A New Robust Method of Hiding Text for Secure Data Transfer Based On Secret Key and Hash Function

Kalaichelvi V, Manimozhi K, Meenakshi P, Manikandan H, Swaminathan S

Abstract: ***There are many steganographic algorithms which are reliable to send messages confidentially to the other end. But every algorithm has a loop hole which is used to retrieve the message back. To overcome this issue, this paper introduces the concept of hash function in steganography. To achieve this, it recommends only the use of colour images. First retrieving the LSB's of the blue pixel, getting a 32 bit input from the user, these two values are considered as the secret key. The secret message which is to be hidden is also obtained from the user and converted to ASCII byte stream. A Hash function is performed between the blue pixel value and the 32 bit secret key. This gives the hash byte stream as output. This is equal to the length of the secret message in bits. An XOR operation is performed between the ASCII byte stream of the secret message and the hash byte stream. This results in pseudo byte stream. Each bit of the pseudo byte stream is replaced in LSB's of the blue pixel to obtain stego-image. On the receiver's side the receiver should know the 32 bit secret key and the message length. Once it is known, the image to be encrypted is selected, 32 bit secret key and the message length is entered. The same process hash process is done and the output byte stream is converted from their ASCII value and the secret message is displayed to the receiver. If the receiver enters a wrong secret key he will never know the secret message and since the hash function is used, it is impossible to trackback the algorithm. The .png format offers lossless compression and thus rendering a safe transmission of the secret message. Thus, the function is safe, secure, reliable, simple and cost effective.***

Index Terms: Hash Function, LSB, Cipher, Secret Key.

I. INTRODUCTION

Security is the primary concern in the field of Information technology. For providing security, there are three important concepts namely Cryptography, Steganography and Watermarking. Arts and science keeping message secure is known as cryptography. In this, the Plaintext is converted into Scrambled message (Ciphertext). It is mainly used for Text encryption. Steganography is a method of hiding secret data, by embedding it into an audio, video, image or text file. Cryptography and steganography are both methods used to protect or hide secret data. i.e., Cryptography makes the data unreadable, or hides the *meaning* of the data, while steganography hides the *existence* of the data. Digital watermarking is the method of embedding data into digital multimedia content. This is used to verify the credibility of the content or to recognize the identity of the digital content's owner. Cryptography is classified into two types such as Symmetric Key Cryptosystem (SKC) and Public Key Cryptosystem (PKC)[9]. In Symmetric Key Cryptosystem, same key is used by both sender and receiver. It is mainly utilized for providing confidentiality. In Public Key Cryptosystem, two different keys are used by both sender and receiver. Using this PKC, one can achieve both confidentiality and authentication services. To achieve Confidentiality, Sender will encrypt the message using receiver's public key and the corresponding private key holder will decrypt the message to get the original plaintext. To achieve authentication, the message is encrypted using sender's private key and it will be decrypted using sender's public key. In Cryptography, there is one more technique used for achieving message authentication is known as hash function. Hash function accepts variable length message as input and produces fixed length output. By applying hash function one can easily construct Message Digest(MD) or h=H(M). But, from the Message Digest (MD) no one can construct original message (M). This property is known as one-way hash function or one-way property [11].

In Information hiding, there are two techniques mainly involved such as Steganography and Watermarking. Steaganography literally means "Covered writing". It's main goal is to hide data within some other data such that hidden data cannot be detected even if it is being sought. Cryptography is protecting the contents of messages whereas steganography is about concealing the existence of data[2-3, 5-7]. Digital watermarking is very similar to steganography, one of its goal is not to be detected. Typicalliy, watermarking is designed to protect intellectual property rights for images , sounds and video. The main goal of steganography is to obnubilate a message m in some audio or video (cover) data d, to obtain new data ***d'***, practically indistinguishable from ***d***, by people, in such a way that an eavesdropper ***cannot detect*** the presence of ***m*** in ***d'***.

