Hybrid encryption algorithm to encrypt sensitive information and hiding it using steganography

Aakash Kumar Sahoo[1], Abdullah Nawroz[2], and Vikash Kumar Mishra[3]

Galgotias University, Greater Noida, Gautam Buddhh Nagar, Uttar Pradesh, India.

rksahoo2806@gmail.com, abdullah.nawroz@gmail.com, and vikash.mishra@galgotiasuniversity.edu.in

ABSTRACT

The Hybrid encoding is associate degree approach to secret writing and decipherment information that blends the speed and convenience of a public uneven encoding theme with the effectiveness of a non-public regular encoding theme. during this approach to cryptography, the sender generates a non-public key, encrypts the key by employing a public key rule then encrypts the complete message (including the already-encrypted personal key) with the initial regular key. The encoded cipher will solely be decoded if the recipient is aware of the personal key the sender originally generated. Asymmetric encoding will bog down the encoding method, however with the synchronal use of regular encoding, each kinds of encoding area unit increased. The result's the superimposed security of the transmitting method in conjunction with overall improved system performance.

Steganography, in other words also termed as the technique of communication that is not visible, is a majorly used mode of sending information from one place to another, that typically focuses on the modes to hide any type of sign that can show the presence of the message to be transmitted. If this concept is effectively achieved, the plain text (message to be transmitted) won't attract the eyes of the intruders, attackers or eavesdroppers or attackers. Data can be embedded in a number of embedding materials termed as carriers, by making the use of concept of steganography. Text, Image, Video and Music files all can be utilized as carriers. By using the concept of steganography one can add an additional layer of security and to the info which may be simply transferred from one system to a different while not obtaining suspicious by the unmotivated person like hacker or enemy.

Keywords— Encryption, Decryption, RSA, AES, Security, Cipher, Hybrid, Security, Image, Video, Audio, Steganography.

INTRODUCTION

With the speedy development of technology and therefore the widespread of web, people's lives area unit undergoing tremendous changes. The alleviation, internationalisation and personalization options of web bring revolutionary reform and receptive government agencies, enterprises and establishments, at an equivalent time facilitate to lift work potency and market response ability to boost their fight by victimization web. However, the way to create the knowledge system of steer isn't leaked, although they're taken it's troublesome to be known, if the area is known, they are very troublesome to be changed. As an example, steer isn't allowed non-authorized personnel to look at, personal content, sensitive data, trade secrets, got to stop others unauthorized access, modify, copy, etc. This series of necessities has become a hot analysis topic within the IT business [1].

Cryptography that is that the art and science of protective data from undesirable people by changing it into a kind indiscernible by its attackers whereas it's keep and transmitted. it's a basic building block for building data systems. It has a relation with the study of techniques of mathematics that are associated with the aspects of the security of information such as the information integrity, confidentiality, and the authenticity of the data [2].

In cryptological word, the info that may be scan and understood with none special measures is named plaintext or clear text. the tactic of disguising plaintext in such the way on hide its substance is named encoding. Encrypting plaintext leads to illegible hokum referred to as cipher text. the method of retrieving the plaintext from the cipher text is named decipherment. A system or product that gives encoding and decipherment is named cryptosystem.

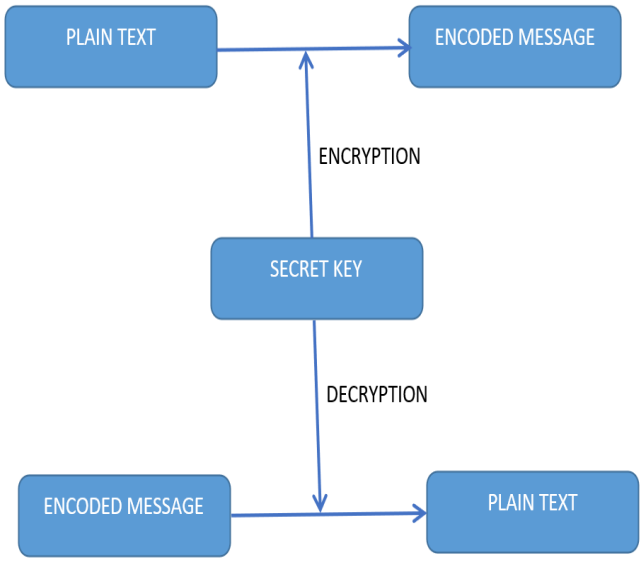

Fig 1. Encryption and Decryption

Depending on the quantity of security keys you want to encrypt/decrypt information, cryptological algorithms area unit classified as uneven algorithms (public key) and regular

