A Novel Approach to Digital Image Steganography of Key-Based Encrypted Text

Sreeparna Chakrabarti
Department of MCA
Acharya Institute of Institute
Bangalore, India
sreeparnachakrabarti@acharya.ac.in

Debabrata Samanta
Department of MCA
Acharya Institute of Institute
Bangalore, India
debabrata.samanta369@gmail.com

***Abstract*—Encryption is the method by which we can encode the intended piece of information in such a way that only the people whom we want to pass that information can understand its actual meaning. Digital Image Steganography the message is hidden in an image in such a way that the onlookers cannot even guess that it is not a normal image. Nowadays security is a vital issue while transmitting a message. So in this paper we have proposed a unique way of transmitting the message securely. First we have encrypted the message to an image which needs a secret key to be decrypted. Then we have hidden that image inside another image by steganographic approach. By this*two level hiding* we can ensure stronger security.**

***Keywords*-Ascii Integer, Cover Image, FiboSum, Pixel Mapping, Stego Image.**

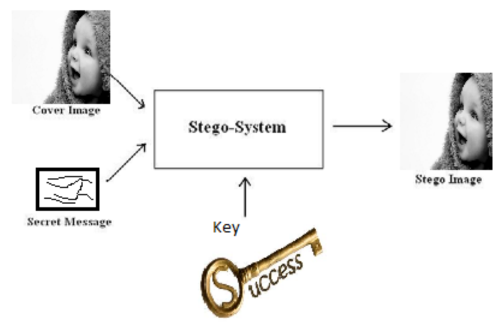

Figure 1. Basic Diagram of Image Steganography

I. Introduction

Steganography is the method used for concealing a piece of information (which can be message, image or file) within another message, image or file. The word "Steganography" is derived by combining the Ancient Greek words steganos , meaning "covered, concealed, or protected", and graphein meaning "writing" [7]. The basic assumption is that if any feature is visible to the onlookers, which makes them understand that some hidden information is present in the message image or file, they might be interested to find what it is. Thus the main aim of steganography is to hide the fact that some hidden information exists! Steganography can be categorized with respect to three types of carriers: Steganography in image, steganography in audio and steganography in video. Private key is a common secret key shared between the sender and receiver of an encrypted message using which an intelligent message can be encrypted and transformed to an unintelligent message and can be again decrypted and recover the intelligent message [8-11].

The key has to be passed to the receiver by the sender while sending the message. In Digital Image Steganography the piece of information is hidden inside an image. Encryption is on the other hand a process by which we can encode our message in such a way that only the person for whom the message is intended can read it. Anyone seeing it will be able to guess that something is hidden inside, but they will not be able to find out what! Hence secure communication is possible even in presence of third parties. So there lies the basic difference between steganography and encryption. Hence, our main purpose is to use both the techniques in a unique way so that security is enhanced.

II. Related Work

In one of the existing systems the original message was encrypted twice using traditional techniques. The cipher is then hidden inside an image. As key they have used a reference matrix for selection of passwords depending on the properties of the image [1]. In one more existing system both the concepts of cryptography and steganography have been combined to get tighter security [2]. The author stated that if data is embedded in the image the color frequencies are changed in a predictable way. To avoid that the encrypted cipher has been hidden inside a multimedia image file. But the cryptographic technique they have used is Asymmetric Key Cryptography [12-13]. As we know that public key encryption uses huge mathematical calculations and hence lot of time is needed for encryption and decryption. Also according to some it is not completely safe. In another existing paper the secret information is fabricated into a binary image to convert it to a gray scale image [14-16]. (2, 2) visual cryptographic shares are generated from this converted gray scale image and these shares are hidden into separate meaningful images [3]. But due to pixel expansion, the width of the decoded image is twice as that of the original image. This leads to loss of information since the aspect ratio is changed. In another existing system a secret message has been inserted into an image using random LSB [17-20]insertion method in which the secret data are spread out among the image data in a seemingly random manner[4]. A secret key has been used in that. But in LSB related method extraction is very easy. In one more system the secret message is encrypted first by using a new cipher which is extended from Hill cipher. Then that message is embedded into certain bit locations of darkest and brightest pixels of the carrier image. [5] But since Hill Cipher is based on linear System plaintext attack is possible. Even in an existing system QR-Crypt block cipher cryptography technique has been introduced. According to the authors QR-Crypts has new features and encryption takes place at dual level of across the string as well as across the cipher image [6]. But as stated by the authors that for IP routing environment one more parameter is needed, which is robustness.

