International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 12, December-2014

A Steganography Algorithm for Hiding Secret Message inside Image using Random Key

Balvinder Singh
Department of Computer Engineering
Govt. Engineering College Bikaner
Bikaner, India

Sahil Kataria
Department of Computer Engineering
Govt. Engineering College Bikaner
Bikaner, India

Tarun Kumar
Department of Computer Engineering
Govt. Engineering College Bikaner
Bikaner, India

Narpat Singh Shekhawat
Department of Computer Engineering
Govt. Engineering College Bikaner
Bikaner, India

***Abstract*—"Steganography" is a Greek origin word which means "hiding writing". The steganography word is classified into two parts: Steganos means "secret or covered"(where you want to hide the secret messages) and graphic means "writing"(Text). This paper introduces a new approach for least significant Bit (LSB) based on image steganography that enhances the existing LSB substitution techniques to improve the security of hidden information. This paper presents an algorithm to hide the secret data inside images using an efficient steganography technique. We use 8-bit random key for encrypting our secret message and also the same key will be used for choosing the pixel in cover image where we will hide our encrypted data. First we are applying XOR operation between our secret text message and 8-bit random key for encrypting our plain secret message. Now this encrypted message will be hide in cover image. We are hiding our secret encrypted message in the LSB of selected pixel. 8-bit random key and 2nd LSB of each pixel choosing the pixel where we have to store our encrypted message by applying some operation. This method also hiding large number of character of secret message into cover image as compare to other existing techniques and also much secure.**

Keywords—Steganography, least significant bit (LSB), Pixel, Information Hiding, Cryptography, image processing, Text Steganography, key-based steganography.

I. INTRODUCTION

"Steganography" is a Greek origin word which means "hiding writing". Todays, all the information is stored in the form of digital media using computer and network technologies that provide easy to use communication channels for steganography. Everyone wants to keep the personal information secret. The steganography word is classified into two parts: Steganos means "secret or covered"(where you want to hide the secret messeges) and graphic means "writing"(Text). So there are two types of mechanisms that provide security for information, first one is cryptography and second one is steganography. Cryptography means converting the text from readable format to unreadable format but the encrypted message is visible to all, the intruder can get the secret message by applying some cryptanalysis on encrypted text, otherwise the intruder can alter the cipher text. Steganography means hiding secret information in any media like – text , image , audio , video. Message to be hidden is concealed in another file called cover media. The combination of cover file and secret message is known as stego. The stego can be transmitted over a network by sender to specified destination and received by the receiver. The data can be hidden in pixels of an image. Every pixel has some integer value, based on the intensity of color. This integer value can be converted into binary format, i.e. in the form of bytes of 1 'sand 0's. Individual bits from these bytes can be used to hide the information. Bits can be selected randomly from a byte and replaced with the secret data. Thus, various algorithmic techniques can be for selecting pixels used for data hiding.

Image steganography allows for two parties to communicate in such a way that no third party can understand the behavior of their communication. Generally, in image steganography the secret message is stored into the specific position of least significant bit of cover image. Changing in LSB of any pixel does not change the original image color as it does only change maximum by 1 bit which would be similar color as original. This stegno image looks like same as original cover image so an intruders can't detect if there is any hidden information in that image or if he found that still they will not able to fetch the secret information from stego image because of encryption and different hiding techniques.

II. REALED WORK

In modern times steganographic technologies have been an important part of the future of security and privacy on open systems such as internet. Stegnaography is one more information security tool like cryptography and watermarking. In steganography, for hiding secret message in a pixel, the physical location of a pixel is considered and then the binary format of that pixels value is used to hide the secret message.

The most common method for steganography in image is LSB insertion method. LSB method comes under substitution techniques of steganography. In this technique of steganography, least significant bit or bits of pixel are

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

replaced by the bits of secret message to be hidden. More than one LSB can be modified for hiding maximum data i.e. 4 LSB substitution method which modifies last four bits of a pixel. The LSB substitution is a versatile technique for steganography and can be used for various file formats.

The simplest approach for hiding secret message in an image is least significant bit substitution method. We are using 24-bit true color image which makes less changes in the image and human can not identify the changes just by looking through prying eyes. Suppose we have three pixels which are adjacent to each other or we can say nine bytes with the following RGB encoding.

00001101	10010010	111011010
10001011	00111001	100111011
10011101	11101010	100010001

Now suppose we want to hide the following 8 bits secret message 110010011. if we change the least significant bits of 24-bit true color image pixels with the 9 bits of secret message then we get the following pixels. Here, bits in bold indicates that bits have been changed.

