. For k = 8, we get,

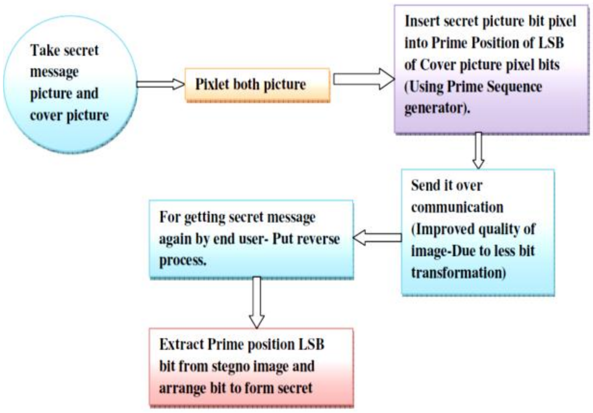
$$n \geq \frac{-1+\sqrt{2^{8+3}+9}}{2} = \frac{-1+\sqrt{2057}}{2} = \frac{44.35}{2} = 22.675 \Rightarrow n = 23$$

Hence, for an 8-bit image, we get 23 (virtual) bit-planes. If we recapitulate our earlier result, as we see from the map, in case of prime decomposition, it yields much less numbers of (virtual)bit planes (namely . Again it is noteworthy that the space to store the map is still increased. Although this computation of the map (one-time computation for a fixed value of k) is slightly more expensive and takes more space to store in case of our natural number decomposition than in case of prime decomposition, the first outperforms the later one when compared in terms of steganographic efficiency, i.e., in terms of embedded image quality, security (since number of virtual bit-planes will be more in case of the first) etc, as will be explained shortly. Next, for each pixel of the cover image, we choose a (virtual) bit plane, say pth bit-plane and embed the secret data bit into that particular bit plane, by replacing the corresponding bit by the data bit, if and only if we find that after embedding the data bit, the resulting sequence is a valid representation in n-bit prime number system, i.e., exists in the map otherwise discard that particular pixel for data hiding.

B. Existing work model

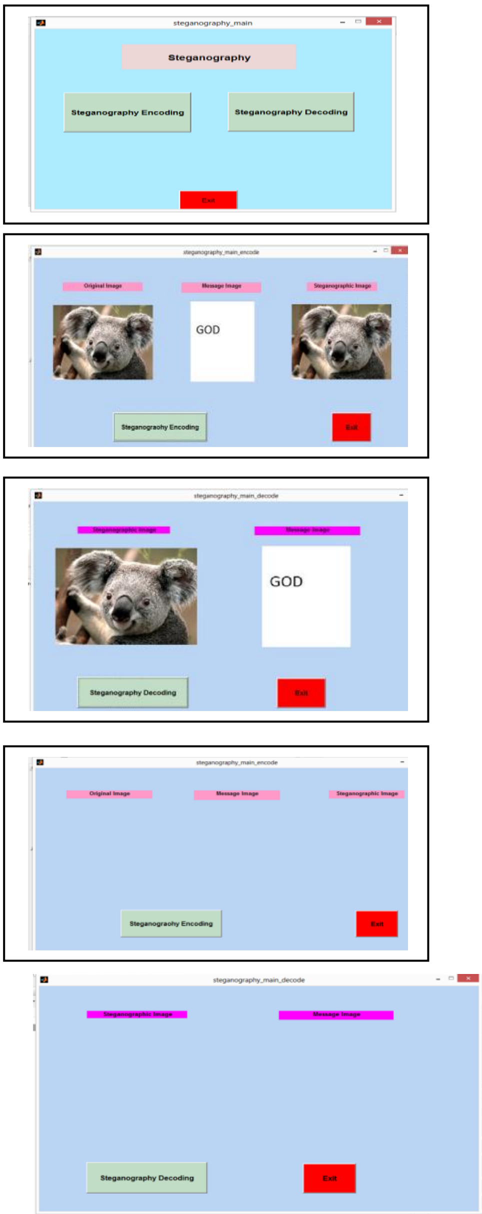

Take secret message picture and cover picture
Pixlet each
Insert secret picture bit pixel into LSB of Cover picture bits.
Send it over communication (degraded quality of image)
For getting secret message again by end user- Put reverse process.
Extract LSB bit from stegno image and arrange bit to form secret image.

C. Proposed work model


Take secret message picture and cover picture
Pixlet both picture
Insert secret picture bit pixel into Prime Position of LSB of Cover picture pixel bits (Using Prime Sequence generator).
Send it over communication (Improved quality of image-Due to less bit transformation)
For getting secret message again by end user- Put reverse process.
Extract Prime position LSB bit from stegno image and arrange bit to form secret

After embedding the secret message bit, we convert the resultant sequence in prime number system back to its value) and we get our stego-image.

3.4 Simulation work



All above figure shows layout of GUI.

DOI 10.17148/IJARCCE.2015.4619

III. RESULT UNDER TESTING PROCESS

In testing we takes five cover images and messages to be hiding then we notice size of CI,MI and EI the result will be shown:

	CI size	MI size	CI size After Extraction	Decode	Result
1	16.5mb	14.1kb	16.5mb	No change	100%
2	2.92 mb	10kb	2.92mb	No change	100%
3	436kb	4.84kb	436kb	No change	100%
4	271kb	11.4kb	271kb	No change	100%
5	1.37 mb	11.4 kb	1.37mb	No change	100%

In our trail we are taking different cover image and message image then we noted the size and write in table and after process encoding and decoding .That means first encode and then decode the cover image and note the size of cover image and message image before encoding and then single encoded message that comes after the insertion of message into cover image. And again note the size of pics that comes after the decoding. After evaluation,the above table clearly justify our experimental success on the basic of above trails. The model is based on prime number sequence insertion Which give every effective encoding and decoding result as above result comes.

