International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Implementation of Steganography with ETC System for Different Data Transmission

Gauri Chavan[1], S. S. Vairagar[2]

[1]Department of Computer Engineering, Siddhant College of Engineering, Sudumbare, Pune, India

[2]Professor, Department of Computer Engineering, Siddhant College of Engineering, Sudumbare, Pune, India

Abstract: ***Data transmission in a secure manner over the internet has gained higher interest since last decade as the use of encryption for transmitting embedded files before compression is very essential. The major challenge is designing the architecture so as to perform the file encryption at sender side and the file compression at the NSP side in order to achieve the distinguished works assigned to senders and NSP. The proposed architecture comprises a novel architecture where resources required for file compression are utilised from NSP quota while resources only for encryption are used from Sender quota. The proposed system makes use of pre-defined AES encryption algorithm for encrypting the files and LSB Steganography for hiding the sensitive data in the images. With the AES, mathematical technique is more productive for efficient compression of files that are been already encrypted. While as far as compression is concerned, Huffman algorithm is not feasible, as it gives less compression proportion, compared to the other lossless coders as inputs.***

Keywords: Steganography; Encryption; Compression,LSB Stegnography

1. Introduction

Let us to consider an illustration where person Charlie is an untrusted channel supplier, and through this channel i.e. bob receives the data via Charlie, a proprietor of data i.e. Alice acts as sender, needs to effectively and additionally safely send file I. This can be proficient as takes after. In the first place Alice pack the image to, then with the help of cryptographic technique he scramble the compressed image into where is the discharge key. The scrambled information is sent to channel supplier Charlie, post encryption. After cryptographic process, this information just sent by to bob via Charlie. At that stage, bob has to undertake two sub-operations. We have first unscrambled information by decoding and after that utilizing decompression, as the decompression decodes information which gives unique images.

Ignoring the probability that existing Compression-then-Encryption (CTE) sample fulfill the prerequisites in terms of protection, it is basically required to switch the grouping of compression application and encryption application at two different conditions. The possibility that he is the information proprietor, through encryption strategy, each time Alice is keen on ensuring the mystery of the image information. At this stage, Alice has no requirement for packing information, and consequently, before the information encryption, for running an algorithm for compression, constrained computational assets won't utilize. There, it's the obligation of the channel supplier to bind the data in compressive manner so that heap space increases, for expanding the usage of system. As the service provider has adequate of computational assets, its better if the compression in carried out at its end. With the (ETC) proposed system the enormous test received is working of compression must be carried over the information which is scrambled, so that emit key is kept safe from system supplier Charlie.

2. Literature Survey

A. On the design of an efficient encryption-then-compression system

Over the expectation mistake space, in this system a change based file encryption strategy is used. To proficiently pack the encoded image, additionally a methodology of number juggling coding based (AC) compression is planned by the author. It can be demonstrated that terrible abnormal security state can be accomplished by the authors proposed plan. All the more strikingly, un-scrambled one on the encoded image contrasted and that of compacting first there is just marginally corruption saw in the execution of compression. Conversely, on the compression execution there impels noteworthy punishment as in the greater part of the current methodologies [1].

B. On the implementation of the discrete Fourier transform in the encrypted domain

In this work, the usage of the discrete Fourier change (DFT) has been explored by the author in the scrambled space by utilizing the homomorphic properties of the basic cryptosystem. For the direct DFT a few imperative issues are viewed as: the quick Fourier algorithms, of the radix-2 and the radix-4 including the greatest size of the succession and the blunder examination that can be changed. Likewise computational many-sided quality investigations and examinations are given. The outcomes demonstrate that for an encoded area execution there is most appropriate the radix-4 quick Fourier change in the proposed situations [2]. Encrypted domain DCT based on homomorphic cryptosystems. In this work, the Discrete Cosine Transform (DCT) application consider by author by utilizing a proper homomorphic cryptosystem to images encoded. A s.p.e.d. by characterizing a helpful sign model 1-dimensional DCT is acquired and by utilizing distinguishable preparing of lines and additionally segments is reached out to the 2-dimensional case. By the cryptosystem the limits forced on the extent of the DCT and the deduction of the number

juggling exactness, the direct DCT algorithm and in addition its quick forms are consider. To square based DCT (BDCT) the specific consideration is given, to various image obstructs by the s.p.e.d. DCT parallel application with accentuation on the computational weight bringing down probability [3].