00001101	1001001**1**	111011010
1000101**0**	00111001	100111010
1001110**0**	1110101**1**	100010001

We can see that there are very less pixel position changed after inserting 8 bit message. Below formula shows a very generic description of the process of steganography technique.

Hidden information + Cover image = Stego image

In this perspective, cover image is our primary part of this process which is an image to hide our secret message. Our secret message is embed into this cover image which results as a stego image (which will be the looking like same type of image as the cover image,just by changing small color which cannot differentiate by human eye).

III. PROPOED APPROACHES

In this paper we are taking binary representation of the hidden information and overwriting LSB of selected byte in cover image. Here we are introducing a 8-bit random key which will be used to decide whether we have to hide one bit of secret key into cover image or not. We are applying a simple Ex-or operation for choosing our hidden method. We are using below formula in our proposed approach.

Secret Plain Text + 8-bit random K=y = Encrypted Text

Cover image + 8-bit random key + Encrypted Text = stegno image

We are using 24-bit color scheme which have 3 bytes for each pixel or we can say 24 bits per pixels in which each byte represent the intensity of the three primary colors Green, Red, and Blue. So, we can split a cover image into three matrices as shown in figure 1.

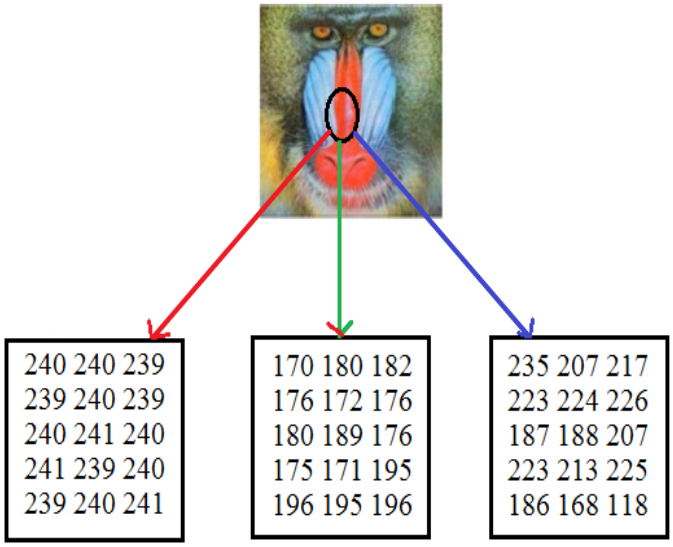

Fig. 1. RGB Matrix representation of cover image

The hidden information is converted from decimal to binary where each character is converted into 8 bit binary value. We used to hide bit by bit of our secret text message in selected pixel of our cover image.

A. *Hinding Techniques of Hidden Infomation*

To hide secret text message we have to take a cover image which is divided into three matrices (Red, Green, Blue) as shown in figure 1.Then we will generate an 8-bit random key. Here 8-bit random key and second LSB of each pixel of cover image used for decision making to replace hidden information into cover image. Here 8-bit random key will work as circular array bit stream. Our first step is to encrypt our plain secret text so we will encrypt our secret message using XOR operation with the same 8-bit random key. This encrypted message will be hide into that cover image. In our next step we will apply XOR operation between one bit of 8-bit random key and 2nd LSB of cover image pixel. If the XOR result of above operation is 1 then we will hide one bit of our secret key into LSB of same pixel of cover image, Otherwise we will not hide any bit in that pixel. The substitution process will be continued depending on the length of encrypted message. We are also hiding our 8-bit random key into same cover image by replacing first byte of cover image with 8-bit random key. The flow chart to hide secret information into cover image is shown in figure 2.

