Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.6, No.7, 2015

An Enhanced Digital Text passing system using SHA-512 and AES

Chetna Mehto
M.tech scholar, Department of CSE, TIT, Bhopal (India)

Rachana Kamble
Asst. Professor, Department of CSE, TIT, Bhopal (India)

Dr. Bhupesh Gour
Professor, Department of CSE, TIT, Bhopal (India)

Abstract
In the present scenario the use of images increased extremely in the cyber world so that we can easily transfer data with the help of these images in a secured way. Image steganography becomes important in this manner. Steganography and cryptography are the two techniques that are often confused with each other. The input and output of steganography looks alike, but for cryptography the output will be in an encrypted form which always draws attraction to the attacker. This paper combines both steganography and cryptography so that attacker doesn't know about the existence of message and the message itself is encrypted to ensure more security. The textual data entered by the user is encrypted using AES algorithm. After encryption, the encrypted data is stored in the colour image by using a hash based algorithm. We have proposed a novel algorithm for mixing the AES ciphertext and the SHA-512 hash obtained from plaintext, which is embedded into an image so that the attacker cannot separate them for applying cryptanalysis.
Keywords - Steganography, Cryptography, Hashing, AES algorithm

1. Introduction

Steganography is of greater importance in situations where the secret information has to be transferred in a secure manner without the knowledge of a third person. The third person couldn't even get a clue regarding this hidden information. Only the sender as well as the receiver comes to know about this secret hidden message. In steganography there is a cover media in which data hiding takes place. The cover media can be a text, or it can be an image, audio, video etc. This paper focus on image steganography that is the cover media used is image. The applications of image steganography are innumerable especially in this high tech world. Areas include copyright protection to sharing trade secrets, ownership identification, transferring of highly confidential data between governments and much more.
Steganography and cryptography are the two techniques that are often confused with each other. The input and output of steganography looks alike, but for cryptography the case is different. In cryptography the output will be in an encrypted form which always draws attraction to the attacker. While considering the case of steganography this never happens as the attacker is unaware of the hidden message. In cryptography, message content is preserved while in steganography both the messages as well as people involved in the communication are preserved. This paper combines both steganography and cryptography so that attacker doesn't know about the existence of message and the message itself is encrypted to ensure more security.
In the past decade, digital technology has accelerated the development of network multimedia systems and introduced many advanced multimedia services. One prominent feature of digital technology is that editing, storage, transmission, and access of multimedia are easily done by any subject. For secure transmission, many early methods exploited encryption techniques to prevent unauthorized access and modification of secret messages. However, the encrypted form may attract special attention of network warders and is thus not fully secret. Current information hiding techniques are developed to deceive warders by embedding messages into multimedia in an imperceptible manner, but still maintain their original formats and quality.

1.1AES Algorithm

AES Algorithm is based over a cryptographic technique "Rijndael" which is a block cipher technique developed by Joan Daemen and Vincent Rijmen[13]. This algorithm is very flexible as it supports 128, 192, and 256 bits combination of data and key size. On the other hand AES mandates that the plain text must be 128 bit long which can be divided into four operation blocks. These blocks functions on an array which is made up of bytes organized in a 4×4 matrix. This arrangement is termed as state. For achieving complete encryption, the data is passed through Nr number of rounds (Nr = 10, 12, 14) .These rounds performs the following transformations:

Subbyte Transformation: This transformation includes a non linear byte Substitution with the help of substitution table (s-box), Affine Transformation and multiplicative inverse are the basic building blocks used for the construction of substitution table.
Shift rows transformation: It is a simple byte transposition method. In this transformation bytes in the last three rows of the state are cyclically shifted and offset of the left shift varies from one to three bytes.
Mix columns transformation: It is based on the method of multiplication of columns of the matrix in which each column vector is multiplied by a fixed matrix. Treating the bytes as polynomials rather than numbers.
Add round key transformation: It is a simple XOR operation between the working state and the round key. This transformation is its own inverse.
Inverse Substitute Bytes: It is the reverse procedure of the Substitute Bytes transformation; here the inverse S-box is applied on each byte of the State. This is obtained by taking the inverse of the affine transformation followed by taking the multiplicative inverse
Inverse Shift rows: It is the inverse process of the shift rows here the first row of the state array remains unchanged. The bytes present in the second, third and forth rows are cyclically shifted by one, two and three bytes to the right respectively.
Inverse Mix columns: In the Inverse Mix Columns transformation, every column of the state array is considered as a polynomial. Modulo x4+1 is multiplied with a fixed polynomial and the result generated is the corresponding column of the output state.