C. Composite signal representation for fast and storage-efficient processing of encrypted signals

In this work, as a result of the cryptosystems working use on logarithmic structures which is extensive to the encoded representation of signs to go from the plaintext, author consider the information development required. Various sign examples pack together is permit us by a general composite sign representation and as a novel specimen process them is proposed. On encoded signals by means of parallel preparing to accelerate direct operations is grants us by the proposed representation and for the decreasing the scrambled signs size [4]. In this work, without either the data theoretic security or bargaining the compression effectiveness ,first encoding and after that packing takes place. Albeit illogical, with side data standards using coding that show shockingly by us, without loss of proficiency of either ideal coding or flawless mystery in a few settings of hobby this inversion of request is in reality conceivable. Where compression goes before encryption our plan requires in the encryption key there was no more arbitrariness than the customary framework is demonstrated that in specific situations by us. For demonstrating the hypothetical attainability a framework which executes scrambled information compression likewise portray this inversion of operations furthermore [5].

D. On compression of data encrypted with block ciphers

With square figures like Advanced Encryption Standard (AES) this work examines compression of information scrambled. It is demonstrated that without information of the mystery key such information can be possibly compressed. In different fastening modes piece figures working are considered and it is appeared without bargaining security of the encryption plan, how compression can be accomplished. Further, to the handy compressibility of square figures it is demonstrated that a principal restriction are exist there when no anchoring is utilized between pieces. For handy code developments there utilized some execution results to pack twofold sources are displayed [6].

E. Lossless compression of encrypted grey-level and color images

The compacting scrambled dark level plausibility and shading images are examined in this work, by decaying them into bit-planes. For abusing the spatial and also cross-plane connection among pixels and in addition the misusing the relationship probability between shading groups a couple methodologies are talked about in this work. For assessing the hole between the arrangements of proposed framework and the execution which is hypothetically achievable, some exploratory results are appeared in this work [7].

F. Lossy compression of encrypted image by compressing sensing technique

In this work, a great image encryption-and-compression strategy is composed by the Author, where the author thought about the lossless and lossy compression. With cyclic change in expectation blunder space and also k-mean bunching, there is worked the recommended image encryption method, for giving the sensibly more security, this procedure is capable. The demonstration that for proficiently encoded images compression, there can be actualized the math coding-based strategy [8].

3. Proposed System

In this system the use of Advanced Encryption Standard (AES) algorithm to encode the data and after that this data is compressed by using Huffman algorithm. A Permutation based image encryption approach for secure and capable image security. Vital focus is on convenient framework of two or three encryption and compression arranges in a way that compacting the scrambled image and packing the decoded one of a kind image is pretty much as compelling. On account of high affectability of estimate bumble course of action against unsettling impacts, sensibly anomalous condition of security could be held. The fig.1. shows the entire building configuration of the proposed system.

A. System Architecture

Proposed structure building plan include steganography and encryption at the sender side and data compression at the NSP side. Same method of data decompression and data unscrambling are performed by the recipient side. This will perform the security moreover low data uses for the sending that data over the web. The proposed system building outline showed up in fig. 1. , includes sender, channel supplier and recipient. In this structure „I" is used to indicate Steganography, for covering/concealing the data in the image. If sender need to send some data to the recipient then first sender encode this data by using AES algorithm. In the wake of encoding data successfully, sender sends this data to the framework supplier. The NSP is the arbiter between the sender and recipient.

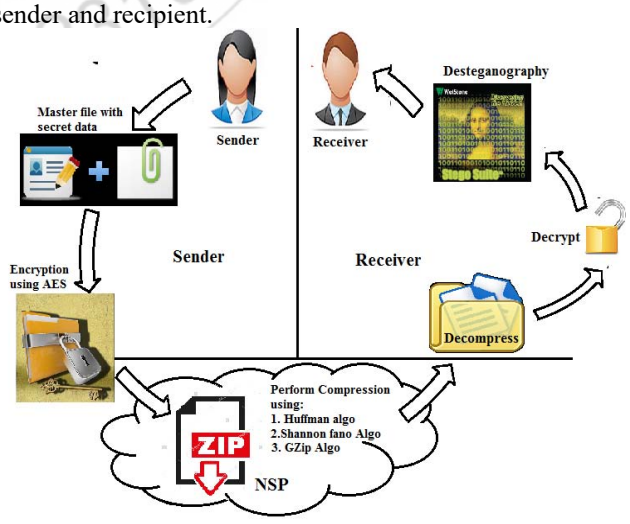

Figure 1: System Architecture

If the development on the channel increases or the data send by sender is considerable, for minimizing the stack of the

channel, NSP pack the data which is sent by sender by using Huffman coding algorithm. Ensuing to performing compression operation on the encoded data, the NSP send this compressed data to the receiver. At the recipient side, the receiver performs either perhaps several operations which are depends on upon the data which is started from channel supplier. If the data sent by channel supplier is compressed, then recipient decompress this data by Huffman coding algorithm. In the wake of decompressing the data, the receiver performs the unscrambling operation on the decompressed data. In the wake of performing the deciphering operation, thusly get the main data which is sent by sender. After decrypting the file receiver extract the secrete data from decrypted file. Thus, in this way the sender send the secret information securely to the receiver.