IJERT

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

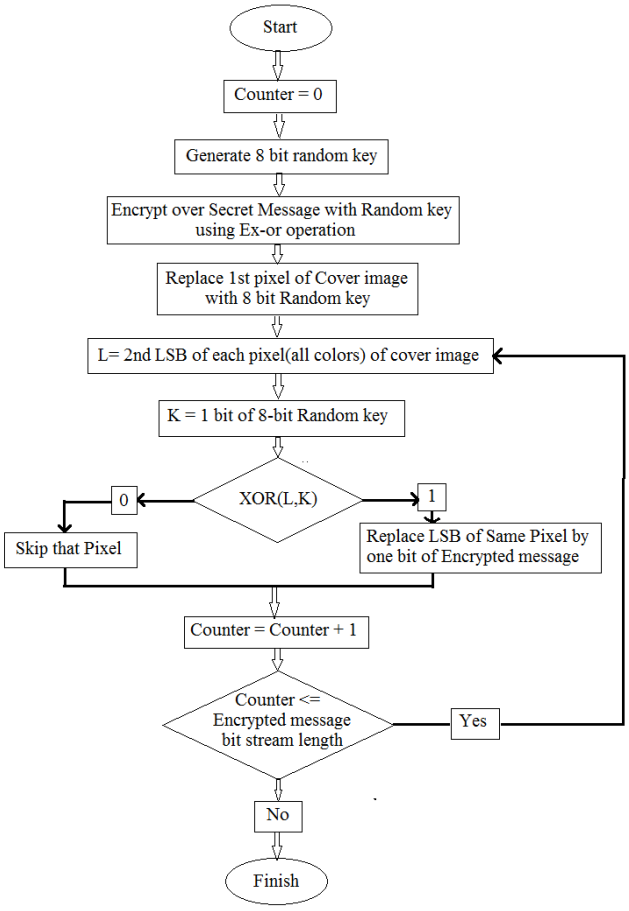

Fig. 2. Flow chart to hide Secret information into cover image

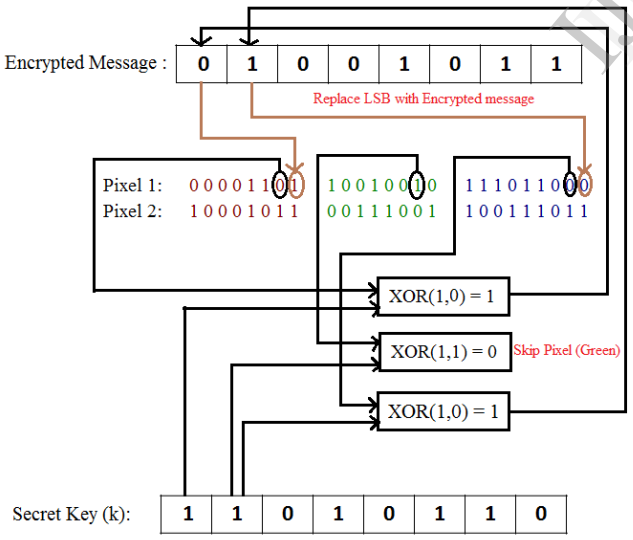

Fig. 3. Array representation of Encrypted message

At Figure 3. , the 2nd LSB of Red matrix of pixel 1 is 0 and the first bit of 8-bit random key is 1.The XOR value of 0 and 1 is 1. So as per our proposed method, if the XOR value is 1 then the LSB of same red matrix is replaced by the first bit of encrypted information. If the XOR value is 0 then we will skip that pixel. In our above example for green pixel XOR value is 0 so we are not hiding any bit in that pixel. The substitution process will be continued depending on the length of hidden information's.

B. Recovery Technique of Hidden Information

To recover secret text message from stego image we have to take a stego image which is divided into three matrices (Red, Green, Blue) as shown in figure 1.Then first we will fetch first 8 bit from stego image which will be our 8-bit random key. Now this 8-bit random key and second LSB of each pixel of cover image will use for decision making to fetch hidden information from stego image. Here 8-bit random key will work as circular array bit stream. Our first step is to perform XOR operation between 2nd LSB of stego image pixel and 8-bit random key If the XOR result of above operation is 1 then we will fetch one bit of our secret key from LSB of same pixel of stego image, Otherwise we will skip that pixel. The fetching process will be continued depending on the length of secret message. After completion of this step our next task is to decrypt our fetched result. We will apply XOR operation between result of above operation and 8-bit random key which will be our secret text message. The flow chart to recovery secret information into cover image is shown in figure 4.

