Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 6, May-2019, ISSN 2230-7540

Enhancement in Security Using Hash- Stegno-Crypto for Secure Communication

Ankit Sharma[1]* Parag Rastogi[2]

[1] Research Scholar, Department of CSE, Swami Vivekanand Subharti University, Meerut (UP) India

[2] Assistant Professor, Department of CSE, Swami Vivekanand Subharti University, Meerut (UP) India

Abstract – There are different security dangers and assaults which can impact the data transmission through the wired and wireless communication networks. By carrying out the secure and safe system for privacy and information reliability for making sure of safe information transmission, the problem can be solved. Digital images are quite well-known due to the fact of their frequency on Web from every varying carrier file format. Through Steganography, it is possible to conceal that there is a communication by concealing the information under other information. Numerous kinds of steganography methods can be found where all of them have their pros and cons. Hashing algorithm, steganography methods; Data encryption can be helpful in securing information exchange through communication sources. It is possible to categorize cryptographic algorithms and protocol as: symmetric and asymmetric. Shared key in the symmetric method can be helpful in privacy service as the blocks or streams of plain text of all sizes are transmitted to cipher text that cannot be read. Current Literature is examined here in the research study which is about improving security through Hash -Crypto- Steganography so the communication source can be safe and sound.

Keywords: Steganography, Cryptography, Security, Communication etc.

----------X----------

I. INTRODUCTION

Steganography does not just help in concealing the information but also conceals the fact of transmission of private information. Steganography helps in concealing private information in some file in a way through which just the receiver would know about that message. Steganography is derived from Greek language that means concealed writing. “Steganos” implies “covered” while “graphical” implies “writing”. In the old age period, information was secured as it was concealed on back of wax, writing tables, and rabbits’ bellies or scalp of slaves. Nowadays, majority of people perform data transmission through text, video, images, and audio.

Steganography is one among the many security methods which embeds a message to a certain carrier data like audio, text, image, or video. Image steganography method can be categorized to two domains which are: image/spatial domain and transform/frequency domain. Steganography can help is concealing the message in data carrier like text, audio, video, and image for transferring it through safe source in communication network. Cryptography and Steganography, both, are methods which are helpful in giving information security though numerous variances could be found in both of them. Cryptography can transform readable secret information to unreadable information for the privacy security facilities.

Information security is among the most considerable issues in the data communication and it is the core of data communication. For solving this issue, cryptography and steganography may be merged. Data transmission security seems to be a major issue in the communication networks. Communication system can be dependable if it offers high security range. At often times, users exchange personal delicate information or vital documents and these are the instances when security, reliability, validity and privacy of exchanged data must be offered through transmission means. Internet multimedia is quite well-known and considerable volumes of information are transmitted each second through means which are not secure and might be unsafe. Thus, it becomes vital that the information is secured from the attacks. Cryptography and steganography methods are the ones which can help secure that information.

II. STEGANOGRAPHY

Zhang and Wang (2015) had a steganographic proposal which utilizes human vision sensitivity for concealing the private parts [1]. For this, initially, private data is transformed to sets of symbols through numerous bases and certain bases can help in measuring extent of local difference of pixel magnitudes in host image. The least significant bit matching (LSBM) steganography was presented with a bit of alteration which offered the wanted alternative of a binary function of two cover pixels instead of being random like in LSBM. For increasing security level, there was a mixed data encoding and hiding procedure which was helpful in tackling the image color change issue following the embedding procedure.

LSB steganography method was formed according to embedding the concealed message to sharper edge areas of image for assurance of the resistance opposing image steganalysis according to the statistical analysis. There was introduction of a new image steganography which was on the basis of integer wavelet transform (IWT) which helps in embedding numerous concealed messages and keys in color cover image.

Steganography is the old subject, and its cutting-edge detailing is usually given as far as the prisoner's concern proposed by Simmons (2013), where two prisoners wish to convey covertly to incubate a departure plan [2]. The majority of their communication goes through a warden who will toss them in isolation should she presume any undercover communication. The warden, who is allowed to look at all communication traded between the detainees, can either be passive or active. A passive warden essentially analyzes the communication to attempt and decide whether it conceivably contains mystery information. In the event that she speculates a communication to contain concealed information, a passive warden observes the distinguished undercover communication, reports this to some outside gathering and lets the message through without blocking it. An active warden, then again, will attempt to change the communication with the presumed shrouded information purposely, so as to expel the information.

