Image Steganography with Double Stegging by PVD and AES Encryption

Mustafa Badlawala[1] Fazeel Ansari[2] Ibrahim Shaikh[3] Nayana Chaskar[4]

[1,2,3,4]Department of Electronics & Communication Engineering

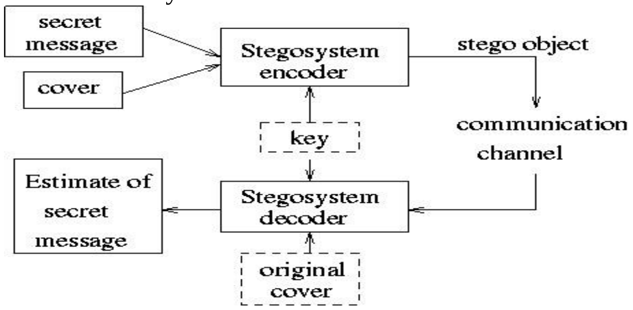
[1,2,3,4]M.H, Saboo Siddik College of Engineering, Maharashtra, India

Abstract— Web is a major means for exchanging parcel of information as pictures, content, and all interactive media. Information security is a noteworthy worry as far as its accessibility, privacy and confirmation objectives. Correspondence channel security additionally assumes an essential part, however channel can be traded off so there is need of information security and its classification. Pictures serve a method for exchanging part of information furtively. The proposed framework utilizes Cryptography and Steganography strategies to guarantee information trustworthiness and security. Cryptography gives encryption of information and Steganography gives secure exchange of correspondence of information through transmitting media. Steganography with Double stegging is connected for the scrambled information into a spread media for concealing its presence.

Key words: Steganography, Cryptography, AES Encryption, Pixel Value Differencing (PVD), Discrete Wavelet Transform (DWT), Double Stegging

I. Introduction

Presently, those day's Internet has turned into an essential medium for communicating and there is a need of security against harmful and accidental assaults. So with a specific end goal to secure privacy and integrity of information against attackers numerous procedures like steganography and cryptography are utilized. Steganography conceals the information into spread media where cryptography encodes the information by changing it into an emit position which is not readable to individual. Picture steganography is the specialty of data covered up into spread picture, is the procedure of concealing secret message inside another message. The data concealing procedure in a steganography with various methods incorporates distinguishing spread mediums repetitive bits. The replacing so, as to insert process makes a stego medium the repetitive bits with information from the concealed message. Amid the procedure of concealing the data three elements must be viewed as that are limit it incorporates measure of data that can be covered up in the spread medium. Security infers to identify shrouded data and Robustness to the measure of change the stego medium can withstand before an attacker can annihilate concealed data. Primary goal of steganography is to Communicate safely in a manner that the genuine message is not readable to the spectator. Utilizing steganography a secret message is implanted inside a bit of unsuspicious data and sent without anybody knowing the presence of the mystery message. Privileged insights can be covered up inside a wide range of spread data that is content, picture, sound, video, and so forth. Most steganography utilities conceal data inside picture, as it is moderately simple to actualize pictures is generally utilized as a part of the procedure or of steganography since it is difficult to break. Cryptography approach for security of mystery information, where the information will be changed over into an in good spirits, which will be then put off the beaten path into a picture. Scrambled mystery. [2] Information is hided into a picture utilizing PVD steganography. So as to empower substantial measure of room of information and supporting great seeing nature of the spread picture, implanting is sent in name for by adjusting the subtle elements coefficients in roll out incredible improvement lands ruled over of Pixel Value Differencing (PVD). The thought of Double-Stegging is utilized and to alter the information into the picture with enhanced secrecy.



Fig, 1: Methodology

The proposed system uses cryptographic and steganography techniques and image segmentation with compression techniques for implementation. The techniques used are listed as follows:

A. *Cryptography*

Cryptography is the art of protecting the data or information by converting the data into an undetectable form unreadable by human being. This type of unreadable data is said as “Cipher Text”. The process of Encryption and Decryption is done on the plain text data with using a key. This process helps to prevents unauthorized access to data of transmitted data via untrusted media. [1]

The Cryptographic system should comprise of:

- Authentication: The process of providing identity to the recipient.
- Integrity: Ensure that data is not modified while transmission and reception of data.
- Confidentiality: Ensure that no unauthorized access is done to system.
- Different cryptography types are there:
- Symmetric key (Secret): It uses single key for encryption and decryption.
- Asymmetric Key (Public): It uses two keys, one for encryption as it is secret to user; and another key public to recipients.

