ISSN [Online]: 2583-2654

Novel Approach to Data Security using Stegnography and Visual Cryptography

[1]Leelavathy S R, [2]Vedhashree.A, [3]Rekha vital biradar, [4]Jayakumari.V, [5]Hemanthkumar.N
Department of Computer Science and Engineering,
Dr.T Thimmaiah Institute of technology

Abstract: In today's Information age, Information sharing and transfer has increased exponentially. The threat of an intruder accessing secret Information has been an ever existing concern for the data communication experts. Cryptography and steganography are the most widely used techniques to overcome this threat. Cryptography involves converting a message text into an unreadable cipher. On the other hand, Steganography embeds message into a cover media and hides it existence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over unsecure communication channel and are vulnerable to intruder attacks. Although these techniques are using to achieve higher levels of security but still there is need of a highly Secure System to transfer Information over any communication media minimizing the threat of intrusion.

Steganography is a data hiding technique which uses images, audio or video as cover medium. Cryptography has become an essential part of security. Image to reduce vulnerability to cryptanalysis. We overcome the drawbacks of using textual steganography as it easier to intercept and decipher. We encrypt the plain text with a randomly generated key using XOR and One Time Pad algorithm and in turn embedding it into Least Significant Bit of the cover Image.

Keywords: Image scrambling , One time pad algorithm , visual cryptography , stego image and datasecurity.

I. INTRODUCTION

Steganography is derived from Greek words 'steganos' meaning protected and 'graphein' meaning writing. This method is used to hide data from unauthorized party which has made the technique popular as it cannot be detected easily. In recent time, steganography has improved. Vital information is being transmitted to the receiver in the presence of third party or unauthorized user without being intercepted. The most popular file formats that are being used are the digital images due to their high availability on the internet. Vital Data in the form of text, image, audio or video can be encrypted and hidden into another form of text, image, audio or video. The method of hiding data in a text file is known as textual steganography. It was very popular before the emergence of the internet. Now textual steganography has become very easy to decipher and is also not preferred as the text file cannot contain more data. Another popular method uses image as its cover medium to hide data. This method is called image steganography. Using an implanting algorithm, the data is implanted over the image which is referred to as a Stego image and sent to the receiver. It is then processed at the receiver end using the extraction algorithm process. This method allows the intruder to know that the information is being transmitted but does not allow them to see the hidden data. Audio steganography is another method that deals with encrypting the vital data in a cover speech which does not allow the unauthorized user to access the data.

ISSN [Online]: 2583-2654

II. SYSTEM ARCHITECTURE

System architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structure and behavior of the system the purpose of system architecture activities is to define a comprehensive solution based on principles, concepts, and properties logically related to and consistent with other.

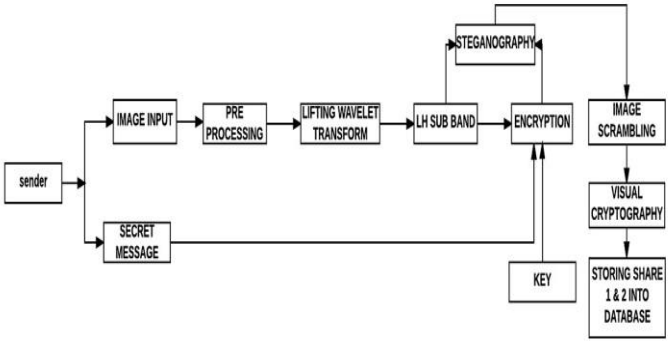

Fig 1: Encryption process

Figure 1 describes the Encryption process. Encryption is carried out at the sender side where the data is converted in such a way that unauthorized party cannot reedit. Here we need two inputs for encryption of any data namely plain text and a key. Sender will send Input as Image with secret message for that secret message we have to encrypt before that we have to do preprocessing of image. Preprocessing procedure must be carried out for the cover image before hiding the cipher text. After preprocessing we obtain LWT It is a technique to merge the all steps LWT consists LH sub band to hide the secret data. Here One Time Pad encryption algorithm provides a lot of security In this we generate a random key that has the length same as of plain text. The Randomness of the output and randomness of the key makes the algorithm unbreakable. Image Scrambling is a method of rearranging the pixels randomly to make the image visually unreadable and break the correlation between the neighbouring pixels. Then Apply visual cryptography is a method where the stego image is plit into different shares based on a threshold value and transmitted to the receiving end.