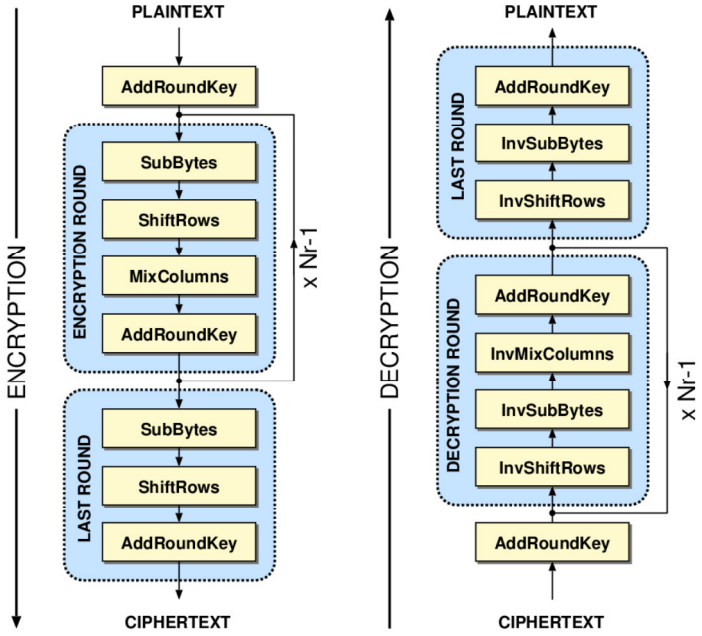


Fig-1: Diagram of AES Encryption Algorithm

The key value cannot be determined by any known means, even if any eavesdropper knows many pairs of plaintext and the cipher text security of AES algorithm remains unchanged. AES algorithm is so well designed that it supports the use one of any of the three key sizes (Nr). AES-128, AES-196 and AES-256 use 128 bit (16 bytes, 4 words), 196 bit (24 bytes, 6 words) and 256 bit (32 bytes, 8 words) key sizes respectively. AES have no known weaknesses and hence is a better approach as compared to DES. AES is extremely fast as compared to other block ciphers (Though there are some mismatches between size and speed). In dedicated hardware where round transformation is parallel by design AES allows even faster execution.

1.2SHA 512

The proposed work also makes use of SHA-512 which is a variant of SHA-256, It is more cost effective to compute as compared to SHA-256 for a given data sizes. The SHA-512 algorithm delivers 50% better performance as compared to SHA-256 [19]. It is basically a 512-bit block cipher algorithm that encrypts the intermediate hash value with the help of message block as key for the calculating hash.

SHA-512 has following strengths: Input message is divided in the multiples of 1024 bits of block. each 1024 additionally divides in 16 sub-blocks of 64 bits of each word size for proceeds.
Each round is having 20 stages. It uses four rounds for performing 80 iterations to generate 512 bits of message digest in output.
SHA-512 uses eight 64 bits buffer's to hold intermediate and final results.