III. Research Methodology

The novel part of our research methodology to convert a user message to a corresponding image matrix using the following methods and shown in figure 1.

1) Convert user message to an array of its ascii equivalent values
2) Normalize the array by subtracting 32 (the least element in a normal keyboard) from each element of the array.
3) Get the number of new sentences in the message by finding out number of "."in the message.
4) Get the sum of the similar number of Fibonacci numbers.
5) Add this sum to each element of the array which results in the final matrix.

   Figure 2 explain our novel research methodology.

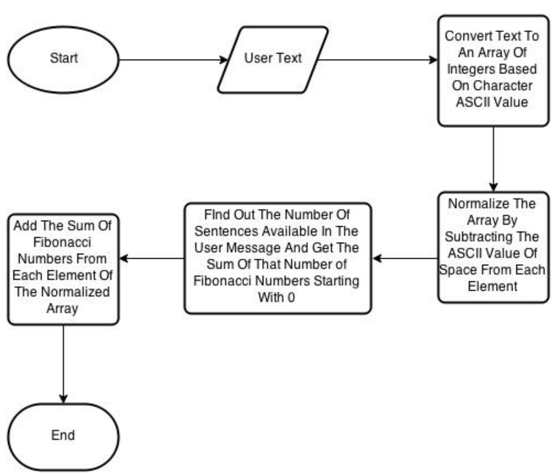

Figure 2. Flow of Novel Methodology

IV. Work Flow Diagram

Figure 3 and figure 4 demonstrate the total work flow of Sender and Receiver side respectively.

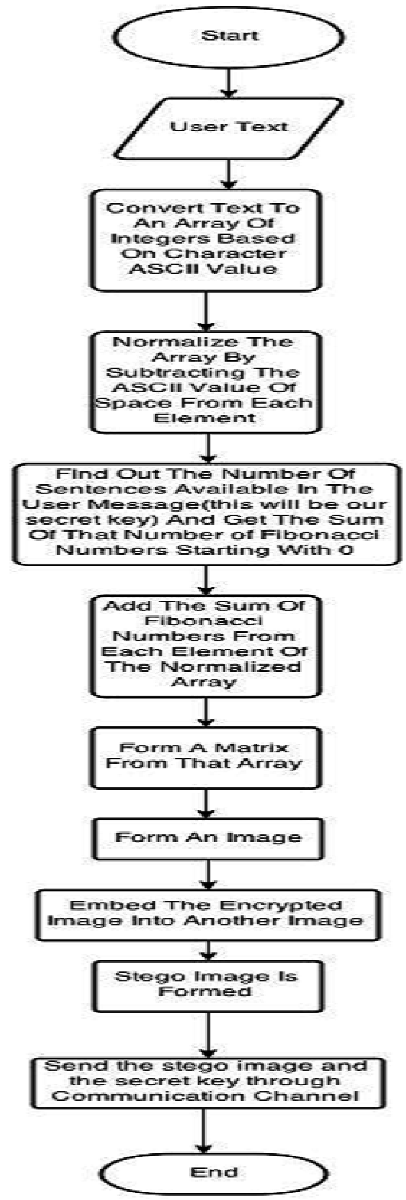

Figure 3. Diagram of Sender

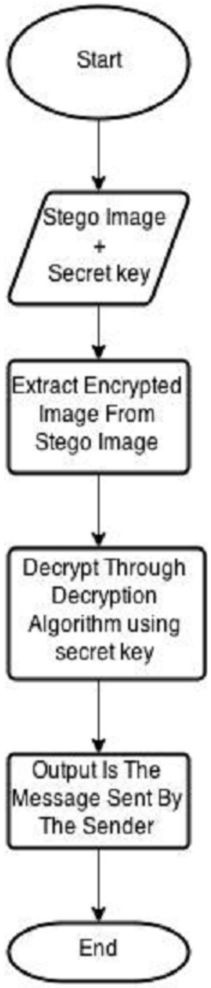

Figure 4. Diagram of Receiver

V. Algorithm of Image Steganography of Key-Based Encrypted Text

Input : Cover Image, Secret Message.
Output : Stego Image.

