International Journal of Advanced and Innovative Research (2278-7844) / # 1/
Volume 6 Issue 11

AN ANALYTICAL STUDY ON COMBINED STEGNO AND CRYPTOGRAPHY SECURITY ALGORITHMS

S.ANITHA[1] Dr. T. RAMAPRABHA[2]

selvianithas@gmail.com #1
ramaradha1971@gmail.com #2

Research Scholar #1
PG & Research Department of Computer Science
Vivekanandha College of Arts and Sciences for Women [Autonomous]
Elayampalayam,Tamil nadu
Professor #2
PG & Research Department of Computer Science
Vivekanandha College of Arts and Sciences for Women [Autonomous]
Elayampalayam,Tamil nadu

Abstract **— In widespread system the number of set of connections technology enhance rapidly. Sometimes the illegal activity also gets increased. That means the not permitted persons can cut the information in which the hackers may be from inside and outside. The costly information is always attack by the invader in the network. Attacks may occur in many ways. These attacks are otherwise called as threat. Using multiple methodologies the attackers may combine many hacks. So an well-organized security system is desired in networking system to avoid hacking. Therefore, an proficient security model is necessary to save from harm undisclosed information over the network system. However, many security systems have been introduced for the protection purpose. Here we use two the latest thing security techniques, cryptography and steganography, which performs better in contrast of other existing regular and mechanical safety methods.**

Keywords: **Cryptography, Steganography, SKC, PKC, AES, KEA, DES, DCT, DWT**

I. INTRODUCTION

These days, the exchange of information has gained marvelous growth by the computer networks without any complicatedness. Though, this type of networks is used for high-speed and unproblematic process to exchange information over the long distance, shelter and safekeeping of not to be disclosed information remains a concern in electronic contact.

Slowly, with the amplification of computer networks number of new technique has come to impacting accessibility, isolation, and integrity of serious data that poses a brutal problem for risky situation. In dissimilarity, a lot of move toward has been probable by using the two stylish fortification techniques, cryptography and steganography, for humanizing the safekeeping of secret messages over the channels in open statement. But these technologies may not be unswerving for transferring surreptitious in sequence for long distance announcement in which additional security mechanisms are wanted to confined secret information every time. Cryptography is used to move the information quickly where the steganography implanted that crypto graphed information into the binding medium. This provides current high-tech inquiry of these two security techniques to raise above the lack of recent applications besides the security methods for customers in a better way to the researchers and for inspiring them to design a better security system that recover the level of the security system.

II. CRYPTOGRAPHY

Cryptography is a most universally used routine that encrypts or converts the plain text into cipher text also called as encrypted text. Data can be read and understand in easy way lacking any special actions is called plaintext or clear text. The method of converting the plaintext to hide its import is called encryption. Encrypting plaintext results in indecipherable format called cipher text. The cryptography ensures the safety from the hackers. So the valid persons alone can access or read the information. Mainly cryptography scrambles data for ensuring privacy of in a row and enables to send out data across unconfident networks so that it cannot be read by anyone apart from the practiced recipient. Cryptology and cryptanalysis are two main underbrush of cryptography. Cryptology is to keep plaintext secret from hackers or simply the enemy where as cryptanalysis deals with the techniques to get better the innovative in sequence that will be customary as genuine. In common, all cryptographic techniques have four basic parts:

(i)Plaintext **-** Unscrambled information to be transmitted. It must be a simple text document, like a credit card number, a password, a bank account number, or personal information such as payroll data, employee data base, salary information, or a company secret formula to be transmitted between organizations. Plain text is the inspired information transmitted by the dispatcher.

(ii)Ciphertext**-** Represents plain text rendered incoherent by the submission of a statistical algorithm. The encrypted plain text which is transmitted from side to side the direct to the recipient is called Cipher text.

(iii)Key**-** A geometric value, principle, or procedure that determines how a plaintext message is encrypted or decrypted. The key is the only way to work out the twisted information.

