Combined Steganography

[1]Sourabh Madane, [2]Rahul Badure, [3]Santosh Sarvade, [4]Prof.S.L.Utpat
Department Of Computer Science And Engineering, SVERI's COE Pandharpur.

Abstract- *One of the explanations that intruders are often productive is that the most of the data they acquire from a system is in a very type that they'll scan and comprehend. Intruders could reveal the data to others, modify it to misrepresent a private or organization, or use it to launch AN attack. One answer to the present downside is, through the employment of steganography. Steganography may be a technique of concealing data in digital media. In distinction to cryptography, it's to not keep others from knowing the hidden data however it's to stay others from thinking that the data even exists. Steganography become additional necessary as additional folks be part of the Internet revolution. Steganography is that the art of concealing data in ways in which prevents the detection of hidden messages. Steganography embrace AN array of secret communication ways that hide the message from being seen or discovered.*

Keywords: Attack, Steganography, Digital media, Cryptography.

1. INTRODUCTION

Due to advances in ICT, most of data is unbroken electronically. Consequently, the safety of data has become a basic issue. Besides cryptography, steganography are often used to secure data. In cryptography, the message or encrypted message is embedded in a very digital host before passing it through the network, so the existence of the message is unknown. Besides activity knowledge for confidentiality, this approach of data activity are often extended to copyright protection for digital media: audio, video and pictures. The growing prospects of recent communications want the special suggests that of security particularly on electronic network. The network security is changing into additional vital because the range of information being changed on the web will increase. Therefore, the confidentiality and knowledge integrity area unit needs to guard against unauthorized access and use. This has resulted in Associate in Nursing explosive growth of the sphere of data activity Information activity is Associate in Nursing rising analysis space, that encompasses applications like copyright protection for digital media, watermarking, process, and steganography.

In watermarking applications, the message contains data like owner identification and a digital time stamp, that typically applied for copyright protection.

Fingerprint, the owner of the information set embeds a serial range that unambiguously identifies the user of the information set. This adds to copyright data to makes it attainable to trace any unauthorized used of the information set back to the user. Visual steganography is one among the foremost secure sorts of steganography on the market nowadays. it's most typically enforced in image files. but embedding knowledge into image changes its color frequencies in a very inevitable method. to beat this foregone conclusion, we tend to propose the construct of multiple cryptography wherever the information are going to be encrypted into a cipher and therefore the cipher are going to be hidden into a multimedia system image come in encrypted format. we tend to shall use ancient cryptographical techniques to realize encryption and visual steganography algorithms are going to be accustomed hide the encrypted knowledge.

2. RELATED WORK

The former consists of linguistic or language kinds of hidden writing. The later, like invisible ink, strive of hide messages physically. One disadvantage of linguistic steganography is that users should equip themselves to own a decent information of linguistry. In recent years, everything is trending toward conversion. And with the event of the web technology, digital media is transmitted handily over the network. Therefore, messages is on the Q.T. carried by digital media by exploitation the steganography techniques, then be transmitted through the web speedily Steganography is that the art of concealment the actual fact that communication is going down, by concealment info in alternative info. many various carrier file formats is used, however digital pictures ar the foremost well-liked attributable to their frequency on the web. For concealment secret info in pictures, there exists an oversized kind of steganography techniques some ar additional advanced than others and every one of them have several robust and weak points. thus we have a tendency to prepare this application, to form the knowledge concealment additional straightforward and user friendly.

3. PROPOSED WORK

Cryptographic algorithms typically would like a reference table that aids the conversion of alittle block of knowledge into another block (may not be a block of knowledge within the original content). so as to supply higher security levels the rule is meant to use a reference information as shown in Fig.. The reference information can accommodates numerous reference grids. every of those grids can have a 3D representation of the encryption schema which can be accustomed represent the characters in terms of specific numbers. (The same range civil authority might not represent completely different|a special|a unique|a distinct} character in an exceedingly different grid)Fig. Matrices in an exceedingly Grid of the Reference information

I. Encryption rule

The message can initial be encrypted victimisation asymmetric Key Cryptography technique. the info are going to be encrypted victimisation basic DES rule. This cipher can currently be hidden into a multimedia system file. The cipher are going to be saved within the image employing a changed bit encryption technique by truncating the picture element values to the closest zero digit (or a predefined digit) then a particular range that defines the3-D illustration of the character within the cipher code sequence are often accessorial to the present range. for each character within the message a particular modification are going to be created within the RGB values of a picture element. (This modification ought to be but five for every of R,G and B values)

This deviation from the first worth are going to be distinctive for every character of the message. This deviation conjointly depends on the precise information block (grid)selected from the reference information. for every computer memory unit

within the information one picture element are going to be altered. therefore one computer memory unit of knowledge are going to be hold on per picture element within the image.

during this methodology the cipher sequence are often decoded while not the first image and solely the altered image are going to be transmitted to the receiver. within the initial few lines of image properties, the attributes of the image are going to be encrypted and saved therefore on give America the knowledge if the image is altered or changed or the image extension has been modified like jpg to gif. These properties are often utilized in the coding (identifying the proper block of knowledge from the info grid). therefore solely the proper encrypted image within the correct format can manufacture the sent message.