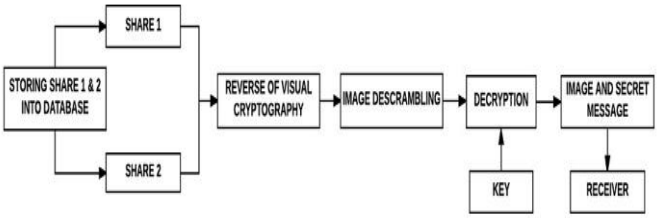

Fig 2: Decryption process

Figure 2 describes Decryption process carried out at the receiver side. The process of getting plain text from the cipher text call it as decryption process. Read the two shares of image from encryption and apply addition operation on both he shares and save the overlapped Image. Using key decrypt the image and extract the secret message at the receiver side.

III. METHODOLOGY

3.1 *XOR Cryptography*

It is one of the simplest cryptographic methods which uses the XOR operation. The data or message is encrypted using a key and XOR operation. The encryption and decryption are carried out by XORing the message and the cipher text respectively. The plain text is converted to its ASCII value and in turn converted to its binary form in 8, 16 or 32-bits form. The key that is being generated is also converted into 8, 16 or 32 bits form respectively. The key could be a single character or a string. In the case of a string each and every character's bits are XORed to form a key. Now each character's bits of the data are logically XORed with bits of the key. The resulting value is the cipher text for the given message. In this system we make use of an 8 bit key for the encryption process. The user provides the input key which is converted into 8 bit binary key. Figure 6.1 shows the flow chart for key generation.

ISSN [Online]: 2583-2654

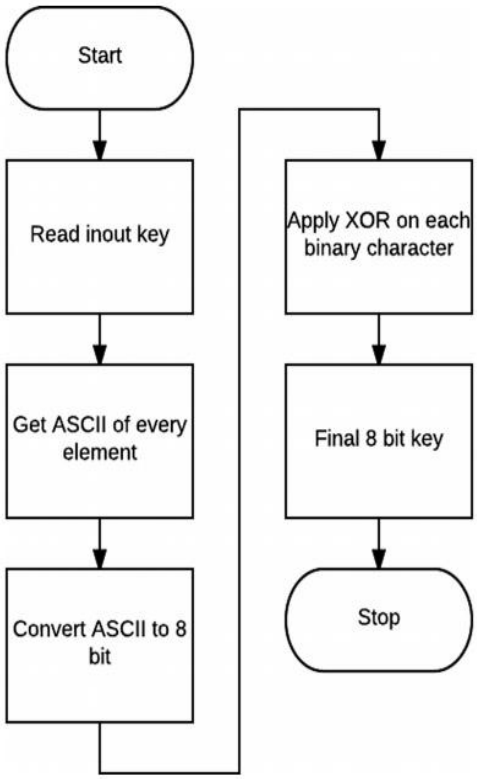

Fig 3.1: XOR key generation

After the key is obtained as XOR encryption is performed. Figure 6.2 shows the flow chart for the XOR encryption process. The plain text characters are given as an input from the user, which is converted into its ASCII format and in turn into its corresponding binary format.

XOR-key generation

Key ASCII Binary format Applying XOR Hello h-104 h-0110 1000 h-0110 1000 e-101 e-0110 0101 he-0000 1101 l-108 l-0110 1100 hel-0110 0001 l-108 l-0110 1100 hell-0000 1101 o-111 o-0110 1111 hello-0110 0010 key-0110 0010

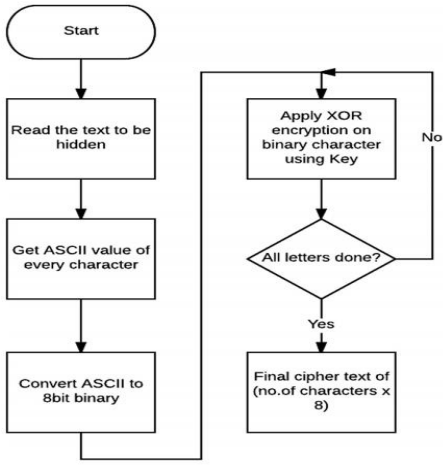

Fig 3.2: XOR encryption process

Combining all the obtained values from cvalue_1, cvalue_2, cvalue_3, cvalue_4 will give us the final cipher text. The final length of the cipher text depends on the number of characters in the plain text. Number of cipher text bits = number of characters in plain text * number of bits in key.

IV. IMPLEMENTION MODULES

- One Time Pad Encryption
- Steganography Process
- Scrambling Process
- Visual Cryptography Encryption
- Visual Cryptography Decryption
- Descrambling Process
- Message extraction
- One Time Pad Decryption

4.1 One Time Pad Encryption

One-Time Image is a program written in Java to encrypt images using the principle of the one-time pad to create a pair of black and white images. Each appears as a 'snow' of black and white pixels, and no information can be extracted from either image on its own - unlike most cryptography, it is not merely 'very difficult' to extract information: an implementation of the one-time image principle with true random numbers is *perfectly* secure and unbreakable (see the section entitled 'Increasing Security' for why this

ISSN [Online]: 2583-2654

is not true of this program, and how to make it so). However, despite the fact that no information can be retrieved from either image on its own, if both are printed onto transparencies and one is laid directly over the other, the original image will immediately and clearly appear.