Quantization-based steganography system exhibited in Tong and Zheng-din (2012) installed the secret message in each chrominance of a shading picture to expand the concealing limit [3]. DWT frequency domain steganographic system was proposed where information is covered up in vertical, diagonal and horizontal segments of the sub – picture. A secret information communication system was introduced, it utilizes RSA with asymmetric keys and AES with symmetric key to scramble the information, after that the encoded information is installed into the spread picture utilizing keen LSB pixel mapping and information revision strategy. Two secure communication systems were proposed to be utilized for voice over IP (VOIP) applications. LSB based steganography was utilized to shroud the data over a sound spread sign. An all-encompassing rendition of SHA-1 (Secure Hash Algorithm) was presented; this system can be utilized to scramble two-dimensional information, for example, picture. It is created to build the opposition of picture-based steganography against the assailants and programmers. A riotous sign was utilized for picture steganography, which displays a dissipating design for the installed information through the spread picture. A high limit and security steganography utilizing discrete wavelet change (HCSSD) was built up; the wavelet coefficients for the spread picture and the payload picture were intertwined to acquire a single picture.

III. CRYPTOGRAPHY

Katzenbeisser and Petitcolas (2010) Cryptographic algorithms can be categories as symmetric key algorithm and public key algorithm [4]. Symmetric key algorithm utilizes a similar key for encryption and decoding, while open key algorithm utilizes distinctive keys for encryption and unscrambling. Steganography system can be actualized utilizing two strategies. Initially, the spatial space-based steganography, where the least critical bits (LSB) of the spread article is supplanted by the mystery message bits. Besides, the change space-based steganography; for this situation, the mystery message is implanted with the coefficient of the spread article. The most widely recognized change areas are discrete Fourier change and discrete wavelet change. To improve the dependability of the communication system; cryptography and steganography can be consolidated to execute a powerful and secure system; for this situation, the encryption and covering up are accomplished in the transmitter, while the extraction and unscrambling are accomplished in the recipient.

Neha et al (2017) Cryptography is a significant component of any system to address message transmission security necessities [5]. Cryptography is the investigation of strategies for sending messages in camouflaged structure with the goal that lone the planned beneficiaries can evacuate the mask and read the message. It is the reasonable specialty of changing over messages or information into an alternate structure, to such an extent that nobody can peruse them without approaching the 'key'. The message might be changed over utilizing a 'code' (in which case each character or gathering of characters is substituted by an elective one), or a 'figure' or 'figure' (in which case the message in general is changed over, instead of individual characters). Cryptology is the science basic cryptography. Cryptanalysis is the art of 'breaking' or 'splitting' encryption plans, for example finding the unscrambling key.

Cryptographic frameworks are conventionally ordered along three autonomous measurements.

Hazaimeh (2013) Cryptography is the study of keeping the transmitted data secure. It gives data encryption to verify communication [6]. The encryption procedure is connected before transmission, and the decryption procedure is connected in the wake of accepting the scrambled data. Steganography is the study of composing shrouded messages inside an alternate advanced substance; it passes on the data by hiding it in other medium, for example, picture or sound which is known as the spread item. The data concealing procedure is connected before transmission and the extraction procedure is connected in the wake of getting. The principle distinction among cryptography and steganography dependent on the presence of the mystery message. Cryptography scrambles the message and transmits it; anybody can see the encoded message, yet is hard to be seen, particularly on the off chance that it has been scrambled with solid cryptographic calculation. Steganography hides the emit message presence by concealing it in a spread item. The spread item can be named Text-based Steganography in which the mystery message is inserted in a content document, sound Steganography to conceal the mystery message in sound sign and picture steganography in which the mystery data is implanted in a picture.