1) Get user message from Console
2) initialize integer data array

$$F_x = \sum_i C_i \tag{1}$$

3) initialize sentence counter to zero
4) while end of line is not reached in message
   get the character of the message
   convert the character to ascii integer
   subtract 32 from integer
   add the integer to the integer data array

$$Q_x = \sum_i [C_i - K_{cont}] \tag{2}$$

$$K_{cont} = 32 \tag{3}$$

5) for all the elements of the array
   if the element value is 14
   increase sentence counter by 1
6) fiboSum = Get the sum of the n number of Fibonacci numbers where n is equal to sentence counter
7) for all the elements of the integer array
   $element = element - fiboSum$
   $Y_i = No.of Sentences.$

$$P_{fib_x} = \sum_i fib_i[Y_i] \tag{4}$$

$$F_{Mtrix} = Q_x + P_{fib_x} \tag{5}$$

8) Display the integer array
9) Return the stego image
10) End

VI. Result

Text 1:
The quick brown fox jumps over the lazy dog.
Text 2:
Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. This paper presents a novel technique for image steganography based on Huffman Encoding.
The steganographic image should appear as a normal image so that it does not attract attention to itself. Below are the results of application of the algorithm on two famous images *Lena and Pepper*.

Figure 5. A) Cover Image B) Stego Image of Lena and Pepper after embedding for Text 1.

Figure 6. A) Cover Image B) Stego Image of Lena and Pepper after embedding for Text 2.

VII. Quality Metric

A. Mean square error (MSE)

The MSE is the cumulative squared error between the compressed and the original image.

$$MSE = 1/MN \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - I'(x,y)]^2 \qquad (6)$$

where $I(x,y)$ is the original image, $I'(x,y)$ is the approximated version (which is actually the decompressed image) and M,N are the dimensions of the images. A lower value for MSE means lesser error. Hence a better compression technique will always have a lower value for MSE.

B. Peak signal-to noise ratio (PSNR)

PSNR is a measure of the peak error.

$$PSNR = 20 * log10(255/sqrt(MSE)) \qquad (7)$$

Logically, a higher value of PSNR is good because it means that the ratio of Signal to Noise is higher. Here, the *signal* is the original image, and the *noise* is the error in reconstruction of the original image after decompression. Hence a better compression technique will always have a higher value for PSNR.

C. Similarity Measure

Image comparison is one of the most difficult and complex problem in image processing. An image has many different parameters to look upon like scale, brightness shape, size orientation. To determine which parameters are relevant in some situations and which are not is a daunting task for humans too. But these are some of the methods we can think of to determine the similarity of the images. An image similarity measure quantifies the degree of similarity between intensity patterns in two images (*Cover Image and Stego Image*). The choice of an image similarity measure depends on the modality of the images to be registered.

1) Correlation coefficient: The Pearson's method is widely used in statistical analysis pattern recognition and image processing. Applications on the later include comparing two images for image registration purposes, disparity measurement, etc.*Correlation coefficient* between two random variables X and Y is defined as

$$\rho(X,Y) = \frac{\mathbf{Cov}(X,Y)}{\sqrt{\mathbf{Var}(X)\mathbf{Var}(Y)}}. \qquad (8)$$

The *correlation coefficient* r between two samples x_i and y_j is defined as $r = S_{xy}/\sqrt{S_{xx}S_{yy}}$.

2) Entropy: E = entropy(I) returns E, a scalar value representing the entropy of gray scale image I. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. Entropy is defined as

$$E = -\sum p * log(p) \qquad (9)$$

where p contains the histogram counts returned from imhist. By default, entropy uses two bins for logical arrays and 256 bins for uint8, uint16, or double arrays.