algorithms (secret key). In regular key encoding, only 1 key's needed to cipher and decode information. The key ought to be distributed before transmission between entities. Therefore, key plays a vital role in regular key encoding. Power of symmetric key encoding technique somewhat depends on the size of the key being used. For an equivalent rule, encoding victimization longer key's tougher to interrupt than the one done victimization shorter key. The weakness of symmetric algorithms lies in the fact that there is need to share the symmetric key between sender and the receiver.

For adding an extra layer of security, steganography can be used which can hide the data in an image or video. Using this, we can hide our encrypted data to make it more secure and make less suspicious from the hackers.

Cryptography scrambles messages in order that they can't be understood. Steganography on the other side, has the capability to hide the message, so it plays a bluff with the existence of data at the very first place. In some things, causing associate degree encrypted message can arouse suspicion whereas associate degree “invisible” message won't do therefore. Both types of sciences may be merged to provide a even higher protection of the message. During this type of case, if somehow intruders manage to get the message that was hidden using Steganography or the Steganography fails, and therefore the message may be detected, still the message is of no use because it is encrypted with the help of two cryptography techniques.

There are 2 styles of materials in steganography: plain text (message) and carrier. Plain text is that secret information that ought to be hidden and the carrier is that material that takes the message along with in it.

This are a various number of cryptographic techniques. In this paper, we will be aiming to take a brief investigation of totally different steganography techniques. Fig. 2 below presents the various types of formats of files that may be used for steganographic strategies [3].

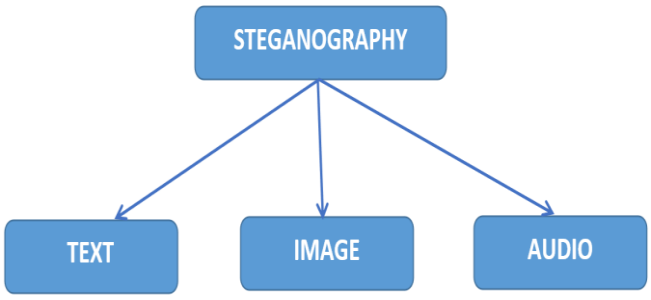

Fig 2. Types of Steganography

Due to the very fact that you simply will hide data while not the quilt supply dynamical, Steganographic technique is also very helpful in the field of watermarking. As we know that the construct of watermarking isn't neccessarily steganography, but there are a lot of steganographic techniques that can be employed efficiently and effectively to store the watermarks in data. The most distinctive thing between Steganography and Watermaking is on intent, the intention of steganography is to hide the data without changing any type of data on the cover source whereas watermarking is simply a technique to add some extra quantity of information on the cover source. Steganography does not leave any visual changes on the cover source, no one can differentiate the steganographed image and non-steganographed image but in watermarking, an extra thing is visible on the cover source.

LITERATURE REVIEW

In the era of speedy development of electronic network data, data encoding rule has become a vital space of package security, created a great deal of analysis. during this paper, we have a tendency to style the hybrid secret writing rule by the direct use of well-known secret writing rule, improve the well-known secret writing rules and outline a replacement low-level formatting secret writing rule so as to realize the planning of hybrid secret writing algorithm.
The two rules utilized in the planning of hybrid algorithm are ‘initial encoding algorithm’ and ‘Base64 algorithm’.

The design of initial secret writing rule, primarily think about the code price of the corresponding calculation, confirm the new string consistent with the new code price.

Base-64 secret writing rule thought of 3 major problems: initial is encrypted; the second is that the complexness and potency of the secret writing algorithm; third, a way to subsume the transmission. encipher is critical, but the sole and only purpose of this technique isn't to encipher the users to send secured Emails, its sole purpose is to prevent the intruders from understanding the contents of the delivered message directly.

From the previous works done, in a large number of simulation results, it had been proved that AES has a far higher performance than different types of encryption algorithms in terms of each encryption-decryption time and turnout [2].

Another analysis work created use 3 writing techniques – Line shift writing, word shift writing, feature writing. The techniques will be used either on an individual basis or together. every technique enjoys sure benefits or pertinence.