How does it work?

The principle of the one-time pad was developed during World War One, though it was 25 years before a mathematician proved it was perfectly secure, as opposed to merely prohibitously difficult to break. It is a very simple substitution cypher (a type of cypher where A becomes C, B becomes D etc, for example), but with the twist that the key is the same length as the message. As a result each letter has its own unique (and random) rotation, making the encoded message proof against any sort of analysis without the key. The final result is a pair of random-looking message (one the encrypted message, one the key used to encrypt it) of the same length, either of which cannot be broken or analysed in any way on its own, but which can easily be decoded once the two are brought together.
One-Time Image extends the principle to that of images. First, the source image is converted to black and white (not greyscale, true black and white with pixels of only these two different colours).

Secondly a key image is generated, of the same dimensions, where each pixel is randomly set to white or black. Third, the original image is encrypted using this key - if the pixel in the key is white then the corresponding pixel in the original image is used in the encrypted image, whereas if the key pixel is black then the corresponding pixel in the original image is flipped (black to white, white to black) for the encrypted image. The result is two images of apparently random black and white pixels.

Finally, each image is then doubled in size - each pixel becomes a 2x2 square of pixels. Black pixels have black pixels in the top-left and bottom-right corners while the other two pixels are while, while a white pixel in the original image produces the opposite 2x2 square. These enlarged images are the final ones. The trick is that, when printed onto transparencies and one is laid over the other (the order is irrelevant), the original image is suddenly revealed! This is because a black pixel in the original image produced pixels of different colour in the key and encrypted images (one black, one white). Since these black and white pixels became 2x2 squares with two black and two white pixels, when overlaid all four pixels in the square become black. However, a white pixel in the original produced pixels of matching colour in the key and encrypted images (both black, or both white). Hence the 2x2 squares in the final images are identical, and when overlaid half the pixels remained white. Hence, when you look at the image from anything but very short range, these 2x2 squares look grey while other look black.

4.2 Steganography Process

It is the process of hiding the plain text or cipher text in an image. The LSBs of the pixels of the image are used to hide the data. All images have smooth color variations (low frequency variations) and sharp color variations (high frequency variations). Both these variations together form a complete image. Separations of these two variations are carried out in many ways, one such way that we are incorporating in out project is the discrete Wavelet transform (DWT) to obtain the frequency bands . The wavelet transforms of any image gives 4 bands of each 1/4th the size of the image. The lower frequency components or the smooth variations forms the base of the image is present in the LL band. This will have the approximate image of the input image . LH and the HL are the middle frequency bangs which extract the horizontal features and vertical features respectively. We can either use LH or HL band for steganography, in this project we make use of LH band.

4.3 Scrambling Process

Now the Stego image is which is the image where in the message or data is hidden or encrypted. To make it more secure we make use of image scrambling.

ISSN [Online]: 2583-2654

Image scrambling is a technique in which the pixel location of the image is modified or rather scrambled to form a chaos image or the scrambled image . This scrambled image can be reconstructed only if the scrambling method and variables are known . We make use of the scrambling method for scrambling the image column wise and row wise. In this project, we first shuffle the column pixels and then the row pixels.

4.4 Visual Cryptography Encryption

Visual cryptography is an encryption technique where the visual information is encrypted by breaking it into shares. It can be decrypted only if the person has all 'n' shares of the image. In visual cryptography, we break the image into two or more shares based on a threshold value. Depending on the threshold, much different number of shares can be formed . The threshold that we make use of can be separating white pixels from the black pixels or separating the even numbered rows from the odd numbered rows or even numbered columns from odd numbered columns . In this project we have chosen the threshold to produce shares by separating even numbered columns and odd number of columns. All columns are numbered alternatively as 1 and 2. The first share has all columns numbered 1 and the second share has all columns numbered 2.

4.5 Visual Cryptography Decryption

In the decryption process, the two shares which are received in image and are combined by using the same threshold that we used for encryption. The two shares are added to form the scrambled image.

4.6 Descrambling Process

Descrambling is the process in which the pixel locations are shuffled . This is the reverse process of the scrambling algorithm. The image that we have recovered after visual cryptography decryption is used and the descrambling process is applied to obtain the Stego image in which the message is hidden as depicted.