(iv)Cryptographic Algorithm **–** A statistical formula used to blend up the plain text to yield cipher text. Converting plain text into (unreadable format) ciphertext using the cryptographic algorithm is called encryption, and converting ciphertext back to plain text using the same cryptographic algorithm is called decryption. Figure 1 depicting the strategy of cryptography.

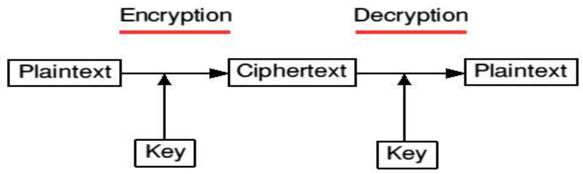

Figure 1 Cryptography

Largely cryptographic algorithms can be divided into two categories:

1) *Stream algorithms*. It can drive on plaintext byte by byte that is one byte at a time, where byte can be a character, number, or special character. This process is instant consuming and useless.
2) *Block* algorithms – Operates on plaintext in groups of bytes, called blocks so it is called as e block algorithms or block ciphers. Usual block sizes for recent algorithms are 64 bytes. Though it is small enough to work with, bulky as much as necessary to determine code breakers. For data security following three types of cryptographic schemes are mostly used nowadays:

A. Secret Key Cryptography(SKC)

It is also called as symmetric-key cryptography design because it uses a single key for both dispatcher and recipient. The Data Encryption Standard (DES) is the best example of this cryptosystem in which the Federal Government extensively employs this technique. The steps followed in secret key cryptography(SKC) to make safe statement has been illustrated .

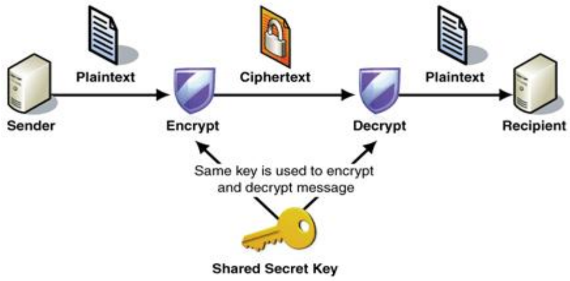

Figure 2 Symmetric key cryptography

Nevertheless, the data security is improved through this method but key allocation between dispatcher and its recipient has become a problematic mission because an not permitted individual may get total information eagerly formerly he/she gets surreptitious solution. Thus the input shelter is an urgent difficulty for harmless communication.

Merits of Symmetric Key Cryptography

- High- speed recital.
- Speedy verify dependability of input recipients.
- To acquire a unadorned copy equivalent key is obligatory as used at significance encrypt point in time.

- Erroneousness appreciation and modification is easy.

Demerits of Symmetric Key Cryptography

- Input distribution is a sturdy assignment. Unofficial personality can admit the complete information without difficulty lacking any attempt if he/she gets undisclosed solution.
- This practice not provides digital signatures that could not be repudiated.

B. Public Key Cryptography (PKC)

Public key cryptography is an asymmetric proposal. It uses a couple of keys, one is performing as a surreptitious type mutually a public solution in addition to confidential explanation in the encryption progression or undisclosed input for decryption practice. In this performance a twosome of keys essential for the development.

various examples for communal explanation Cryptography are, the RSA, Diffie-Hellman, Digital Signature Algorithm (DSA), Public-Key Cryptography Standards (PKCS), Key Exchange Algorithm (KEA) are scarcely any examples of Asymmetric-Key Algorithms.