In this paper we are using Symmetric key (Secret) cryptography i.e. AES (Advanced Encryption Standard) algorithm.

1) *AES (Advanced Encryption Standard)*

The most mainstream and broadly utilized till date symmetric encryption calculation is the Advanced Encryption Standard (AES). It is found no less than six time quicker than triple DES. A need to supplant DES was required as its key size was too little. With expanding figuring power, it was viewed as attackable against comprehensive key hunt assault. Triple DES was intended to defeat this weakness yet it was discovered moderately slowly. [9].

The components of AES are as per the following –

- Symmetric key, symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and speedier than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java [9]

AES is an iterative as opposed to Feistel figure. It depends on 'substitution–permutation system'. It contains a progression of connected operations, some of which include supplanting inputs by particular yields (substitutions) and others include rearranging bits around (permutations).Interestingly, AES performs every one of its calculations on bytes instead of bits. Henceforth, AES treats the 128 bits of a plaintext obstruct as 16 bytes. These 16 bytes are organized in four sections and four columns for preparing as a lattice − Unlike DES, the quantity of rounds in AES is variable and relies on upon the length of the key. AES utilizes 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds utilizes an alternate 128-bit round key, which is computed from the first AES key. [9]

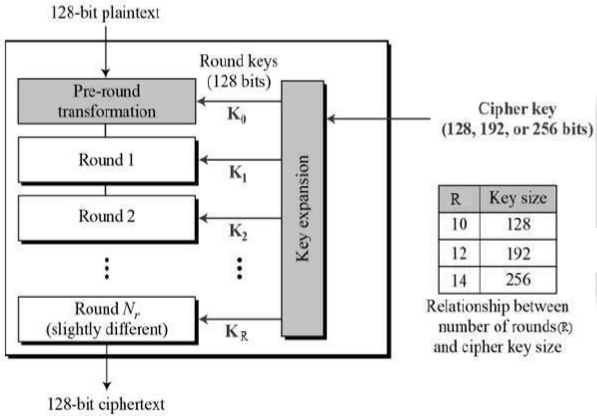


Fig. 2: Operation of AES [9]

a) Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below

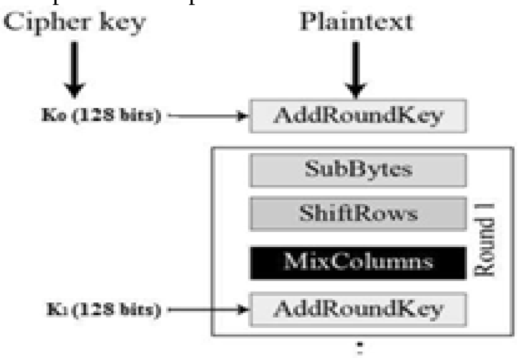


Fig. 3: AES Process [9]

- First Round Process

Byte Substitution (Sub Bytes)

The 16 information bytes are substituted by turning upward a settled table (S-box) given in configuration. The outcome is in a grid of four lines and four segments. [9]

- Shift lines

Each of the four lines of the framework is moved to one side. Any sections that 'tumble off' are re-embedded on the right half of line. Movement is completed as takes after −

To begin with line is not moved. Second line is moved one (byte) position to one side. Third line is moved two positions to one side. Fourth line is moved three positions to one side.

The outcome is another framework comprising of the same 16 bytes however moved as for each other. [9]

- Blend Columns

Every section of four bytes is presently changed utilizing an extraordinary scientific capacity. This capacity takes as data the four bytes of one segment and yields four totally new bytes, which supplant the first section. The outcome is another new lattice comprising of 16 new bytes. It ought to be noticed this stride is not performed in the last round. [9]

- Include round key

The 16 bytes of the framework are currently considered as 128 bits and are XOR'ed to the 128 bits of the round key. On the off chance that this is the last round then the yield is the figure content. Something else, the subsequent 128 bits are deciphered as 16 bytes and we start another comparable round. [9]

B. Decryption Process

The procedure of unscrambling of an AES figure content is like the encryption process in the converse request. Each round comprises of the four procedures led in the opposite request −

Include round key
Blend segments
Shift columns
Byte substitution

Since sub-forms in each round are backward way, not at all like for a Feistel Cipher, the encryption and decoding calculations should be independently executed, in spite of the fact that they are firmly related.

C. AES Analysis

In present day cryptography, AES is generally embraced and bolstered in both equipment and programming. Till date, no reasonable crypt analytic assaults against AES has been found. Moreover, AES has worked in adaptability of key length, which permits a level of 'future-sealing' against advancement in the capacity to perform comprehensive key quests.