4.7 Message Extraction

This process is used to extract the hidden message from the Stego image. In this paper we have hidden the message in the LSB's of the image. Once the message is obtained, we must check if the message is in plain text format or cipher text format. If it is in the cipher text format, we must perform the required decryption process and obtain the plain text.

4.8 One Time Pad Decryption

OTP is one of the most secure and unbreakable algorithms. It can only be decrypted with the help of a key that was used for encryption. The key is a randomly generated one which makes the process unbreakable. If the intruder manages to find two different keys, then two different plain texts are obtained which will make it difficult for the intruder to guess the right plain text The obtained message is grouped into 8's, where 8 bits represent a character. Now they are converted back into their respective ASCII character hence forming cipher text. Now the decryption of this cipher text is carried out to get the plain text.

V. CONCLUSION AND FUTURE SCOPE

The proposed method has multiple encryption and decryption process such as XOR, OTP, Steganography , Image scrambling and visual cryptography. All these processes when used individually would give protection but not as much protection as it would give when all of them are combined it increases confusion as well as diffusion to the unauthorized party.

It can be concluded that with the use of multiple cryptographic techniques,it is made difficult for the unauthorized party to get the message. The One time pad algorithmis one of the most secure type of encryption which makes it impossibleto decrypt the code because of the ramdom key used. Thus, the proposed system can with stand any kind of attacks. Using visual cryptography and image scrambling we have been able to enhance the regular image security.

ISSN [Online]: 2583-2654

REFERENCES

[1]. Prema,G.,and S. Natarajan. ***"Steganography using genetic algorithm along with visual cryptography for wireless network application."*** *In international Conference on Information Communication and embedded system ,pp.398-461, 2013.*

[2]. Liping, Shao, et al. ***" Image scrambling algorithm based on random shuffling strategy."*** *In Conference on industrial Electronics and Applications, pp.2278-2283, 2008*

[3]. Kanan, Hamidreza Rashidy, and Bahram Nazeri. ***" A Novel image steganography scheme with high embedding capacity and tunable visual image quality based on genetic algorithm."*** *A Journal on Expert systems with applications vol.41, no.14 ,pp.6123-6130, 2014.*

[4]. Hussian, M., et al. ***"Image steganography in spatial processing."*** *A Journal on Signal processing:Image Communication vol. 65, pp.46-66 ,2018.*

[5]. Blesswin,J., Rema, Joselin,J. ***"Recovering secret image in visual cryptography."*** *In International Conference on Communication and Signal Proccessing pp.538-542, 2011.*

[6]. Jena, D., Jena, S,K. ***"A novel visual cryptography scheme."*** *In : International Conference on advance Computer Control, pp.207-211, 2009.*

[7]. Che, S., Che, Z., Ma,B. ***"An improved image scrambling algorithm."*** *In Second International Conference on Genetic and Evolutionary Computing, pp.495-499, 2008.*

[8]. Ghasemi,e.,Shanbehzadeh, J., Faassihi, N. ***"High capacity image steganography using wavelet transform and genetic algorithm."*** *Manuscript received vol.2188, pp.495-498, 2011.*

[9]. AI-Bahadilli, H. ***"A secure block permutation image steganography algorithm."*** *Cryptography information Secure. Vol.3, no.3, pp.11-22, 2013.*

*[10]. Usha, B.A.,Srinath, N,K., Sangeetha, K,N.*** **"A secure data embedding technique in image steganography for media imges."*** *International journal od advanced research in computer and communication engineering vol.2, no.5, pp.2319-5940, 2013.*

[11]. Gundapuneni, Manas Abhilash,. ***"Enhanced Security Architecture for visual cryptography based on image secret sharing."*** *In ubiquitous computing, Electronics & mobile communication conference, pp.0749-0755, 2020.*

[12]. Manimurugan,S., and C.Narmatha. ***"Secure and efficient medical image transmission by new tailored visual cryptography scheme with LS compressions."*** *International Journal of Digital Crime and Forensics vol.7, no.1, pp.26-50, 2015.*

[13]. Shao,Z., Shang,Y., Zeng,R., Shu, H., ***"Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography."*** *Signal Processing:Image communication vol.48, no.5, pp.12-21, 2016.*

[14]. A Imagawa, Takanori, Suyama, Shiro,Yamamoto,Hirotsugu. ***"Visual crptography using polarization modulation films."*** *Japanese journal of applied physics vol.48, no.9S2, pp.492-587, 2009.*

[15]. Shankar,K., and P.Eswaran. ***"RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography."*** *Journal of china Communication vol.14, no.2, pp.118-130, 2017.*

[16]. A Shanakar, K , Eswaran, P. ***"Sharing a secret image with encapsulated shares in visual cryptography."*** *Journal procedia Computer Science vol.70, no.3, pp.462-468, 2015.*