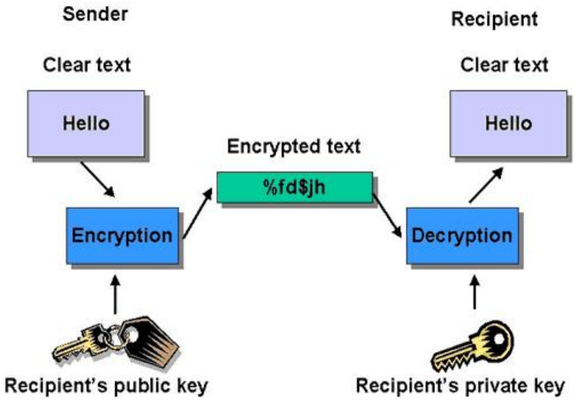

Figure 3 shows the operational steps of this algorithm

Merits of Asymmetric Key Cryptography

- conquer the input distribution issues of symmetric key algorithms.
- Public-key cryptography is supplementary safe than the secret-key cryptography.
- By means of using brace of keys it increases the rank of safekeeping.
  Be capable of offering digital signatures so as to be repudiated

Demerits of Asymmetric Key Cryptography

- The foremost inconvenience of using public-key cryptography meant for encryption is extra rapidity.
- Public-key cryptography might be dependent in computerization.
- It results in official recognition troubles; numerous public key systems utilize a third party to attest the regularity of unrestricted keys.

III. STEGANOGRAPHY

In several cases, transferring the encrypted message might depict consideration, whereas indiscernible information will not describe the concentration of others. As a consequence, cryptography will not be the greatest resolution for safer communication. To trounce this Steganography is worn, which is consequently commencing the Greek word steganos means "enclosed" and graphia means "text", in addition to Steganography revenue "enclosed inscription". In this process, the secret image is surrounded in the wrap image and which results in the invisible transfer of the exits information. For embedding the in sequence digital images, videos, sound files and other computer files can be used as a transporter. The outline of the Steganography system is represented in the outline.

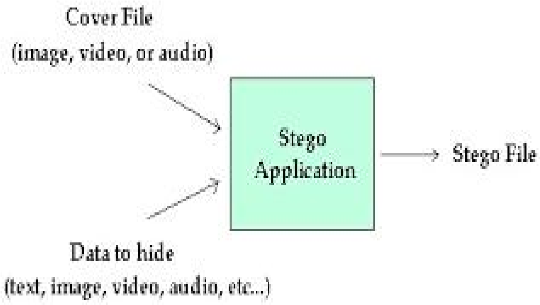

Figure 5 General Steganography Model

The thing in which the secret information is masked is called unknown object. Stego image is an image which is obtained by embedding secret image into hidden or covert image. The hidden message to be transferred can be any route like plain text or cipher text and may be images too. The steganography method provides rooted data in an invisible manner with high payload facility.

Three important types of steganography system are as follows:

1) *Image Steganography*:

The unknown undisclosed letter is reproduced as transporter image, which is then renewed into stego outline.

2) *Video* Steganography:

This style divides the video into audio and image frames wherever the process of embedding is performed in the auditory file as in audio Steganography .

3) *Audio Steganography:*

In this practice, the undisclosed message is implanted into idle audio bits.

Steganography techniques that are used in day to day life include:

A. Discrete Cosine Transform (DCT)

In this technique, the wrap picture is altered from spatial area to regularity area. Yet, two aspect DCT transformations are used. The encryption of undisclosed picture is rooted, after the submission of IDCT on DC coefficient and quantization. This scheme uses JPEG density algorithm, which is used to renovate 8X8 pixel blocks into 64 DCT co-efficient. Further it is personalized to embed the encrypted surreptitious information. Since the methods works on occurrence domain, it produces unremarkable changes in the graphic exterior of the picture. The main weakness of this revolution is, it works only on JPEG files. In DCT, Encrypted undisclosed picture is to be found in the low down and normal occasion co-efficient that is cannot be operated in all occurrence level which is also a weakness of this structure.

B. *Discrete* Wavelet Transforms (DWT)

Discrete Wavelet Transform (DWT) converts spatial area in sequence to the regularity province in sequence wavelet which are used in the image steganographic form because the high frequency and low –frequency information are unmistakably partitioned by the wavelet transform on a pixel by pixel basis. Thus the weakness in DCT can be beat all the way through this creation. Many practical tests inform to use the wavelet transform domain for steganography because of a number of damages. The use of this insurrection will primarily concentrate on the competence and healthiness of the in turn beating structure skin.