Line-Shift writing – it's a technique of fixing a file by vertically relocating the positions of text lines to encipher the file unambiguously. This coding is also implemented either on the format of a file or to the electronic image of the image of a page. The encrypted codeword is also achieved from the file to store format or electronic image.

Word-Shift writing – it's a technique of fixing a file by horizontally relocating the positions of words at intervals of text lines to encipher the file in a very unique way. This type of coding will be applicable to either the electronic image or the format file of the page of a image. decryption is also performed from the format file or electronic image.

Feature writing - it's a encoding technique that can be applicable either in case of bitmap image or to format file of any document. The image is then analysed for the chosen features of the image file, and then totally depending on the codeword, it is decided whether to alter those features or not. In the decryption part, there is the need of initial image, or even specifically, a proper specification of the alteration in pixels of a feature of the image. There are a lot of options of text features available; here, we can select to change upward endlines – which is the topmost of letters c, e j, etc. These endlines can be changed by elongating or lessening the lengths of endlines by one or more pixels, but it should be done carefully so that the feature of the image is not altered [3].

In an extra analysis work, a hybrid cryptographic system was presented that made use of the advantages of both the encryption algorithms – asymmetric and symmetric for giving the cloud user a security for its data. The decryption and encryption of the plain text have only single encryption -decryption key, that is used in case of decryption and also encryption. One more asymmetric key is employed, to encode the key of AES algorithm, that gives an increased security. As the hybrid encryption system offers two security layers, it has the capability to emerge as the more secure and sturdy algorithms [4].

A research work created use of mixture of improved AES and error correction code secret writing rule has been planned. this rule can't only enhance the speed of information secret writing and secret writing, however additionally substance the matter of distribution of key. During the same time, with the help of this hybrid plan, one can totally finish the authentication doubt, and also it has the high speed of computation, a capability of anti -attack, and also improves the safety of effective method of data transmission [5].

Steganography, particularly combined with cryptography, could be a powerful tool that allows folks to speak while not attainable eavesdroppers even knowing there's a variety of communication within the initial place. The ways utilized in the science of steganography have advanced a great deal over the past centuries, particularly with the increase of the pc era. though the techniques are still not used fairly often, the probabilities are endless. many alternative techniques exist and still be developed, whereas the ways in which of police investigation hidden messages additionally advance quickly [6].

PROPOSED SOLUTION

Our proposed solution makes use of two encryption algorithms – RSA & AES to create much more secure and safe transfer of data from one system to another, we've given a hybrid type of connection between these two given algorithms as pictured in Fig 3. Within the planned structure, plain text (information) is initially encrypted with the use of the AES encoding technique. The key that is employed for this encoding is then encrypted again using the RSA algorithm. This key (encrypted by RSA) packed with the plain text encoded by AES technique is then forwarded to the designated receiver. By using the public or private key of the RSA algorithm, initially the AES key is decoded by RSA technique. This decoded key is then finally used to decode the encoded message to get the original message.

As RSA makes use of 2 types of keys – public and private, there's not any need to communicate keys between the two parties that are sender and receiver. This type of theme provides a two layer security and in a literal sense, makes the encoded message uncrackable.

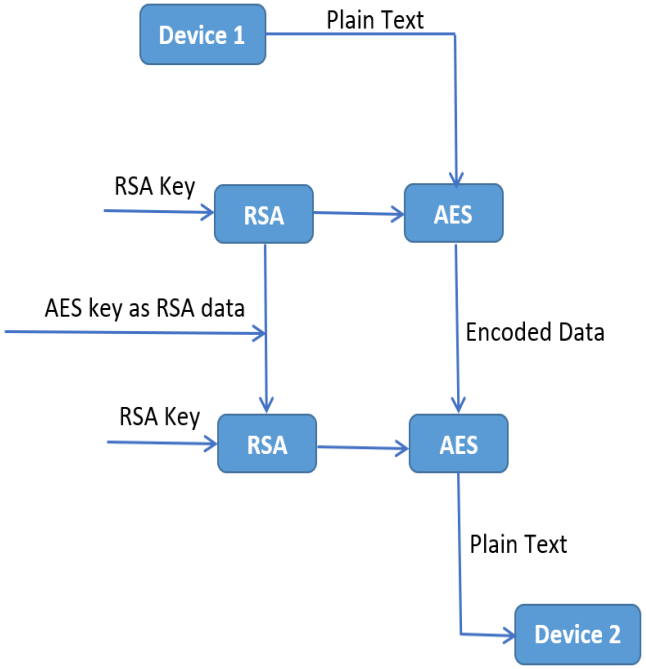

Fig 3. Flow of solution

After we have a tendency to get the encrypted key by applying RSA rule, the 'RSA encrypted key' and knowledge encrypted by AES rule is distributed to steganography rule and also the encrypted knowledge alongwith Encrypted secret's embedded within the image file.

