Improvement of Hybrid Technique of Data Security

Shishupal Sidar[1] Gourav Chandel[2] Deepak Garg[3]
[1,2,3]National Institute of Technology, Kurukshetra, Haryana, India

Abstract— At the present times, somewhere the lot seems like it should be digitized, danger to the security of data is at the peak level. Data is careful as an important strength then is essential to be secure. Data Security contains data, authenticity, integrity, and confidentiality besides considerable more. In the face of some approaches toward data security like encryption, compression, steganography, the data is static and likely to have prospective safety threats. The chief motive acknowledged is the shortcomings of these separate techniques at what time sure factors are occupied addicted to account. Cryptography certifies security then it also produces suspicion just before data as the data is transformed into worthless form. Compression techniques protect and encrypt data space on disk so compressed records can without difficulty to uncompress through attackers. Steganography is a method which is used to hide information rather than encrypting this one also has its advantages and limitations. In this paper, we tried to focus on devising an organization which not alone make available multilayer information security but then again also tends to cross those techniques after Encryption, compression and steganography that forms a safety system actually hard to break but at the similar period keeping computational speed as fast as imaginable keeping in mind the plainness of the approaches selected. For completing this assignment, approaches aimed at security of data (Encryption, Compression, and Steganography) and their possible merits and drawbacks remained assessed in point. Data security differentiation of these techniques will be there planned successfully.

Keywords: Encryption, Steganography, Compression, Cryptography, Data Security, Decryption

I. Introduction

Security of data presents the performance of protective information as of uncertified access. In the least kind of information shifted finished the internet has an opportunity of existence distorted. From this time several approaches like cryptography, compression, and steganography are used for protection of data as of threat though distribution it over the Internet. Cryptography presents an approach which creates usage of mathematics designed for the safety of data. It helps through a shuffling plaintext obsessed by cipher text, at that time back once more. Towards the data encryption, and two unique keys moreover symmetric (encryption and decryption be there completed with those same keys) then asymmetric (encryption and decryption be there completed with private key and public key individually) key algorithms Compression be there a technique that decreases the numeral of bits working. It does everything through rejecting redundancy passing data. That one safeguards reduced storing, needs less quantity and lowest cost of time toward sharing a file done network Steganography be there a technique that covers the message now an approach it cannot be there seen through an unauthorized being. This one hides the detail that a top-secret message be there existence transferred.

II. Gaps

Security testing now a traditional cascade improvement procedure exists generally established on the finale of an improvement cycle. Even though it is able to be rushed, due to the necessity to arrange subsequently expected delays in improvement, the situation is a lot likely and done. Delays in organization, if essential, be there suitable to make sure application stability, especially while this application is connected along with significant returns which is not considered up until these days.

III. Challenges

1) Encryption- It produces doubt by way of the data being changed into meaningless usage.
2) Compression- It be a technique used for data compression also the algorithms are located weak toward delivering data safety only within reach.
3) Steganography- It shortages to make sure data security by way of once the shelter media are there identified the hidden data be able to simply be there breached.

Safety level vs time complexity

- In instruction toward continuing high security, which is the most significant requirement in current situations, computational speed/time complexity can be there compromised toward a better lengthen. Towards protecting the system, structure multilevel security systems are mandatory to be located devised but then this system breaks in expressions of computational speed.
- Just before determining the greatest possible approaches however preserving high data security as well as more time complexity/ computational speed.
- The highest task is in creating a hybrid system for security to select the greatest possible approaches available for encryption, compression and steganography therefore for example to keep up the high security of data as well as lowest time complexity.

A. Benefits:

- It is a best Integrity, Availability Confidentiality in a designed for Data secure
- This is a theoretically safe
- They are Faster approaches
- Overriding separate demerits

IV. Comparative Study

A. Asymmetric key encryption as well as Symmetric key encryption:

Arranged the source of a huge literature survey as regards encryption approaches it was decided that encryption ratio which exists to be reduced designed for speedy computational speed more in with the symmetric key encryption techniques [1-6]. The key size is in height on the asymmetric form of encryption; from this time contravention the code exists difficult popular RSA. Now the phase of speed, the

Symmetric key encryption, is observed as decent. Now the Asymmetric encryption technique, the RSA algorithm exists other secure then it usages the factoring of in height major number used for key generation. Thus, Blend of Modify play fair cipher also RSA would arrange for good results now in terms of security, best time complexity as well such as Simplicity.