Be that as it may, generally with respect to DES, the AES security is guaranteed just in the event that it is effectively executed and great key administration is utilized. [9]

1) Steganography

Image steganography is the art of information hidden into cover image, is the process of hiding secret message within another message. The word steganography in Greek means “Covered Writing”. The information hiding process in a steganography with different techniques includes identifying cover mediums redundant bits. The embedding process creates a stego medium by replacing the redundant bits with data from the hidden message. During the process of hiding the information three factors must be considered that are capacity it includes amount of information that can be hidden in the cover medium. Security implies to detect hidden information and Robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

Algorithm used is Pixel Value Differencing for Steganography

2) Pixel Value Differencing

The pixel-value differencing (PVD) scheme uses the difference value between two consecutive pixels in a block to determine how many secret bits should be embedded. There are two types of the quantization range table in Wu and Tasi's method. The first was based on selecting the range, widths of [8, 8, 16, 32, 64, 128], to provide large capacity. The second was based on selecting the range widths of [2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, 64], to provide high imperceptibility. Most of the related studies focus on increasing the capacity using LSB and the readjustment process, so their approach is too conformable to the LSB approach. There are very few studies focusing on the range table design. Besides, it is intuitive to design it

By using the width of the power of two. This work designs a new quantization range table based on the perfect square number to decide the payload by the difference value between the consecutive pixels. Our research provides a new viewpoint that if we choose the proper width for each range and use the proposed method, we can obtain better image quantity and higher capacity. In addition, we offer a theoretical analysis to show our method is well defined. The experiment results also show the proposed scheme has better image quantity and higher capacity. [10]

In PVD strategy pixel values in the stego picture might surpass the dim scale range which is not alluring as it might prompts dishonorable representation of the stego picture. In this area we acquaint a strategy with conquer this issue. In the proposed strategy we have utilized the first. PVD strategy to install mystery information. In the event that any pixel esteem surpasses the reach (0 to 255), then check the bit stream ’t’ to be covered up. In the event that MSB (most huge bit) of the chose bit stream "t" is 1 then we implant one less number of bits, where MSB position is disposed of from t; generally the bit number of concealed information relies on upon bit. For example, if pixel esteem surpasses the extent and chose bit stream t=101, then set t=01 and implant it. On the off chance that it is seen that the pixel esteem again surpassing reach, then insert the worth at one pixel, as opposed to both pixels(of the pixel bit), which won't surpass the extent subsequent to installing; where the other pixel is kept unaltered. It will keep the pixel values inside of the reach on the grounds that both pixels of a square can't surpass in the time according to the PVD technique. Keep the data inside of every bit, whether one less bit is implanted or not, as overhead. [10]

Step 1: Steganography is connected to cover picture to implant the encoded information into one of the point of interest Coefficients which brings about stego-picture.

Step 2: Steganography is again connected to insert that detail coefficient to another zone of point of interest coefficient of that picture. The picture with mystery information is then prepared for Transmission. The extraction handle likewise requires 2 stages for unraveling.

D. Extraction Process

It requires two phases of disentangling to recuperate the first mystery information. The principal phase of interpreting is done to recuperate the primary subtle elements coefficient from the second points of interest coefficient. The second stage disentangling includes recuperating the first mystery information from the main subtle elements coefficient. The benefit of this technique is that the first cover picture does not need to be available on the beneficiary side for the fruitful reproduction of the first information. Subsequently, the danger of divulgence of mystery correspondence is lower.

Step 1: The unraveling procedure is done to remove the initially itemized coefficients from the second detail coefficient.

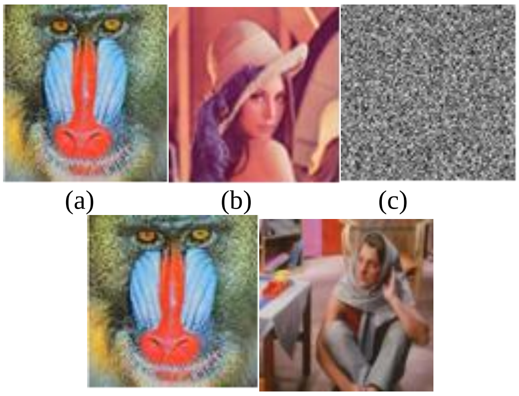
Step 2: The second deciphering includes extraction of mystery information from first detail coefficient. This procedure incorporates straightforward modulo operations of stego-picture coefficients. The last stage at the beneficiary side incorporates the decoding procedure of the figure content by unscrambling key utilizing AES calculation.