B. Modules

1) Sender Module

In this module, firstly sender login by entering valid username and password. After login the sender selects the master file and data file. Using LSB substitution algorithm sender hides the data file into the master file. Then encryption of newly generated file is done by using AES algorithm. After encryption the file is sent to the NSP.

2) NSP Module

In this module, NSP first login to the system by entering valid username and password. After login he select the encrypted file which was sent by sender and compresses this selected file by using compression algorithms like Huffman algorithm, Shannon fano algorithm or GZipstream algorithm. After file is successfully compressed, the NSP sends it to the receiver.

3) Receiver Module

In this module, sender first login to the system by entering valid username and password. After successfully logged in, he selects the compressed file which was sent by NSP. Then, the decompression is performed on the selected compressed file by using compression algorithms like Huffman algorithm, Shannon fano algorithm or GZipstream algorithm. Then he decrypts the file which is generated after decompression with the help of AES algorithm. After decryption, receiver extract the data file from master file using LSB substitution algorithm and get the original secrete data file successfully.

4. Algorithms

1. LSB Substitution

i. Read the file to be embedded
ii. Read the file inside which message is embed
iii. set numSignificantBits = n ; where n= 1,2……8
iv. Size1 = size(secret); and size2 = size(coverfile);
v. Set the "numSignificantBits"n significant bits of each byte of cover file to zero by using bit by AND operation on cover and size1 matrix
vi. Embedd the "numSignificantBits" most significant bits of secret file to create the stego file by using stego= (cover zero+ secret)/28-n
vii. Recover the embedded file, by using bit by shift operation
viii. Display Figure of cover file, file to be hidden, stego file and recover file
ix. End.

2. AES Algorithm

3. Huffman Algorithm

1. Shannon fano Algorithm

i. For a given symbol list, build up a corresponding list of probabilities or recurrence counts so that every image's relative recurrence of event is known.
ii. Sort the list of symbols as indicated by recurrence, with the most much of the time happening images at the left and minimal basic at the right.
iii. Divide the list into two sections, with the aggregate recurrence numbers of the left part being as near the aggregate of the right fine.
iv. The left part of the list is doled out the paired digit 0, and the right part is relegated the digit 1. This implies the codes for the images in the main part will all begin with 0, and the codes in the second part will all begin with 1.
v. Recursively apply the steps 3 and 4 to each of the two parts, subdividing amasses and adding bits to the codes until every image has turned into a comparing code leaf on the tree.

4. GZip Algorithm:

i. Set the coding position to the start of input stream
ii. If coding position is not toward the end of input stream, scan the window for the longest match with the lookahead cradle; else algorithm ends.
iii. If discover match, output (off, length,c), c is the character after the match, coding position and window advance length+1 bytes; else goto step4.
iv. Output current character at coding position, coding position and windows propel 1 byte; goto step2. Taking after is an illustration to clarify the algorithm. Accept the extent of window is 10, the substance is "abcdbbccaa", and the string to be coded is "abaeaaabaee".

5. Results

In sender module, firstly sender has to login by entering valid username and password. As shown in below fig. 2.

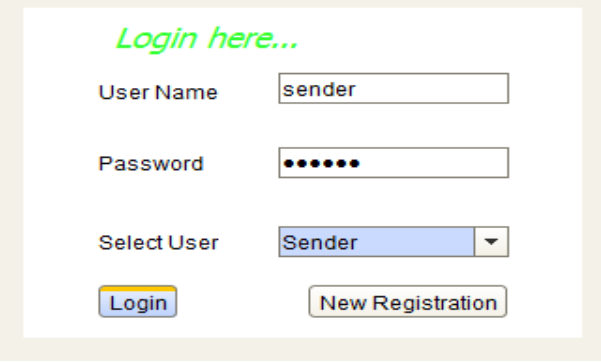

Figure 2: Sender login

The sender selects the master file and data file. Using LSB substitution algorithm sender hides the data file into the master file as shown in the figure 3.

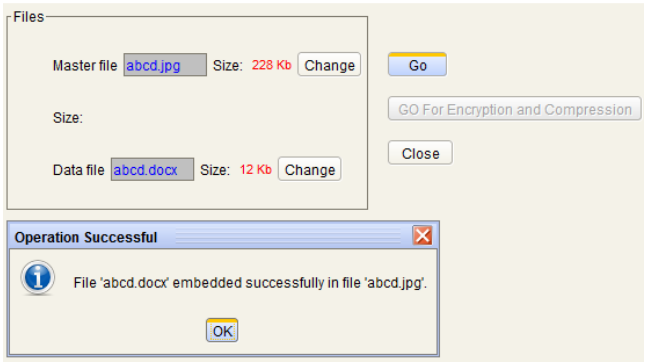

Figure 3: Steganography

Here as shown in fig.4 the sender selects the embedded file for successful encryption in which sender has to generate encryption key and also specifies number of rotations for security as it uses AES algorithm for encryption.