2.Literature Survey

Hemalatha et al. [4] proposed a novel image steganography technique to hide multiple secret images and keys in color cover image using Integer Wavelet Transform (IWT). Authors claim that there is no visual difference between the stegoimage and the cover image, also a very good PSNR (Peak Signal to Noise Ratio) values obtains for both stego and extracted secret images.
Shamim Ahmed Laskar et al. [5] proposed a high capacity data embedding approach by the combination of Steganography and cryptography. In the process a message is first encrypted using transposition cipher method and then the encrypted message is embedded inside an image using LSB insertion method. The authors claim that combination of these two methods enhances the security of the data embedded, and this combinational methodology will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.
Usha B.A. et al. [6] proposed a neural network based technique for steganography. The amount of data that can be hidden inside the cover image chosen depends on the properties of the image like number of noisy pixels. The neural network based image steganography ensures that quality and size of the image remains same after embedding the data.
Current trend in steganalysis generally suggests two extreme approaches (a) little or no statistical assumption about the image under investigation. Statistics are learnt using a large database of training image and (b) a parametric model is assumed for the image and its statistics are computed for steganalysis detection. P. T. Anitha et al. [4] developed a new hybrid approach which comprises of neural network and S-DES encryption scheme which is used to detect the stego content in corporate mails. For this purpose, authors implemented the combination of Compression, Encryption, Steganography to enhance the security of the data sent and Steganalysis methods.
Inderjeet Kaur et al. [8] a transform domain based technique with the aid of segmentation and watermarking (TDSSW) that combines steganography and watermarking to provide copyright protection to the information being transmitted secretly. The carrier (cover image) is segmentated into 8×8 blocks and Discrete Cosine Transform (DCT) is applied on each segment. The MSB of payload is embedded into DCT coefficients of the cover image based on the values of DCT coefficients, to obtain the stego image. Authors claim that this technique is capable to improve peak signal to noise ratio.
In [9], authors Atallah et al. proposed a method that hides the secret message based on searching about the identical bits between the secret messages and image pixels values. They claimed that this technique works better as compared to LSB. They also claim that the proposed technique is efficient, simple and fast it robust to attack and improve the image quality, which obtains an accuracy ratio of 83%.
Pragya Agarwal et al. [10] proposed a scheme under which, a SHA-1 hash code is generated from original text message, which is sent to the receiver through a secure channel. The receiver can authenticate the received hash to ensure the integrity of the original message. The message is sent to receiver by hiding it into an image using image steganography.
Soumik Das et al. [11] proposed a technique in which, a 32-bit secret key is provided by encrypter, which is applied on the text with a hash function to generate a pseudo byte stream. This stream is written directly to image pixels and thus the text becomes physical property of encrypted image. An intruder cannot succeed if he tries to perform the extraction of text with a wrong secret key. The extraction of the text is blind i.e. except the secret key nothing is needed for text decryption.
In [12], Rinu Tresa et al. came up with a technique that combines both steganography and cryptography so that attacker doesn't know about the existence of message and the message itself is encrypted to ensure more security. The textual data entered by the user is encrypted using AES algorithm. After encryption, the encrypted data is stored in the colour image by using a hash based algorithm. This technique does not corrupt images quality in any form. Its major advantage is that it is suitable for almost all image formats such as JPEG/JPG, BMP, TIFF and GIFF.
Kritika Singla et al. [13] proposed a scheme that achieves high embedding capacity and enhances the quality of the encoded image. It first detects the edges in the image by well known canny edge method and then the hash sort is employed to embed the text data in to the edges of the color image. The hash function provides a secure and fast approach for image steganography.

Seongho Cho et al.[14] proposed A block-based image steganalysis system and conducted extensive performance evaluation of block-based image steganalysis studied the performance of the block-based steganalysis by varying different parameters, including block number, the block size, the effects of block overlapping, the class number of block, the classifier choice and the decision fusion scheme. It was practically seen that the performance of block-based image steganalysis is not as much of sensitive to the decision fusion approach but more responsive to classifier choice.
Firas A. Jasim[15] proposed a novel method for steganography which is based on FMM method The stego images obtained has been tested using PSNR value. Author analysed the PSNR value and proved that the stego images are having high PSNR, the ST-FMM novel steganography algorithm is very effective in hiding the information inside the image.
Dr. Ekta Walia et al.[16] proposed LSB & DCT based Steganography. Authors implemented LSB and DCT based steganography and calculated PSNR ratio. The result shows that PSNR ratio for DCT based steganography scheme is higher than LSB based steganography scheme for different types of images. Results shows that as DCT based steganography scheme has the minimum distortion of image quality, so DCT is preferred over LSB steganography scheme inspite the fact that amount of secret data which can be hidden using this technique is quite small.
Deepesh Rawat et al. [17] proposed a technique for hiding text information in color images they have improved the well known LSB method they had chosen bitmap and jpeg format image and calculated PSNR, MSE (Mean Squared Error) and also histogram analysis. Results shows that on increasing the size of the cover image large amount of secret information can be embed. because only a single bit of every pixel get changed there is minor change in histogram hence stego-image is visually identically same as was the original cover-image.