For coding, the receiver should grasp that image to rewrite and within which format as dynamical the image format changes the colour distribution of the image. each image provides a random information on coding that has no which means. however solely the proper format coding provides the first message. once activity the info within the image, the image are going to be sent to the receiver. The receiver ought to have the coding key (private key) which can be accustomed rewrite the info.

II Decryption rule

- The message are often decoded victimisation Associate in Nursing mathematical function (as utilized in ancient techniques) victimisation the receiver's non-public key. This key are often a neighborhood of the image or a text or any attribute of the image.
- The receiver's non-public secret is accustomed determine the network from the reference information.
- once choosing the proper grid, the x and y element of the image will outline the block that has been accustomed cypher the message and also the RGB values will purpose to the info within the block known by the x, y element as shown in Fig. 3.Fig. three Matrix in an exceedingly grid of Reference information
- The cipher is retrieved by getting the distinction within the picture element worth from the nearest predefined value(zero truncation). These numbers can currently outline the saved bit and can kind the cipher text.
- This cipher will currently be decrypted victimisation Associate in Nursing mathematical function of the Drug Enforcement Administration rule to induce the message text.

4. RESULT & DISCUSSION

The system was designed using an image of size 200x150(30000) pixels. Initially, the pixel values were incremented tothe next higher multiple of 5. The message text was converted into cipher text using DEA algorithm. The secret key used was 'This is the Secret Key'. Maximum possible size (29 Kb) of message data was taken considering one byte per pixel. The cipher text was then embedded into the jpeg image by pixel variation (decrement) of the selected value that was between 0-3 for R, 0-4 for G and 0-4 for B values of the pixel. The reference database consisted of 3 data grids. The data grid was selected on the basis of the number of pixels of the image. If the pixels were less than 1, 00,000pixels the data grid 1 was selected, if they were between 1,00,000 and 10, 00,000 then the data grid 2 was selected else the data grid 3 was selected. Each data grid had 20 matrices which were selected on the basis of the height to width ratio. The image containing message data was found to have no visible distortion. Encryption result of the application. For decryption the cipher was retrieved by checking the pixel variations and inverse DEA function was applied to retrieve the message. To retrieve the cipher from the image, the difference in the pixel value from the next higher multiple of5 was calculated. The correct data grid from the reference database was selected on the basis of the number of pixels in the image. The correct matrix from the data grid was selected on the basis of the height to width ratio. After this the encrypted message was retrieved from the image. The inverse DEA function was applied to this encrypted message in order to retrieve the original message text. The steganocryptic algorithm combines the features of cryptography and steganography and hence provides a higher level of security than either of the techniques alone. The algorithm also is more secure than a normal cryptographic system as the encrypted data is hidden into a multimedia file and then transmitted. It is also more secure than a Steganography system as the data to be hidden is in an encrypted format. The algorithm scores over traditional visual steganography systems like LSB encoding as it implements multiple encryptions. The image bits are used not to store the message but a slight deviation which correspond to a unique character. This deviation is then retrieved from the image and used to decrypt the original message. The image used for encryption is jpeg as it has the least deviation of embedding data.

5. CONCLUSION

Cryptography and steganography are renowned methods for data security. to enhance the security we can use combined cryptography and steganography instead of using cryptography or steganography alone. In this paper we have reviewed various mixtures of cryptography and steganography strategies. Here we tend to square measure dealing with image primarily based steganography thus reduce the image quality degradation is that the main task so as to enhance security. From the a bovecomparison we will infer that DWT primarily based steganography with AES coding will give higher security as a result of this methodology can retain the image quality.

9. REFERENCES

[1] A. Joseph Raphael Dr. V. Sundaram, "A Survey on cryptography and steganography", Int. J. Comp. Tech. Appl., Vol 2 (3), ISSN:2229- 6093

[2]Dipti Kap
oor Sarmah, Neha bajpai, " Proposed System for Data Hhiding Using Cryptography and Steganography", International Journal of Computer Applications (0975 –8887), Volume 8 –No. 9, October 2010.

[3]Sashikala Channalli and Ajay Jadhav, "SteganographyAn Art of Hiding Data", International
Journal on Computer Science and Engineering Vol.1(3), 2009.

[4]Ramakrishna Mathe, Veera RaghavaRao Atukuri, Dr. Srinivasa Kumar Deviredd "Securing
Information: Cryptography and Steganography", International Journal of Computer Science and
Information Technologies, Vol. 3 (3), 2012.

[5]Khalil Challita and Hikmat Farhat, "Combining Steganography and Cryptography: New Directions", The

Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085).

[6].Anjali A. Shejul, Prof.U.L Kulkarni, "A DWT based Approach for Steganography Using Biometrics" 2010 International Conference on Data Storage and Data Engineering.

[7].C.P.Sumathi, T.Santanam and G.Umamaheswari "A Study of Various Steganographic Techniques Used for Information Hiding" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[8] Dr. Ekta Walia a , Payal Jain b , Navdeep c, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology Vol. 10 Issue 1 (Ver 1.0), April 2010.