B. Factor analysis of Encryption techniques:

1) Encryption Ratio (inversely related to the computational speediness):-

Modify play fair cipher: Less (hence fast computational speed)
Columnar cipher: less level
AES: high level
DES: high level
RSA: high level

2) Key length (directly proportional to the security rate)

Modify play fair cipher: key depend on 7*7 metrics
Columnar cipher: key depends on order in which text is writing
AES: 128, 192 and 256 bits
DES: 56 bit
RSA: >1024 bits

3) Computational speeds:

Modify play fair cipher: fast speed
Columnar cipher: fast speed
AES: less fast speed
DEA: fast speed
RSA: fast speed

4) Security against attacks:

Modify play fair cipher: Brute force
Columnar cipher: brute force
AES: chosen plain text or known plain text
DES: brute force
RSA: timing attack

V. COMPRESSION TECHNIQUES

Arranged the source of a huge literature survey as regards compression techniques that one is determined that speed [7] be there of greatly worry used for compression. Furthermore, it is there the informal technique to appliance which doesn't need some extra hardware or software. Therefore, Run Length Encoding (RLE) would deliver moral results now terms of security, best time complexity also simplicity [8].

A. Factor analysis of compression techniques

1) Run length:

This is a variable type input and output is fixed, there drawbacks is a cannot achieve high compression ratio, and time complexity is a O(n) and space complexity O(2n) Decoding (No prior information of input is required, and there cost is complicate decoding process so increase time cost, and there applications: BMP, PDF,TIFF).

2) Huffman:

This is a fixed type input and output is variable, the speed is fast and there drawbacks are troublesome because of variable code lengths. And time complexity is O(n(lon n) and space complexity O(k) for the tree and O(n) for the decode text Decoding prior information of input is required, and there cost is cost of word is number of it has. Cost increase as a tree now will also be transferred, extra cost of transmitting the encoding tree and their applications: MPEG, JPEG, ARJ, and GIF).

3) LZW:

This is a variable type input and output is fixed, the speed is fast. Compression their drawbacks is the execution of string is troublesome. and time complexity is a O(n) and space complexity O(n) Decoding is no prior information about the data stream, and there cost is Low time cost of transmission less as table is not passed and their applications: PDF, TIFF, GIF).

VI. STEGANOGRAPHY TECHNIQUES

Arranged the source of a huge literature survey regarding steganography techniques that one be there decided that image before used by way of a cover media verifies out just before be the greatest medium [10-11] for hiding data ahead In line for to in height level of recurrence. In images it is able to hide data very simply. Text which exists hidden ahead of the protection media is very challenging to identify then also it is there very strong to adjust which verifies it toward being the greatest protection media [11]. Thus, Image used as protection media would make available good results in terms of safety as well as simplicity [10].

A. Factor analysis of Steganography techniques

1) Audio: in steganography audio is least more prone to attacks and it is most difficult in hiding data in audio file and this main feature is embedded in cover audio file as “noise” at frequency which is out of hearing range. And their application is the Phone call/ Skype, detectability is poor, bit rate is medium and there resistance to modification is wake.
2) Image: in steganography image is less and more prone to attacks and it is a less difficult level and image main feature is computerized pictures are the most famous spreader media because of their high level of repetition. And their application is the IP/TCP packages. Detectability is very large, bit rate is very good and there resistance to modification is also very good.
3) Text: in steganography text type is more prone to attacks and difficult least and this main feature is the content steganography is a strategy for utilizing composed common language to cover a mystery message. And there application is the CSS, Emails, SMS Texting, detectability is very small size, bit rate is poor there resistance to modification is average.

VII. SETTINGS & TOOLS

A. Limitations of Encryption, Compression and Steganography

Now encryption, plaintext, 7X7 matrix such as key in Modify modifier play fair cipher & 1024bit size key in RSA is used.

Now Compression, cipher text achieved on or after Encryption procedure is nurtured as per plain text popular RLE.

Now Steganography, cipher text hence got on or after compression is hidden ahead of the image protection media with LSB technique.

B. Language semantic used:

Java, a prevalent general-purpose program design language also works out as a platform that exists synchronized, class-based, and object-oriented as well as being fast, dependable and protected. That one be there projected to occupancy application designers "compose once, run somewhere".

1) Python: - is a prevalent language used by systems analysts used for development mathematics, software, web development, system scripting and an allocation other. It exists as a very pretentious language through syntax to some extent parallel on the way to English language.
2) Libraries used:
3) java.lang:- that one is all the time indirectly present trade in as it contains the lot you really cannot program without String, Double, Enum, Math, etc.
4) java.util:- This one contains the assembly's framework, event model, inheritance collection classes, time facilities and date in java
5) java.io:- Contains closely each one class that strength be wanted to implement input and output (I/O) operations over data streams. requests.txt: Supplies file holds the result as of pip check for completing repeatable installation.