3.Problem Statement

In the previous work proposed by Soumik Das et al. [11], it was not a tough job for an attacker to generate a ciphertext and hash code of a new plaintext and replace them both. The entire problem is due to the reason that the attacker has both ciphertext and the hash code separately. We propose a solution to this problem by mingling up the hash code and ciphertext, and embed them both in a single image so that it becomes very hard for an attacker to separate them and replace. On the one hand, proposed algorithm will benefit the sender and receiver as they will not need to send two different files. On the other hand, it will be much more difficult for the attacker to break the algorithm as he never knows the ciphertext and hash code. The proposed technique makes use of the AES algorithm.

4.Proposed Scheme

(i) Proposed Architecture

The architecture of proposed steganography scheme is shown in Fig.2 and Fig.3. On sender side, first of all AES encryption and SHA-512 are applied on plaintext (P) to obtain the ciphertext (C) and hash (H). The C, H, and cover image (I) are applied as input to Mixing algorithm to form the mingled code. This mingled code (M) is embedded into the cover image (I) and the stego-image is generated.

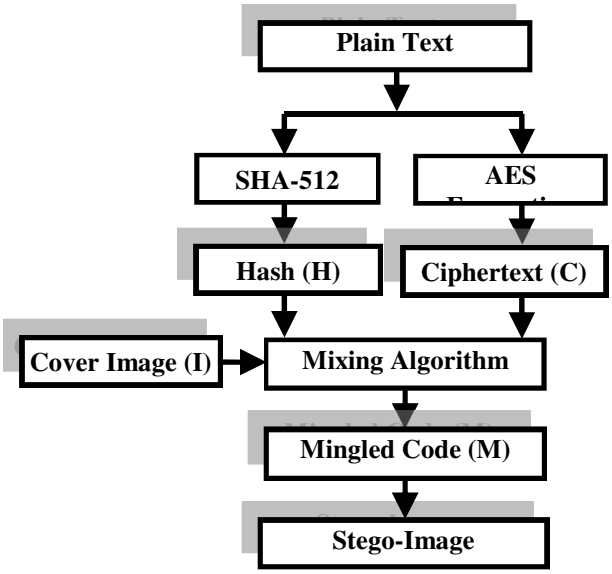


Fig. 2. Architecture of proposed scheme on sender side

Upon receiving the stego-image, the receiver applies reverse mixing algorithm on it yielding C and H. AES decryption algorithm is applied on C to obtain plaintext P. Again SHA-512 is applied on P to obtain H'. Now H and H' are compared, if they are same then the message obtained is the required one.

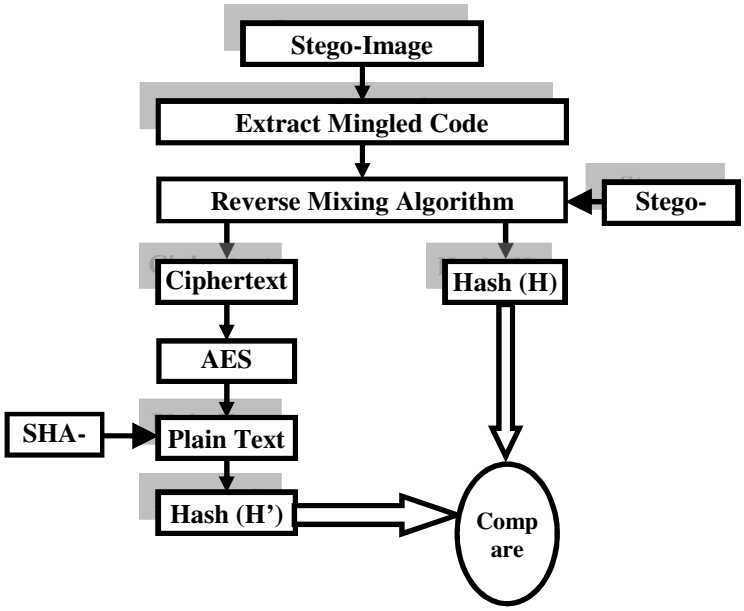


Fig.3. Architecture of proposed scheme on receiver side

(ii) Mixing algorithm

Sender Side

1. Let the plaintext be denoted by *P*, and *C* is the ciphertext generated from *P* using AES algorithm.
2. Let *H* be the hash code generated from *P* after applying SHA-512, and *I* be the cover image.
3. Create an intermediate byte array *B,* and the resultant mingled code array M.