In wavelet, both time answer and frequency answer in sequence are known specific. The modernization is made easy because of incorporation and isolation of the image. The main plus point of DWT over DCT is the allotment of the key coding into non overlapping 20 blocks. Secondly, it allows excellent localization mutually in moment and spatial event area because of its high concreteness ratio that avoids blocking artifacts. Thirdly, conversion of the complete image introduces inbuilt scaling. Finally, better detection of the data which is correlated to individual sharpness is made through high density ratio. Also, this method provides a high beating competence and a better eminence stego-image is produced which results in the analyses of the constraint hit the highest point signal to sound ratio by comparing the DCT domain and DWT domain. Peak gesture to sound proportion procedures the importance of the stego-image by manipulating the distortions taking place among the stego-image and cover image that is elevated the PSNR ratio more will be the image security.

Though, the Steganography is narrowly connected to the cryptography process to look after the in turn to be send from the useless parties but only this equipment is definitive and can be compromised as the best system. As soon as the existence of unknown information is exposed or even the presence is assumed, the reason of steganography is partially running scared. Thus the force of steganography can thus be enlarged by combining it with the crypto graphical system. In case, the steganography fails to send the unseen message which is detected it is encrypted with the cryptography methods, If encryption is not performed, it is immobile. So, it is clearly implicit DWT is the most professional system which is the transformation of steganography and cryptography system.

IV. RELATED WORK

In [5] the author used the technique of AES extension along with bit wise operation in which 128 bit keys are used for image pixels. The usage of keys with AES opening out operation is autonomous of dispatcher and recipient. The main plus point is it requires less memory and time intense with high encryption excellence.

In [7], stretched remoteness announcement Steganography with cryptography ensures prevailing tools for image security. This adopts various methodologies like DES, S- box mapping etc for enhanced protection. Even if the information is safe the progression is very convoluted and involves large calculations.

In [8] a proportional investigation for value and image size is performed between Joint Picture Expert Group (JPEG) image stegano and Audio Video Interleaved (AVI) video stegano. Here the key strength is monotonically improved by using UTF-32 programming in the transaction algorithm and lossless stegano system in the AVI file. But payload competence is small.

In [9] an adaptive invertible in sequence thrashing method for Moving Picture Expert Group (MPEG) video is projected. Unseen data can be well again without requiring the goal to have a earlier copy of the stealthy video and the original MPEG video data can be improved if needed. This procedure works in timekeeping domain only. It has the reward of low convolution and low diagram deformation for stealthy announcement applications. However, it suffers from low payload facility.

In reference [10], various methodologies used in image steganography are anticipated. A appraisal is made for trouncing a secret message or image in spatial and transform domain as followed in DCT. It not only hides the in sequence but also provides techniques for detecting the undisclosed message or image which is called as steganalysis.

The paper at [11] introduced a method where secret message is first condensed using wavelet transform procedure and then embeds into wrap image using LSB where the bits of secret message is inserted into image by using random number originator.

In [12], authors give brief review of above technique used for ensuring safety measures. It proved in this paper that using these techniques, data can be made more locked and strong.

In [13] Author tries to prevail over the capacity imperceptibility through proposing three main steganography challenges. This is achieved by fusion data thrashing scheme in commercial LSB method with a key combination process. A two layers of precaution system anticipated in [14] namely login formula followed by key embedding. Username and secret word are mandatory for login course of action only once. Secondly, key is used to entrench the secret data. By this, dependability and discretion is achieved effectively.

In [15] the idea of dual safety measure is traditional, all the way through which undisclosed data is firstly renewed to encrypted type and then LSB performance of steganography is used to entrench it within plaster object. By this method, message is transferred with maximum protection and can be retrieved exclusive of any hammering of data.

In reference [6], author anticipated a new method of elevated precaution presentation by using LSB steganography and cryptography. In this method, RSA algorithm is used before embedding the particular image through which the undisclosed in sequence is encrypted. Though this method possesses some difficulties in time outflow, it is ideal for its high safekeeping ignoring the outlay.