VIII. ANALYSIS OF THE RESULTS

The proposed steganography approach for hiding information of a gray scale is tested to get the measure of its effectiveness. The embedding capacity of the proposed method is better than most of the existing methods. The MSE and PSNR values are calculated after embedding the message in several coefficients of the cover image. The MSE and PSNR values are better than the existing methods. The steo image and the cover image are almost identical. This has been proven by analyzing the similarity measure between the two images.

Table 1 : Quality Metric for Text1

	Lena		Pepper	
Quality Metric	Cover Image	Stego Image	Cover Image	Stego Image
MSE	25.13	24.93	27.01	26.43
PSNR	47.69	48.01	44.14	45.25
Correlation coefficient	0.9972	0.9914	0.99104	0.99276
Entropy	25.24	25.73	24.01	23.97

Table 2 : Quality Metric for Text2

	Lena		Pepper	
Quality Metric	Cover Image	Stego Image	Cover Image	Stego Image
MSE	24.252	23.014	25.68	25.01
PSNR	48.92	48.07	46.27	46.001
Correlation coefficient	0.9912	0.9971	0.99912	0.99891
Entropy	23.01	21.25	24.83	24.16

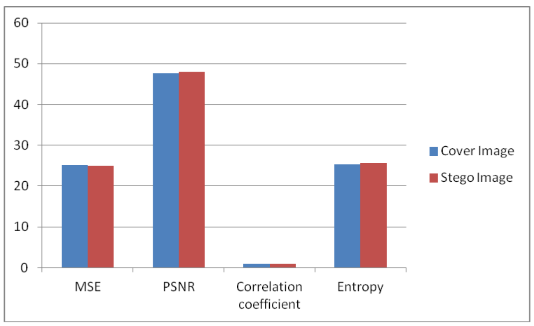

Figure 7. Graphical representation for Lena in TEXT 1

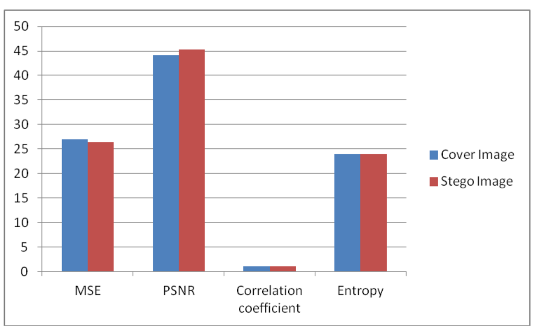

Figure 8. Graphical representation for Peepar in TEXT 1

IX. Conclusion and Discussion

The proposed technique for steganography is to deal with gray scale image which can embed the secret message into image without causing much distortion of the cover image. Although this technique maps each two bit of the secret message to the pixels of the cover image, the technique can be extended to map n number of bits too by considering the number of features of the embedding pixels. The technique is also capable of extracting the secret message from steno image without the cover image. The future work should concentrate on applying this technique on color images.

References

[1] Usha, S. ,Dept. of Electron. Commun. Eng., Sri Venkateswara Coll. of Eng., Chennai, India, Kumar, G.A.S. ; Boopathybagan, K. , "A secure triple level encryption method using cryptography and steganography", Computer Science and Network Technology (ICCSNT), December 2011.

[2] Marwaha, P, Infosys Technol. Ltd., Bangalore, India, "Visual cryptographic steganography in images", Computing Communication and Networking Technologies (ICCCNT),July 2010.

[3] Mandal, J.K. Dept. of Comput. Sci. Eng., Univ. of Kalyani, Kalyani, India,Ghatak S, "Secret image / message transmission through meaningful shares using (2, 2) visual cryptography (SITMSVC)", in Recent Trends in Information Technology (ICRTIT), June 2011.

[4] Sutaone, M.S. ET/C Dept, PIET's Coll. of Eng., Pune, Khandare,M V, "Image based steganography using LSB insertion technique", IET International Conference,Jan 2008.