IV. HASH FUNCTION

Kallam et al (2017) Hash function is a single direction encryption, the hash function is a properly characterized methodology or scientific equation that speaks to a little size of bits which is produced from an enormous measured document, the consequence of this function can be called hash code or hashes [7]. The creating of hash code is quicker than different strategies which make it increasingly wanted for confirmation and uprightness. Cryptographic hash functions are quite utilized for advanced signature and modest developments are exceedingly alluring. The utilization of cryptographic hash functions for message confirmation has turned into a standard methodology in numerous applications, especially web security conventions. The confirmation and the respectability considered as primary issues in data security, the hash code can be connected to the first record then whenever the clients can check the verification and trustworthiness subsequent to sending the safe information by applying the hash function to the message again and contrast the outcome with the sender hash code, if it's comparable that is mean the message originated from the first sender without adjusting in such a case that there is any changed has been made to the information will changed the hash code at the collector side.

Sasaki and Wang (2014) the hashing procedure is executed with the use of Message Digest Algorithm (MD5) which is a hash work that intends to produce 128-bits hash esteem and it is considered as a quick hashing calculation [8]. The embedding procedure of the encrypted information into a spread picture is finished by utilizing the discrete wavelet transforms (DWT) based steganography. It depends on steganography and symmetric encryption procedures to give the classification, while the hashing calculation is utilized to give the information uprightness. To accomplish privacy, the mystery information is encrypted and afterward implanted through a specific spread item. Besides, the information reliability has been executed by utilizing a hashing calculation to get a hash an incentive for the secret message.

V. SECURITY OF THE ENCRYPTED DATA

Goudar et al (2012) introduced a system for using TCP/IP header to be the stenographic carrier in embedded private information. Encryption on the basis of DNA cryptography and steganography was put forth by Mathew (2017) [9] [10].

This methodology builds the privacy for a delicate message by giving multilayer security. The mystery information encoded to DNA bases, at that point DNA based AES calculation was done on it. The aftereffect of the encryption was inserted in another DNA arrangement. A triple layer security was actualized in this strategy. The AES encryption and MD5 hash function were utilized by Indrayani et al (2017) to improve the security by utilizing MP3. In this methodology the MP3 sound was utilized as spread media and the secret information was scrambled by utilizing Advance Encryption Standard (AES) calculation [11]. The mystery key was handled utilizing MD5 single direction hash function.

Edi Kresnha and Mukaromah (2014) put forth a strong technique of encryption and steganography [12]. The ElGamal encryption method helped in encryption of private messages which was embedded in MP3 through dispersed private message with the use of frequency distribution method. For enhancement in information transmission security through communication means, there are some ways introduced. ID3v2 tag space in the steganography by Galiah and Salman (2014) saw message being encrypted through the use of McEliece cryptosystem [13]. Public key helped the technique which was installed in MP3 file format and it offered superior data security though not the maximum range.

Masud et al (2011) introduced a new technique which used LSB through a private key. Cover image here is categorized to Red, Green and Blue substances and 1D assortment of bit sources of secret key being produced [14]. Furthermore, Red

matrix and transformed secret key can be helpful in decision-making for substituting confidential information to Blue or Green substances. For drawing out private information, reverse procedure is used. There was introduction of RSA encryption algorithm through LSB steganography and it helped in encryption of concealed messages and embedding those encrypted messages through proper image in library of a user. Thus, the concealed messages are not recognized with steg-analysis devices.

There was another method presented for securing image steganography through the use of encryption and hash function and it utilizes the RSA algorithm and Diffie-Hellman for offering data security. Concealed information was embedded through LSB steganography. For obtaining double layer of security, there was a blend of technique introduced by Hamed et al (2016) [15]. Here, concealed information can be seen being transformed into DNA format which is implemented as outdated encryption method. Encrypted information was embedded in DNA through the use of LSB method. Under Siddaramappa and Ramesh (2015, 2016) methodology, concealed information is transformed to DNA bases where DNA synchronization rule is implemented in DNA-based information and key [16]. After that, XOR function is used among binary form of data and key.

VI. CONCLUSION

Guaranteeing data security is a major test for PC clients. Business people, experts, and home clients all have some significant data that they need to verify from others. Data that has been encrypted, albeit indiscernible, still exists as a doubt stimulating record exchange. Steganography, the specialty of imperceptible communication, is accomplished by concealing mystery data inside a transporter record, for example, a picture. Subsequent to concealing the mystery data, the transporter record ought to seem unsuspicious with the goal that the very presence of the embedded data is covered. A noteworthy downside to encryption is that the presence of the message data isn't covered up. Frequently, utilizing encryption may recognize the sender or collector as somebody with something to cover up. The upside of steganography is that it very well may be utilized to furtively transmit messages without the reality of the transmission being found. Despite the fact that the two strategies give security, to include numerous layers of security it is dependably a decent practice to utilize Cryptography and Steganography together. By joining, the data encryption should be possible by a product and after that install the figure message in a picture or some other media with the assistance of stego key. The blend of these two strategies will upgrade the security of the data embedded. This consolidated science will fulfill the prerequisites, for example, limit, security and strength for secure data transmission over an open station. Data encryption, hashing calculation and steganography method are utilized to secure data transmission over communication channels. The proposed methodology joins these strategies together to acquire a protected and solid communication framework.