Revised Manuscript Received on May 10 , 2019

Kalaichelvi V, Senior Assistant Professor, Dept. of CSE, SASTRA Deemed University, Kumbakonam, Tanjore, India
Manimozhi K, Assistant Professor, Dept. of CSE, SASTRA Deemed University, Kumbakonam, Tanjore, India
Meenakshi P, Assistant Professor Dept. of CSE, SASTRA Deemed University, Kumbakonam, Tanjore, India
Manikandan H, Assistant Professor Dept. of CSE, SASTRA Deemed University, Kumbakonam, Tanjore, India
Swaminathan S, Assistant Professor Dept. of ECE, SASTRA Deemed University, Kumbakonam, Tanjore, India

The main goal of watermarking is to hide a message m in some sound or video (cover) data d, to get new data d', practically the same as d, by people, in such a way that a person who secretly listens to conversations cannot remove or replace m in d'.[1,4,8] It is also often said that the goal of steganography is to hide a message in one-to-one communications and the goal of watermarking is to hide message in one-to-many communications [9-10]. Shortly, one can say that (the science of making secret codes) is about protecting the content of messages, steganography is about hiding its very existence.

II. PROPOSED METHODOLOGY

The proposed system *shown in Fig.1.* consists of the following phases such as Pixel hashing, Embedding, Extraction and Obtaining Secret message.

A. Pixel hashing

The user after starting the application is prompted to enter his secret message first and then is allowed to select a picture from his directories. Then the user is supposed to enter the secret key to start hiding the text in the image. Once the ok button of the secret key is clicked the blue pixels from the image is retrieved and their LSB's are converted to zero. The hash function is performed between each pixel and the 32 bit secret key. On the other hand, the secret message is converted in to its ASCII byte stream simultaneously.

B. Embedding

The result of the hash function is a byte stream which is equal to the bit length of the secret message. An XOR operation is performed between this hash byte stream and the ASCII byte stream obtained as one from the output in the previous module. The resulting byte stream is called the pseudo byte stream and these bits are replaced in the LSB' of the blue pixels .These pixels are converted back into an image with .png extension and it is saved in the path selected by the user and with the name specified by the user.

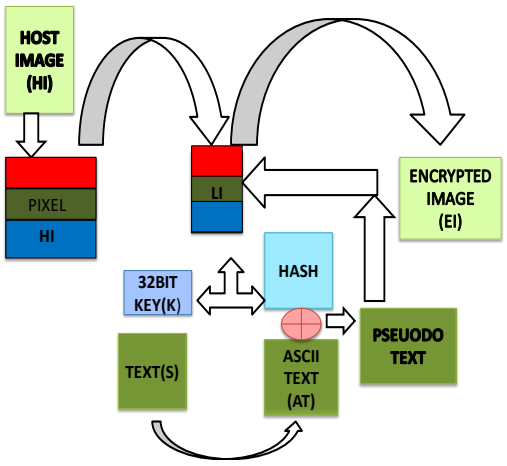

Fig.1.a) Proposed System (Sender Side)

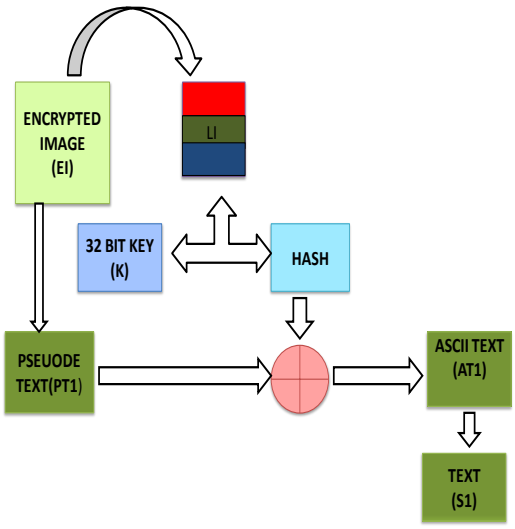

Fig. 1.b) Proposed System (Receiver Side)

C. Extraction

In order to retrieve the message embedded secretively in the image, the user has to Load the appropriate image and enter the correct secret key and secret message length. Once they are entered the blue pixels are retrieved from them and their LSB's are retrieved into a byte stream. These places are replaced with '0' bit and each of these pixels according to the message length is hashed and the resultant byte stream is obtained.

D. Obtaining Secret Message

The resultant hash byte stream obtained from the previous module is XOR'ed with the pseudo byte stream obtained already. This results in the original ASCII byte stream of the secret message. This byte stream is converted to the original message using their ASCII value and the message is displayed to the user.

Proposed Hash Function

The following hash function was proposed (shown in *Fig.2*) and used to convert the 8- bit pixel along with the 32-bit secret key to convert to a single bit, which enhances the security multiple times making it almost retractable.