4. Write alternate bytes from *C* and *H* continuously into it until all the bytes from *C* and *H* are written into it.

5. Repeat until all the bytes of *B* are processed:

   - Pick Next 16 bytes from *B* and XOR them with last 16 bytes of *I*.
   - Group the resulting 16 bytes into four bunches, each of four bytes.
   - Perform a right circular shift in all four bunches separately
   - Join the bunches to reproduce the resultant 16 bytes
   - Append the above 16 bytes into *M*

6. Write *M* into *I* using LSB technique.

Receiver Side

1. Let the ciphertext be denoted by *C*, and *P* is the plaintext generated from *C* using AES decryption algorithm.

2. Let the stego-image be denoted by *I*.

3. Let *H* be the hash code received along the stego-image..

4. Create an intermediate byte array *B,* and the resultant mingled code array M.

5. Read the LSB values from *I* and store them into byte array M.

6. Repeat until all the bytes of *M* are processed:

   - Read next 16 bytes from M and create four separate bunches, each of four bytes.
   - Perform left circular shift in all four bunches separately
   - Join the bunches to reproduce the resultant 16 bytes
   - Perform XOR between the 16 bytes generated above and last 16 bytes of stego-Image *I*.
   - Append the resultant 16 bytes into *B*

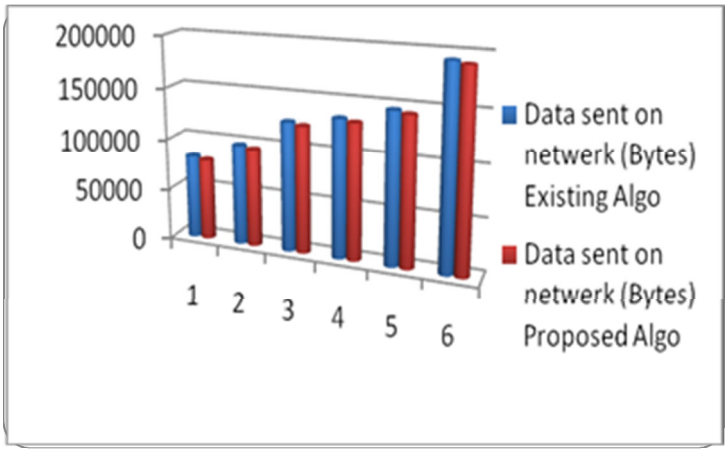
7. Write alternate bytes from B into *C* and *H* continuously until all the bytes from *B* are processed.

8. Apply AES decryption algorithm on *C* to generate plaintext *P*.

9. Apply SHA-512 on C to generate hash code *H'*.

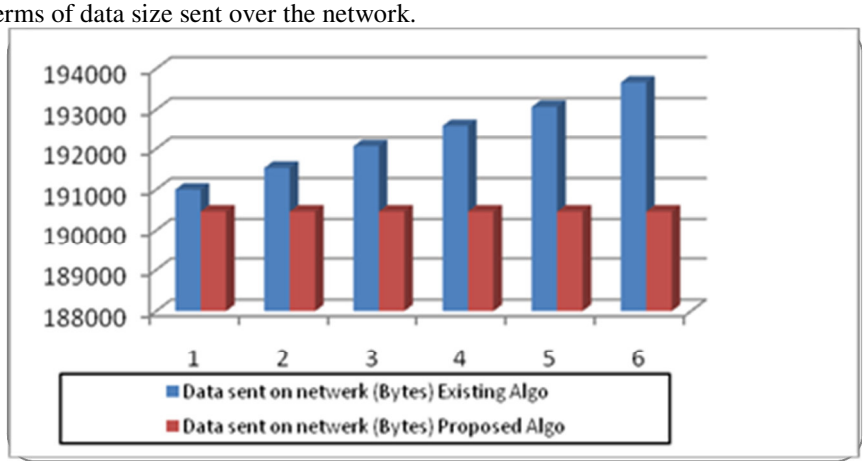
10. Compare *H* and *H'*, if they are equal then the image has been authenticated successfully. Otherwise the received image has been compromised.