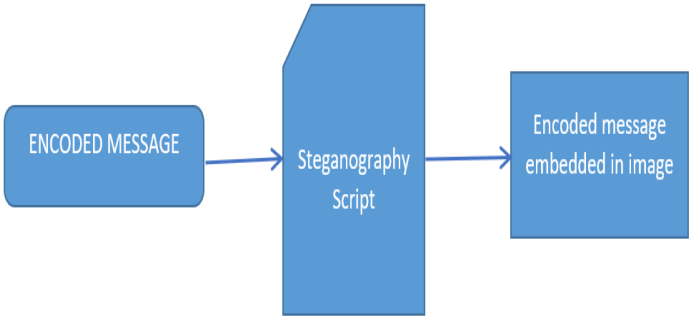

Fig 4. Steganography process

RESULT

The runtimes for the processes employed in the proposed solution are as follows –

RSA Enryption/Decryption process runtime

Data size (in MB)	Runtime (in millisec)	
	Encryption	Decryption
1	425.6	3.8
2	710.9	3.5
5	1710.9	3.7
10	3017.1	3.7
20	6641	4.0

Table 1. RSA Enryption/Decryption runtime

AES Enryption/Decryption process runtime

Data size (in MB)	Runtime (in millisec)	
	Encryption	Decryption
1	80	118.9
2	154.7	197.6
5	376.1	457.7
10	683.7	897.5
20	1350.5	1844.5

Table 2. AES Enryption/Decryption runtime

Encoding/Decoding runtime for Steganography process

Data size (in MB)	Runtime (in millisec)	
	Encoding	Decoding
1	481.5	4.1
2	691.5	4.5
5	1031.7	4.7
10	1437.1	4.7
20	1816	4.7

Table 3. Steganography Encoding/Decoding runtime

CONCLUSION

In this new generation of very quick developments, in the field of computer information and networks, there is an urgent and continuous need of secure ways and standard that can aid in our information sharing or in other words we can say, the algorithms that can help us to communicate electronically in a secured environment, so that no unethical person can gain access to our information.

Our communication through electronic medium consists of some sensitive and private information, so it is very important that it is made sure that the information does not get leaked.

Keeping in mind the above scenario, we have proposed a solution, i.e. Hybrid Encryption Algorithm that makes use of two advanced encryption standards that are AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adelman). After encryption the information using these two encryption standards, the ciphered text is encoded in an image file for improved security.

REFERENCES

[1] Lili Yu, Zhijuan Wang, Weifeng Wang "The Application of Hybrid Encryption Algorithm in Software Security" 2012 Fourth International Conference on Computational Intelligence and Communication Netwoks

[2] Madhumita Panda "Performance Analysis of Encryption Algorithms for Security" International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016

[3] Masoud Nosrati, Ronak Karimi and Mehdi Hariri "An introduction to steganography

[4] methods" World Applied Programming, Vol (1), No (3), August 2011. 191-195

[5] Vikrant Shende, Meghana Kulkarni "FPGA based Hardware Implementation of Hybrid Cryptographic Algorithm for Encryption and Decryption", 2017 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT)

[6] Xiang Li, Junli Chen, Dinghu Qin, Wanggen Wan, "Research and Realization based on hybrid encryption algorithm of improved AES and ECC" 978-1-4244-5858-5/10/$26.00 ©2010 IEEE

[7] J.R. Krenn, January 2004, http://www.krenn.nl/univ/cry/steg/article.pdf

[8] Christian Cachin, Digital Steganography, Encyclopedia of Cryptography and Security, 2005

[9] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, Data Hiding Through Multi Level Steganography and SSCE, Journal of Global Research in Computer Science Journal Science, ISSN: 2229-371x, Volume 2, No. 2, February 2011, pp. 38-47