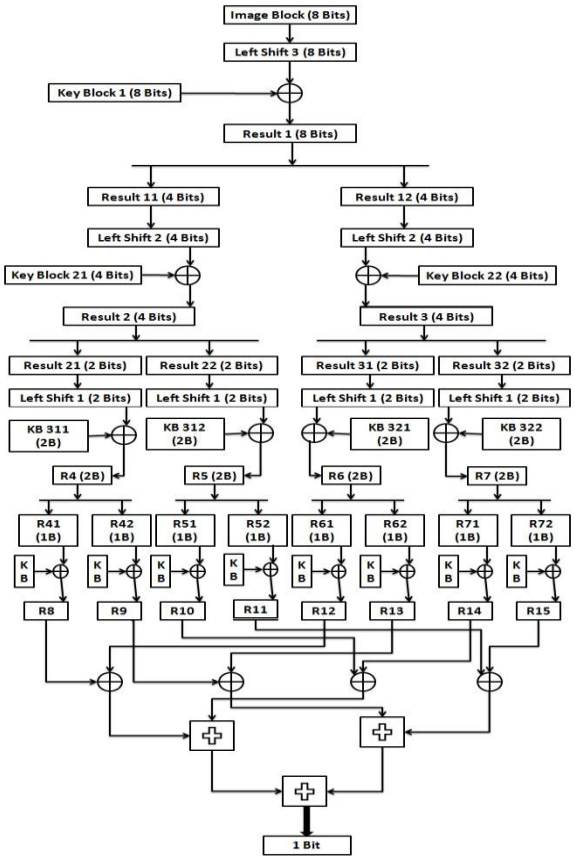

Fig.2. Proposed Hash Function

II. IMPLEMENTATION

In this section, the implementation of the various phases of proposed system is given in *Fig.3.*

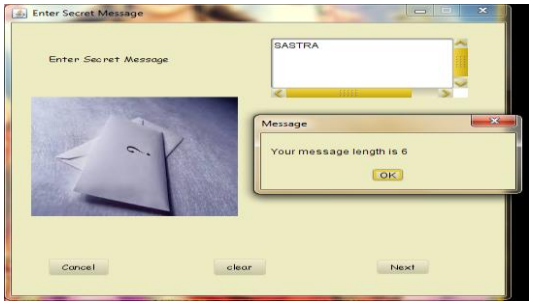

Fig.3.a) Getting Secret Message

Fig.3.b) Loading Cover Image

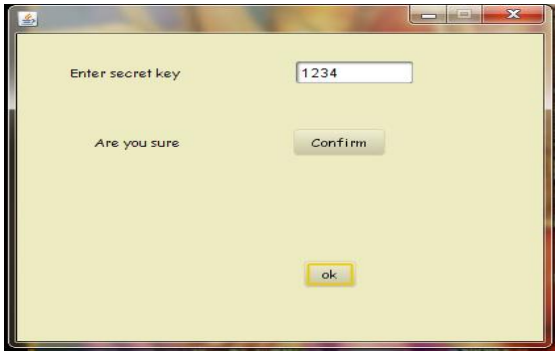

Fig.3.c) Getting Secret Key

Fig.3.d) Storing Stego Image

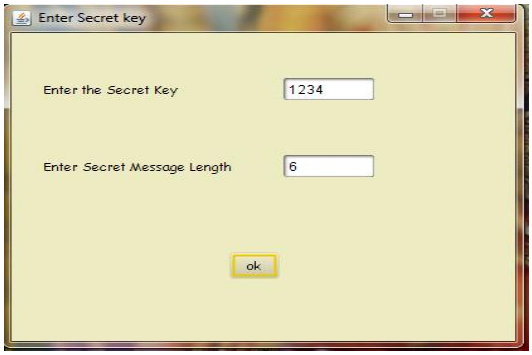

Fig.3.e) Getting Secret Key (Receiver Side)

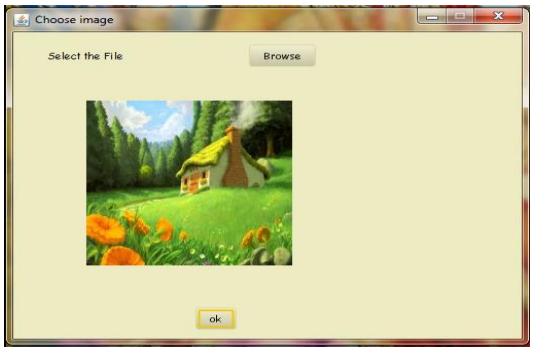

Fig.3.f) Loading Stego Image

Fig.3.g) Extracting Secret Message

III. CONCLUSION

The proposed algorithm is able to embed text strings into the color host images. With the proposed application, text passing in obnubilated form through digital color images is done in a very efficient manner. In the encrypted image the embedded text is entirely invisible. The text extraction framework is visually impaired that ensures except the secret key and message length nothing is needed to extract the obnubilated text from encrypted image. The 32-bit secret key and an efficient hash function ascertain high security aspects. Moreover, the implemented application software application software is extremely user friendly.