[5] Swain, G, Dept. of IT, GMR Inst. of Technol., Srikakulam, India,Lenka S.K, titled "A hybrid approach to steganography embedding at darkest and brightest pixels", Communication and Computational Intelligence (INCOCCI),Dec 2010.

[6] Qayum, A. Sch. of Comput. Integrative Sci, JNU, New Delhi, India,Kumar P, "QR decomposition-based cryptography: Via image generation (QR-CRYPT)",Dec 2012.

[7] Marwaha, P, Infosys Technol. Ltd., Bangalore, India, "Visual cryptographic steganography in images", Computing Communication and Networking Technologies (ICCCNT),July 2010.

[8] Mandal, J.K. Dept. of Comput. Sci. Eng., Univ. of Kalyani, Kalyani, India,Ghatak S, "Secret image / message transmission through meaningful shares using (2, 2) visual cryptography (SITMSVC)", in Recent Trends in Information Technology (ICRTIT), June 2011.

[9] Sutaone, M.S. E T/C Dept, PIET's Coll. of Eng., Pune, Khandare,M V, "Image based steganography using LSB insertion technique", IET International Conference,Jan 2008.

[10] Qayum, A. Sch. of Comput. Integrative Sci, JNU, New Delhi, India,Kumar P, "QR decomposition-based cryptography: Via image generation (QR-CRYPT)",Dec 2012.

[11] Upreti K,Dept of Computer Science Engineering,JSS Acad of Tech.Educ,India,Verma K;Sahoo A, "Variable Bits Secure System for Color Images", Advances in Computing, Control and Telecommunication Technologies (ACT), 2010 Second International Conference,Dec 2010.

[12] Neeta, D. ; Dept. of Comput. Sci., K.K. Wagh Inst. of Eng., Nashik ; Snehal, K. ; Jacobs, D., "Implementation of LSB Steganography and Its Evaluation for Various Bits", Digital Information Management, 2006 1st International Conference, Dec 2006.

[13] Wai Wai Zin ; Univ. of Comput. Studies, Mandalay, Myanmar ; Soe, T.N.,Implementation and analysis of three steganographic approaches", Computer Research and Development (ICCRD), 2011 3rd International Conference,March 2011.

[14] Mishra, M. ; ECE Dept., NERIST, Itanagar, India ; Tiwari, G. ; Yadav, A.K., ”Secretcommunicationusing Public Key steganography”, Recent Advances and Innovations in Engineering (ICRAIE),May 2014.

[15] Selvi, G.K. ; Dept. of Comput. Sci. Eng., R.M.K Eng. Coll., Chennai, India ; Mariadhasan, L. ; Shunmuganathan, K.L., ”Steganography using edge adaptive image”, Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference, March 2012.

[16] Tayel, M. ; Electr. Eng. Dept., Alexandria Univ., Alexandria, Egypt ; Shawky, H. ; Hafez, A.E.S., ”A new chaos steganography algorithm for hiding multimedia data”, Advanced Communication Technology (ICACT), 2012 14th International Conference, Feb. 2012.

[17] Agham, V. ; Dept. of Comput. Eng., R.C. Patel Inst. of Technol., Shirpur, India ; Pattewar, T., ”A novel approach towards separable reversible data hiding technique”, Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference, Feb. 2014.

[18] Ritchey, P.C. ; Dept. of Comput. Sci., Purdue Univ., West Lafayette, IN, USA ; Rego, V.J., ”Hiding Secret Messages in Huffman Trees”, Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference, July 2012.

[19] Das, S. ; MCA Dept., Techno India, Kolkata, India ; Bandyopadhyay, P. ; Chaudhuri, A. ; Banerjee, M., ”A secured key-based digital text passing system through color image pixels”, Advances in Engineering, Science and Management (ICAESM), 2012 International Conference, March 2012.

[20] Bai Sen ; Inst. of Autom., Chongqing Univ., China ; Cao Chang-Xiu, ”A novel algorithm for scrambling the details of digital image”, published in Intelligent Control and Automation, 2002. Proceedings of the 4th World Congress on (Volume:2), 2002.