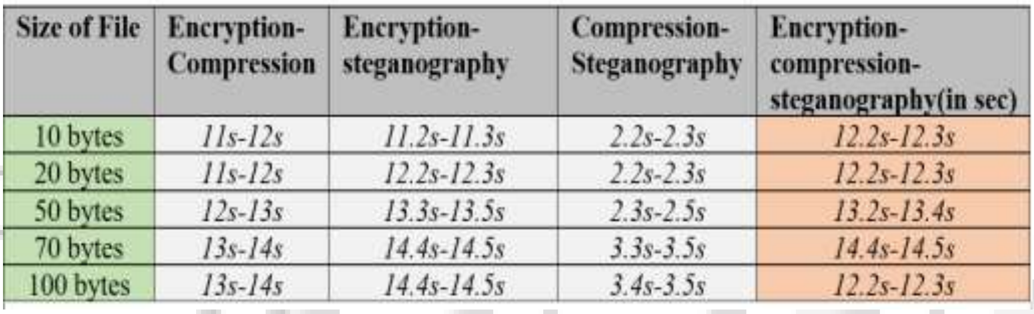
When pip freeze runs, a pinned version of it is stored in the Requirement file.

VIII. SIMULATION RESULTS AND ANALYSIS

The enactment comparison of the hybrid data security system Encryption Compression, Steganography mentioned overhead be located through three other existing systems.

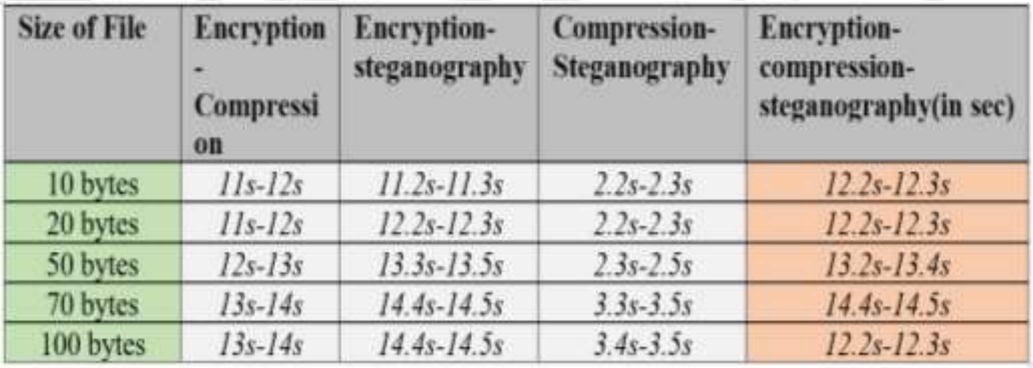
The performance conditions are–

1) Encryption time
2) Decryption time



Size of File	Encryption-Compression	Encryption-steganography	Compression-Steganography	Encryption-compression-steganography(in sec)
10 bytes	*11s-12s*	*11.2s-11.3s*	*2.2s-2.3s*	*12.2s-12.3s*
20 bytes	*11s-12s*	*12.2s-12.3s*	*2.2s-2.3s*	*12.2s-12.3s*
50 bytes	*12s-13s*	*13.3s-13.5s*	*2.3s-2.5s*	*13.2s-13.4s*
70 bytes	*13s-14s*	*14.4s-14.5s*	*3.3s-3.5s*	*14.4s-14.5s*
100 bytes	*13s-14s*	*14.4s-14.5s*	*3.4s-3.5s*	*12.2s-12.3s*

Table I: Records for Encryption runtime of Text Files



Size of File	Encryption-Compression	Encryption-steganography	Compression-Steganography	Encryption-compression-steganography(in sec)
10 bytes	*11s-12s*	*11.2s-11.3s*	*2.2s-2.3s*	*12.2s-12.3s*
20 bytes	*11s-12s*	*12.2s-12.3s*	*2.2s-2.3s*	*12.2s-12.3s*
50 bytes	*12s-13s*	*13.3s-13.5s*	*2.3s-2.5s*	*13.2s-13.4s*
70 bytes	*13s-14s*	*14.4s-14.5s*	*3.3s-3.5s*	*14.4s-14.5s*
100 bytes	*13s-14s*	*14.4s-14.5s*	*3.4s-3.5s*	*12.2s-12.3s*

Table II: Records for Decryption runtime of Text Files

Starting table I then table II, we decided that while the encryption and decryption time designed for Encryption Compression, Steganography system is considerably further than the other standing security systems but then owing to the 3-tier security different the 2-tier standing systems, Encryption Compression, Steganography system popular extra secure and is durable to be located broken through the attacks.

IX. IMPROVEMENT

The improvement results of Encryption Compression Steganography along with the new approaches have presented that it may possibly not be very good in relations of speed or complexity, but it will be good in terms of security. For the future stays, this speed interruption can be improved by moving the evaluation order, changing the separate approach with a low complex one.