Figure 4: Encrypt file

After successful encryption the file cannot be opened and viewed.

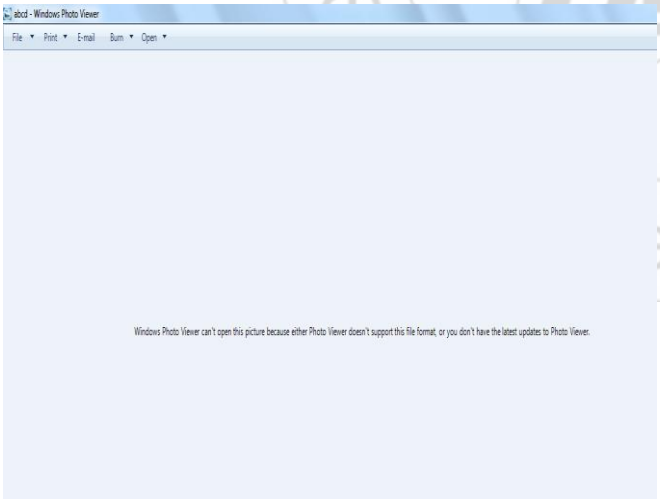

Figure 5: Encrypted file

As the job of sender is completed , as shown in fig the NSP hs to login with his unique ID and password.

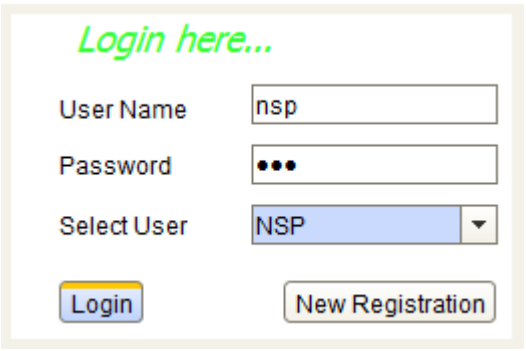

Figure 6: NSP login

6. Conclusion

In this framework, the designing of an effective image and different documents, for example, videos Steganography Encryption-And then-Compression (SEAC) framework is done. In the proposed framework, through LSB substitution the data is hidden and can also extract the same secret information. Using AES algorithm here the accomplishment of image encryption and decoding is done. By utilizing different compression algorithms, for example, Huffman Algorithm, Shannon Fano Compression Algorithm, and proposed algorithm GZip compression algorithm execution which do exceedingly proficient compression and decompression of the information which is encoded has then been figured it out. The examination of the different compression proportions will demonstrate the proficiency of the proposed framework when contrasted with existing frameworks.

References

[1] J. Zhou, X. Liu, and O. C. Au, "On the design of an efficient encryption-then-compression system," in Proc. ICASSP, 2013, pp. 2872–2876.
[2] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.
[3] T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357.
[4] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.
[5] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process. , vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
[6] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers,"IEEE Trans. Inf. Theory, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.
[7] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey-level and color images," in Proc. 16th Eur. Signal Process. Conf., Aug. 2008, pp. 1–5.
[8] Praveen Kumar, Maitreyee Dutta, "Lossy compression of encrypted image by compressing sensing technique", Lossy compression of encrypted image

by compressing sensing technique, Volume 3, Issue 4, April 2015.
[9] A. Kumar and A. Makur, "Distributed source coding based encryption and losslesscompression of grey scale and colour images," in Proc. MMSP, 2008, pp. 760-764.
[10] W. Liu, W. J. Zeng, L. Dong, and Q. M. Yao, "E_cient compression of encryptedgrayscale images," IEEE Trans. Image. Process. vol. 19, no. 4, pp. 10107-1102, Apr. 2010.
[11] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images,"IEEE Trans. Image. Process. vol. 22, no. 6, pp. 3108-3114, Jun. 2012.
[12] X. Wu and N. Mammon, "Context-based, adaptive, lossless image codec," IEEETrans. Commune., vol. 45, no. 4, pp. 437-444, Apr.
[13] M. Barni, P. Faille, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, "Privacypreserving ECG classification with branching programs and neural networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 452-468, Jun. 2011.
[14] Z. Erwin, T. Vaughn, T. Toft, and R. L. Lagendijk, "Generating private recommendations eficiently using holomorphic encryption and data packing," IEEE Trans. Inf. Forensics Security, vo 7, no. 3, pp. 1053-1066, Jun. 2012.
[15] Zuyuan et. Al “On the Security of Compressed Sensing-Based Signal Cryptosystem”, current version 4 September, 2015.