REFERENCES

1. F.Y.Shih, Digital watermarking and steganography: Fundamentals and Techniques, CRC Press, 2017.
2. Dr. Rajesh Kumar Pathak, Neha Jain, "AN IMPROVED LSB METHOD OF STEGANOGRAPHY WITH JPEG COLORED IMAGE", International Journal of Innovations in Scientific Engineering, (IJISE) 2017, Vol. No. 5,Jan-June-ISSN: 2454-6402, p-ISSN: 2454-812X
3. Mamta Juneja , and Dr. Parvinder S. Sandhu, "An Improved LSB based Steganography Technique for RGB Color Images", 2nd International Conference on Latest Computational Technologies (ICLCT'2013) June 17-18, 2013 London (UK)
4. Pradosh Bandyopadhyay , Soumik Das ,Monalisa Banerjee "A Fragile colour image watermarking framework focusing a new invisible domain"—published in International Conference on Communication and Computer Security, on February 2011.
5. N. Provos, P. Honeyman, Hide and seek: An introduction to steganography, IEEE Secur. Privacy 1 (2003) 32–44.
6. M. M Amin, M. Salleh, S. Ibrahim, M.R. Katmin, and M.Z.I.Shamsuddin, "Information Hiding using Steganography", 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 2003 IEEE.
7. N.F.Johnson, S.Jajodia, Exploring steganography: Seeing the unseen,Computer(Long Beach.Calif), 1998.
8. Stefan Katzenbeisser, Fabien,"Information hiding Technique for Steganography and Digital Watermarking"—published by Artech House Boston London.
9. William Stallings, "Cryptography and Network Security", 5th Edition, TMH
10. http://imagesteganography.codeplex.com
11. http://en.wikipedia.org/wiki/Hash_function

AUTHORS PROFILE

Kalaichelvi V. received her M. E. degree in Computer Science and Engineering from Annamalai University, Chidamabaram in 2004 and Ph.D. degree in Information and Communication Engineering from Anna University, Chennai in 2013. She is working as an Senior Assistant Professor in the department of Computer Science and Engineering since 2004 at SRC, SASTRA University – Kumbakonam. She has published more than 20 papers in various referred journals. Her research interests include Cryptography, Steganography and security issues in various IT fields.

Manimozhi K. received her M.C.A. degree from Bharathidasan University, Trichirappalli in 2005 and M.Tech. degree in Computer Science and Engineering from SASTRA University, Thanjavur in 2009. She is pursuing Ph.D degree in SASTRA University from 2016. She is currently working as an Assistant Professor in the department of Computer Science and Engineering since 2005 at SRC, SASTRA University – Kumbakonam. Her research interests include Cryptography, Algorithms, Steganography, Natural Language Processing, Artificial Intelligent and Expert Systems.

Meenakshi P. received her M.E. degree in Computer Science and Engineering from SASTRA university in 2007. She is pursuing Ph.D degree in SASTRA University from 2016. She is currently working as an Assistant Professor in the department of Computer Science and Engineering since 2007 at SRC, SASTRA University – Kumbakonam. Her research interests include Cryptography, Algorithms, Steganography, Wireless Sensor Networks and security issues in various fields.

Manikandan. H. received his M.E. degree in Computer Science and Engineering from Annamalai university in 2005. He is pursuing Ph.D degree in SASTRA University from 2016. He is currently working as an Assistant Professor in the department of Computer Science and Engineering since 2007 at SRC, SASTRA University – Kumbakonam. His research interests include Networking, Cloud Computing, Mobile Computing and Wireless Sensor Networks.

Swaminathan S received his M.S degree from SASTRA University in the year 2009. He is pursuing Ph.D degree in SASTRA University. He is currently working as an Assistant Professor in the department of Electronics and Communication Engineering since 2004 at SRC, SASTRA University – Kumbakonam. His research interests include wireless communication, optical communication and Wireless Sensor Networks.