Encryption Compression, Steganography: From the time when encryption is located a technique that changes data into worthless and safeguarded procedures that cannot be directly read through a somewhat unauthorized manipulator, it be present kept on level 1 in our 3- tier system. Toward more secure our data and compressing it to some extent possible, compression is applied to the data and hence compression is at level 2. At last, since encrypted data becomes a matter of suspicion for the attacker, this two-level encrypted form of data is hidden behind the image cover media using steganography.

From this time, we proposed a 3-tier information security system which consist of Modify play fair cipher by way of symmetric encryption technique, RSA such as asymmetric encryption technique, RLE for example compression technique also Image protection media now steganography to sustenance difficulty, Time Complexity and security.

X. Conclusion

Afterward studying the surviving encryption, compression and steganography techniques in theory as well as practically, we approached to a conclusion that no one of the techniques there self-sufficient to be responsible for data security in a period somewhere threatening to data security be situated at a shocking rate. Thus, we proposed also Evaluated Encryption Compression, Steganography the 3-tier data security through with Modify play fair cipher and RSA at level 1 (through benefits of asymmetric key encryption including difficulty symmetric), RLE next to level 2 (with the benefit of speed, no extra hardware and software and simplicity) and Steganography at Level 3 (due to informal execution, more level of detectability as well as conflict to modification). Evaluated results of Encryption Compression, Steganography through further approaches showed that this one couldn't be also better in the terms of speed else complexity but then absolutely will exist well in terms of the Security. Used for the future scope, the delay in speed could be enhanced through exchanging imperative evaluation by changing different approaches through more complex approaches.

References

[1] Kaushal A., Enhancement in Data Security using Cryptography and Compression. In: International Conference on Communication Systems and Network Technologies, pp 212-215(2017).

[2] Vaithiyanathan, A Survey on Image Steganography IEEE International Conference on Technological Advancements in Power and Energy (TAP Energy) (2017).

[3] Rajani.T, Importance of Cryptography in Network Security. International Conference on Communication Systems and Network Technologies (2013), pp 462-467(2013).

[4] Seral D., Sms Security: An Asymmetric Encryption Approach. In Sixth International Conference on Wireless and Mobile Communications, pp 448-452(2010)

[5] Gaba, J., Sharma, M.k.: A Review Based Study of Hybrid Security Schemes Based on Compression, Encryption, and Steganography. In: International Journal of Engineering Trends and Technology, vol. 4(7), pp. 3243-3246 (2013)

[6] Panda M. , Performance Analysis of Encryption Algorithms for Security, In International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016

[7] Kodituwakku S.R. , Amarasinghee U.S. , Comparison of lossless data compression algorithms for text data. In: Indian Journal of Computer Science and Engineering ISSN: 0976-5166 Vol 1, No 4 416-426.

[8] Sharma R., Bollavarapu S., Data Security using Compression and Cryptography Techniques. In : International Journal of Computer Applications ISSN: 0975 – 8887 Volume 117 – No.14, May 2015.

[9] En.wikibooks.org. (2019). Steganography/Covers - Wikibooks, open books for an open world. [online] Available at: https://en.wikibooks.org/wiki/Steganography/Covers#Photos [Accessed 25 Mar. 2019].

[10] Nameer N. EL-Emam, Hiding a large amount of data with high security using Steganography Algoithms. In: Journal of Computer Science ISSN: 1549-3636 Volume 4 2007.

[11] Roy R., Changder S., Sarkar A. , Debnath NC., Evaluating Image Steganography Techniques: Future Research Challenges in IEEE 2013 978-1-4673-2088-7/13/$31.00 ©2013 IEEE

[12] En.wikibooks.org. (2019). Steganography/Covers - Wikibooks, open books for an open world. [online] Available at: https://en.wikibooks.org/wiki/Steganography/Covers#Text [Accessed 25 Mar. 2019].

[13] En.wikibooks.org. (2019). Steganography/Covers - Wikibooks, open books for an open world. [online] Available at: https://en.wikibooks.org/wiki/Steganography/Covers#Audio [Accessed 25 Mar. 2019].

[14] Ansari A., Mohammadi M.S. , Parvez M.T. , A Comparative Study of Recent Steganography Techniques for Multiple Image Formats in International Journal of Computer Network and Information Security · January 2019.

[15] Shrivastva A., Singh L., A new hybrid encryption and steganography technique : a survey. In International Journal of Advanced Technology and Engineering Exploration, ISSN: 2394-7454 Vol 3(14) (2016).

[16] Maan, A.J. :Analysis and Comparison of Algorithms for Lossless Data Compression. In: International Journal of Information and Computation Technology, vol. 3(3), pp. 139-146(2013)

[17] Ibrahim, A.M.A., Mustafa, M.E.: Comparison Between (RLE And Huffman) Algorithmsfor Lossless Data Compression. In: International Journal of Innovative Technology and Research, vol. 3(1), pp. 1808-1812(2015).