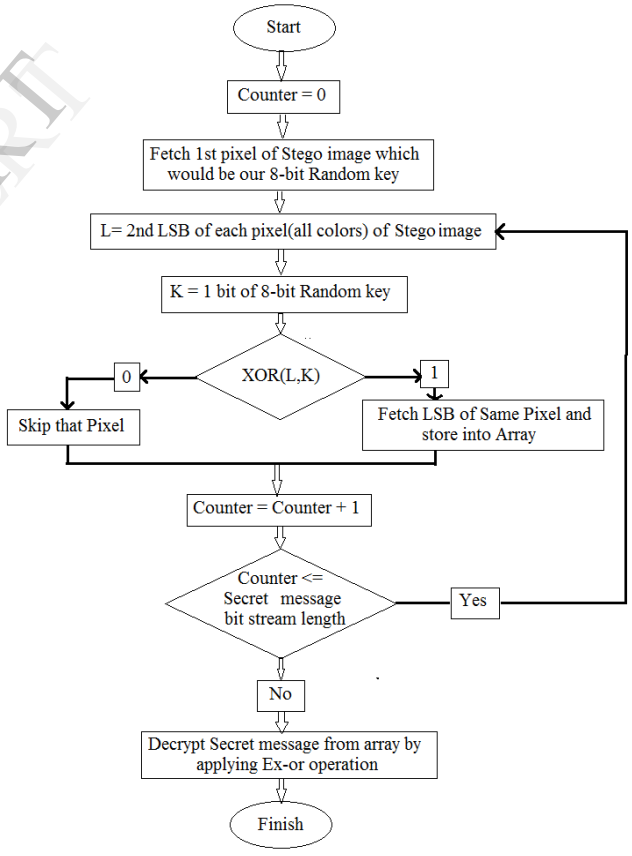

Fig. 4. Flow chart to retrieve secret message from stego image

IJERT

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

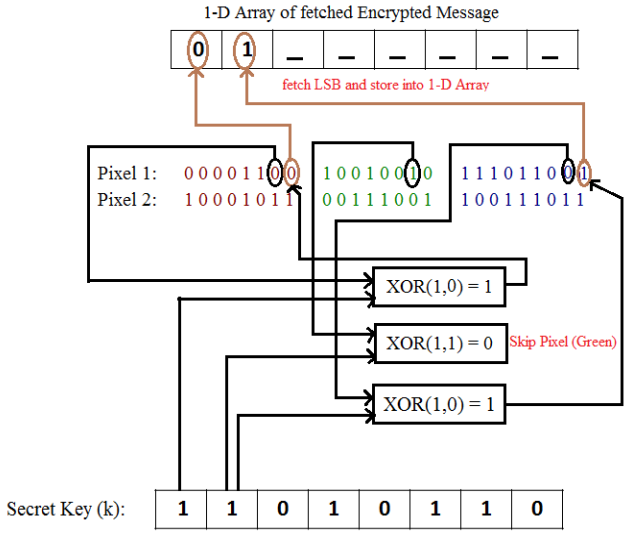

Fig. 3. Process to recover Encrypted message

At Figure 3.5, The 2nd LSB of Red matrix of pixel 1 is 0 and the first bit of 8-bit random key is 1. The XOR value of 0 and 1 is 1, so as per our proposed method, if the XOR value is 1 we will fetch 1st LSB of the same red matrix in an array. If the XOR value is 0 then we will skip that pixel. In our above example for green pixel XOR value is 0 so we will not fetch any bit from that pixel and just skip this pixel and continue the same process for all pixel. This process continues depending on the length of hidden information's.

IV. EXPERIMENTAL RESULT

To demonstrate the performance of our proposed method experimental result are given in this section. The two standard RGB true color images are used as cover images in which Secret message to be hidden. Lets assume our secret message is "I am Indian" which we want to hide in cover image. Here the secret message "I am Indian" is inserted into cover image according to our proposed method using 8-bit random key. The distortions comes in the stego images due to embed a large amount of private message using our proposed method are undisclosed to human eye.

Below are the procedure to get stego image from cover image which is shown in figure 5.

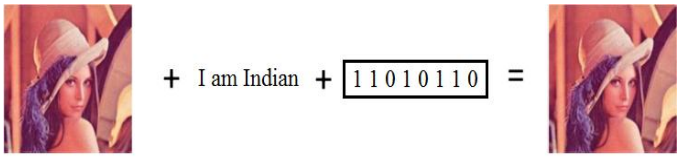

Fig. 5. (a) Stego image produced by using secret message and secret key

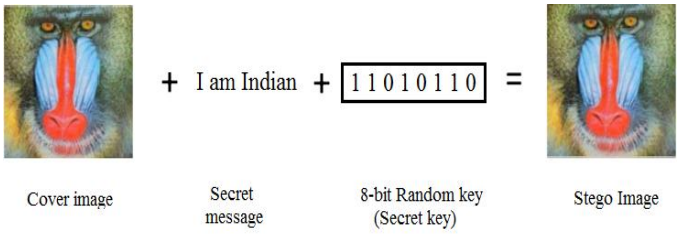

Fig. 5. (b) Stego image produced by using secret message and secret key

In the above experimental result the PSNR value is between 70-75(in dB). In our approach the PSNR value depends on choosing random key and on the size of secret message.

V. COMPARISON

The experimental results by applying our proposed method on deifferent standard images (Like- Leen,pappers,Colors) are alos compared wtih other methods and we have reviewed. Wu's method modifies almost all of the pixels in an image while hiding the secret data. Four Neighbor and Diagonal Neighbor method modify 3 or more bits of the pixel. But in our approach using random key scheme we may modifies three bits of a pixel. And also have the better PSNR value from these methods depending on the secret key.