5.Simulation & Results



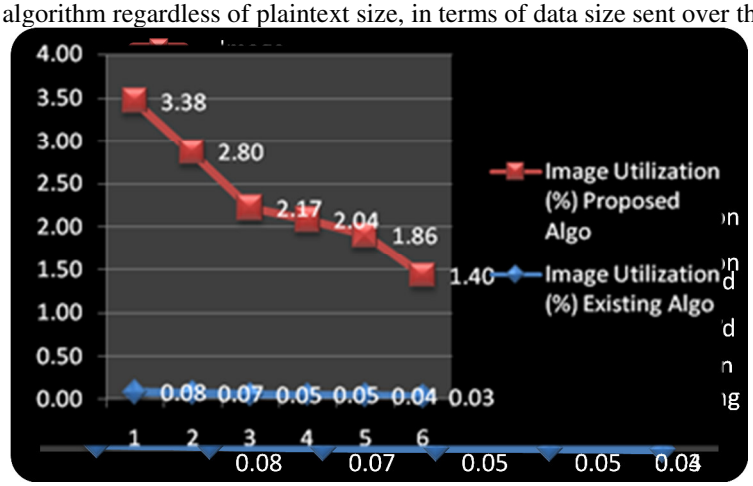
Graph1: Overhead reduction1

In the first experiment (Graph1), plaintext size was set constant (2000 bytes) with varying size of cover images. Results show that the size of data sent over the network using proposed algorithm is always smaller as compared to existing algorithm. It signifies that proposed algorithm outperforms existing algorithm regardless of cover image size, in terms of data size sent over the network.



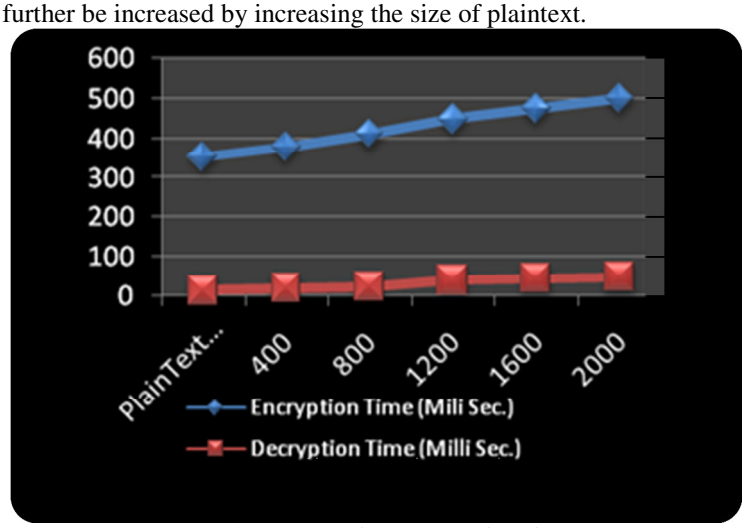
Graph2: Overhead reduction2

In the second experiment (Graph2), cover images size was set constant (190464 bytes) whereas size of plaintext was varied from 400 to 2500 bytes. Results show that the size of data sent over the network using proposed algorithm is always significantly smaller as compared to existing algorithm. It reveals that proposed algorithm outperforms existing algorithm regardless of plaintext size, in terms of data size sent over the network.



Graph3: Pixel utilization

In third experiment (Graph3), plaintext size was set constant (2000 bytes) with varying size of cover images. The image utilization can be termed as the percentage of pixels in stego-image that are rewritten by the algorithm. This percentage is analyzed in the third experiment where results reveal that as compared to existing algorithm, this percentage is considerably high when proposed algorithm is used. Thus it is apparent that the proposed algorithm is far better in terms of image utilization regardless of cover-image size. It should be noted that the image utilization can further be increased by increasing the size of plaintext.