V. Conclusion

Thus the state of the art exploration work in the area of two fashionable in sequence protection and safety measures approaches, called as cryptography and steganography. Though these both techniques come up with the money for safety measures for secret information, the cryptography amend the taken as a whole situation of the in turn from the dispatcher in such a way that only its sanctioned or accepted recipient person can gain the text message, where as in the steganography system the complete hidden information is in the sheltered form, so no one can easily figure out the unseen message in the accessible content but no one dissimilar come near is so good for practice. Therefore the in turn from the dispatcher should be transmitted with more security to the recipient through the unsecured channel needs a new advance performance for data security. Though advance techniques like DWT were optional, future work should be done by combining the concepts of cryptography and steganography, for ensuring more protection to the secret message while communication.

VI.REFERENCES

[1] Menezes, Alfred , Paul C van Oorschot ,Scott A. Vanstone, " Handbook of Applied Cryptography. CRC Press", October 1996 , ISBN 0-8493-8523-7.

[2] William Stallings, "Cryptography and Network Security: Ethics and practices", Pearson education, Third Edition, ISBN 81-7808-902-5.

[3] W. Stallings, Cryptography and network security: Philosophy and practice. Prentice Hall, 2010, vol. 998.

[4] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osama M. Al-Qershi "Image Steganography Techniques: An Overview" International Journal of Computer Science and Security (IJCSS), Volume (6) :Issue (3) : 2012

[5] B. Subramanian "Image encryption based on AES key expansion" in IEEE functional second international forum on emerging application of information technology, 978-0-7695-4329-1/11, 2011.

[6] Shailender Gupta, Ankur Goyal and Bharat Bhushan "Steganography and Cryptography using LSB" International Journal Modern Education and Computer Science, vol.6,pp.27-34,2012.Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishor Saxena, "Security inventiveness in image Steganography using DES",3rd IEEE Trans. intercontinental Conference IACC -2013, Page(s): 1094 – 1099.

[7] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishor Saxena, Monika Sharma "Image Stenography: Self mining Mechnanism", UACEE International Journal of Advances in Computer Science and its Applications- IJCSIA Vol -3 Issue -2 ,ISSN 2250-3765 Pg-145-148, 2013.

[8] R.Kavitha and A. Murugan, "Lossless Steganography on AVI File using Swapping Algorithm", International Consultation on Computational Intelligence and Multimedia Applications, pp. 83-88, Sivakasi-Tamil Nadu, Dec. 2007

[9] Yueyun Shang, "A New Invertible Data Hiding in Compressed Videos or Images", Third

International Conference on Natural working out (ICNC 2007), Vol. 4, pp. 576-580, Haikou, Aug. 2007.

[10] S.Ashwin, J.Ramesh, K.Gunavathi, "Novel and Secure Encoding and Hiding Techniques Using Image Steganography: A Survey", IEEE Xplore International Conference on Promising Trends in Electrical Engineering and Energy supervision, Dec 2012, pp. 171-177.

[11] Humanth Kumar, M.Shareef, R. P. Kumar, "Securing in sequence Using Steganography", IEEE Xplore International Conference on Circuits, Pwer and Computing Technologies, March 2013, pp. 1197-1200.

[12] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "Stegocrypto - A Review of Steganography Techniques using Cryptography", International Journal of Computer Science & Engineering Technology, ISSN: 2229-3345, Vol. 4, 2013, pp. 423-426.

[13] Marghny Mohamed"Data hiding by LSB exchange using genetic optimal key incarnation " in International arab journal of e-technology ,vol.2,no 1,11-17, January 2011.

[14] Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Algorithm to Hide Secret significance inside an Image",Computer Technology and Application, vol. 2, pp. 102-108, 2011

[15] K.Sakthisudhan, P.Prabhu, "Dual Steganography move toward for Secure Data Communication" International Conference on Modeling, Optimization and Computing, Elsevier, Procedia Engineering, vol. 38, pp. 412-417, 2012