E. Embedding Using Double Stegging

Stegnography is performed twice here. The information is initially hided in a picture and after that for a twofold watch to the security of that information the picture is again stegnographed in another picture. For inserting information figure content is changed over into 8-bit twofold code. This twofold code is implanted into spread picture. It utilizes the way that, Human visual framework is having low affectability to little changes in computerized information. It adjusts pixel estimations of picture for information covering up. Spread pictures is parceled into non-Overlapping bits of two sequential pixels. Contrast between the two successive pixel qualities is figured. These distinction qualities are ordered into number of reaches. Range interims are chosen by qualities of human vision's affectability to dim worth varieties from smoothness to differentiate. A little distinction esteem demonstrates that the bit is in a smooth territory and an expansive one shows that the square is in an edged range. The pixels in edged zone can endure bigger changes of pixel qualities than those in the smooth territory. So we can insert more information in the edged territories than the smooth zones. The distinction esteem then is supplanted by another worth to implant the estimation of a sub-stream of the mystery message. The quantity of bits which can be installed in a pixel pair is chosen by the width of the reach that the distinction esteem has a place with. The technique is composed in a manner that the change is never out of the reach interim. This strategy not just gives a superior approach to installing a lot of information into spread pictures with imperceptions, additionally offers a simple approach to achieve mystery. This technique gives a simple approach to create a more impalpable result than those yielded by straight forward slightest huge bit substitution strategies.

II. RESULTS

Below shown are some examples of steganography techniques applied on images.



(a) (b) (c)

(d) (e)

(Left to Right): (A) Cover Image, (B) Secret Image, (C) Encrypted Image, (D) Steganography image (1st time stegging), (E) Double Stegged Steganography image.

MSE of Steganography Image (1st time stegging): 5.16986

PSNR of Steganography Image (1st time stegging): 40.996

MSE of Steganography Image (Double stegging): 2.70019e-09

PSNR of Steganography Image (Double stegging): 195.37

III. Conclusion

A different approach for steganography technique has been discussed. The steganography is done using pixel value differencing method (PVD) with AES Encryption standard. This paper provides more accurate approach towards security and data hiding. AES Encryption standard is presently active security, and is used overcoming previous RSA, DES and its variants. AES thus providing security of 3 different type of keys as 128 bit, 192 bit and 256 bit keys thus enhancing security of data. The steganography technique takes on hiding data gives more and good performance than previous techniques used like LSB. For Image segmentation DWT (Discrete wavelength transform) is used. It segments the image into non-overlapping structures in an image for applying the steganography technique. The following technique segments the image and finds out a suitable area in an image for hiding and substitution of data by Differencing parameter, thus overcoming the previous disadvantages of LSB, Hash LSB those are more vulnerable to attacks. The techniques provides good PSNR (Peak Signal to Noise Ratio), and MSE (Mean Square Error) values required for determining image quality. It shows the deflection of the value from its original image value before hiding of secret data.

References

[1] Whitfield Diffie and Martin E. Hellman, "New Directions In Cryptography", IEEE International Symposium on Information Theory on 1976, Ronneby, Sweden.

[2] Chandra M. Kota and Cherif Aissi1, "Implementation Of the RSA algorithm and its cryptanalysis", ASEE Gulf Southwest Annual Conference on 2002, Houston, USA.

[3] Vladimir BANOCI, Gabriel BUGAR, Dusan LEVICKY, "A Novel Method of Image Steganography in DWTDomain", Technical University of Kosice, Slovak Republic.

[4] Colm Mulcahy Ph. D, "Image Compression using Haar Wavelet Transform", Spelman Science and Math Journal, 22-31.

[5] Sally Adee, “Spy vs. Spy", Http://Spectrum.Teee.Org/ComputingjSoftware/Spy-vs-Spy, IEEE Spectrum, 2008.

[6] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", the International Arab Journal of Information Technology - IAHT, Vol. 7, No. 4, P g. 358 364, 2010.

[7] K B Shiva Kumar, "Bit Length Replacement ‘ ‘Steganography Based on DCT Coefficients", International Journal of Engineering Science andTechnology, Vol. 2(8), Pg: 3561-3570, 2010.

[8] Mamta Juneja, Parvinder S. Sandhu, Ekta Walia, "Application of LSB Based Steganographic Techniquefor 8-bit Color Images", World Academy of Science, Engineering and Technology, 2009.

[9] Web:www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[10] Web: www.hindawi.com/journals/jam/2013/189706/