Table 1. Comparison results with different approaches.

Cover Images	PSNR (in dB) in Na-Wu's	PSNR (in dB) in Four Neighbour	PSNR (in dB) in New approach [1]	PSNR (in dB) in our method
Leena	34.4	41.14	53.76	72.5
Colors	30.41	36.54	53.75	72.35
Peppers	33.74	41.03	53.78	72.7

IJERT

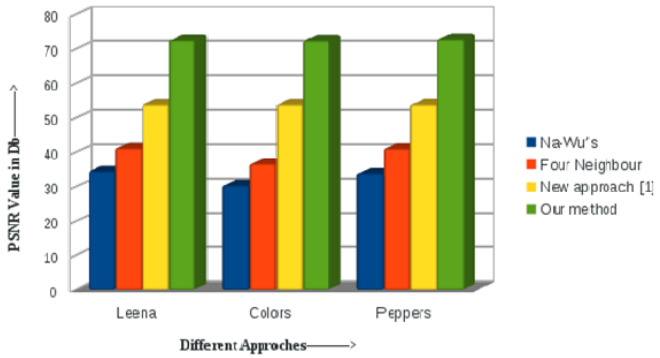

Fig. 6. PSNR value in different approaches

In the above graph we are showing the comparison of our proposed approach with some of popular existing approaches for 3 basic test cover images. By looking into this graph we can examine that our proposed approach is far better than existing approaches in all way or by applying different types of cover images.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

V. CONCLUSION

Our proposed approach showing that how we are hiding our secret text in some cover image without significant distortion. This process makes difficult for the unauthorized users to identify the changes in stego image or if any one find the changes they can't get the secret message from stego image as without the 8-bit random key no one able to know which pixel have hidden information and which have not. Our hidden information are also in encrypted form which will make our process more secure. Our proposed method gives better PSNR value where greater PSNR value indicates better quality of the image or we can say lower distortion in original image. This method also not taking too much time for hiding our secret message into cover image. This method also hides more number of bytes of secret data into cover image compare to other existing method.

REFERENCES

[1] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key" Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 201I) 22-24 December, 201I, Dhaka, Bangladesh.

[2] Tarun kumar, Abhinav Pareek, Jyoti Kirori, Maninder Singh Nehra Development of Crossover and Encryption Based Text Steganography (CEBTS) Technique" Lecture Notes in Electrical Engineering volume 298) International Conference on Emerging Trends in Computing and Communication (ETCC) 2014 DOI: 10.1007/978-81-322-1817-3_12 and ISBN: 978-81-322-1817-3.

[3] Sahil Kataria, Balvinder Singh, Tarun Kumar and Hardayal Singh Shekhawat "PDAC (Parallel Encryption with Digit Arithmetic of Cover Text) Based Text Steganography" Proc. of Int. Conf on Advances in Computer Science, ISSN: 9789351071020 © Elsevier 2013.

[4] Sahil Kataria, Balvinder Singh, Tarun Kumar and Hardayal Singh Shekhawat "An Efficient Text Steganography using Digit Arithmetic" Proc. of Int. Conf on Advances in Computer Science, ISSN: 9789351071020 © Elsevier 2013.

[5] M. Kutte and Hartung "Information hiding-a survey, " Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Content, Volume: 87 Issue: 7, pp. I062-I078, July. 1999.

[6] M. Hossain, F. Sharmin, S.A. Haque, "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation", Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December 2009, Dhaka, Bangladesh.

[7] Atallah M. Al-Shatnawi A New Method in Image Steganography with Improved Image Quality Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915

[8] M. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source– Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.

[9] D.C. Lou, J.L. Liu, H.K. Tso, Evolution of information – hiding technology, in H. Nemati (Ed.), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.

[10] Morkel T. , Eloff J.H.P. , M.S. Olivier, "An overview f image steganography", http://mo.co.za/openistegoverview.pdf, on January 2009.

[11] Sellars, Duncan, "Introduction to Steganography", http://www.cs.uct.ac.za/courses/CS400WINIS/papers99/dsellars/stego.html.

[12] N Ghoshal, J K Mandal "A steganographic scheme for colour image authentication (SSCIA)", Recent Trends in Information Technology ICRTIT 2011 International Conference on (2011), 826-831.

[13] M. M Amin, M. Salleh, S . Ibrahim, M.R.K Atmin, and M.Z.I. Shamsuddin, "Information hiding using steganography," IEEE 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, pp. 21-25, January 2003

IJERT

(This work is licensed under a Creative Commons Attribution 4.0 International License.)