REFERENCES

1. Xinpeng Zhang and Shuozhong Wang, (2015), "Steganography Using Multiple Base Notational System and Human Vision Sensitivity", IEEE signal processing letters, Vol. 12, No. 1.

2. Simmons, G. (2013). “The prisoners problem and the subliminal channel”, CRYPTO.

3. Tong L. and Zheng-ding, Q, (2012), "DWT-based color Images Steganography Scheme", IEEE International Conference on Signal Processing, 2: pp. 1568-1571.

4. Katzenbeisser, S. and Petitcolas, F.A.P. (2010), Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston, London.

5. Neha Sharma, J.S. Bhatia and Dr. Neena Gupta, (2017) “An Encrypto-Stego Technique Based secure data Transmission System”, PEC, Chandigarh.

6. Obaida Mohammad Awad Al-Hazaimeh, (2013) "A New Approach for Complex Encrypting and Decrypting Data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2.

7. Kallam Ravindra Babu, Dr. S.Udaya Kumar, Dr. A.Vinaya Babu, “A Survey on Cryptography and Steganography Methods for Information Security”, International Journal of Computer Applications (0975-8887), Volume 12 – No. 2, November 2010.

8. Y. Sasaki and L. Wang, “Improved Single-Key Distinguisher on HMAC-MD5 and Key Recovery Attacks on Sandwich-MAC-MD5,” International Conference on Selected Areas in Cryptography, Springer Berlin, Heidelberg, 2014, pp. 493–512.

9. R. M. Goudar, P. N. Patil, A. G. Meshram, S. M. Yewale, and A. V Fegade (2012). “Secure Data Transmission by using Steganography,” Inf. Knowl. Manag., vol. 2, no. 1, pp. 1–7.

10. S. Mathew (2017). “An Encryption based on DNA cryptography and Steganography,”

in 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), pp. 162– 167.

11. R. Indrayani, H. A. Nugroho, R. Hidayat, and I. Pratama (2017). “Increasing the security of MP3 steganography using AES Encryption and MD5 hash function,” in Proceedings - 2nd International Conference on Science and Technology-Computer, ICST, pp. 129–132.

12. P. E. Kresnha and A. Mukaromah, (2014). “A Robust Method of Encryption and Steganography Using ElGamal and Spread Spectrum Technique Based on MP3 Audio File,” in Proceeding Conference on Applied Electromagnetic Technology (AEMT), 2014, pp. 11–15.

13. A. Galih Salman and B. Kanigoro (2014). “Steganography Application Program Using the ID3v2 in the MP3 Audio File on Mobile Phone,” J. Comput. Sci., vol. 10, no. 7, pp. 1249–1252, 2014.

14. S. M. Masud Karim, M. S. Rahman, and M. I. Hossain (2011). “A new approach for LSB based image steganography using secret key,” in 14th International Conference on Computer and Information Technology, ICCIT pp. 286–291.

15. G. Hamed, M. Marey, S. A. El-Sayed, and M. F. Tolba (2016). “Hybrid technique for steganography-based on DNA with n-bits binary coding rule,” in Proceedings of the 2015 7th International Conference of Soft Computing and Pattern Recognition, SoCPaR 2015, pp. 95–102.

16. V. Siddaramappa and K. B. Ramesh (2016). “Cryptography and bioinformatics techniques for secure information transmission over insecure channels,” in Proceedings of the 2015 International Conference on Applied and Theoretical Computing and Communication Technology, ICATCCT 2015, pp. 137–139.

Corresponding Author

Ankit Sharma*

Research Scholar, Department of CSE, Swami Vivekanand Subharti University, Meerut (UP) India

csengg.ankit@gmail.com