IV. SECURITY AND CONCERN

There is nothing common in between two numbers rather than both of them are odd prime number. If one number is known to the adversary, he cannot deduce the other number. In case of a 32 bit machine (long integer of 32 bits), each number can be 32 bits long. If one number is fixed, the other number can be any one of 232 possibilities and the first number can be one of 232 possibilities. So the number of possible alternatives becomes 32*32 = 264. Trying possible alternatives are not so easy. Further the steganography itself will hide the converted information in a secured way so that human eye cannot easily detect it.

In this paper a specific secret-key image based data hiding model has been proposed which uses an image as the cover data and the secret information is embedded in the cover to form the stego image.

V. CONCLUSION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. After applying the prime number sequence algorithm we can get very good result in loss of degradation of image and better security that earlier one. Applying prime sequence generator over the algorithm and coding give a very clear image of secret image.

Due to unpredictability of prime sequence of insertion of bits it is quite hard to break out the position of bits by any introducer. So it has very hard to detect the inserted message code from stegno image whatever one can have the full idea of amalgamation. Over all we can have very good approach to work on steganography.

REFERENCES

[1] R.C. Merkle and M. Hellman, Hiding Information and Signatures in Trap Door Knapsacks, IEEE Trans. Inform. Theory, vol 24 1978, pp 525-530.

[2] Souvik Bhattacharyya. and Gautam Sanyal. Study of secure Steganography model In Proceedings of International Conference on Advanced Computing and Communication Technologies (ICACCT-2008), Panipath , India 2008.

[3] G. Simmons, The prisoners problem and the subliminal channel, CRYPTO, 1983

[4] Souvik Bhattacharyya. and Gautam Sanyal. An Image Based Steganography Model for Promoting Global Cyber Security. In Proceedings of International Conference on Systemics, Cybernetics and Informatics, Hyderabad, India , 2009.

[5] J.Silman,Steganography and Steganalysis:An Overview,SANS Institute, 2001

[6] Raja K B, C R Chowdary, Venugopal K R, L M Patnaik. (2005) :"A Secure Steganography using LSB, DCT and Compression Techniques on Raw Images," IEEE International Conference on Intelligence Sensing and Information processing, pp.171-176.

[7] Kumar V and Kumar D. (2010): "Performance Evaluation of DWT Based Image Steganography," IEEE International Conference on Advance Computing, pp. 223-228.

[8] Mathkour H, Al-Sadoon B and Touir A. (2008): "A New Image Steganography Technique. :" International Conference on Wireless Communications, Networking and Mobile Computing, pp.1-4.

[9] V Vijaylakshmi,G Zayaraz and V Nagaraj. (2009):"A Modulo Based LSB Steganography Method," International Conference on Control,Automation,Communication and Energy Conservation, pp. 1-4.

[10] Wien Hong, Tung-Shou Chen and Chih-Wei. (2008):"Lossless Steganography for AMBTC-Compressed Images," Congress on Image and Signal Processing, pp.13-17.

[11] A W Naji, Teddy S Gunawan, Shihab A Hameed, B B Zaidan and A A Zaidan. (2009): "Stego-Analysis Chain, Session One," International Spring Conference on Computer science and Information Technology, pp. 405-409.

[12] M Hassan Shirali-Shahreza and Mohammad Shirali-Shahreza. (2008): "A New Synonym Text Steganography," International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1524-1526.

[13] Chen Ming, Zhang Ru, Niu Xinxin and Yang Yixian (2006): "Analysis of Current Steganographic Tools: Classifications and Features," International Conference on Intelligent Hiding and Multimedia Signal Processing, pp. 384-387.

[14] Mankun Xu, Tianyun Li and Xijian Ping. (2009): "Estimation of MB Steganography Based on Least Square Method," International Conference on Acoustics, Speech and Signal Processing, pp. 1509-1512.

[15] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt. (2008): "Enhancing Steganography in Digital Images," Canadian Conference on Computer and Robot Vision, pp. 326-332.

[16] Aos A Z, A W Nazi, Shihab A Hameed, Fazida Othman, B B Zaidan.(2009): "Approved Undetectable-Antivirus Steganography," International Spring Conference on Computer and Information Technology, pp. 437-441.

[17] Daniela Stanescu, Valentin Stangaciu, Loana Ghergulescu and Mircea Stratulat. (2009): "Steganography on Embedded Devices," International Symposium on Applied Computational Intelligence and Informatics, pp. 313-318.

[18] A W Naji, Teddy S Gunawan, Shihab A Hameed, B B Zaidan and A A Zaidan. (2009): "Stego-Analysis Chain, Session One," International Spring Conference on Computer science and Information Technology, pp. 405-409.

[19] Neha Agarwal and Marios Savvides. (2009): "Biometric Data Hiding: A 3 Factor Authentication Approach to Verify Identity with the Single Image using Steganography, Encryption and Matching," International Conference on Computer vision and pattern recognition, pp.85-92

[20] Vladimir Banoci, Gabriel Bugar and Dusan Levicky (2009): "Steganography Systems by using CDMA Techniques," International Conference on Radioelectronika, pp.183-186.

[21] Mci-Ching Chen, Sos S Agaian and C L Philip Chen. (2008): "Generalised Collage Steganography on Images," International Conference on Systems, Man and Cybernetics, pp.1043-1047.

[22] Weiqi Luo, Fangjun Huang, and Jiwu Huang. (2010): "Edge Adaptive Image Steganography Based on LSB Matching Revisited," IEEE Transactions on Information Forensics and Security, no. 2, vol. 5, pp. 201-214.

DOI 10.17148/IJARCCE.2015.4619