Graph4: Encryption Decryption time

In forth experiment (Graph4), encryption and decryption time taken by our proposed work is plot in a line graph, the experiments are performed and we have found that the encryption time for the same text is more than the decryption time of the same text, it is because in the encryption phase the write operation is performed over the bits while on the other hand in case of decryption only read operations are performed and it is obvious that the read operation takes lesser amount of time as compared to the write operation

6.Conclusion

In this research we have proposed Encryption Decryption technique which is developed for highly secure transmission of text. . This research combines both steganography and cryptography hence the attacker is not aware of the existence of any message and the message is itself encrypted to guarantee extra level of security. The research proposed a novel algorithm for mixing the AES ciphertext and the SHA-512 hash obtained from plaintext, which is embedded into an image so that the attacker cannot separate them for applying cryptanalysis. The experiment results obtained are better as compared to the previous work.

References

[1] Abbas Cheddad, *"Digital Image Steganography: Survey and Analysis of Current Methods,"* Elsevier, Signal Processing, Vol.90, No.3, Mar.2010, pp.727–752.

[2] Atallah M. Al-Shatnawi, *"A New Method in Image Steganography with Improved Image Quality,"* Applied Mathematical Sciences, Vol.6, No.79, 2012, pp.3907-3915.

[3] Kritika Singla et al., *"Hash Based Approach For Secure Image Steganography Using Canny Edge Detection Method,"* IJCSC, Vol.3, No.1, Jan.-Jun.2012, pp.155-157.

[4] P. T. Anitha et al., *"An Efficient Neural Network Based Algorithm For Detecting Steganography Content In Corporate Mails: A Web Based Steganalysis,"* IJCSI International Journal of Computer Science Issues, Vol. 9, No.1, May.2012, pp.509-513.

[5] Shamim Ahmed Laskar et al., *"High Capacity data hiding using LSB Steganography and Encryption,"* International Journal of Database Management Systems (IJDMS) Vol.4, No.6, Dec.2012, pp.57-68.

[6] Soumik Das et al., *"A Secured Key-based Digital Text Passing System through Color Image Pixels,"* IEEE International Conference On Advances In Engineering, Science And Management (ICAESM-2012), Mar.2012, pp.320-325.

[7] Hemalatha S et al. *"A Secure and High Capacity Image Steganography Technique,"* Signal & Image Processing: An International Journal (SIPIJ) Vol.4, No.1, Feb.2013, pp.83-89.

[8] Inderjeet et al., *"Transform Domain Based Steganography Using Segmentation And Watermarking,"* International Journal of Computing and Business Research (IJCBR), Vol.4 No.1 Jan.2013.

[9] Mehdi Hussain et al., *"A Survey of Image Steganography Techniques,"* International Journal of Advanced Science and Technology, Vol.54, May.2013, pp.113-124.

[10] Pragya Agarwal et al., *"Transmission and Authentication of Text Messages through Image Steganography,"* IJCA Proceedings on 4th International IT Summit Confluence 2013, No.2, pp.16-20.

[11] Sandeep et al., *"A Review on the Various Recent Steganography Techniques,"* IJCSN International Journal of Computer Science and Network, Vol.2, No.6, Dec.2013, pp.142-156.

[12] Usha B A et al., *"Data Embedding Technique In Image Steganography Using Neural Network,"* International Journal of Advanced Research in Computer and Communication Engineering, Vol.2, No.5, May.2013, pp. 2177-2180.

[13] Rinu Tresa et al. *"A Novel Steganographic Scheme Based On Hash Function Coupled With Aes Encryption,"* Advanced Computing: An International Journal (ACIJ), Vol.5, No.1, Jan.2014, pp.25-34.

[14] Seongho Cho et al. "Block-based image steganalysis: Algorithm and Performance evaluation," J. Vis. Commun. Image R .24(june 2013) Elsevier 846-856.

[15] Firas A. Jassim, "A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method," International Journal of Computer Applications(IJCA), Vol.72, No.17, June 2013.

[16] Dr. Ekta Walia et al. "An Analysis of LSB & DCT based Steganography," Global Journal of Computer Science & Technology,Vol.10 Issue1(Ver 1.0),April 2010.

[17] Deepesh Rawat et al. "Steganography Technique for Hiding Text Information in Color Image Using Improved LSB Method," International Journal of Computer Applications(IJCA), Vol.67, No.1, April 2013.

[18] Chetna Mehto et al. "Investigation of Digital image Steganography: A Survey," Int.J.Computer Technology & Applications,Vol 5 (5), 1711-1717

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar