Encryption Based Approach to Find Fake Uploaders in Social Media

Shereena T Abdul Rasheed [1], Sadakathulla P.K [2]

[1]MCA student, Centre for Computer Science and Information Technology, University of Calicut, Kerala
[2]Assistant Professor, Centre for Computer Science and Information Technology, University of Calicut, Kerala

Abstract - *In the digital era, we can see rapid growth in digital contents through different Medias. As we know social media plays an important role for generating digital contents using modern electronic devices and sharing of data and other digital contents. Digital images are the one of the frequently used media. In the context we have a challenge to find out the fake uploaders. In this paper we are proposing a new strategy to find out such fake uploaders by using encryption based method. The proposed system uses steganography based encryption to identify the fake uploaders in an easy way. Here we embed some personal information In to the digital image while uploading the content. By using this we can easily find the individual easily.*

Key Words: Encryption, Decryption, Steganography, social media security, LSB Substitution.

1. INTRODUCTION

In the modern world, there exists a wide range imaging techniques for capturing, storing and modifying digital images. With the increase in consumer generated image content using handheld devices such as mobile cameras and ease of sharing, fake news via images are spreading rapidly on social media. There has been a very active research area in the last decade. Cryptography and steganography can be used to provide security for digital content. Cryptography uses mathematics to encrypt and decrypt data to provide security by transforming plaintext into ciphertext. Steganography is the art of hiding information in other information.

With this paper, we mean that along with the photograph, we also have related meta-data as contact number of the person who upload that photograph firstly. Here, the person behind the photograph can be identified easily by this application. Identifying person will eliminate the system of easily spreading the image and this will also act as big tool to give evidence in front of justice court. Here we use an algorithm that hides the contact number of the person who uploads the image. The contact number that embedded with the image never loses even if it is shared among different people. Whenever a situation arises to find out the person who has uploaded the image, we can easily find out the contact number of the person by just applying the reverse algorithm.

2. LETERATURE REVIEW

Besides cryptography, steganography can be used to secure information. Steganography is a technique of hiding data/information in digital media. Both Cryptography and steganography methods of digital images are widely used to protect and frustrate opponents' attacks from unauthorized access. Thus, image encryption techniques are required to protect the data [1]. There is a difference between cryptography and steganography. Cryptography scrambles messages so that they cannot be understood. On the other hand, steganography hides the actual message in another [2]. Over the last few years, there are many different steganographic methods are proposed. Most of them are very simple techniques so that those can be broken easily by careful analysis of statistical properties of the channel's noise [3]. Recently, some new steganographic algorithms have been proposed for two-color binary images [4]. Johnson and Sushil explain what steganography is and provide a brief history of steganography, describe how steganography is applied to hide information in images, and survey a few steganography software applications [5]. TsungYuan and Wen-Hsiang proposed a new steganographic method that uses change tracking technique for hiding data in Microsoft Word documents [6]. Sinha and Singh proposed a method to encrypt an image for secure transmission [7].This method use the digital signature of the image. Digital signatures enable the recipient of a message to authenticate the sender and verify that the message is intact. Kisik et al [4] proposed a steganographic algorithm which embeds a secret message into bitmap images and palette-based images.

Y.K Jain and R.R Ahriwal proposed Least Significant technique to hide a message in an image. This technique generates a steganography key after embedding the message. The key has different layers. Every layer has a fixed number of bits. These bits are embedded in least significant of the image [8].The method proposed by Mohammad A Ahmed uses Least Significant technique to hide data in digital image. Then the digital image will be implemented in hash significant technique to get the result in hashing value[9].El-Emam proposed a method which hides message in an image in form if pixels. To retrieve the hidden message these pixels are called. Steganography is used to hide and retrieve the message [10]. Akhtar N, Johri P and Khan S implemented a variation of traditional Least Significant Bit (LSB) algorithm. It uses bit inversion method to enhance the quality of the image which the message is hidden. This method has lesser modification in pixels compared to traditional LSB method [11]. P. U. Deshmuk and T. M. Pattewar proposed the edge adaptive steganography based on LSB substitution method. They hide secret message in sharp regions of the image.

This technique also improves the quality of stego image [12]. D. Baby, J. Thomas, G. Augustine, E. George and N.R. Michael presented "Novel DWT based image securing method using steganography". They proposed a new steganography technique in which multiple RGB images are embedded into single RGB image using DWT steganography technique. This method has level of PSNR (Peak signal - to - noise ratio) and structural similarity (SSIM) index values [13]. G. Prashanti and K. Sandhyarani have done survey on LSB based image steganography and also two new techniques are presented. First technique hides secret message in the cover image and second one embeds a gray scale image into another gray scale image. These two techniques have great security because secret information is hidden on random selected location of LSBs of the image [14].

3. LETERATURE REVIEW

The proposed system aims to hides the contact number of the person who uploads the image. The following figure shows the working of the proposed system.

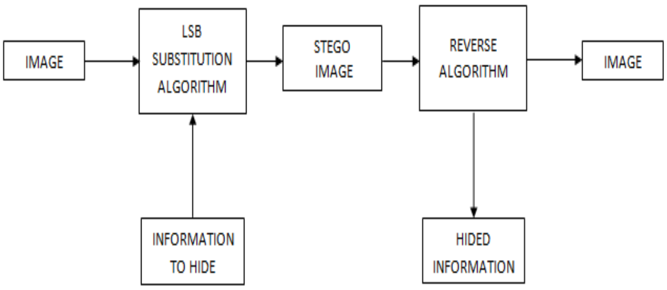

Fig -1: Working of proposed system

Here we use the Least Significant Bit (LSB) substitution method to hide the data within the image. This method replaces the pixels of image by the secret data. The image is stored as m-by-n matrix having several pixels. Each pixel in the image is represented as RGB components and that determine color of each individual pixel. RGB images are stored as 24 bit format, where the RGB components are of 8 bits each.

Here we use the contact number of the person who uploads the image and a string as a secret data. The string is used to check whether the image already contain any contact number or not. This secret data is then converted into byte array.

Here we use 3 bit of R, 3 bit of G and 3 bit of B to hide 1 byte of string. Here we replace first some pixels of the image and the length of the secret data determines the number of pixels to be replaced. This results only a small change in the value of RGB component, which human eyes can't detect.

Whenever any situation arises, the reverse algorithm helps to identify the contact number of the person who firstly uploads the image. This secret data will not loss even if it shared by different people.

3.1 Algorithm to hide data

```
Step 1: Load image into a variable 'image'.
Step 2: Check whether the image is already contains any
        contact number or not by reverse algorithm.
Step 3: If the image does not contain any number then checks
        the mode of image.
Step 4: If the image is an RGB image then store the secret
        message into a variable 'msg' and set,
        length= len(msg)
        width, height= image . size
        index= 0
        encoded= image.copy()
Step 5: Repeat the following steps 6 to 8 until reaches the last
        pixel
Step 6: Store RGB component of 1 pixel into variables r, g and
        b
Step 7: if index < length then
          c= msg[index]
          imsg= int (ord(c))
          r1= imsg & 7
          imsg= imsg >> 3
          g1=imsg & 7
          imsg= imsg >> 3
          b1=imsg & 7
          r= r & 248
          g= g & 248
          b= b & 252
          r= r | r1
          g= g | g1
          b= b| b1
Step 8: encode.putpixel((col,row),(r,g,b)) index= inex+1
Step 9: Stop
```

3.2 Algorithm to retrieve data

```
Step 1: Load image into a variable 'image'
Step 2: Check whether the image is already contains any
        contact number or not
Step 3: If the image does not contain any number then checks
        the mode of image
Step 4: If the image is an RGB image then store the secret
        message into a variable 'msg' and set ,
        width, height= image . size
        index= 0
Step 5: Repeat the following steps 6 to 8 until reaches the last
        pixel
Step 6: Store RGB component of 1 pixel into variables r, g and
        b
Step 7: if index < length then
          r1= r & 7
          g1= (g & 7) << 3
          b1= (b & 3) << 6
          val = r1 | g1 | b1
          msg = msg + (str ( chr ( val ) ) )
Step 8: index= inex+1
Step 9: Stop
```

4. CONCLUSION

We have studied about the spreading of fake news through social media and this project aims to control these fraudulent activities. We have used LSB substitution algorithm to hide the secret data within the image. This method is very simple and we can easily extract contact number from the image by just applying the reverse algorithm. We have tested our solution on a sample network. This method proves that it is possible to extract the contact number of the uploader even if it shared many times.

REFERENCES

[1] H. Zenon, V. Sviatoslav, R.Yuriy, "Cryptography and steganography of video information in modern communications," 1998, Citeseer.ist.psu.edu/hrytskiv98cryptography.html

[2] M.M. Amin, M. Salleh, S. Ibrahim, M.R Katmin, M.Z.I. Shamsuddin, "Information hiding using steganography," Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National

[3] Elke, Fraz, "Steganography preserving statistical properties," proceeding of the 5th internationally Workshop on information Hiding, Noordwijkerhout, The Netherlands, October 2002, LNCS 2578, Springer 2003, pp. 278-294.

[4] EE. Kisik Chang, J. Changho, L. Sangjin, "High Quality Perceptual Steganographic Techniques," Springer, Vol. 2939, 2004, pp.518-531.

[5] N.F. Johnson, J. Suhil, " Exploring Steganography:Seeing the Unseen," Computing practices, 2006, 2006, http://www.jjtc.com/pub/r2026.pdf

[6] L. Tsung-Yuan, T. Wen-Hsiang ,"A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique," Information Forensics and Security, IEEE Transactions on Vol. 2, Issue 1, March 2007 Page(s):24 – 30, Digital Object Identifier 10.1109/TIFS.2006.890310.

[7] A. Sinha, K. Singh, "A technique for image encryption using digital signature," Source: Optics Communications, vol.218, no. 4, 2003, pp.229-234.

[8] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.

[9] Mohammad A. Ahmad, Dr. Imad Alshaikhli, Sondos O. Alhussainan, "Achieving Security for Images by LSB and MD5", Journal of Advanced Computer Science and Technology Research, Vol. 2, Issue No.3, Pages No. 127-139, Sept., 2012.

[10] N.N. El-Emam, Hiding a large amount of data with high security using steganography algorithm, Journal of Computer Science 3 (2007) 223-232.

[11] Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.385,390, 27-29 Sept. 2013.

[12] P.U. Deshmukh and T.M. Pattewar, "A Novel Approach for Edge Adaptive Steganography on LSB Insertion Technique" IEEE International Conference on Information Communication and Embedded Systems (ICICES), Feb. 2014, pp. 1-5.

[13] D. Baby, J. Thomas, G. Augustine, E. George, N.R. Michael, " A Novel DWT based Image Securing method using Steganography", International Conference on Information and Communication Technologies (ICICT), Procedia Computer Science, April 2015, pp. 612-618.

[14] G. Prashanti, K. Sandhyarani, "A New Approach for Data Hiding with LSB Steganography", Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer 2015, pp. 423-430.